Multilaterally Secure Pervasive Cooperation

Vom Fachbereich Informatik
der Technischen Universität Darmstadt
genehmigte

Dissertation

zur Erlangung des akademischen Grades
eines Doctor rerum naturalium (Dr. rer. nat.)

von

Dipl.-Inform. Stefan G. Weber

geboren in Mainz

Gutachter:
Prof. Dr. Max Mühlhäuser (TU Darmstadt)
Prof. Dr. Simone Fischer-Hübner (Karlstad University)

Tag der Einreichung: 30.09.2011
Tag der Disputation: 01.12.2011

Darmstadt 2011
Hochschulkennziffer D17

Abstract

People tend to interact and communicate with others throughout their life. In the age of pervasive computing, information and communication technology (ICT) that is no longer bound to desktop computers enables digital cooperations in everyday life and work in an unprecedented manner. However, the privacy and IT security issues inherent in pervasive computing are often associated with negative consequences for the users and the (information) society as a whole.

Addressing this challenge, this thesis demonstrates that carefully devised protection mechanisms can become enablers for multilaterally acceptable and trustworthy digital interactions and cooperations. It contributes to the design of multilaterally secure cooperative pervasive systems by taking a scenario-oriented approach.

Within our reference scenario of ICT-supported emergency response, we derive the following scientific research questions. Firstly, we investigate how to enable real-world auditing in pervasive location tracking systems, while striking a balance between privacy protection and accountability. Secondly, we aim to support communication between a sender and mobile receivers that are unknown by identity, while end-to-end security is enforced. The required concepts and mechanisms define the scope of what we denote as *multilaterally secure pervasive cooperation*.

We take a novel *integrated approach* and provide the supporting security techniques and mechanisms. The main contributions of this thesis are (i) *pseudonyms with implicit attributes*, which is an approach to multilevel linkable transaction pseudonyms that is based on a combination of threshold encryption techniques, secure multiparty computation and cryptographically secure pseudo-random number generators, (ii) *multilaterally secure location-based auditing*, a novel consideration of auditing mechanisms in the context of real-world actions that reconciles privacy protection and accountability while proposing location traces as evidence, (iii) a *hybrid encryption technique for expressive policies*, which allows encrypting under policies that include a continuous dynamic attribute, leveraging an efficient combination of ciphertext-policy attribute-based encryption, location-based encryption and symmetric encryption concepts, and (iv) *end-to-end secure attribute-based messaging*, a communication mechanism for end-to-end confidential messaging with receivers unknown by identity that is suitable also for resource constrained mobile devices.

Harnessing these buildings blocks, we present an integrated architecture that supports *location-aware first response*. We therein consider location as the central integrating concept for pervasive cooperations. Both communication during incident handling as well as ex-post auditing are conceived as being location-based.

Our research draws from experiences with potential real users (first responders and emergency decision makers) and from an interdisciplinary study. We contribute results derived from simulated court cases, indicating the trustworthiness and practicality of our proposal. Experiments conducted with prototype systems support the claim that our concepts are suitable for resource-constrained devices. In a theoretical analysis, we show that our security requirements are fulfilled. Our proposals have multiple further applications, e.g. to pseudonym-based access control.

Zusammenfassung

In ihrem Alltagsleben interagieren und kommunizieren Menschen auf vielfältige Weisen miteinander. Durch den Einsatz moderner Informations- und Kommunikationstechnik (IKT) ist digitale Kooperation nicht mehr an eine stationäre Nutzung gebunden, sondern auch mobil und allgegenwärtig möglich. Die dahinter stehenden technischen Entwicklungen werden häufig unter dem Begriff des Pervasive Computing zusammengefasst. Als Kehrseite und Hemmnis der sich vollziehenden "Computerisierung der Alltagswelt" werden oft die Auswirkungen auf die Privatsphäre des Einzelnen und Datenschutz- und Datensicherheitsprobleme im Allgemeinen angeführt.

In diesem Spannungsfeld hat die vorliegende Dissertation das Ziel, Konzepte und Mechanismen für eine *mehrseitig sichere digitale Kooperation* zu entwickeln. Es werden neue Mechanismen vorgestellt, welche die Sicherheitsanforderungen aller beteiligten Kooperationspartner berücksichtigen und somit auf einen ausgewogenen Interessensausgleich abzielen. Dies dient als Grundvoraussetzung für eine vertrauenswürdige Kooperation.

Im Mittelpunkt der Arbeit stehen die folgenden Forschungsfragen: wie kann eine datenschutzgerechte Auditierung von Vorgängen der realen Welt realisiert werden? Insbesondere wird dabei der Aspekt berücksichtigt, wie mit dem Zielkonflikt zwischen dem Schutz der Privatsphäre und der Zurechenbarkeit von Aktionen umgegangen werden kann. Weiterhin wird die komplementäre Fragestellung adressiert, wie eine sichere Kommunikation mit mobilen Kooperationspartnern, deren Identität einem Sender unbekannt ist, realisiert werden kann. Ein Hauptaugenmerk liegt dabei auf der Sicherstellung von Ende-zu-Ende Sicherheit auf Basis kryptographischer Techniken.

Die Inhalte der Arbeit werden szenarioorientiert motiviert und präsentiert. Als Basis dienen dabei realitätsnahe Anwendungsfälle im IKT-unterstützten Katastrophenschutz. Die Handhabung von Großschadenslagen kann durch digitale Kooperation entscheidend verbessert werden. Die Anwendbarkeit der vorgestellten Beiträge ist jedoch allgemeiner und nicht auf diese Domäne beschränkt.

Die Arbeit stellt einen neuartigen *integrierten Ansatz für mehrseitig sichere digitale Kooperation* im Hinblick auf die genannten Forschungsfragen vor. Dabei wird auch eine Systemarchitektur eingeführt, die am Anwendungsfall *ortsbezogene Koordinierung und Auditierung von Rettungseinsätzen* illustriert wird.

Die technischen Hauptbeiträge sind (i) *Pseudonyme mit impliziten Attributen*, ein Vorschlag zur Realisierung flexibel verkettbarer Transaktionspseudonyme, basierend auf Schwellwertkryptographie, Berechnungen auf verschlüsselten Daten und Zufallszahlengeneratoren; (ii) ein Ansatz zur *mehrseitig sicheren ortsbezogenen Auditierung*, der einen fairen Interessensausgleich zwischen informationeller Selbstbestimmung, Nachvollziehbarkeit und Strafverfolgung durch transparente, pseudonyme Auditierung bietet; (iii) eine *ausdrucksstarke, hybride Verschlüsselungstechnik*, die kontinuierlich dynamische Attribute wie GPS-Informationen in kryptographischen Operationen berücksichtigt, sowie (iv) Mechanismen für den *Ende-zu-Ende sicheren*

attributsbasierten Nachrichtenaustausch, die eine gezielte und nachvollziehbare Kommunikation mit unbekannten Empfängern implementieren.

Abschließend werden Evaluationsergebnisse und sowohl theoretische als auch praktische Sicherheitsanalysen der Beiträge vorgestellt. In einer Nutzerstudie mit Mitgliedern des deutschen Katastrophenschutzes wurde die Praktikabilität der Kommunikationsmechanismen positiv evaluiert. Eine zweite Studie, die ebenfalls präsentiert wird, hat noch stärkeren interdisziplinären Charakter: auf Basis simulierter Gerichtsverfahren wurden die Rahmenbedingungen für den Einsatz der vorgeschlagenen Auditierungsmechanismen bestimmt. Als weiterer Bestandteil der Evaluation wird die Prototyp-Implementierung vorgestellt und gezeigt, dass der Ressourcenverbrauch der entwickelten Konzepte auch für mobile Endgeräte angemessen ist. Zur Abrundung werden weitere Anwendungsmöglichkeiten der entwickelten Beiträge diskutiert, diese liegen beispielsweise auf dem Gebiet der pseudonymbasierten Zugriffskontrolle.

Acknowledgements

This thesis documents and presents results of several years of scientific research. Just like Alf, the alien life form, I was confronted with a jiggsaw puzzle - a *quite complex one* - that I did not even break on my own.

Fortunately, I was continuously supported and encouraged by my family, my friends, colleagues, as well as several fellow researchers. It is about time to express my gratitude and appreciation to all people that contributed to the outcome of this thesis. This result would not have been possible without you, one way or another. Thank you!

First and foremost, I would like to thank my advisor Max Mühlhäuser for his steady guidance and encouragement throughout the years, and for giving me the opportunity to explore the aspects that I was interested in. I am also grateful to Simone Fischer-Hübner, who kindly agreed to act as second advisor and helped to improve the overall quality of this work. Tusen tack!

Many members of the Telecooperation group and the Center for Advanced Security Research Darmstadt (CASED) have had a positive impact on my research. Sebastian Ries, Leonardo A. Martucci and Andreas Heinemann provided valuable feedback throughout the years, merci! Further support came from Alexander Behring, Andreas Petter and Dirk Bradler, just to name a few of my great colleagues. Vielen Dank!

I am grateful for some very interesting collaborations with external researchers. In particular, I would like to thank Achim D. Brucker and Helmut Petritsch, the cool guys from SAP Research Karlsruhe, for sharing knowledge about security and catastrophes; and Michael Nagenborg, for inviting me to an information ethics symposium as well as for fruitful interdisciplinary discussions. Moreover, it was a pleasure to explore legal aspects related to my research together with the PROVET group of Alexander Roßnagel.

Finally, my gratitude goes to my parents, for supporting me in every possible way, and to Konstantina, for standing by my side. *Ευχαριστω*!

Contents

List of Figures

List of Tables

1 Introduction

Computerization is robbing individuals of the ability to monitor and control the ways information about them is used. [...] As computerization becomes more pervasive, the potential for these problems will grow dramatically.
David Chaum, 1985 [44]

1.1 Motivation

People tend to interact and communicate with others throughout their daily lives. In the last decades, oral and postal communications have been complemented by digital approaches. In particular, electronic mail has been adopted by tremendously large user groups. Recently, also mobile communication devices, powerful networked computing facilities and personalized information services have started to support digital cooperations in everyday's life and work in an unprecedented manner.

Today, information and communication technology (ICT) is no longer bound to desktop computers; we are closely approaching the age of *Pervasive Computing* [194]. This post-desktop era of computing is attended by a large scale collection, distribution and aggregation of information related to individuals and their activities.

As with most things, there is always a second side of the coin, also with technological progress. Already more than a century ago, the rise of photographs combined with media that was able to widely spread the pictures taken amplified discussions of the concept of privacy [228]. Means for restricting and controlling the ways that personal information is used by others were demanded.

From the beginning of pervasive computing research [44, 244], its inherent privacy issues and the associated unforeseeable consequences for the individual were mentioned. Throughout the last years, the actual demand for security mechanisms and privacy protection principles that are compatible with pervasive ICT has increased the same way as ICT application scopes have broadened [221].

It is therefore a fundamental conviction of the research community [39, 77, 8] that, in the long run, assurance has to be provided that digital interactions bear little additional risks and threats. A major challenge is thus to design the multiple ways

of pervasive information brokering in a manner that is multilaterally acceptable by the users and the (information) society as a whole .

1.2 Object of Research

With pervasive computing becoming reality, the usage of ICT naturally tends to happen as part of real life contexts. In particular, it can also be associated to organizational liabilities or engagements. Especially, it takes place within legal frameworks. This indicates that digital protection concepts applicable to pervasive system do not only have to consider the privacy protection of individuals. Also, they need to adhere to the broader perspective of multilateral security [183]. Multilateral security aims at reconciling contrary security interests, which is a prerequisite that parties can concentrate on reaching a common goal.

Effectively, in a vision of a multilaterally secure pervasive computing environment, the possibly conflicting security interests of all legitimately concerned parties would a) be thoroughly considered, and b) fairly balanced, while c) system functionality would not be confined.

This thesis contributes to the understanding and design of multilaterally secure cooperative pervasive systems.

1.3 Thesis Goals and Research Questions

The main objective of this thesis is to demonstrate that pervasive computing and communication concepts can be realized such that a multilaterally acceptable and thus trustworthy cooperation between different players can be supported. In particular, we consider this objective in the face of highly demanding and even conflicting IT security and privacy requirements, as explained in the following.

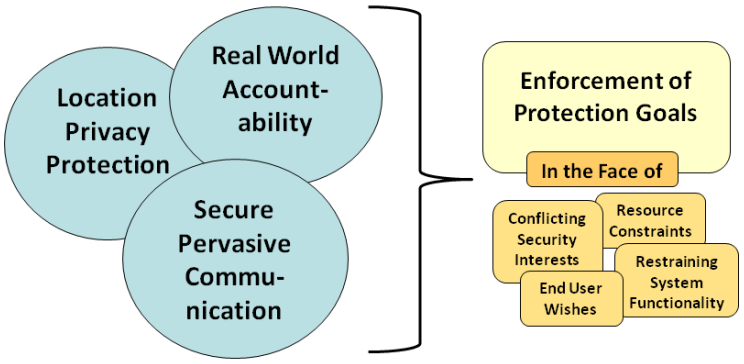

Figure 1.1: Research challenge

In most cooperative systems, the mechanisms that support efficient and secure

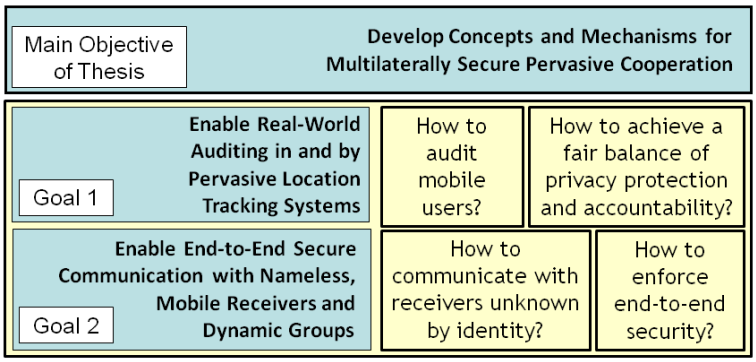

Figure 1.2: Goals and research questions

communication, privacy protection and accountability are considered as major functional parts. In pervasive systems, these functionalities are facing an extension of their scopes. This includes new facets of privacy protection, accountability for digitally recorded real-world actions and novel forms of communication.

Thus, a major research challenge is to devise solutions that face the constraints dictated by the embedding of ICT in the real world. In particular, system design has to take into account conflicting security interests, resource constraints of mobile devices and wishes of end users, without restraining functionalities. This challenge is summarized in Figure 1.1.

In this thesis, we address it by specifically aiming to

- enable real-world auditing in and by pervasive location tracking systems, and
- enable end-to-end secure communication between a sender and mobile, nameless receivers as well as dynamic groups.

For this thesis, the required concepts and mechanisms define the scope of what we denote as *multilaterally secure pervasive cooperation*. In order to implement these enablers, we have to address the following identified research questions, that are also summarized in Figure 1.2:

- In order to support auditing of real-world actions, novel auditing mechanisms are required. We investigate how to audit mobile users that are participants of a location tracking system. Additionally, in order to achieve acceptance of such a novel auditing approach, we investigate how to fairly balance the inherently conflicting security requirements of (location) privacy protection and accountability.
- Communication in pervasive computing settings has to consider that receivers are mobile and nameless or parts of dynamic groups. Thus, we investigate how to realize communication mechanisms suitable for targeted one-to-many

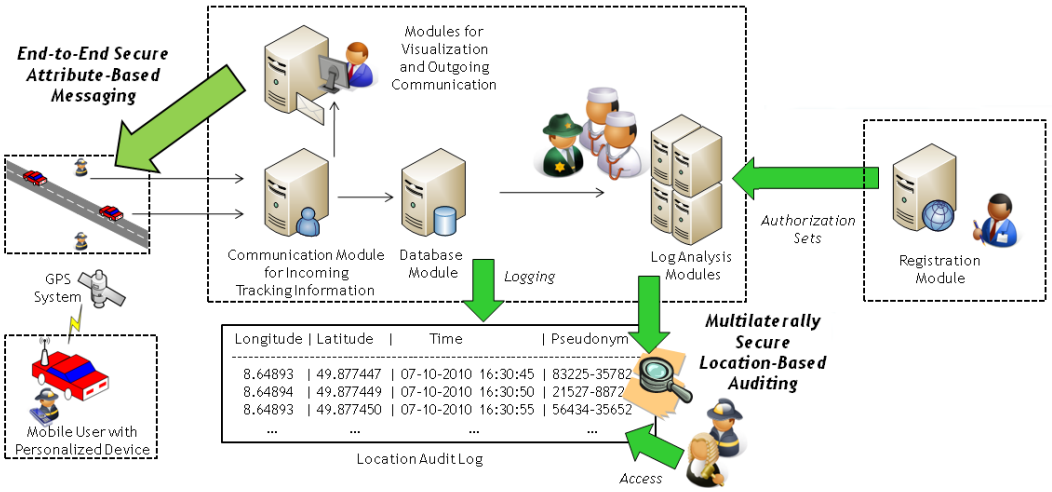

Figure 1.3: Integrated architecture in overview

communication given the fact that identities of the receivers are unknown. Additionally, we investigate how to achieve end-to-end security for this kind of communication, which is a security requirement relevant to many forms of communication.

1.4 Approach and Scientific Contributions

This thesis follows a scenario-oriented approach. We derive the introduced research questions within a specific reference application scenario; we also generalize our findings. In particular, our research is instantiated within the challenging context of ICT-supported emergency response. We stress that pervasive ICT may enhance rescue efforts in the face of large scale emergencies, which can only be handled by multiple parties that cooperate.

In this setting, communication has to be end-to-end secure due to legal requirements, and real-world accountability is a key means for handling liability issues that may arise during rescue missions.

In order to mitigate the acceptance issues of pervasive computing systems in such challenging real-world contexts, we develop and contribute a novel integrated approach to multilaterally secure pervasive cooperation; it is depicted within the use case of location-aware first response.

Our approach builds upon two main principles:

- Firstly, we propose to make mobile users implicitly addressable for secure communication on a different level of abstraction than identity. In particular, this is realized by means of attributes that represent the user properties, including the current location.

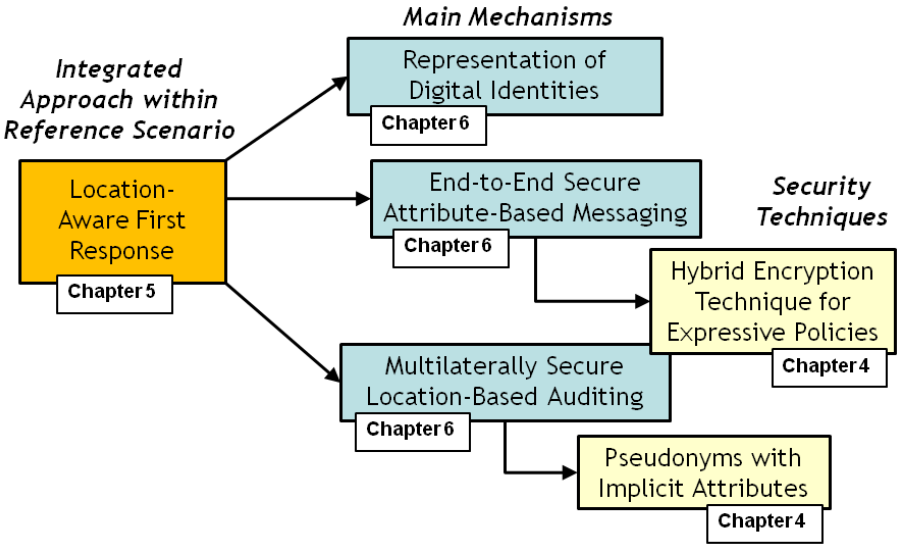

Figure 1.4: Overview of contributions and thesis contents

- Secondly, we propose that a every user regularly provides location updates along with transaction pseudonyms. Since we employ particular pseudonyms that are flexibly linkable by authorized parties, we thus enable a real-world auditing. Based on stored pseudonymized location information, location traces can be created, re-identified and used as evidence in disputes.

In particular, we propose and describe an integrated architecture that supports end-to-end secure one-to-many communication and multilaterally secure auditing of rescue missions. An overview of this architecture is provided in Figure 1.3.

On a technical level, we additionally develop several novel security techniques and mechanisms that are suitable for the given reference scenario and a range of further applications. Our main contributions are

- *Pseudonyms with implicit attributes*, a novel approach for multilevel linkable transaction pseudonyms. We extend the work by Juels and Pappu [125] on encryption-based transaction pseudonyms, by developing new mechanisms for controlled pseudonym linkability, including support for cooperative, step-wise re-identification as well as individual authentication of pseudonyms. Our proposal builds on the employment of efficient techniques for secure multiparty computation (SMPC) and cryptographically secure pseudo-random number generators (PRNGs).

- *Multilaterally secure location-based auditing*, a novel consideration of auditing mechanism towards real-world actions. Harnessing our novel pseudonym construction, we propose mechanisms that support a fair balance of privacy

protection and accountability. In contrast to previous work, a cooperative log analysis is introduced that is tailored more closely to human-oriented dispute resolution processes. We propose transparency as a second level of accountability and provide means that support individuals in repudiating false accusation. Additionally, the approach can flexibly be instantiated with and without law enforcement capabilities.

- A *hybrid encryption technique for expressive policies*, which is suitable for handling encryption policies that may include a continuous dynamic attribute. Leveraging an efficient combination of ciphertext-policy attribute-based encryption, location-based encryption and symmetric encryption according to AES, we devise an expressive encryption technique that is suitable also for resource-constrained mobile devices.

- *End-to-end secure attribute-based messaging*, a novel communication mechanism that supports end-to-end secure messaging with receivers unknown by identity. Based on our hybrid encryption technique, we conceptualize an approach that flexibly supports important communication patterns, including location addressing as well as notification of a priori unknown recipients, e.g. qualified persons and external specialists. The proposal also allows querying human sensors and was tailored according to the needs of potential end users within the emergency response domain. Harnessing an implicit addressing mechanism, also location privacy of mobile receivers is protected.

- A novel *representation of digital identities*, which supports mobile users to be addressable in communications, to be able to provide pseudonymous location updates, to be re-identifiable in a log analysis and to individually access log content. The proposed representation is organized in three logical layers; on the user's side, a personal communication device provides the digital container, platform and technical trust anchor for our proposal.

An overview and the conceptual connection of our main contributions is given in Figure 1.4. Based on our integrated, scenario-oriented presentation, this thesis, on the one hand, depicts how cooperation based on pervasive ICT can enhance mission-critical settings that inherently require multilateral security. On the other hand, we show how cooperation can be a key mechanism to implement multilateral security (cf. Figure 1.5).

1.5 Evaluation

We argue that technical feasibility, security and appropriateness for certain application contexts is given by our contributions.

Firstly, prototype implementations serve as a proof-of-concept; they enable us to conduct experiments which support our claim that the proposed concepts are tech-

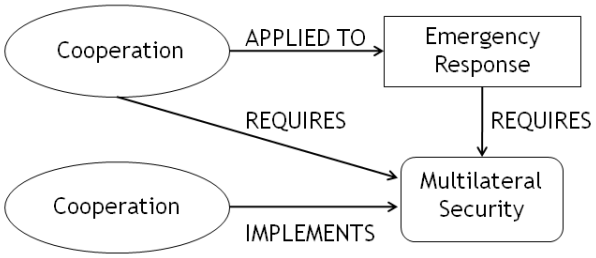

Figure 1.5: Cooperation and multilateral security

nically feasible as well as suitable to current standard mobile devices and storage systems.

By means of security analyses, we depict the achieved level of security. Main results are also confirmed by an external security evaluation that was conducted by the independent German trust provider TÜViT, and by additional considerations derived from an interdisciplinary simulation study. Within this study, we conducted simulated court cases in order to identify the main factors for leveraging location traces as legally acceptable evidence. Our appropriateness claims also draw from experiences with potential real users, i.e. first responders, decision makers and lecturers from German police and fire departments as well as relief organizations. In particular, we conducted a user study in order to assess the usage potential of attribute-based messaging concepts. The derived results were also incorporated in our proposal.

1.6 Publications

The present thesis builds upon a number of scientific publications that were published in a peer-reviewed book, articles, conference as well as workshop proceedings and reports, and have also been presented and discussed at a symposium and a poster session.

Initial discussions of IT security and privacy challenges inherent in pervasive computing as well as in the emergency response context were published in [240, 72]. Related social and ethical aspects were discussed in [235]. Early conceptions of this work have been published in [171, 236]. The mechanisms for end-to-end secure attribute-based messaging were introduced in [232, 231]. Refinements and additions were presented in [241, 237, 226], together with the construction of the proposed hybrid encryption technique, that was also presented in [234]. Specific aspects related to the security architecture of mobile communication devices are given in [32, 238]. The approach to multilevel linkable transaction pseudonyms was presented in [230, 239], along with the concepts for multilaterally secure location-based auditing. The comprehensive concepts for the representation of digital identities as well as an overview of main principles of this work were presented in [238]. Fur-

thermore, a cooperation lead to an additional publication [136], addressing issues of multilateral security and principal limits of privacy protection as well as of transparency and audit mechanisms in a related e-government services context.

1.7 Thesis Structure

Beyond this introduction, this thesis consists of seven chapters, as follows:

Chapter 2: Background and Requirements introduces to pervasive computing and the inherent IT security and privacy issues. It then analyzes ICT-supported emergency response, as well as defines the reference use case of location-aware first response. Based on the introduced background, the security requirements for multilaterally secure pervasive cooperation are elicited and defined.

Chapter 3: State of the Art discusses the state of the art of existing research w.r.t. to goals of this thesis. It points to shortcomings of current security techniques and mechanisms that have to be overcome in order to fulfill the goals of this thesis.

Chapter 4: Novel Security Techniques introduces a novel pseudonym construction and a hybrid encryption approach. These techniques constitute key building blocks for the integrated approach of this work.

Chapter 5: Integrated Approach within Reference Scenario presents the main principles for realizing a multilaterally secure pervasive cooperation and describes an integrated system for location-aware first response, which applies them.

Chapter 6: Mechanisms contains a detailed description of the mechanisms underlying the depicted approach.

Chapter 7: Evaluation and Discussion presents a multifaceted security evaluation and discusses further fields of application of our concepts and mechanisms.

Chapter 8: Summary concludes and summarizes the present thesis and also provides directions for future research.

2 Background and Requirements

In this chapter, the background of this thesis is introduced. This includes a brief discussion of pervasive computing basics as well as an introduction to its inherent IT security and privacy issues. Also, the research questions that were formulated in the previous chapter will be substantiated from an application-oriented perspective. In order to do so, we elicit a set of security requirements that need to be satisfied by a system in order to meet our understanding of a *multilaterally secure pervasive cooperation* within our reference scenario of ICT-supported emergency response.

This chapter is structured as follows: Firstly, our perspective on pervasive computing respectively pervasive cooperation is briefly explained in Section 2.1. A discussion on inherent IT security and privacy issues follows in Section 2.2. Then, Section 2.3 investigates a concrete application example of pervasive ICT in the emergency management domain. In order to depict how pervasive ICT could efficiently support rescue missions, we introduce the vision of location-aware first response. In Section 2.4, we illustrate the privacy and IT security challenges within this setting by descriptive examples. Based on this, we formulate a set of security requirements relevant to our goals, as well as a set of communication patterns. Finally, this chapter is summarized in Section 2.5.

2.1 What is Pervasive Computing?

The term *Pervasive Computing* [194] refers to the paradigm and vision that information and communication technologies and digital services become constantly available, personalized, and are even more, seamlessly embedded into everyday's life and work activities and processes in manifold aspects. With pervasive computing, the creation, exchange, storage and consumption of digital information potentially happens *anytime and anywhere*, while the computing devices and facilities per se are designed in an unobtrusive manner, or become even invisible to the users. It thus refers to a post-desktop era of computing.

Beside pervasive computing, the terms *Ubiquitous Computing* (UbiComp) [243] and *Ambient Intelligence* (AmI) [242] are also commonly used in the literature to describe this computing paradigm as well as the associated technologies. While there are slight differences between the terms, they are often considered synonym

[161]. This is also true for the scope of this thesis.

Additionally to the term pervasive computing, we make recurrent use of

- *pervasive computing environment* and *pervasive system* to refer to loosely interconnected computing facilities that belong to a common logical and/or organizational scope,
- *pervasive ICT* and *pervasive technologies* in order to subsume the technological components and mechanisms that are present within such an environment, and
- *pervasive applications* is used to emphasize that the targeted concepts focus on the application level.

A major goal of pervasive computing research is to devise novel applications and useful interactions, by leveraging interconnected ICT infrastructures and components found therein [1]. It also investigates and tries to convey "what (it) would be (..) like to live in a world with pervasive computing" [194], thus it is often scenario-oriented.

From a technical point of view, research on pervasive computing often has an integrating nature. Hereby, it touches many subfields within the computer science domain, ranging from the development of hardware over networking and interaction concepts to IT security and privacy topics. A focus lies on investigating how to realize the technical support required for envisioned applications.

However, pervasive computing is not defined by a concrete technology, rather it encompasses and connects a wide range of technological disciplines and neighboring areas [12, 79].

2.1.1 Perspective of this Thesis

The research presented in this thesis follows the aforementioned comprehensive perspective. We indicate that pervasive computing does not only need to be understood from a pure technological point of view, but also in close connection to application contexts and with special attention to possible implications, e.g. acceptance questions.

In the following sections, we give a brief introduction to our understanding of pervasive computing, as relevant to this thesis[1]. We do this by giving application examples and abstractly describing major technological building blocks and associated concepts found in pervasive systems.

As shown in Figure 2.1, the following sections describe the *design and requirements space* of this research. In particular, we discuss the security challenges that we address, elaborate on the privacy issues inherent in pervasive computing as well as develop a certain application perspective. These aspects contribute to the elicitation of security requirements w.r.t. to the main goals of this thesis.

[1] For more detailed technical and conceptual introductions to the broad topic of pervasive computing, we refer the reader e.g. to [162, 242, 144, 91].

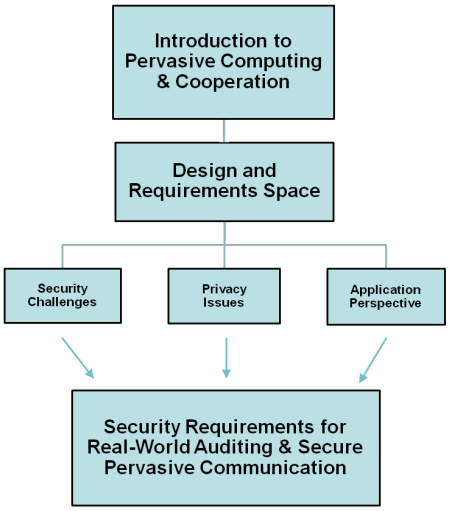

Figure 2.1: Background and design space

2.1.2 From Product Traceability ...

Radio Frequency Identification (RFID) technologies (see e.g. [187, 73]) and the Global Positioning System (GPS) are often seen as enabling technologies for pervasive computing. This is due to the fact that they provide means for connecting and bridging the real and the digital world [227]. For example, real world items and entities can be associated with digital information that refers to the environment and the conditions they are used in.

Historically, a major application context has been given within the field of logistics and supply chain management. We next refer to the example of product traceability. Here, appropriately equipped items, e.g. manufactured goods and products, can continuously generate and provide situation- and product-related informations that can be interpreted automatically or by human administrators (such as "these apples were grown in California and shipped to Europe."). Also, associated real-world conditions may be covered (such as "the temperature of the product's storage room never exceeded 5 degrees Celsius") or products can distinctly by re-identified on demand.

In this setting, thoroughly integrated technologies enable to continuously trace and monitor the products' flow through a complete supply chain. Also, real time stock holding as well as the detection of inappropriate conditions that appeared during product dispatching can be supported. While the given examples do not provide an in depth description of the technologies in use, we use them to convey the potential of pervasive technologies: underlying real-world processes can continuously be enhanced and optimized; also product safety and security can be improved.

Moreover, the examples illustrate important questions that are closely associated to pervasive computing:

- Who is allowed to access which kind of information generated within the pervasive system under which circumstances?
- In which ways is it possible to interact and communicate with and within a computerized environment?

2.1.3 .. to Human-Centric Pervasive Applications

Beyond the application on products and industrial goods, a major goal of pervasive technologies is to support that "people live, work, and play in a seamlessly interweaving computing environment" [243]. This was expressed in an early vision by Mark Weiser, who is acknowledged as one of the key innovators and researchers of pervasive computing.

Throughout the last years, the benefits of pervasive technologies have been investigated in multiple application domains, just to name a few examples:

- in the scenarios of ambient assisted living, domestic health care and smart homes [102, 50, 48, 10, 97], pervasive ICT aims to support elderly people in living independently in their homes by providing convenience and health care functionalities;
- intelligent transportation systems [49, 180, 63] are designed to make efficient use of the transportation infrastructures, both from an individual as well as from an economical perspective;
- in emergency response scenarios [119, 196, 120, 145, 220, 65], approaches to pervasive computing and communication aim to provide relevant information to the right actors at the right time in order to speed up incident responses and to implement safe and secure rescue missions.

ICT-supported emergency response also serves as major reference application scenario throughout this thesis. As common property, the mentioned fields of application aim to support individuals in their everyday tasks and are thus human-centric.

As a consequence, employed technologies also have to fit with pre-existing conventions of everyday's life and expectations of potential users, in order to be successful. Thus, the development of pervasive computing is often accompanied by technology assessment research [75, 77, 101, 8]. This shall assure that technological development remains consistent with social, ethical and legal perceptions. Especially, inherent acceptance issues need to be identified before the real world deployment of pervasive applications.

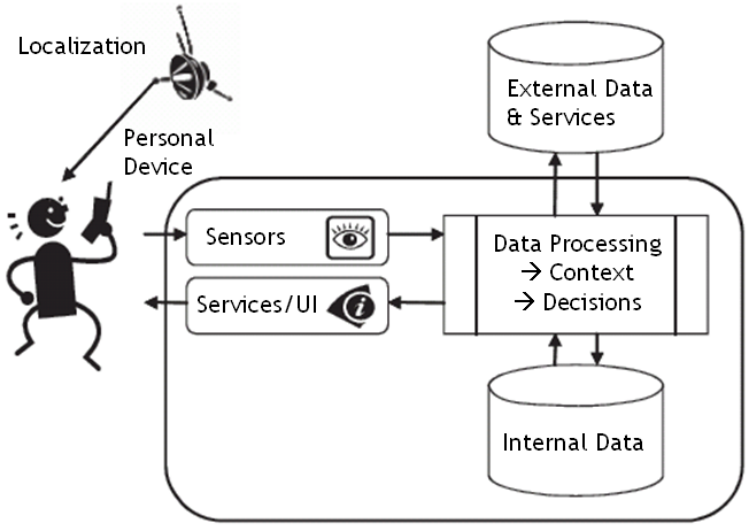

Figure 2.2: Components of a pervasive system according to [77, 144, 8]

2.1.4 Main Components of Pervasive Systems

A primary aim of pervasive computing is to render access to and interaction with the computing facilities as intuitive and easy as possible for human users. A common way to achieve this is to automate the provision of digital services, based on information that is collected about the situation of use. This approach, on the one hand, can minimize the cognitive load within human-computer interactions, and on the other hand enables interactions with computing facilities that are only present in the background.

Technically, the realization of such a pervasive systems requires data collecting facilities, mechanisms for wirelessly transferring and meaningfully connecting data in the background and consecutively providing personalized services to the users.

While there is no distinct reference architecture of pervasive systems, there is a set of main functional components that are found in most pervasive systems. In the following, we provide a brief introduction to common basic building blocks of pervasive systems, according to [77, 144, 8]. An overview is given in Figure 2.2.

In the figure, arrows indicate information flows. The icon that depicts an eye refers to the system's capability to sense the real world, the other icon represents higher-level information and services provided to the user. In this setting, basic components are:

- A *personal device* is carried by a user, in order to enable interaction with the pervasive environment. It is the user's primary connection point and gateway to the digital world.
- The term *sensors* relates to all components that collect information, e.g. about

the user and the environment. Such sensing facilities can e.g. be embedded in devices, the environment or even be provided by humans in various ways.

- By means of *localization*, a user's position, which represents sensor information, can be computed and provided to the environment's data processing facilities.

- The *data and information transfer* between the distributed system components is supported by a wireless, possibly distributed communication infrastructure.

- The *collection, processing and storage of data* can happen both locally on the user's personal device as well as centrally, e.g. on a server hosted by a service provider as part of the "invisible" computing infrastructure.

- The provided *data processing* functionalities facilitate an evaluation of sensor information in order to compute user and environmental *context*, i.e. meaningful information that characterizes the situation of use. Based on context information, it is possible to compute decisions w.r.t. the user's information or service needs and thus automate system reactions. In this task, collected and available internal data can be complemented by external data, that is requested from external data brokers, possibly over the Internet, to broaden the information basis.
  The emerging capability of the environment to react upon (and possibly adapt to) external situations is referred to as *context awareness* [198, 197, 96].

2.1.5 Towards Pervasive Cooperation

In a pervasive system, the tight interplay and cooperation of the components supports the targeted system functionality. In this thesis, we focus on the following aspects:

- The presentation given above focused on a single-user setting. We will extend it to a multi-user setting. In this setting, pervasive ICT can support interactions and cooperations between human users by means of pervasive computing resources and pervasive communication.

- In order to address the inherent acceptance issues, we will investigate the collection and subsequent storage of location information as well as communications from a certain IT security-related as well as functional perspective.

- Within many pervasive application, location information presents a primary type of context information [4]. In this thesis, we will additionally consider *location as a central integrating concept*. In particular, we leverage location as enabler for several types of pervasive interactions and cooperations.

2.2 Some Security Issues in Pervasive Computing

In the last sections, a brief and selected introduction to the conception of pervasive computing has been presented. In the present section, we will explain why the provision of IT security is considered as a major issue for the realization and deployment of pervasive computing applications and point to main factors that are relevant to this thesis. Firstly, we introduce our perspective on how IT security needs to be conceived in pervasive computing settings. This is followed by a brief investigation on the challenge of securing a pervasive system. Furthermore, the concept of privacy and associated issues are described.

2.2.1 IT Security, Multilateral Security and Pervasive Systems

According to [88], IT security is "concerned with the measures we can take to deal with intentional actions by parties behaving in some unwelcome fashion" within a computing system. To be able to deal with actions that can be considered as *unwelcome fashion*, IT security traditionally refers to *protection goals* or *security requirements*. These requirements need to be fulfilled for actions which are performed by means of computers and within computing systems, and are often determined by a concrete application. The parties that aim to intentionally violate protection goals are denoted *adversaries*.

The most common protection goals are often summarized by the *CIA triad*:

- *Confidentiality:* information should not be disclosed to unauthorized parties;
- *Integrity:* information should not be modified without detection by unauthorized parties;
- *Availability:* information should not be made inaccessible by unauthorized parties;

Cooperative pervasive computing applications typically involve multiple parties, that harness ICT for interaction and cooperation or provide services within the system. This renders the elicitation of protection goals a possibly complex issue.

For example, a user might provide her current location to further users to foster some sort of location-based social interactions, or use a location-based information service that recommends nearby places of interest. In this simple example, the user may articulate the protection goals that only authorized further users may access her location information, and she may insists on privacy protection against the provider of the information service. On the other hand, if the service is of a commercial nature, the provider wants to assure to be paid for the service and to be able to re-identify users that do not pay [36]. Further interests may be to profile the user, e.g. an employer could want to control that contracted working hours are actually served.

Analyzing an collaborative application scenario can highlight inherent conflicts w.r.t. underlying security and privacy requirements, that are due to different personal, legal or organizational backgrounds of the participants [95]. Generally speaking, security requirements of parties and entities involved in digital transactions are often conflicting. In order to deal with this issue, the concept of multilateral security has be coined: multilaterally secure systems take into account security requirements of all involved parties and aim at balancing contrary interests in an acceptable way [182]. Consequently, after conflicting security requirements have been traded against a multilaterally accepted compromise, the parties should have an incentive not to cheat and only need to minimally trust in the honesty of others, which is, more generally, an ultimate goal of designing security protocols and systems [62]. Rather, the parties can concentrate on reaching a common goal.

This is especially true in pervasive systems, which aim to foster cooperation. However, apart from this academic point of view, the actual implementation of multilaterally secure system is a highly difficult and complex task [174].

2.2.2 The Challenge of Securing a Pervasive System

In the last section, we argued that, firstly, a system can be considered secure if defined protection goals are satisfied, and, secondly, security in pervasive computing should be multilateral, i.e. consider legitimate goals of all involved parties.

But implementing and providing security mechanisms always has a cost, e.g. in terms of resource consumptions, in terms of development and deployment efforts and in terms of user awareness, or protection may confine system functionality.

Over the last years, a tremendous amount of literature has reviewed challenges that arise in order to make pervasive systems secure, e.g. [13, 137, 109, 163, 112, 57, 18, 80, 37, 252, 171, 190, 215, 214, 107].

Since the term pervasive computing does not refer to a distinct reference architecture, the discussions often remain little comparable. However, they indicate, that pervasive system are full of potential risks to security and privacy prominent on various layers, that also go well beyond the mere protection of confidentiality, integrity and availability.

For the scope of this thesis, we address the challenge of securing a pervasive system from the following, three layered perspective:

- *Device/Technique layer:* Which available basic security mechanisms and techniques can be applied for securing a pervasive system? How does a chosen approach interplay with pervasive devices, e.g. w.r.t. to resource constraints?
- *Protocol/System layer:* How can secure protocols and schemes be built on the foundations that are given in a pervasive systems? Which security concepts are suitable to effectively integrate the loosely connected parts into the emerging larger, yet secure systems?
- *Human/Organizational layer:* How is a pervasive application perceived by its users? What is the achieved acceptance level? Which further organizational

issues have an influence on establishing targeted protection goals? How can the level of protection be conveyed to the users?

On every layer, we mentioned security challenges by formulating abstract questions. We will consider the questions within a concrete application scenario of pervasive computing, in order to support our design process. The proposed framework informally reflects that

- IT security research has proposed a broad range of basic mechanisms a system designer may choose from, e.g. encryption or authentication techniques, yet the suitability for resource constrained devices is often questionable and needs to be investigated;
- bootstrapping security properties of larger systems has to be carefully aligned with the design of the targeted system functionalities;
- a real world usage of a theoretically secure approach can cause practical problems and thus conflict with security goals, e.g. imposed by limitations of human end users or administrators.

2.2.3 Privacy and the Need for Privacy Protection

The consideration of IT security in the sense of multilateral security also emphasizes the issue of privacy protection. On the one hand, privacy protection is a security requirement that is often articulated by individual users. On the other hand, it is also implied by existing data protection regulations.

Privacy issues been noted from the beginning of pervasive computing research [244]. They are considered as threats inherent in pervasive computing [139], and have often been mentioned with strongly negative connotations. E.g. pervasive systems have been compared to "surveillance infrastructures" [39]. Also, privacy was considered the "achille's heel of pervasive computing" [195].

However, privacy is a complex social, legal and technical issue [211, 2, 70]. In order to understand the meanings attached to the concepts of privacy and privacy protection, in the following sections we will take a brief look on legal foundations, discuss the problem of location privacy as well as summarize important privacy related notions. Finally, we will elaborate on the fact that privacy protection itself can be in conflict with the protection goal of accountability.

Legal Foundations

The concept of privacy has evolved along with the capabilities and social perceptions of new technologies and their influence on the individual.

The first notably definition as *the right to be left alone* was given by Warren and Brandeis [228]. It came up during the late nineteenth century, in times when photography became broadly available and newspapers could widely spread pictures

taken. This development added a new dimension to the scope of disclosure of sensitive information. In turn, legal foundations were required to protect individuals from unwanted importunity.

More recently, after the introduction of electronic data bases allowed collecting and searching personal data on a much larger scale, an important definition has been given by Westin [245]:

"Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

Westin's definition led to the articulation of the fair informations practices (FIPS) [224], which are a basic set of guidelines for the management of personal information. In summary, the FIPS include the following principles:

- *Notice and awareness:* An individual must be aware which entities are collection personal information about her and for what purpose this happens.
- *Consent and use limitation:* Data about an individual may only be collected if the individual agrees, and the use of the collected personal information must be limited to the specified and agreed purpose.
- *Access and participation:* An individual must be able to access stored personal data which refers to her, and be able to contest the data's accuracy.
- *Integrity and security:* Data that is collected must be assured to be accurate and must be protected against unauthorized access, disclosure and usage.
- *Enforcement and recourse:* There must be mechanisms established which enforce privacy protection as stated by the given principles. Even more, a data collector must be accountable for any failures to comply with the principles agreed to provide protection.

The FIPS have an important impact in the legal as well in IT security domains [113]. On the legal side, this is e.g. reflected by the fact that US, Canadian, European as well as OECD privacy legislations build on and extend them [83].

In addition to the FIPS, the *principle of data minimization* has evolved as one of the main legal anchors[2] for privacy protection:

- *Data minimization:* The collection of personal information should be limited to what is relevant and necessary for accomplishing a specified purpose. The data should only be retained for as long as it is needed.

In further directives[3], also legal principles for dealing with violations and breaches of data protection are given.

[2]The principle derives from *EU Directive 95/46/EC* and *Regulation EC 45/2001*, cf. HTTP://WWW.EDPS.EUROPA.EU/EDPSWEB/.

[3]In particular, this issues is addressed by the *EU Directive 2009/136/EC*, which extends *Directive 2002/58/EC*, cf. HTTP://WWW.EDPS.EUROPA.EU/EDPSWEB/.

The introduced principles provide abstract guidelines for privacy protection from a legal point of view. However, they do not specify in detail the necessary means for a technical implementation or enforcement.

This complex task is often addressed by more technical research communities, e.g. P3P [52], the *platform for privacy preferences* refers to the FIPS; they are also frequently interpreted in pervasive computing research contexts [137, 83, 212, 74, 128].

Location Privacy

Along with the development of pervasive ICT, new aspects and new forms of privacy have emerged and been identified. As argued by Langheinrich [137], this is due to following properties of pervasive computing:

- *Invisibility:* computing facilities aim to disappear in the environment, thus ICT usage is invisible to the users, yet possibly creates data related to individuals;
- *Sensing:* sensors constantly perceive possibly sensible aspects of the environment and associated actions of its users;
- *Memory amplification:* collected data can be stored and made accessible later.

In particular, location information represents one of the most important types of context information exploited by pervasive systems. For example, the availability of GPS allows continuously sensing the location of individuals with a high degree of precision and accuracy. This has lead to the conception of the term of *location privacy*[4].

Referencing to the more general definition given by Westin, Duckham and Kulik [58] state: *"location privacy can be defined as a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others."*

The importance of providing location privacy can be conveyed by considering negative consequences [93, 89, 58, 134]. These may include *intrusive inferences* and *attacks on personal safety*.

Firsthand, locations are often meaningfully associated to real-world actions, e.g. presence at meetings, visits of medical facilities, personal homes or even crime scenes. Based on available location information, further sensitive facts might be inferred, e.g. individual preferences or issues of physical health that may have negative impacts on social and economical life. Also, the knowledge of a current location can be maliciously exploited for physical attacks on an individual or on her property, if absence is indicated.

Yet, the actual and future scope of such negative effects can hardly be estimated.

[4] Location privacy is also addressed by regulations, e.g. in the *Location Privacy Protection Act of 2001* (cf. HTTP://WWW.TECHLAWJOURNAL.COM/CONG107/PRIVACY/LOCATION/S1164IS.ASP), the *Wireless Privacy Protection Act of 2003* (cf. HTTP://WWW.THEORATOR.COM/BILLS108/HR71.HTML) and the *EU Directive 2002/58/EC* (cf. HTTP://WWW.EDPS.EUROPA.EU/EDPSWEB/).

Important Privacy Notions and Metrics

The aspects of privacy that were discussed thus far derive from legal definitions, or are related to scenarios. They are thus little formal. Yet, in the privacy research community, a broad background on the formal treatment of privacy issues has been developed [175], that helps to describe privacy issues on the technical level. We next introduce two fundamental notions related to privacy protection: anonymity and unlinkability.

Within these notions, when speaking about an adversary, we refer to an entity that tries to circumvent given protection means in an unwelcome fashion.

- *Anonymity:* as defined by [175], anonymity is state of not being identifiable within a set of subjects, the so-called anonymity set. Anonymity can hide entities that perform a transaction. Given that a transaction can be carried out completely anonymously, i.e. in the absence of identifiers, an adversary is unable to associate that action to any subject (or its identifier) within the set of possible subjects. Thus, the degree of anonymity can be measured by the cardinality of the anonymity set.

- *Unlinkability:* Unlinkability is the property that aims at hiding relationships between items in a system [35]. If unlinkability is given, an adversary cannot link together multiple actions, e.g. uses of resources or services or sending messages, of the same subject.

Both anonymity and unlinkability refer to the inability of an adversary to behave in some unwelcome fashion, thus they refer to an implemented state of protection. More generally speaking, technical security mechanisms that aim to implement a privacy-related protection goal often aim to provide anonymity and unlinkability.

2.2.4 Privacy Protection versus Accountability

As discussed so far, privacy protection is a security requirement associated to the interests of individuals. In a pervasive system that aims for multilateral security, also further interests have to be considered. One of them, that is of major importance to the present thesis, is accountability. This section motivates the necessity of accountability and explains the inherent conflict to privacy protection.

Section 2.1.2 introduced an product traceability application example. Here, the functionality of the system enables to continuously monitor the flow of the products throughout a supply chain in order to optimize processes and detect inappropriate conditions and states. This system functionality is possible since products are associated to unique identifiers, which renders them linkable.

Abstracting from this setting and replacing the product by a human user emerges a system that could support accountability. Accountability is the protection goal that ensures that entities can be made accountable for their actions, by making it

possible to uniquely link and associate actions of an entity to that entity. Accountability is often required due to legal or organizational regulations, e.g. law enforcement is a primary example. A complementary concept is that of *digital evidence*, i.e. "any information of probative value that is either stored or transmitted in digital form" [217].

A pervasive system that senses real world facts and actions as well as records these facts in data logs possibly produces large amounts of digital evidence, in case that kind of information can be considered to be of probative value. This can be the case if captured data allows or supports linking actions to an entity. Here, the conflict of security interests is obvious: while privacy protection aims at hiding relations between users and actions, accountability aims at establishing relations. From this point of view, accountability is a security requirement that is inherently conflicting with privacy protection [67, 19, 20]. On a technical level, linkability for authorized parties has to be balanced with unlinkability that protects against unwanted profiling.

Yet, the concept of accountability can also be viewed from a different perspective: as a user has to accept accountability for his actions in certain cases, also a data collector shall be held accountable for complying with data protection principles (cf. Section 2.2.3). This is often considered in the protection goal of transparency: a user should be able to find out how information about her is processed and especially whether the responsible parties comply with the applicable rules for privacy protection [99, 100].

2.3 Reference Scenario: ICT-Supported Emergency Response

In the last sections, we provided a brief introduction to main concepts of pervasive computing and approached the issue of establishing security within pervasive systems on an abstract level. The present section concretizes these considerations.

In order to develop a better understanding of security and privacy issues inherent to pervasive computing, we investigate a certain reference application scenario in order to analyze

- how pervasive ICT may enhance important processes, and
- to which extent security and privacy protection goals have to be considered to support multilateral security.

Thus far, security issues of pervasive systems have been investigated in a broad range of application contexts and scenarios [80]. Within this thesis, we use the real life context of emergency responses as our major application scenario[5].

Presented findings result from discussions and experiences with German emergency workers, ranging from executive levels over trainers to volunteers, build upon available technical standards [141, 164], benefit from an exchange with the

[5]Yet, the contributions of this work are also relevant to further application contexts (cf. Section 7.4).

scientific research community [72, 231, 32, 31, 29] as well as from extensive literature studies, e.g. [223, 47].

The remainder of this section is structured as follows: after a brief introduction to area of emergency response, we depict how pervasive ICT may effectively support response and rescue-related actions. We do this by introducing our vision of *location-aware first response*. Then, we describe and identify inherent security trade-offs, formulate protection goals and elicit communication patterns concretely.

2.3.1 Introduction to Application Domain

Emergency responses are part of the area of emergency management. This term summarizes the measures and procedures that are taken in order to protect lives, property and infrastructure in the face of crisis situations and major incidents, including natural catastrophes, technical incidents or even man-made accidents. Emergency management includes preventive measures as well as actions taken and technologies applied to reestablish pre-incidental states.

Emergency responses need to be initiated as quickly as possible after a disaster strikes, in order to save lives, infrastructure and property, as many victims might not survive long without appropriate assistance [225]. Thus, the management and coordination of available resources becomes a crucial task. Especially, the availability of relevant information and effective means for communication are of highest importance, to improve command and control of rescue missions. Yet, especially in the beginning, emergency responses have to deal with unpredictable local emergency situations that harden the establishment of communication structures and with incomplete situational information. This beginning is often referred to as the chaotic phase of emergency responses [158], and resulting incident missions are then denoted as first responses.

2.3.2 Disaster Management Information Systems

In crisis situations, ICT may enhance existing processes that are traditionally required by emergency management workers or can even allow for the implementation of new support functionalities. Yet, emergency responses are nowadays broadly supported by so-called disaster management information systems (DMIS)[6].

Such a system aims at supporting the entities, players and organizations involved in rescue efforts in various manners. DMIS may provide technical solutions and tools for assessing the current situation, planning of responses and resources and possibly also the simulation of alternatives.

DMIS have received increasing attention from industry and academic research throughout the last years [157, 156, 120, 145, 119, 81, 191, 146, 38, 148, 220, 114, 3, 76]. The research on disaster management information systems spans from high-level organizational views up to questions of how field forces can be supported

[6] Furthermore, different yet comparable notions can be found in the literature, e.g. emergency response management information systems [223], incident management systems [132] and so on.

by mobile response devices [135], whereas questions from cooperation of involved parties, organizations and actors, visualization and decision-making are examined [143]. The research is often scenario-oriented and -related, e.g. Johnson [121] draws conclusions from a flooding in UK in 2007 and points out, among others, a need for a better cooperation of organizations and involved actors.

As core functionality, a DMIS provides means for the efficient communication within an operational command and control center as well as to the outside world. The latter may include the communication between several centers as well as the communication between a center and first responders and further entities in the field, which are equipped with mobile communication devices.

An important property of emergency response work is that many people involved in the execution of rescue missions are volunteers. In practice, e.g. in Germany, this means that a large part of the responders are trained for responses, but not continuously prepared to engage. Rather, these volunteers can be contacted during their normal life and work via a pervasive communication mechanism, in order to be able to support urgent incident response missions.

2.3.3 Towards Location-Aware First Response

In this section, we outline examples of ICT-based cooperations between control center members and the entities in the field respectively at the incident site.

Throughout this work, we represent the group of people working inside a control center by a single entity called *central user*[7]. The later ones are called *mobile users*. In the following, we denote the targeted cooperation between a central user and mobile users for the purpose of incident management *first response coordination*.

An abstract view of this setting is given in Figure 2.3. We assume that a digital emergency communication network is available, that enables two-way communication between a central user and the mobile users. By means of this network, data is exchanged between the command center and the incident scene as well as the outside world. In Europe, examples of such networks are currently established according to the TErrestrial Trunked RAdio (TETRA) standard[8]. TETRA networks promise to reliably connect organizations, parties and individuals involved in rescue efforts.

A major finding relevant to this setting is that locations and location-related informations are key factors to first response coordination [47]. Firsthand, aggregated information, displayed on a digital map, which visualizes and annotates the current disaster situation, can effectively support decision making processes in control centers. For example, a responsible central user might have to send commands and instructions to mobile users in order to facilitate an evacuation of citizens that are affected by a toxic gas cloud which spreads out. In this task, the central user may be

[7] In real world settings, the emergency management work within a command and control center is strictly organized, e.g. in Germany according to a set of roles, see [61] and references therein for more background information. For simplicity reasons, our setting is reduced to an abstract view.

[8] Cf. WWW.TETRAMOU.COM.

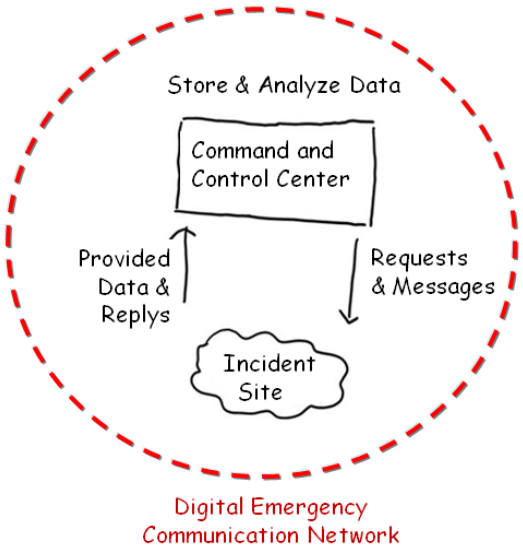

Figure 2.3: First response coordination setting

supported by location-depend information that is received from the incident site, e.g. by reports received from eye witnesses, by photos taken locally and sent in, or by measurements of sensors that are potentially embedded into an incident scene or even body worn by responders.

Also, current locations of responders or specialist nearby can be useful to define and coordinate rescues and treatment plans. In the crisis scene sketched above, available specialists for toxic matters could be leveraged for a timely local treatment of injured people, especially if they also could be contacted dependent on their locations.

In addition, since any action takes place in time and space, location-related informations are important to understand and analyze what happens during a disaster situation and induced rescue missions. A "crisis memory" [223], made up of collected information, is some kind of audit log for real-world actions and could support the handling of liability issues. It could also help to improve future incident responses.

Based on the presented considerations, we conclude that incident handling can benefit from

- a location-based visualization of disaster situations, annotated by localized informations and events, which are caused by the incident itself or occur during rescue missions,

- exploiting measurements of local sensors, possibly worn by rescue forces, embedded in the environment, or even harnessing humans as eye witnesses (and thus as certain kind of sensors),

Figure 2.4: Approach to context-aware first response coordination

- facilities to communicate with mobile users, based on location,
- location-based documentation and auditing of incident responses in crisis situations.

In sum, we denote this setting as *location-aware first response*. Throughout this thesis, we aim to devise pervasive ICT that supports cooperation, while demanding and possibly conflicting security and privacy requirements are satisfied. The cooperations relevant to location-aware first response hereby serve as our reference scenario.

2.4 Protection Goals Motivated within Reference Scenario

The system that shall provide the envisioned functionality that was described in the last section is a special example of a pervasive system (cf. Section 2.1.4, Figure 2.3.).

In particular, mobile users carry personal devices and are able to provide their current geographical position and further data to a central place, i.e. the command and control center. Within the control center, a central user (cf. Figure 2.4) is able to *see* and visualize received information; she can analyze the facts related to an incident and *think* about required actions; she can provide information to the outside world in order to re-*act* upon perceived external situations (cf. [232]).

Thus, in our setting, the decision component is realized via a human being, instead of being fully automated as part of the context processing facilities. Since this human part is inherently limited in her scalability, information services provided to the outside world are realized via a one-to-many communication mechanisms.

In order to implement the system, certain protection goals have to be fulfilled. We deal with these issues in the following sections. In our descriptive application scenario, a two-way communication between the command and control center and the incident scene and outside world is a major functionality to support cooperation.

According to the goals of thesis, which are now instantiated in the context of emergency response, we thus investigate properties of

- one-to-many emergency communication, between a central user and mobile users, i.e. mobile receivers that are unknown by identity and form dynamic groups, and of
- auditing of real-world actions by means of continuously provided location information of mobile users.

in order to elicit concrete protection goals.

2.4.1 One-to-Many Communication in Emergency Situations

The capability to communicate and provide the right information to the right receivers is of highest importance for successful incident responses.

From an IT security perspective, instructions and requests sent out from a control center in a crisis situation are also of highest sensitivity: they contain information that may be the key to the survival of victims affected by a disaster, may contain information about critical infrastructures, or hazardous materials. If such sensitive information is not properly secured, it may be subject to malicious tampering, manipulation or even terroristic exploitation.

At this point, a failure of security can have drastic consequences: inadequate handling of tactical information on the IT security level may become a threat to public security. Actually, the lifes of first responders partly depend on correct information. Injured persons, that shall be immediately rescued, and physical assets the first responders are chosen to protect, may be affected by IT security vulnerabilities, in the second line, as well. These threats have to be reflected in the security architecture of the employed DMIS.

A further important aspect is that a pervasive communication system that supports first response coordination may not be designed to send out instructions in a context-aware, thus automated manner. The decision must always be taken by the responsible user itself, and not by the system [213, 59], in order to comply with legal demands and to mitigate acceptance issues.

Process of Requirements Elicitation

The present research involved both theoretical and practical considerations.

In the theoretical part, we analyzed our application scenario, relevant technical standards for secure emergency emergency communications (in particular the TETRA standard according to [164, 141]) as well existing scientific research.

In the practical part, experiences and discussions with real users (first responders, decision makers and trainers from police and fire departments as well as relief organizations and volunteers) helped to understand the emergency response domain.

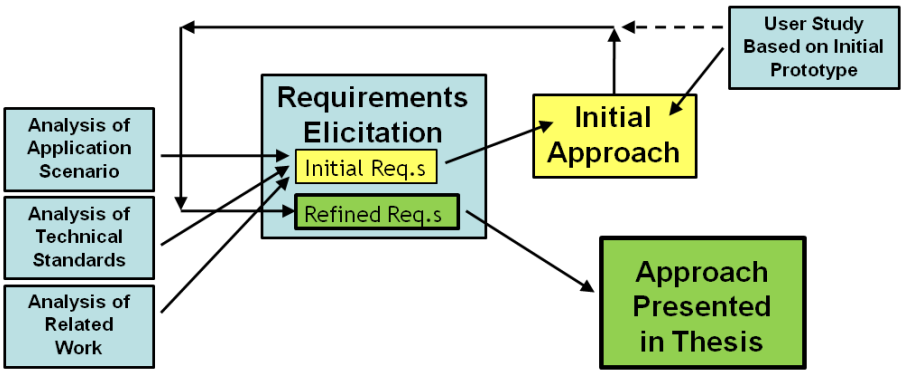

Figure 2.5: Research method w.r.t. communication mechanisms

Based both on the theoretical and the practical insight, we extracted the characteristics of emergency communications relevant to this thesis. The pursued iterative research method is shown in Figure 2.5. As part of the process of research, we defined an initial set of security requirements for pervasive emergency communication and developed an initial conceptual approach (cf. [232, 231]) as well as a corresponding prototype of communication mechanisms. The prototype was used to conduct a user study that involved domain experts[9]. Based on the results of the study, we refined the requirements and re-designed the conceptual approach (which is presented in this thesis).

A basic finding is that messages are the preferred communication mechanism in emergency management work [61]. Messages are also used to organize, inform and document any progress and internal actions. In particular, we thus focus on the communication between a central user in a command and control center and the outside world via messaging.

The following lists give the main *identified communication patterns* (`CPs`) as well as the *refined set of security requirements* (`SReqs`) relevant to this communication.

2.4.2 Emergency Communication Patterns

- `CP1: Communication by location addressing`: Fast participation in a disaster response fundamentally depends on both the nature and location of a disaster. In order to handle large-scale disasters, several parties need to cooperate and communicate based on location. Some rescue efforts require the participation of local relief agencies, while others require local specialists to participate, rendering location both as a comfortable and necessary mean to select receivers.

- `CP2: Requests to unknown entities`: Some parties, like fire and po-

[9]The conducted study is described in detail in Section 7.3.2.

lice departments, are involved in most responses. But since the geographical scope of a disaster cannot be pre-determined before it actually happens, the real identities of responsible people are often not directly known or available. Yet, support for efficient communication with unknown entities is required.

- `CP3: Communication with dynamic groups of entities`: When decision makers and central users need to communicate with local groups of first responders, the actual identities are also not known beforehand, or groups are even dynamically formed. These groups need to be addressable comfortably.

- `CP4: Deposition of information for future use(rs)`: In many cases, information has to be deposited for entities that will join operations in future.

2.4.3 Security Requirements for Emergency Communication

- `SReqC1: Basic security`: In emergency communication, mutual authentication, message integrity, availability and revocation of devices are basic requirements, e.g. detailed by the TETRA standard [141].

- `SReqC2: End-to-end confidentiality w/o online PKG`: Beyond that, preserving end-to-end confidentiality through encryption is legally implied for public security reasons. For scalability and efficiency reasons, the end-to-end encryption mechanism also shall not rely on an online private key generator (PKG).

- `SReqC3: Protection against replay attacks`: Means that protect against replay attacks are required, in order to prevent an attacker from injecting a valid message a further time.

- `SReqC4: Non-repudiation of senders`: Emergency communication requires to document who sent which messages.

- `SReqC5: Documentation of readers`: Also, the parties and entities who read received messages, requests and commands need to be documented for post-hoc audit purposes.

- `SReqC6: Efficiency of security mechanisms`: Employed security mechanisms need to be suitable for resource-constrained mobile devices that are widely used in emergency communications. Especially, a real-time communication must be possible.

- `SReqC7: Appropriateness to users`: In order to foster end user acceptance, security mechanisms must be understandable by and appropriate to casual users [72]. For senders of messages, this implies minimum learning efforts as well as an intuitive use.

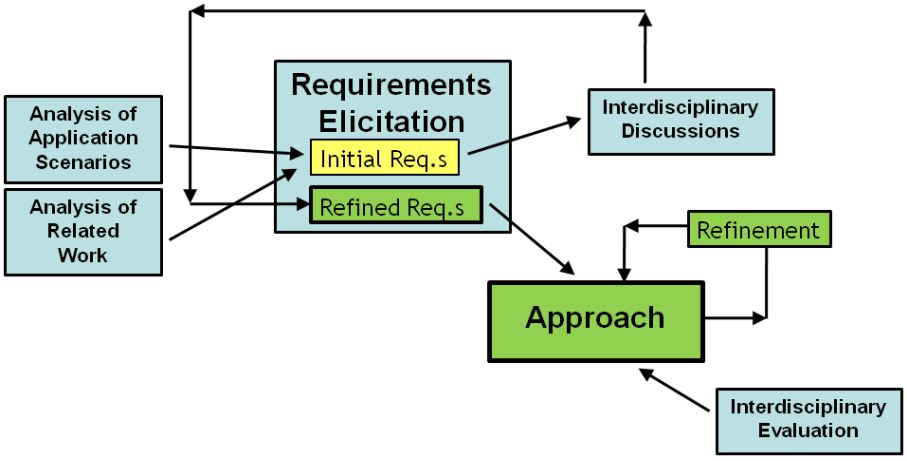

Figure 2.6: Research method w.r.t. auditing mechanisms

- `SReqC8: Location privacy protection of receivers`: Many participants involved in responses, like specialists, doctors or volunteers, are only available on requests sent to their mobile communication devices. Yet, the individual participation depends on the compatibility with individual preferences. Especially, many receivers demand location privacy protection as far as possible, while being available for location-based addressing and participation in rescue missions.

2.4.4 Privacy and Accountability Issues of Real-World Auditing

In the following, we investigate protection goals relevant to the auditing of real-world actions during incident missions.

Throughout this chapter, we have argued that an important aspect of pervasive computing research is the investigation of acceptance issues w.r.t. novel technologies and applications. In the context of this thesis, we address the particular issue of reconciling privacy protection and accountability.

Process of Requirements Elicitation

This section describes the pursued research method which led to the definition of our security requirements (and to the technical approach presented in this thesis). These requirements aim to fairly balance privacy protection and accountability. Our method is shown in Figure 2.6.

As part of our research process, we analyzed relevant application scenarios and related scientific research. Then, we defined an initial set of security requirements and basic concepts for technically balancing conflicting requirements (cf. [236]). In order to analyze which factors constitute a fair balance and to refine our proposals,

we followed an interdisciplinary approach. In particular, we discussed the trade-off of privacy protection and accountability with parts of the German information ethics research community, e.g. in workshops that addressed privacy issues in pervasive computing and the Future Internet [240, 235]. Based on the derived insights, we presented a refined set of requirements as well as our conceptual approach in [230]. Technical details were refined in [239].

Finally, we complemented the interdisciplinary embedding of our research by participating in a legal study. This so-called simulation study investigated accountability issues by means of simulated court cases and legal disputes[10].

2.4.5 Application Examples within Reference Scenario

Having described the method and process of our research, we now switch back to the application perspective.

In our reference scenario of location-aware first response, we assume that mobile users continuously provide current GPS locations to the control center for the duration of their missions. While this may support the coordination of rescue missions, collected historical position information creates a log which documents the rescue missions. It thus documents real-world actions to a certain degree. This kind of audit log is what we call a location audit log throughout this thesis.

Such a log can be analyzed for several purposes in the postprocessing phase of an emergency. In the following, we assume that an location audit log obeys to a simple structure: it contains several entries in the form *identifier - time - location*. The organization which accounts for the emergency response wants to be able to analyze processes after a rescue mission. Additionally, the goal of location audit logs is to be able to assign responsibility for real-world actions, since organizations tend to verify compliance.

In the following, we describe motivating real-world examples that could benefit from a such a location audit log.

Example: Emergency Car Driving

During the course of a rescue mission, rescue vans or especially ambulance vehicles sometimes are in need of violating general traffic rules, such as disregarding traffic lights. This may lead to road accidents or injured pedestrians. Usually, emergency cars beckon their emergency missions with sirens, however, there may be situations where no acoustic signals is available. This may also be the case when a volunteer is driving a personal car to quickly reach his designated destination during a rescue mission.

[10] The study is described in detail in Section 7.3.1.

Example: Destruction of Properties and Cases of Omitted Assistance

While mobile first responders are on their missions, they have to strongly prioritize actions, according to given instructions. However, sometimes they have to depart from that, based on local decision making. Some actions might be considered as cases of omitted assistance by eye witnesses. This is especially true, when it comes to rescuing injured persons, and the witnesses are not aware of the actual priorities assigned, that may demand postponing or even skipping assistance.

Moreover, there are a lot of situations that entail the destruction of properties, like breaking doors to enter a building, that are relevant to ex-post liability and accountability discussions.

2.4.6 Security Requirements for Multilaterally Secure Auditing

As motivated, a location audit log contains information that could help to answer questions whether a mobile user acted beyond her competences and authorizations and exploited the current situation for inappropriate, suspicious or even malicious purpose. However, this is a highly critical issue, since, in real-world rescue missions, first responders actually need to break common regulations in some cases in order to save lives, and the underlying decisions often have to be made under time pressure. Therefore, the psychological burdens of possibly having to face legal consequences due to being digitally accountable need to be addressed, in order to foster acceptance for the use of location tracking technologies.

In the following, we introduce our elicited security requirements that have to be met in order to implement a multilaterally secure location auditing. Here, multilateral security is considered in the sense that we take into account security and privacy requirements of mobile users, organizations responsible for emergency response, and law enforcement agencies, as well.

We stress that accountability and thus auditing mechanisms inherently conflict with individual privacy protection. Based on our practical and theoretical considerations that were presented throughout this chapter, we propose the following set of security requirements in order to balance and reconcile location privacy protection and accountability as fair and as far as possible.

Firstly, regarding the perspective of the individual mobile user:

- `SReqA1: Data minimization`: The use of identifiers that are directly associated to users should be avoided as far as possible or minimized in the data collection, in order to provide a basic location privacy protection.

- `SReqA2: Individual access`: The user should be able to access the audit log, in order to be able repudiate false accusations by providing evidences of exoneration [9].

Secondly, regarding the perspective and role of third parties, e.g. organizations responsible for emergency response and public security:

- `SReqA3: Privacy-respecting log analysis`: It should be possible to selectively analyze the entries that are recorded in a log in a privacy-respecting manner[11].

- `SReqA4: Minimal disclosure`: It should be possible to partially re-identify sample entries, i.e. to check if a log entry relates to a common organizational structure or function, without disclosing the complete identity in question.

- `SReqA5: Distribution of powers`: An operational distribution of powers should be enforced, i.e. no single entity should be able to (mis)use the audit functionalities.

- `SReqA6: Transparency`: The whole process of the log analysis should be transparent to an affected user. Especially, it should be detectable if the parties that are responsible for it do not comply with the rules set up for the privacy protection of the individual user.

Thirdly, the legal perspective needs to be taken into account:

- `SReqA7: Law enforcement`: It should be possible to exercise a global law enforcement functionality, i.e. a law enforcement authority should be able revoke privacy protection of every user in question, once convincing evidences of inappropriate behavior have been identified. This is a requirement for many ICT applications, that actually may lead to court proceedings for accused offences [179].

2.5 Summary

In this chapter, we provided a brief introduction to our understanding of pervasive computing, as it is relevant to this thesis. Also, we introduced to the topic of pervasive cooperation. Then, we abstractly described the IT security and privacy issues that are inherent in pervasive systems, from legal as well as technical perspectives.

Subsequently, in order to convey a better understanding of these issues, we introduced our application domain of ICT-supported emergency response. Within our reference scenario of location-aware first response, we depicted how pervasive ICT could efficiently support rescue missions. In particular, we used this setting to instantiate and illustrate the research goals and questions of this thesis.

We then described the pursued methods of our research; we draw from theoretical, practical and interdisciplinary considerations that are integrated by means of iterative requirements elicitation and design processes. Elicited security requirements for secure emergency communication and auditing mechanisms that fairly balance privacy protection and accountability were given in the last part of this

[11] Viewed differently: it should by possible to selectively analyze the entries that are recorded in a log despite that privacy protection is given.

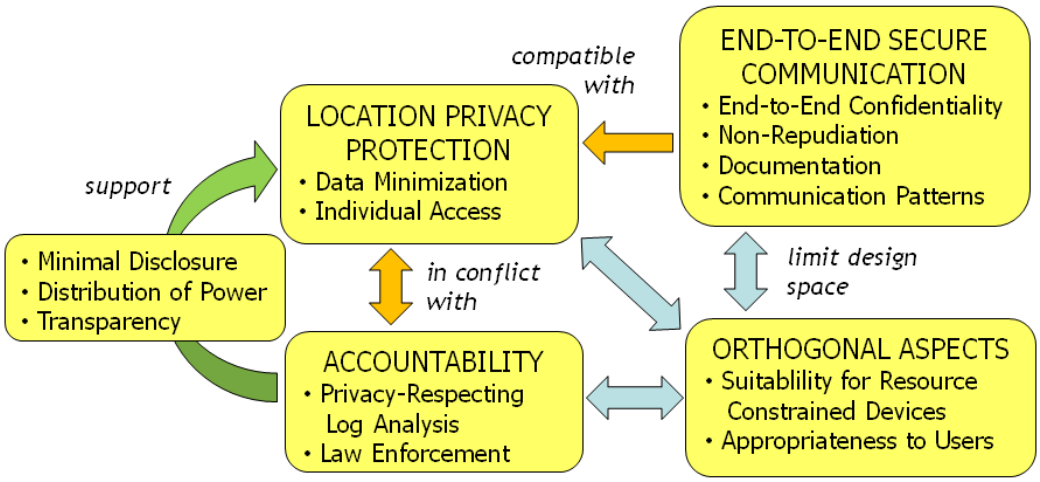

Figure 2.7: Overview of security requirements

chapter. Figure 2.7 gives an overview of the elicited requirements and their dependencies.

In Chapter 3, we will review the state of the art of previous research w.r.t. to our research goals. We will compare the existing proposals to the requirements elicited in this chapter.

3
State of the Art

This chapter reviews the state of the art of security mechanisms relevant to the main goals of this thesis. The main goals and the associated research question were introduced in Chapter 1 and further substantiated in Chapter 2. They serve as structuring element of the discussion.

In our envisioned system for multilaterally secure pervasive cooperation, security mechanisms are required that support two main functionalities: real-world auditing and targeted secure communication with entities unknown by identity. In particular, security and privacy protection are required to render the system acceptable to user expectations and to satisfy security requirements. However, the system functionality shall not be confined by the employed protection mechanisms.

The discussion of the state of the art and thus the remainder of this chapter is structured as follows. Firstly, in Section 3.1, we briefly describe the broader context of security and privacy research in pervasive computing. Then, in the block that is starting in Section 3.2, we analyze security mechanisms that may enable auditing while a fair balance of privacy protection and accountability is given. Hereby, we discuss and review existing work on pseudonymous auditing, location privacy protection and digital pseudonyms. In an additional block (Section 3.3), we review the state of the art of communication mechanisms suitable for settings with unknown, mobile receivers as well as dynamic groups. Our focus is put on approaches to one-to-many messaging, which was identified as a key communication means in emergency response scenarios in the last chapter. Furthermore, mechanisms for the enforcement of end-to-end security suitable for one-to-many messaging are discussed.

3.1 The Broader Context

In this chapter, we focus our discussions on work that is closely related to the goals of this thesis. Yet, we are aware of a broad range of further works on security and privacy protection adequate for pervasive computing.

This topic has e.g. been addressed by several PhD theses [108, 126, 103, 138, 14, 56, 111, 199, 7] in the last years. The described approaches are mostly *complementary*

to our work w.r.t. the development of more comprehensive security architectures for pervasive systems.

However, to the best of our knowledge, research that explicitly targets the design of multilaterally secure pervasive system is still in its infancy. In this area, Ortmann et al. [168] address conflicting individual privacy requirements in multi-user pervasive computing environments. In addition, Gürses et al. [94] propose a method for analyzing multilateral security requirements that is applicable to pervasive computing environments. This method takes into account varying privacy interests.

On the other hand, there is a broad body of research that addressed the issue of privacy protection in different computing settings. In particular, existing privacy-enhancing technologies (PETs) can be the starting point to devise multilaterally secure mechanisms for pervasive systems. We refer the reader to [2] for a general overview, to [113] for a discussion of privacy issues related to human-computer interaction (HCI) and to [117] for a discussion of cryptographic PETs. They represent one of the main topics of this thesis, on a technical level.

3.2 Towards Multilaterally Secure Pervasive Auditing

A basic mechanism that is often exploited in the design of multilaterally secure systems is that already the detectability of inappropriate actions and accountability for origination suffices to prevent misbehavior from happening. Especially, it is used to enforce correct behavior in computing and also many real life settings, e.g. road traffic regulation.

In a computing system, the traditional technical means to deal with this issue are audit logs [200, 229]. Basically, an audit log contains tamper evident entries that aim at recording irrefutable evidences of all users' actions. While the log content helps to detect inappropriate actions, users that behave appropriately could use it to defend themselves against false accusations.

In this thesis, we aim for a special kind of audit log that helps to document real-world actions. Application examples in the area of first response missions are used to illustrate it. We discussed and derived security requirements that have to be met to implement multilaterally secure auditing functionalities in Section 2.4.4. We consider multilateral security in the sense that we take into account security and privacy requirements of users, organizations and law enforcement agencies, as well. Our goal is to achieve a fair balance of privacy protection and accountability.

A "classical" principle for balancing privacy protection and accountability is due to Chaum [45]: the given privacy protection of a user shall be revoked in case a misuse has been detected. On a technical level, this may mean that a certain threshold has been exceeded. A primary application example is that of e-cash: the user remains initially private, when spending her electronic coins in a legitimate way. Yet, in case she tries to illegally spend coins multiple times (which is possible since coins are represented as mere digital information), her true identity shall be disclosed and

the misuse be made obvious by authorized parties[1]. Yet, distinguishing between legitimate and illegal or malicious actions is more difficult in different applications.

In our setting, the basic privacy protection can be implemented due to the use of *pseudonyms* in the location tracking. Pseudonyms are identifier of entities that are used instead of the entities' real-world names. Pseudonyms then also implement the central reference point to evidence stored in an audit log. Consequently, following this approach requires that auditing functionalities are compatible with pseudonymized log data.

Making use of pseudonyms allows reconciling privacy protection and accountability in audit logs [67, 71] to a certain extent. Pseudonymous auditing was first proposed by Fischer-Hübner in [69]. In recent work [71], the following principles are considered for achieving a fair balance:

1. Pseudonymized entries of a log and thus pseudonymized entities can be made accountable again. This is called *re-identification* or *disclosure of pseudonyms*. Technically, the disclosure of pseudonyms requires to make use of the pseudonym-to-identity-mapping.

2. The disclosure capability should be controlled, i.e. only authorized parties shall be able to re-identify entities. Also, it should adhere to a priori specified purposes and rules. In this thesis, we denote such a specification as *disclosure policy*.

In this thesis, we have defined a more extensive set of requirements to fairly balance privacy protection and accountability. Additionally, re-identification shall only be possible in a cooperative manner and proceed stepwise. Also, affected users shall further be supported by enabling individual log access and transparency to reconcile security interests. Thus, a main challenge is to implement a selective control on the pseudonym-to-identity mapping, i.e. a flexible control functionality regarding the pseudonym linkability. Viewed differently, it is our aim to provide certain degrees of pseudonym linkability for users, organizations as well as authorities.

To the best of our knowledge, there is no approach to auditing described in the literature that meets all of our requirements. However, there are existing approaches and security mechanisms that partly address our research questions. In particular, we next discuss

- relevant properties and the constructions of digital pseudonyms,
- location privacy protection based on pseudonyms,
- approaches to pseudonymous auditing,

Our discussion starts with properties of pseudonyms in order to put forward our line of argumentation.

[1] Arguing about parties that are authorized to disclose identities in case of detected misuse leads to a further question: who should be authorized for such kind of capability? Possibly, parties with a legal or organizational mandate are candidates for this task, yet it depends on the application.

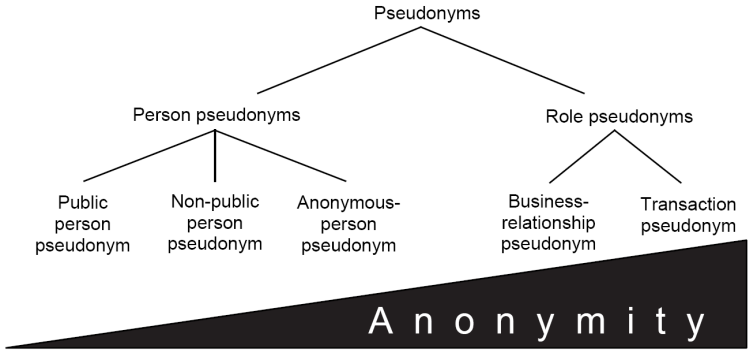

Figure 3.1: Classification of pseudonyms according to [178]

3.2.1 Relevant Properties of Digital Pseudonyms

Historically, the term pseudonymous relates to the Greek word pseudonymos, which means having a false name [68]. In a technical sense, a digital pseudonym[2] is an identifier of an entity that is used instead of the entitys real-world name [175]. Pseudonymity is the use of pseudonyms as identifiers.

Chaum [43] introduced digital pseudonyms as a basic tool for privacy protection in computing systems. Since a pseudonym replaces identity-related information, it firsthand implements unlinkability between a real-world identity and a pseudonymized identity. In a computing system, a user can act among one or multiple pseudonyms in digital transactions, e.g. in order to use a digital resource or service without disclosing her identity. In recent years, a rich scientific background has evolved [175] and several types of pseudonyms and fields of applications have been identified.

Pseudonyms can be classified according to the degree of protection provided by them, which is also given in Figure 3.1. The degree of protection manifests by the unlinkability to a given user. Main types of pseudonyms[3] that can be classified are *person pseudonyms*, *role pseudonyms* and *transaction pseudonyms*. A person pseudonym is a substitute for a person's name and represents the user's civil identity. Role pseudonyms are used for specific applications or tasks. Transaction pseudonyms are pseudonyms that are only used in a single transaction. Thus, in the literature, transaction pseudonyms are sometimes also denoted as *short-lived pseudonyms* or simply as *changing pseudonyms*.

The provided degree of unlinkability and thus anonymity is stronger, the more often pseudonyms are changed over time. Thus, anonymity is highest for transaction pseudonyms,

[2]For simplicity, we consider pseudonym as synonym to digital pseudonym.

[3]For more details see [175]. In [175], also further classes of pseudonyms that are not relevant to this thesis are described.

Furthermore, pseudonyms can classified depending on how and by whom given pseudonyms can be re-translated into the user's identity (by making use of the pseudonym-to-identity-mapping). This is also captured in the notion of *linkable pseudonyms* [19]. Technically, enabling such a mapping requires that a pseudonym additionally encodes some kind of or is associated to trapdoor information, to enable attribution of pseudonyms to real-world identities. According to [67], major types of pseudonyms are:

- *Reference pseudonyms:* In a simple case, a (non-changing) pseudonym can be mapped back to an identity based on existing reference information, e.g. if issued public keys are used as pseudonyms. Access to the referencing registration information then limits pseudonym disclosure.
- *Self-generated pseudonyms:* In case that pseudonyms are only generated by the user herself and no reference is stored together with identities, only the user herself can link a pseudonym, e.g. based on secret information. A self-chosen nickname is a simple example.
- *Cryptographic pseudonyms:* Given that pseudonyms are constructed by applying a cryptographic function to identity-related information, the function itself and possibly further input parameters control the re-identification. In case of relying on encryption functions, e.g. the keys that enable decryption have to be known.

Cryptographic pseudonyms have been applied and are key building blocks to implement pseudonymous auditing functionalities [67]. We discuss applications of pseudonyms for location privacy protection in the next section, in order to convey the protection granted by pseudonyms. Then, we review existing approaches to pseudonymous auditing. Finally, we investigate relevant approaches to cryptographic transactions pseudonyms w.r.t. their suitability as possible building blocks for multilaterally secure auditing. Where applicable, security requirements that are addressed (+) / not addressed (-) / partially addressed (∘) are marked.

3.2.2 Location Privacy Protection based on Pseudonyms

In the context of location tracking systems and pervasive computing, pseudonyms have been proposed as one of the basic means for *location privacy protection*. None of the following approaches considers all our requirements. Thus, we will mark requirements that are satisfied in order to refer to the relevant aspects of a certain approach.

In a traditional direction of research, pseudonyms are used to protect against an adversary that tries to link transactions and users in order to construct movement profiles and comprehensive user traces (SReqA1: +). In early work, Kesdogan et al. [131] proposed to use short-lived pseudonyms in mobile GSM networks (SReqA1: +). Beresford et al. [15] combined the use of changing pseudonyms with a geographic abstraction of mixnets, to form so called mix-zones. For users

of location-based services, a mix-zone is a region without service use, in which the actual pseudonym change is done, to hinder profiling (SReqA4: +). Recent follow up work [78] addresses non-cooperative location privacy models and evaluates the effect of unsynchronized pseudonym changes on the degree of anonymity achieved (SReqA4: +).

A different use of pseudonyms is presented by Delakouridis et al. [53, 149, 150], applying pseudonyms to the problem of securely storing and accessing location information in a privacy-preserving, decentralized manner (SReqA2: +). The authors propose to use pseudonyms as reference points for data access, and to additionally split the location information to be protected according to Shamir secret sharing [202], and to distribute those shares on several servers, addressable via pseudonyms.

Jorns et al. [122, 123] describe a further approach for location privacy protection based on transaction pseudonyms (SReqA1: +). The authors propose to create pseudonyms via iterative hashing. Differently from our goals, the focus of this work is to realize privacy-respecting authentication mechanisms for the access of location-based services.

3.2.3 Pseudonymous Auditing

Pseudonymous auditing refers to the analysis of audit logs[4] that contain pseudonymized entries. It is now a widely recognized approach to balance the conflicting security requirements of accountability and privacy protection to a *certain extend*. The manual analysis itself, which is employed to derive evidences about the occurrence or non-occurrence of misuse documented by the log[5], is often denoted as audit.

In contrast to this kind of manual ex-post process, an automatic analysis of logs during run time is called intrusion detection. Intrusion detection systems (IDS) are often considered in combination with audit logs. A broad discussion on intrusion detection systems is given by Flegel [71]. Typically, IDS approaches do not consider (at least) the individual access requirement (SReqA2: -); a distribution of powers is mostly only partially addressed (SReqA5: ○). In the present discussion, we will also consider IDS approaches that are applicable to our setting. This discussion helps the reader trace the historical evolution of concepts.

Early IDS approaches and implementations that targeted pseudonymous auditing were presented in the seminal work of Fischer-Hübner et al. [69, 66].

In [210], Sobirey et al. present an approach that makes use of symmetric encryption for pseudonymization. Here, secret keys are updated in regular intervals to produce some degree of linkability w.r.t. pseudonyms. The approach could be extended to a distribution of powers (SReqA5: ○), e.g. by secret sharing the secret key in use [67].

[4] In some literature, the term *audit trail* is used interchangeable to audit log.
[5] We restrict our discussion concerning the use of logs to the context of accountability.

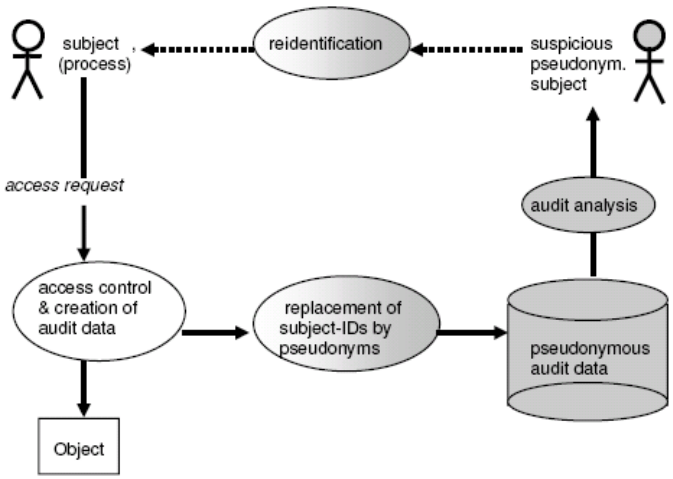

Figure 3.2: Pseudonymous operating system auditing according to [209, 67]

An overview of the follow-up approach of Sobirey et al. [208, 209] is shown in Figure 3.2, to depict a common approach to pseudonymous auditing. It is described within the context of operating system auditing. It proposes the three basic steps of the creation of pseudonymous audit data (which is in some work also referred to as logging), the audit log analysis and the consecutive re-identification. In this approach, the pseudonymization takes only place after transactions, such that data minimization is only partially supported (SReqA1: ○). Also, individual access (SReqA2: -), partial re-identification (SReqA4: -), distribution of powers and transparency (SReq6: -) are not considered.

Biskup and Flegel propose to use transaction pseudonyms [20, 71] in audit logs as well as a method for the re-identification [19, 71] based on secret sharing [202]. The aim of the approach is to model the concept of initial suspicions that lead to the disclosure of pseudonyms, in case a threshold of detected actions of possible misuse is exceeded in the log analysis. Technically, pseudonyms are represented as shares of a secret that relates to a users identity. The approach allows for a fine-grained pseudonymization of logs while the analysis provides a higher degree of privacy protection than previous approaches. Yet, mechanisms for individual access (SReqA2: -), distribution of powers (SReqA5: -) and transparency (SReqA6: -) are not described.

Differently, Shen et al. [204] describe an approach that focuses on the distribution of powers (SReq5A: +). The authors propose mechanisms based on variants of secure multiparty computation techniques [248]. Here, the focus is on realizing privacy-preserving query mechanisms for analyzing a log without explicitly considering the concept of pseudonyms. Also, mechanisms for individual access (SReqA2: -), partial re-identification (SReqA4: -) and transparency (SReqA6: -) are

not addressed.

In [99, 100], Hedbom et al. introduce concepts that are applicable to privacy-respecting transparency logs (SReqA6: +). This work complements existing proposals to pseudonymous auditing, yet the authors do not describe a fully integrated approach which addresses auditing and transparency.

	SReqA1: Data minimization	SReqA2: Individual access	SReqA3: Privacy-respecting log analysis	SReqA4: Minimal disclosure	SReqA5: Distribution of powers	SReqA6: Transparency	SReqA7: Law enforcement
Fischer-Hübner [69, 66]	○	-	+	-	○	-	○
Sobirey et al. [210, 208, 209]	○	-	+	-	○	-	○
Biskup and Flegel [19, 20, 71]	○	-	+	+	○	-	○
Shen et al. [204]	○	+	+	+	+	-	-
Hedbom et al. [99, 100]	○	○	+	-	-	+	-

Table 3.1: Approaches to pseudonymous auditing

In Table 3.1, an overview of the discussed state of the art approaches to pseudonymous auditing and the addressed security requirements is given. Within the table, we use the same notation as before (requirement addressed: + / not addressed: - / partially addressed: ○).

None of the existing proposals addresses all the listed requirements.

3.2.4 Efficient Constructions of Transaction Pseudonyms

From the discussion of existing approaches to pseudonymous auditing, we conclude that the underlying pseudonym construction has a major impact on the pro-

vided flexibility of the re-identification of pseudonymized users. In the following, we will investigate prominent constructions of transaction pseudonyms w.r.t. their applicability for our auditing setting. Hereby, we focus on approaches that are considered computationally efficient, since we target a use on resource-constrained mobile device. Such efficient approaches have e.g. been proposed in and applied to the area of RFID systems.

Several authors propose to use the output of hash functions as transaction pseudonyms. In this context, Henrici et al. [104] propose the so-called hash-based ID variation approach, which in fact means a hash-based construction of transaction pseudonyms. Since the scheme makes also use of session numbers, it requires an initial synchronization with the backend side. The backend also triggers the change of pseudonyms, making it unpractical for our setting, since we require a random access facility for the log analysis. Ohkubo et al [166, 167] and Gruteser et al. [92] propose to use a different constructions called hash-chains, to construct short-lived pseudonyms. Here, the client itself changes the transaction pseudonym by deriving it (via hashing) from a hash chain, i.e. an iterated application of a hash on a base identifier. A main drawback is the computational load for the backend, which basically also has to execute hash iterations on all stored reference identifiers. This leads to some sort of brute force search in order to authenticate (or thus re-identify) a pseudonym. Advancements and combinations of the approaches are discussed in [105].

A common property of such schemes is that different outputs (given a suitable hash function) are pseudorandom and thus unlinkable. Also, since hash-functions are one-way, the encoded identity is protected in the output. Yet, this class of constructions does thus far not support a partial re-identification (SReqA4: -). Also, mechanisms for a distribution of power (SReqA5: -) are not described.

A different approach to efficiently derive transaction pseudonyms is proposed by Juels et al. [125]. This work makes use of ElGamal encryption. Transaction pseudonyms are derived by updating random factors in re-encryption operations. Here, unlinkability and identity protection stems from the semantic security property of ElGamal encryption. The approach supports law enforcement (SReqA7: +), yet, no mechanisms for a partial re-identification (SReqA4: -) are described. Since it employs a public key encryption, the ciphertexts and thus the pseudonyms exhibit some kind of underlying algebraic structure, which could be harnessed to devise extended linkability mechanisms. Also, a distribution of powers could by achieved by secret sharing the private key, which makes this approach a candidate building block for multilaterally secure auditing.

3.2.5 Conclusion

In the last sections, we have reviewed the state of the art of existing approach towards the realization of multilaterally secure auditing. This included discussions of suitable pseudonym constructions, location privacy protection via pseudonyms as well as an investigation of existing approaches to pseudonymous auditing. None of

the presented approaches has satisfied all our requirements.

However, the existing work provides insights in designing suitable mechanisms. In particular, pseudonyms can implement main reference points to the detection of evidence inside a log. In addition, transaction pseudonyms can provide the highest degree of privacy protection. A key challenge is thus to devise a flexible approach to linkable transaction pseudonyms, which can support users, organizations and law enforcement authorities. We identified re-encryption-based pseudonyms as a relevant base construction that we will consider for further advancements.

So far, the existing auditing concepts were applied within traditional computer security applications like operating system audit logs. In our work, we aim to extend the application perspective also to real-world audit logs, which emerge from location tracking applications[6]. A further challenge is thus to conceptualize auditing mechanisms that are suitable for our novel real-world application scenario.

3.3 Towards End-to-End Secure Pervasive Communication

Communication technologies already have become an integral part of our modern information society. Personal communication devices, as forerunners of pervasive computing, enable locally distributed users to participate in communication contexts of everyday's life and work. In some application scenarios, communication technologies even constitute a critical service: considering e.g. the case of a sudden emergency, efficient communication support can mean the difference between success and failure of rescue missions, possibly between life and death of affected persons and between the loss and safeguard of infrastructure and property. Thus, efficient emergency communication is of high practical importance, but has specific challenges: unpredictable local emergency situations harden the establishment of communication structures, legal requirements dictate the use of end-to-end secure and documentable approaches, while end users demand ease-of-use and possibly location privacy protection.

In our work, we use the setting of emergency communication as a kind of descriptive worst-case-application-scenario with special demands. In Section 2.4.2, we described major characteristics of emergency communications. Especially, a mechanism is required that enables one-to-many communication with mobile and possibly unknown and thus nameless receivers, that may also locally form dynamic groups. Additionally, end-to-end encryption for the communication is legally implied, which constitutes an additional challenge.

However, the targeted type of communication is also relevant to further pervasive computing settings beyond first response, e.g. in vehicular ad-hoc networks (VANETs) [110] or Future Internet settings [238].

To the best of our knowledge, there is no approach to communication described in the literature that meets all of our requirements. However, there are existing

[6] In [219], the application of accountability concepts to comparable settings is denoted as *accountability of presence*.

approaches and security mechanisms that partly address our research questions. In particular, we discuss

- approaches to secure one-to-many messaging,
- techniques for achieving end-to-end encryption.

Our discussion starts with a review of existing approaches to one-to-may messaging. Within this discussion, we also sketch the employed security mechanisms. Yet, a more detailed consideration of the issue of end-to-end encryption follows in Section 3.3.2.

3.3.1 Approaches to Secure One-to-Many Messaging

Work on secure one-to-many messaging started with the introduction of secure role-based messaging [42, 160]. The scheme of Chadwick et al. [42] allows specifying the recipients of a message based on a single organizational role. It employs traditional public key infrastructure (PKI) [154] and role-based access control (RBAC) [193] mechanisms, but does not provide end-to-end encryption suitable to our setting (SReqC2: ○), since a trusted entity is required for each message decryption. Issues related to resource-constrained devices are not addressed (SReqC6: ○).

The proposal of Mont et al. [160] allows combining several roles in order to form a logical policy for recipient selection. The messaging scheme harnesses identity-based encryption [86], such that logical policies are mapped to a single cryptographic keys. Furthermore as a main drawback, it requires frequent interactions with an online private key generator (PKG) in order to receive message decryption keys (SReqC2: ○). The authors focus on the security mechanisms for receivers, thus they do not address sender non-repudiation (SReqC4: -).

In the work of Karabulut et al. [127], a one-to-many messaging service that provides end-to-end confidentiality is described. This approach harnesses IBE and also requires an online PKG (SReqC2: ○). The focus of this work is to achieve an integration of mobile devices into an enterprise system. In the messaging, only a single attribute is considered. Requirements related to privacy protection are not addressed (SReqC8: -).

In Bobba et al.'s approach, [23], the concept of attribute-based messaging is introduced. ABM allows logically specifying the group of receivers of a message in form of a flexible combination of attributes. ABM can be seen as a generalization of role-based messaging. Bobba et al.'s approach builds on attribute-based access control (ABAC) [249] as main security mechanism and thus does not provide end-to-end encryption at all (SReqC2: -).

After the introduction of attribute-based encryption (ABE) techniques [192, 90, 181], which provide mechanisms for fine-grained cryptographic access control, end-to-end encrypted attribute-based messaging schemes [232, 24] were proposed.

Both schemes employ ciphertext-policy attribute-based encryption (CP-ABE) [17], which allows for a flexible cryptographic encoding of sending policies. Especially,

[24] extends the earlier work of Bobba et al. [23], by integrating encryption into ABAC mechanisms, but addressed neither the handling of continuous dynamic attributes like location (CP1: -) nor the requirements related to mobile receivers (SReqC6: ○).

Generally, the application of ABE enables a flexible specification of receivers and content by means of multiple attributes. Yet, due to the inherent use of computationally demanding pairing-based cryptography, the practical applicability of ABE concepts in scenarios with mobile and resource-constrained devices remains highly challenging.

The approach reported in [232] is part of the research presented in this thesis. It contains a proposal of an attribute-based messaging scheme and system for emergency communication. While it was limited w.r.t. handling continuous dynamic attributes as selectors, handling replay attacks (SReqC3: -) and issues related to ease-of-use (SReqC7: -), a prototype was used to initiate discussions with real users, enabling a cognitive walkthrough[7][21] of emergency communication scenarios.

In a different line of research, Mayrhofer et al. [155] describe a one-to-many messaging approach that also considers location addressing (CP1: +) and some sort of location privacy protection (SReqC8: +). However, it is tailored for applications scenarios that do not require end-to-end encryption (SReqC2: -).

In Table 3.2, an overview of the discussed state of the art approaches to secure one-to-many messaging and the addressed security requirements is given. Within the table, we use the same notation as before (requirement addressed: + / not addressed: - / partially addressed: ○).

None of the existing proposals addresses all the listed requirements.

3.3.2 Techniques for End-to-End Encryption

The discussion of approaches for secure one-to-many messaging identified that a flexible combination of attributes is a considered as an appropriate means for the selection of receivers that are unknown by identity. However, enforcing end-to-end confidentiality in such settings is challenging.

Firsthand, attribute-based messaging is usually implemented by some form of access control mechanism, which allows securing the information in transmission. Only user who can access the content of a message are considered as readers. For wireless transmission, as found in our reference scenario, access control mechanisms that do not rely on encryption are not suitable.

In the following, we review existing techniques that can be used to implement end-to-end encryption. As already partly mentioned in the last section, end-to-end secure communication can be implemented based on

- Symmetric Encryption

[7] A cognitive walkthrough, an usability evaluation method, builds on practical user experiments with a system. This helped to understand how real users interact by and with an emergency communication system. Findings contributed to Section 2.4.2 and Section 7.3.2.

	SReqC1: Basic security	SReqC2: End-to-end confidentiality w/o online PKG	SReqC3: Protection against replay attacks	SReqC4: Non-repudiation of senders	SReqC5: Documentation of readers	SReqC6: Efficiency of security mechanisms	SReqC7: Appropriateness to users	SReqC8: Location privacy protection of receivers	Communication patterns
Chadwick et al. [42]	+	o	o	+	-	-	+	o	o
Mont et al. [160]	+	o	o	-	-	-	+	o	-
Karabulut et al. [127]	+	o	+	+	-	+	-	-	o
Bobba et al. [23]	+	-	+	+	+	o	o	-	o
Bobba et al. [24]	+	+	+	+	+	o	o	-	o
Weber [232]	+	+	-	-	-	+	-	+	o
Mayrhofer et al. [155]	o	-	o	o	-	+	-	+	+

Table 3.2: Approaches to secure one-to-many messaging

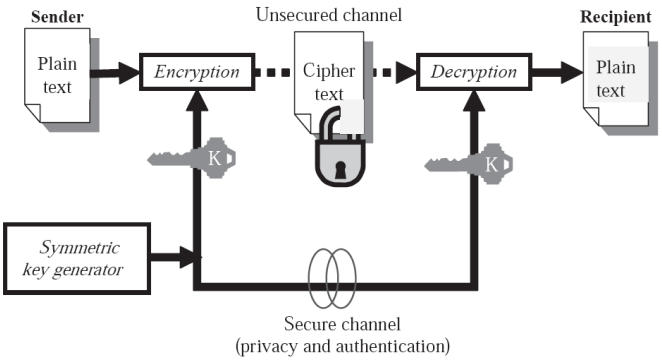

Figure 9.1 Symmetric cryptography

Figure 3.3: Principle of symmetric encryption according to [41]

- Asymmetric Encryption
- Identity-based Encryption
- Attribute-based Encryption

We discuss these approaches next.

In a large-scale or distributed setting, traditional cryptographic constructions suffer from key distribution problems (symmetric encryption) or problems related to the efficiency of encryption operations (asymmetric encryption).

Figure 3.3 depicts the basic approach how symmetric encryption can be applied to achieve secure communication. The main drawback is that a symmetric key has to be distributed between any relevant combination of senders and recipients. In case the group of recipients is not known when a message is send out, this approach is not applicable.

Figure 3.4 illustrates how public key encryption can solve the key distribution problem of symmetric encryption. Here, instead of using a single symmetric key for both encryption and decryption, a pair of keys is used. It consists of a public key and a private key. By publishing the public keys of all possible recipients, a sender can send encrypted messages. Yet, this approach does not consider one-to-many settings. Also, operations of asymmetric encryption are more resource demanding than symmetric ones. Therefore, both concepts alone do not fit well in our setting.

Identity-based encryption, which is a certificateless alternative to public key encryption, allows encrypting messages under textual strings, instead of public keys. Such a string originally refers to the identity of a recipient. This is also shown in overview in Figure 3.5. However, this approach requires a complete list of all intended receivers. This allows realizing encryption that is partly suitable for one-to-many settings, by describing a group by a single textual string.

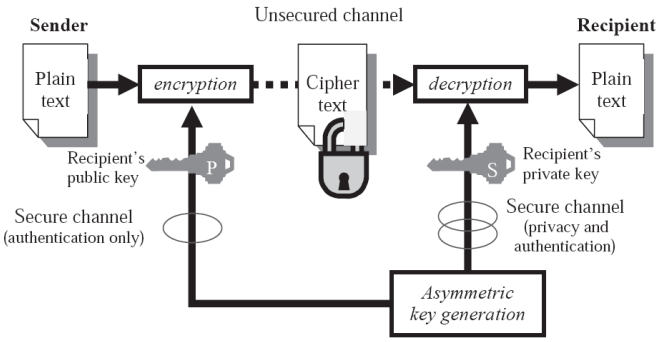

Figure 9.4 Asymmetric cryptography

Figure 3.4: Principle of asymmetric encryption according to [41]

Yet, we seek to employ an encryption technique that is able to handle more expressive messaging policies, which may translate to and thus support the concept of attribute-based messaging more directly.

Attribute-based encryption (ABE) is a natural candidate building block for this setting: here, groups of recipients can be selected in an elegant way, by specifying combinations of descriptive attributes. Especially, ABE is a generalization of IBE. In fact, the first variant was described as fuzzy identity-based encryption [192].

Yet, current ABE proposals lack an efficient way of handling dynamic attributes. One common way is to add an expiration date to attributes as revocation mechanism, as proposed by Bethencourt et al. [17]. Yet, this is not applicable to attributes that change in an unpredictable manner, as in the case of location attributes, where attributes additionally have a continuous range of values.

3.3.3 Conclusion

In the last sections, we have reviewed the state of the art of existing approach towards the realization of end-to-end secure group communications suitable for pervasive settings.

This review included a discussion of approaches to secure one-to-many messaging and techniques for achieving the required end-to-end encryption. None of the presented approaches has satisfied all our requirements.

However, we identified the concept of attribute-based messaging (ABM) as communication approach that is suitable to our setting. Existing ABM approaches harness ciphertext-policy attribute-based encryption for achieving end-to-end confidentiality. Our setting requires taking into account also continuous dynamic attributes, which is currently not supported by existing ABE techniques.

Beyond developing encryption techniques that support dynamic attributes, a main scientific challenge is to devise an attribute-based messaging concept that is suit-

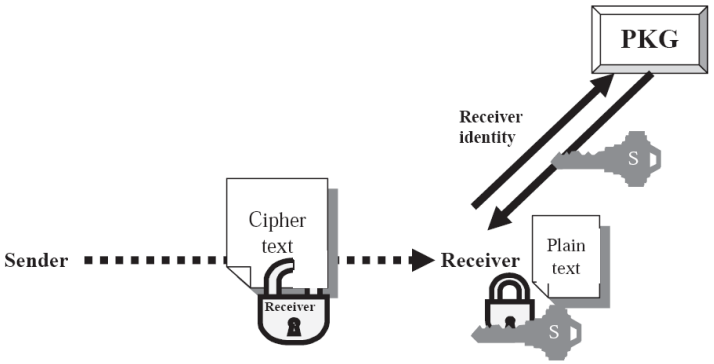

Figure 9.9 Use of identity-based cryptography

Figure 3.5: Principle of identity-based cryptography according to [41]

able to our setting. In particular, end-to-end encryption has to meet the resource constraints of mobile devices.

3.4 Summary

This thesis aims to support multilaterally secure pervasive cooperations, especially w.r.t. the two main system functionalities of real-world auditing and secure pervasive one-to-many communication. This chapter reviewed the state of the art of security mechanisms found in the the research literature, which can be applied to our setting.

Our discussion of the state of the art lead to insights on how to design the required functionalities in a secure way. Also the shortcomings of existing proposals were identified. In particular, no existing approach satisfied all our requirements.

The first part of our state of the art review analyzed how to achieve a fair balance of privacy protection and accountability. We identified pseudonym constructions that provide flexible degrees of linkability for users, organizations and law enforcement authorities as major building block for the realization of multilaterally secure auditing mechanisms. In particular, re-encryption-based transaction pseudonyms will further be considered in the next chapter.

The second part of our investigation focused on enabling end-to-end secure communication with mobile entities that are unknown by identity. We identified attribute-based messaging as the candidate communication mechanism for our setting. The required end-to-end encryption can potentially be addressed by means of attribute-based encryption techniques. However, resource constraints of mobile devices have to be met and the handling of continuous dynamic attributes has to be supported.

4
Novel Security Techniques

In this chapter, we describe two novel security techniques which overcome identified limitations of current state-of-the-art techniques (cf. Chapter 3). They constitute important building blocks for the realization of our approach to multilaterally secure pervasive cooperation. In particular, we introduce:

- *pseudonyms with implicit attributes*, a novel method to realize multilevel linkable transaction pseudonyms,
- a *hybrid encryption technique for expressive policies*; this novel encryption technique may handle static attributes and continuous dynamic attributes in combination as part of conjunctive encryption policies.

In later parts of this thesis, we show that pseudonyms with implicit attributes support balancing privacy protection and accountability. We describe this in the context of real-world auditing. The novel encryption technique is a key mechanism for realizing end-to-end security within our messaging mechanisms. Beyond this instantiation, both techniques have further applications, which will later be discussed in Section 7.4.

In the description of both techniques, we refer to the term *attribute*. In this work, attributes represent properties of users and are thus parts of digital identities of users (cf. Section 6.2.1). However, it is important to note that we introduce two different techniques that digitally handle specific properties of users by means of attributes. In Chapter 5 and in Chapter 6, we will describe how these two approaches can be combined in order to support a multilaterally secure pervasive cooperation.

This chapter is structured as follows: Firstly, we introduce the basics of pseudonyms with implicit attributes in Section 4.1. We describe the construction, which harnesses threshold ElGamal encryption, pseudo-random number generators and secure multiparty computation mechanisms to establish several levels of linkability between a pseudonym and its holder. Details on the setting and the main protocols are introduced in Section 4.2. Then, in Section 4.3, we introduce a novel hybrid encryption technique which is able to handle expressive encryption policies. This technique is based on an efficient combination of attribute-based encryption and location-based encryption techniques. The setting and main concepts are described in Section 4.4. The chapter is concluded in Section 4.5.

4.1 Pseudonyms with Implicit Attributes

In this section, we describe how to construct *pseudonyms with implicit attributes*, a novel approach for realizing multilevel linkable transaction pseudonyms. While a transaction pseudonym provides statistical unlinkability to further pseudonyms created by the same user, multilevel linkability refers to a controlled capability to make pseudonymous users accountable again in several levels of re-identification. In order to achieve these seemingly conflicting properties, pseudonyms with implicit attributes encode specific access informations that allow defining and enforcing security policies (cf. Section 2.4.6) on transaction pseudonyms:

- users are empowered to authenticate own pseudonyms after use,
- authorized parties may cooperatively re-identify pseudonyms in multiple levels of granularity, i.e. link them to attributes that are only implicitly associated with pseudonyms due to specific registration information,
- an (optional) law enforcement authority may completely disclose every transaction pseudonym.

Our approach builds on and extends earlier work of Juels and Pappu [125], which proposed encryption-based transaction pseudonyms (cf. Section 3.2.4). In existing work, a controlled linkability is usually limited to law enforcement or does neither consider a stepwise nor a cooperative re-identification. The next section introduces the proposed construction principle, followed by a description of the main primitives than we build upon. Then, the mechanisms are explained in detail.

4.1.1 Construction Principle

As discussed in Section 3, pseudonyms implement central reference points w.r.t. the handling of access to personal data in pervasive systems. Thus, pseudonyms can allow balancing conflicting accountability and privacy requirements to some extent. Since a pseudonym is an identifier of an entity that is used instead of the real-world name of the entity, it implements a certain degree of unlinkability and thus privacy protection. By using the identifier-to-pseudonym-mapping, a re-identification of entities' real world names is possible; thus making pseudonymized entities accountable again. Hence, a fair balance of interests depends on the provided degrees of (un-)linkability implemented by a pseudonym and by controlling who can use the pseudonym-to-identity-mapping.

Existing types of pseudonyms (reference pseudonyms, self-generated pseudonyms and cryptographic pseudonyms (cf. Section 3.2.1)) allow constructing particular forms of pseudonym linkability. We strive for a construction that integrates all these different levels of linkability. Thus, we propose to combine useful properties of every of this types.

It is known that techniques from the area of secure multiparty computation (SMPC) can theoretically be applied to a large range of problems in the area of privacy-preserving data analysis and in the construction of privacy-preserving protocols

[106, 142]. Basically, SMPC mechanisms [248] allow implementing multiparty protocols that do not rely on a single trusted third party (TTP). The intention of these cryptographic techniques is that a number of distinct, but connected parties may jointly compute an agreed function of their inputs in a secure way. Hereby, the correctness of the output as well as the privacy of each input shall be preserved, even if some participants cheat. Thus, secure multiparty computation is a general approach to distribute the functionality and powers of a single TTP among several parties[1]. In most SMPC approaches, this is only achieved with very high computational costs [142], due to the intensive use of secret sharing [202] and operations on secret shared data in SMPC protocols. Yet, more efficient special purpose approaches to SMPC have been proposed. E.g. in the *mix-and-match* approach [118], secret sharing techniques are replaced by *operations on encrypted data*. We exploit this capability in our proposal.

Hereby, we follow basic ideas of the *mix-and-match* approach. We formulate the pseudonym generation in terms of specific non-deterministic encryption operations. Since the encryption is non-deterministic, this allows deriving multiple transaction pseudonyms by updating the inherent random factors. Also, this enables us to apply efficient concepts from the mix-and-match framework in order to realize privacy-respecting data analysis functionalities *on the pseudonym level*. Especially, we realize the mechanisms for multilevel linkability of pseudonyms based on extended mix-and-match concepts.

Additionally, we propose to make use of cryptographically secure pseudo random number generators [133] in order to control random factors inside the encryption operations. This allows implementing a further direct pseudonym-to-identity-mapping, that can be exploited by a user, in order to authenticate pseudonyms that relate to herself.

4.1.2 Main Primitives

Having introduced the construction principle, in this section, we briefly describe the main primitives that are employed in order to implement the pseudonyms with implicit attributes approach.

Cryptographically Secure PRNGs

A pseudo-random number generator (PRNG) [133] is a deterministic algorithm that generates sequences of numbers that appear random. In order to achieve this, a PRNG incorporates an internal source of entropy, which is called a seed, for deriving and computing the output. A cryptographically secure PRNG is a special kind of PRNG that produces sequences of numbers with stronger security requirements: it is practically impossible to guess or derive any forward or backward numbers by

[1] A classic example of SMPC is the millionaires' problem due to Yao [248]: some millionaires (*the parties*) want to find out, who is the richest (*agreed function*) without revealing the precise amount of their individual wealth (*input privacy*).

analyzing the output of a cryptographically secure PRNG. Therefore, such a PRNG is suitable for cryptographic purposes. Our constructions actually employ cryptographically secure PRNGs. For simplicity, we often refer to this tool simply as PRNG.

Threshold ElGamal Cryptosystem

A key primitive in our approach is the ElGamal cryptosystem [60], over subgroups $\mathbb{G}_q$ of order q of the multiplicative group $\mathbb{Z}_p^*$, for large primes $p = 2q + 1$. The primes p, q and a generator g of $\mathbb{G}_q$ are common system parameters. ElGamal encryption is semantically secure in $\mathbb{G}_q$, under certain complexity assumptions [222]. Practically, semantic security means that no partial information about a plaintext is leaking from the corresponding ciphertext. Thus, an adversary can neither recover any information about the plaintext from the ciphertext, nor distinguish whether a ciphertext is the encryption of a known plaintext or not.

More specifically, we utilize a threshold variant of the ElGamal cryptosystem, according to Pedersen [172, 173], which allows distributing cryptographic operations. It thus supports distributability of powers. In this threshold system, an ElGamal private key $s \in_R \mathbb{Z}_q$ can be defined in two ways[2]:

- Firstly, it can be initially generated by a trusted dealer and then be secret shared (according to Shamir secret sharing [202]) among all n participating authorities.
- Secondly, it can be generated via the distributed key generation protocol of Pedersen [172][3], whereby no single party knows the complete private key.

In both key generation approaches, the power to decrypt is distributed among all of the participating authorities. A quorum, i.e. a minimal majority of t out of n authorities need to cooperate to perform a threshold decryption protocol, as specified in [172, 173]. Thus, a threshold ElGamal system can tolerate a maximum of $t - 1$ corrupt authorities, yet still requires a majority of t participating authorities. The total number of authorities n has to be (at least) $n = t - 1 + t = 2t - 1$, so $t - 1$ is a minority of authorities. The authorities share a common public key, $h = g^s \bmod p$. In this ElGamal setting, a message $m \in \mathbb{G}_q$ is non-deterministically encrypted by choosing $r \in_R \mathbb{Z}_q$ and by computing $(g^r, h^r m)$. Messages that are not in $\mathbb{G}_q$ can efficiently be mapped onto $\mathbb{G}_q$ [118]. Thus, arbitrary strings can be ElGamal encrypted.

Since different parties cooperate within distributed protocols, there is a need for a communication channel and a synchronization of individual inputs. Following the standard assumption in the literature, we assume that the communication channel is a broadcast channel with memory. This channel, which is also referred to as bulletin board, is used to store, exchange and synchronize inputs in any protocol that involves distributed computations. For example, partial decryptions and

[2] In the key generation, the private key is chosen at random.

[3] Or using alternative protocols for the same task, e.g. according to Gennaro et al. [84, 85].

identifiers of every participating authority are provided to the bulletin board in a threshold decryption. Moreover, this broadcast channel is append-only, i.e. once the information is published, it is stored and cannot be changed or deleted afterwards. Thus, its content can later be analyzed to support audit and verifiability purposes.

The ElGamal system parameters p, q, g and the public key h as well the mentioned communication channel are also relevant and available to the following primitives, i.e. non-interactive zero-knowledge proofs, plaintext equality tests and ElGamal reencryption mixnets.

Non-Interactive Zero Knowledge Proofs

Zero knowledge proofs (ZKPs) [87] are basically generalized challenge-response authentication protocols which are used to guarantee correctness of and verify participation in distributed cryptographic operations and protocols. A special feature of ZKPs is that they disclose no further information beyond that a statement is true. Non-interactive zero knowledge proofs (NIZKPs) [22] are variants which allow rendering the challenge-response process non-interactive, i.e. they can be executed by a single party. This is achieved by applying the Fiat-Shamir heuristic [64] and thus produces transcripts of the NIZKPs. See e.g. [51] for a broader discussions of zero knowledge techniques. A NIZKP it thus comparable to a digital signature, it can be stored and may also be verified, after its execution. Thus, incorrect or inappropriate actions can be deduced by assessing the transcripts. NIZKPs are a common cryptographic approach to implement auditability[4]. They are involved in some of the distributed cryptographic operations in order to assure that only correct inputs of individual parties are considered for computing a function. It is important to notice that zero knowledge techniques are integral parts of many protocols, yet, we mostly abstract from details throughout this thesis.

Plaintext Equality Tests

A plaintext equality test (PET) [118] is a primitive for pairwise blind comparison of ciphertexts of non-deterministic threshold cryptosystems like ElGamal. A PET allows testing whether two ciphertexts represent the same plaintext by performing algebraic operations on ciphertexts, but without revealing the plaintext. Plaintext equality tests exploit properties of the algebraic division of two ciphertexts, which is introduced next:

Let $(x_1, y_1) = (g^{r_1}, h^{r_1} m_1)$ and $(x_2, y_2) = (g^{r_2}, h^{r_2} m_2)$ be two ElGamal ciphertexts with plaintexts m_1 and m_2. In case that m_1 and m_2 are equal, the algebraic division of both, $(x_3, y_3) = (x_1/x_2, y_1/y_2) = (g^{r_1 - r_2}, h^{r_1 - r_2} m_1/m_2) = (g^{r_3}, h^{r_3} m_3)$ is an encryption of 1, since $m_1/m_2 = m_3 = 1$.

In a PET, the ciphertext (x_3, y_3) is firstly blinded by raising each component to a random exponent $z \in \mathbb{Z}_q$, $(x_4, y_4) = (x_3^z, y_3^z) = (g^{r_3 z}, h^{r_3 z} m_3^z)$, and then decrypted to the blinded value, m_3^z. The decryption reveals $m_3^z = 1^z = 1$ in case that the plaintexts

[4] In research dealing with cryptographic protocols, this is often referred to as *verifiability*.

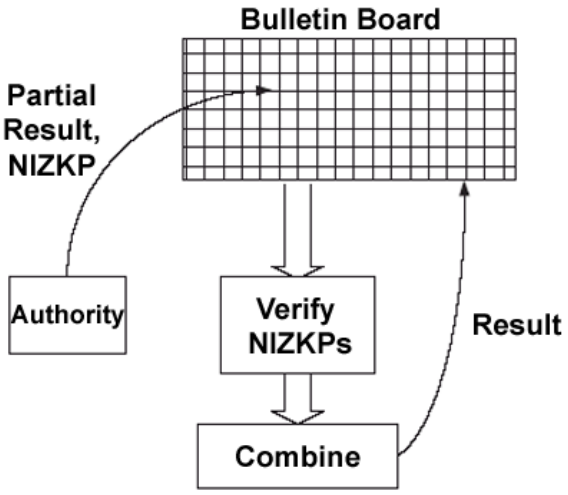

Figure 4.1: Distributed computations and bulletin board

are equal and a random integer $(m_1/m_2)^z$ otherwise[5]. Due to this, only negligible information beyond whether the plaintexts are equal is leaking due to the execution of the protocol. In order to prevent misuse of the power to decrypt, PETs can be performed in a distributed setting, i.e. harnessing a threshold ElGamal system. In this case, blinding and decryption are realized as distributed operations.

PETs and applications thereof are key primitives to implement multilevel linkability of transaction pseudonyms.

Figure 4.1 shows the interplay of the primitives relevant to distributed (threshold) computations and operations. Every authority submits the result of her partial operation to the bulletin board, accompanied by a NIZKP. After verifying the proofs, the bulletin board combines the inputs in order to produce the result of the operation, e.g. the result of a PET or a threshold decryption.

ElGamal Reencryption Mixnets

A mixnet, originally introduced by Chaum [43], is a primitive that can be used to anonymize sets of ciphertexts by a set of mix servers. Together, the mix servers form the mixnet. In our work, we build on ElGamal reencryption mixnets [169], which basically reencrypt and permute ciphertexts in order to anonymize them. In this setting, reencryption can be executed without a private key, i.e. it is not required to decrypt the ciphertext in order to produce a reencryption. Moreover, we assume that the mixnet is additionally verifiable and thus auditable, i.e. it provides NIZKPs of correctness of the operations. This can e.g. be achieved by employing

[5]Given that the group order of the underlying group is prime, then $(m_1/m_2)^z$ is a random non-identity group element [147, 184, 40]. This is true in our setting, i.e. the underlying group $\mathbb{G}_q$ is of prime order q.

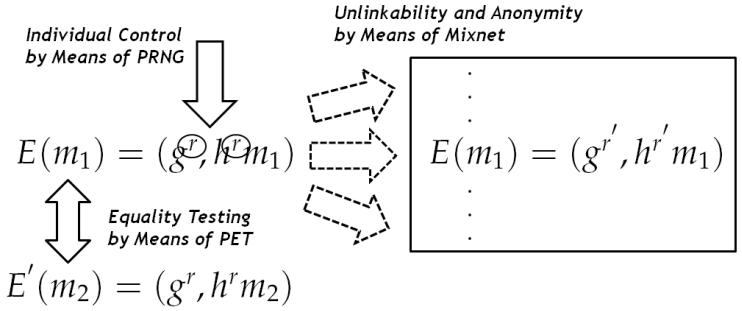

Figure 4.2: Interplay of primitives

the verifiable mixnet proposed Furukawa et al. [82], detailing the cryptographic auditability concepts for reencryption mixnets.

Basically, a mixnet consists of a set of mix servers M_i, that consecutively process ciphertexts. In our work, the operation of a reencryption mixnet consists of the following two main steps:

1. *Submission of Inputs:* A batch of ElGamal encrypted inputs $(g^r, h^r m_i)$ is submitted to the mixnet. Every input is an ElGamal encryption of a message m_i.

2. *Mixing Phase:* Mix server M_i receives the batch of ciphertexts output by the previous mix server M_{i-1} (or the initial input respectively). M_i reencrypts each ciphertext $c_i = (g^r, h^r m_i)$ by selecting a random value $r' \in \mathbb{Z}_q$ and computing $c_i' = (g^r * g^{r'}, h^r * h^{r'} m_i) = (g^{r+r'}, h^{r+r'} m_i)$. Then it permutes the batch of all ciphertexts randomly and passes it to the next mix server M_{i+1}. The last mix server outputs the batch of ciphertexts.

Within our work, mixnets help to build up anonymous reference sets used in the re-identification of pseudonyms (cf. Section 4.2.4). In particular, mixnets anonymize sets of ElGamal ciphertexts that represent transaction pseudonyms. These sets are used to blindly compare a given transaction pseudonym with the resulting reference set, based on variants of PETs, in order to perform a re-identification operation. The underlying concept of reencryption is also employed in order to derive transaction pseudonyms (cf. Section 4.2.2).

Primitives in Combination

Having introduced the main primitives, we now sketch the conceptual interplay of the primitives. Figure 4.2 shows the relation of PRNGs, mixnets and PETs. In this figure, $E(m)$ represents the ElGamal encryption of an arbitrary plaintext m. By means of a PRNG, the random factors used in the encryption can individually be

controlled. A mixnet can implement unlinkability and anonymity within a set of ciphertexts. A PET can be used to detect the equality of plaintexts.

In particular, the given primitives in combination allow making use of the several degrees of (un-)linkability that are given in ElGamal settings.

4.2 Setting and Main Protocols

We introduce the basic concepts of our approach in the following. The provided protocols implement functionalities for the generation, authentication, linking, partial re-identification and complete disclosure of transaction pseudonyms.

4.2.1 Parties

We consider the following authorities and entities in our setting:

- A user is an entity that intents to act pseudonymously. A user provides a transaction pseudonym as identifier during the relevant digital interactions instead of her identity.
- A Registration Authority (RA) is an entity that is responsible for registration processes. This authority interacts with users in order to register them to the system and sets up a registration list, which contains registration information.
- Linkability Brokers (LBs) are authorities that are able to cooperatively link and partially re-identify pseudonyms that are stored in a data repository after use.
- A Law Enforcement Authority (LEA) is an authority that is able to completely re-identify a pseudonym. This is called disclosure of pseudonyms. The misuse of the privacy protection granted by pseudonyms can be prevented by allowing such a trusted party to revoke pseudonymity in certain cases.

We assume that each entity is equipped with an appropriate computing device, that is able to store keys, execute operations and provides communication facilities.

4.2.2 Registration and Generation of Transaction Pseudonyms

In this section, we introduce the concepts for pseudonym generation. Basically, we propose to encode a static reference inside malleable pseudonyms, by generating pseudonyms as reencryptions of the reference value under the public key of a threshold ElGamal cryptosystem. The resulting construction is what we call a *pseudonym with implicit attribute*. This notion reflects that every transaction pseudonym is implicitly associated with information - the implicit attributes - that can logically be derived from the registration context. Thus, implicit attributes are defined on the semantics of available registration information and support the partial re-identification of pseudonymous users.

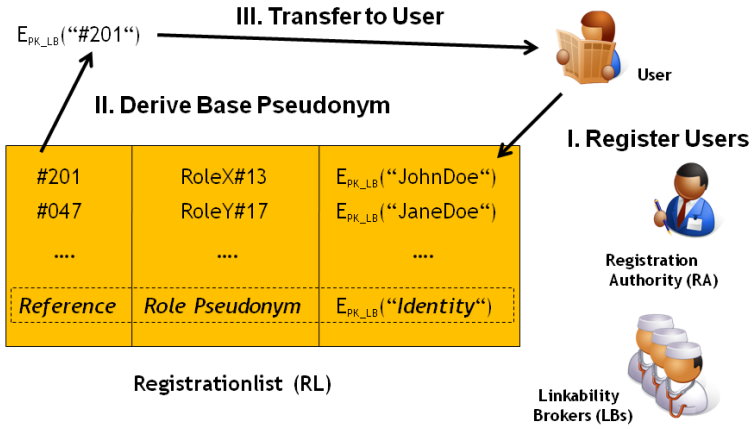

Figure 4.3: Registration process

Firstly, in our approach, every user must participate in a registration process, which is also shown in Figure 4.3. In this process, each user receives a base pseudonym, that enables her to derive transaction pseudonyms. We assume that the user is in possession of a personal device which also implements a cryptographically secure PRNG. In order to register, the user interacts with a trusted registration authority (RA). The registration consists of the following main steps:

I. Each user is added to an integrity protected registration list. She receives a distinct role pseudonym, which associates the user with some meaning in the application context, e.g. with a role relevant to the issuing organization. For example, a user can be registered as *RoleX*#13[6]. The user's unique real-world identity, e.g. *JohnDoe*[7], is encrypted and stored together with the role pseudonym on the registration list. Also, the user receives a distinct reference value, which is added to the respective entry of the registration list.

II. The RA derives a base pseudonym by encrypting the unique reference value. Thus, a base pseudonym encodes a distinct reference.

III. The RA transfers the base pseudonym to the user's personal device.

IV. The user generates and registers a seed in the PRNG of her device to enable it for pseudonym generation.

[6] A registration list may contain additional information that can be used to define (implicit) attributes. Such additional information is then included in additional columns of the registration list, cf. Figure 6.2

[7] We assume that the real world identity can be presented as a string, denoted as ID in the following. This string could also contain legal identification numbers, in order to make it unique.

In the registration phase, the encryptions are done under the public key belonging to a set of so called linkability brokers[8] relevant to the application context, e.g. they may belong to the issuing organization, or even include a party that represents interests of the users:

- The real-world identity ID is encrypted as: $E_{PK_{LB}}(ID) = (g^r, h^r ID)$.
- To generate the base pseudonym for a user, the registration authority encrypts the chosen reference value, which we denote RV, as: $P = E_{PK_{LB}}(RV) = (g^{r_s}, h^{r_s} RV)$. Moreover, the random value r_s, the start value for pseudonym generation, is also transferred to the user and stored on her device.

The user is now able to derive *transaction pseudonyms* from her base pseudonym in the following way:

1. The seeded PRNG is used to generate a sequence of random numbers.
2. Each random number r_i is used to compute a randomization factor $F_{r_i} = (g^{r_i}, h^{r_i})$.
3. F_{r_1} is used to construct the *first* transaction pseudonym by multiplying it with the base pseudonym: $P_B = P_0 = (g^r, h^r RV) * (g^{r_1}, h^{r_1}) = (g^{r+r_1}, h^{r+r_1} RV)$.
4. Further transaction pseudonyms are created by repeated multiplications: $P_{i+1} = P_i * F_{r_{i+1}}$.

By this procedure, which is also shown in Figure 4.4, a user creates a set of different transaction pseudonyms that all contain the same reference value. The procedure includes two factors that initialize pseudonym generation: an organizationally defined one, the base pseudonym, as well a personally defined one, the seed. The generated pseudonyms are used instead of static identifiers during the relevant digital interactions.

4.2.3 Authentication of Transaction Pseudonyms

Due to the construction, presented in the last section, users are also enabled to authenticate a transaction pseudonym that is stored in a data repository after it was used. Therefore, a user needs to show that she is in possession of the base pseudonym and the correct aggregated random factor, which allows reproducing a recorded pseudonym, thereby authenticating it.

[8] In the description, we assume that cryptographic keys have been generated and distributed before. The linkability brokers thus *share* the private key associated with the single public key. Due to the use of SMPC, variants with different distributions of power are possible. We elaborate on this issue in Section 7.2.1.

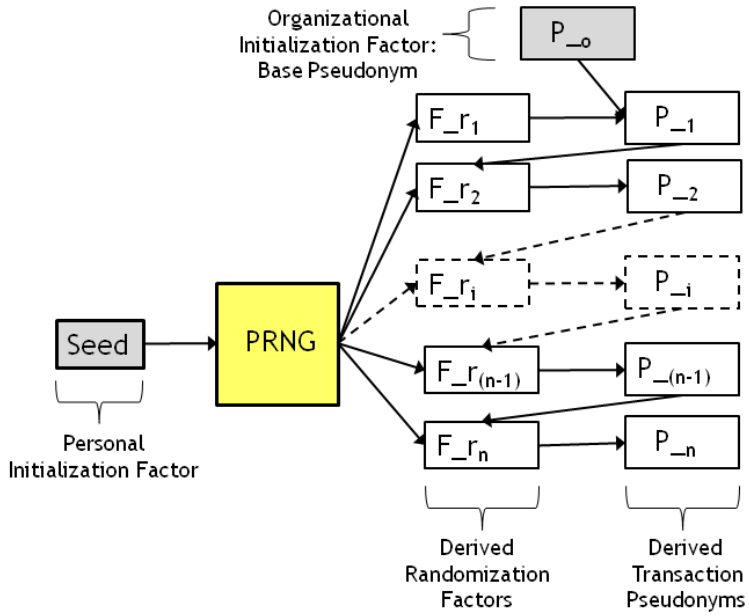

Figure 4.4: Overview of pseudonym generation

4.2.4 Linking and Partial Re-Identification

In this section, we describe the concepts for linking and re-identifying transaction pseudonyms. Basically, we harness the possibility to do algebraic operations on the non-deterministic encrypted ciphertexts that represent transaction pseudonyms.

We assume that the transaction pseudonyms are recorded in a data repository after they were used. Then, the linkability brokers are able to execute the following *two basic operations*:

1. *Linking:* check if two recorded pseudonyms relate to the same entity but without revealing the actual identity of the entity;

2. *Partial Re-Identification:* check if one entry relates to a group of entities with a common organizational role or function, i.e. if an implicit attribute is satisfied.

Overview of Linking

The linking operation is implemented by executing a *plaintext equality test* on the pseudonym values of two recorded pseudonyms. Suppose that $P_a = (g^{r_a}, h^{r_a} RV_a)$ and $P_b = (g^{r_b}, h^{r_b} RV_b)$ represent two entries of that kind. If they relate to the same entity, they contain the same reference value. In order to verify this, the pseudonyms can be algebraically divided: $P_c = P_a / P_b = (g^{r_a - r_b}, h^{r_a - r_b} RV_a / RV_b)$. Given that RV_a equals RV_b, this is an encryption of the value "1". By performing

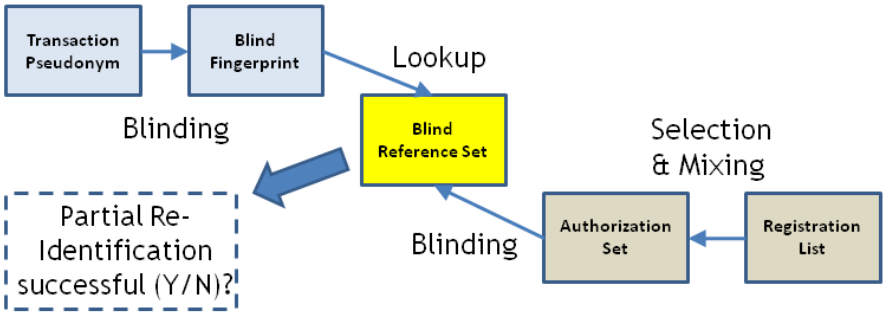

Figure 4.5: Steps of partial re-identification

a threshold decryption, the linkability brokers reveal a value which is either "1", indicating that the reference is matching, or a meaningless different value.

Overview of Partial Re-Identification

The second operation, the partial re-identification, is an extension of the procedure above to a global instead of pairwise comparison of pseudonyms. It allows testing if a given transaction pseudonym relates to an implicit attribute, i.e. a certain organizational unit, a function or even place. The implicit attributes are defined on the semantics of available registration information. This test does not disclose which of the possibly involved users is the originator of the pseudonym. Thus it implements a partial re-identification.

An overview of the method of partial re-identification is presented next. It consists of building up anonymous reference sets, supported by mixnets, and mechanisms for blind set lookups. The main steps are also presented in Figure 4.5. Again, it is based on operations of an ElGamal threshold cryptosystem. Basically, it works as following:

1. *Distributed Key Generation:* Firstly, the participating linkability brokers jointly generate a shared key z, which is used for blinding purposes in later steps.

2. *Selection:* Then, the registration authority selects all entries of the registration list that are relevant to the implicit attribute that shall be checked[9] (see Figure 4.6 for an example) and creates encryption of each chosen reference value.

3. *Mixing:* Next, all encryptions are processed by a reencryption mixnet. This creates an anonymized list of the ciphertexts, i.e. the positions of the individual entries in the list as well as the ciphertext representations are changed. The result is called an authorization set.

[9]The selected entries define the implicit attributes. Given that further information is attached to the registration list (cf. Figure 6.2), more meaningful implicit attributes can be set up.

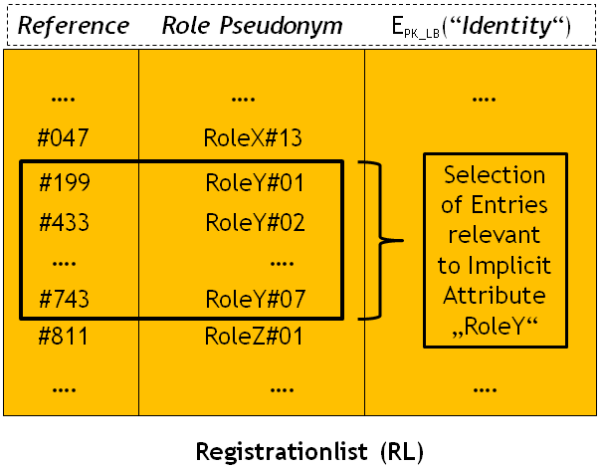

Figure 4.6: Example of selection of registration list entries

4. *Blinding:* The linkability brokers cooperatively apply their shares of z to each ciphertext in the authorization set. This process achieves blinding of the reference inside the ciphertext.

5. *Distributed Decryption:* After that, each blinded ciphertext is jointly decrypted. This yields a blinded reference, which is used as a deterministic yet blind fingerprint of the originally chosen reference value.

6. *Reference Set Definition:* All processed blinded references define a blind reference set. The set can be used for matching without leaking the original reference value, by comparing only the blind fingerprints, which is called a set lookup. Defined reference sets can be used in multiple lookups.

7. *Lookup:* In order to execute the lookup, the authorities derive a blind fingerprint of the chosen transaction pseudonym. Then, the lookup on the blind reference set is performed.

Partial Re-Identification in Detail

Having outlined the abstract steps, we now describe the method in detail. The whole scheme makes use of secret sharing techniques according to Shamir [202] as well as of the distributed key generation protocol according to Pedersen [172]. Firstly, to jointly generate the secret shared key z used for blinding, the linkability brokers employ the distributed key generation protocol due to Pedersen. In this protocol, each linkability broker LB_j receives a share z_j of the key z. Also, each broker is publicly committed to the share z_j by a public value $\rho_{z_j} = g^{z_j}$, due to the execution of the protocol.

In the following, we describe the complete protocol for *distributed blinding*, which proceeds analog to the distributed decryption protocol [172, 173] of the ElGamal threshold cryptosystem. This protocol can be used to blind an arbitrary element $x \in \mathbb{G}_q$ using the shared key z. The following steps are executed in order to cooperatively apply z to the chosen pseudonym(s)[10]:

1. Each linkability broker computes $b_j = x^{z_j}$, a partial blinding of x, by applying its secret z_j. Also, each officer publishes b_j together with a NIZKP for assuring

$$\log_g \rho_{z_j} = \log_x b_j$$

   The latter is realized using a non-interactive proof of knowledge for equality of discrete logs [46]. The proof assures that the officer indeed utilized the correct share to produce the partial blinding[11].

2. For any subset Λ of t linkability brokers with valid zero-knowledge proofs, the complete blinded value x^z is reconstructed using the discrete Lagrange interpolation

$$x^z = \prod_{j \in \Lambda} b_j^{\lambda_{j,\Lambda}} \bmod p$$

   where

$$\lambda_{j,\Lambda} = \prod_{l \in \Lambda \setminus \{j\}} \frac{l}{l-j} \bmod q$$

   are the appropriate Lagrange coefficients.

Now, let $RV_i \in \mathbb{G}_q$ be the algebraic representation of a reference value, and $(g^r, h^r RV_i)$ a pseudonym derived from RV_i, with $r \in_R \mathbb{Z}_q$. The linkability brokers produce the deterministic fingerprint through the following steps:

1. To each component of $(g^r, h^r RV_i)$ the distributed blinding protocol is applied, blinding it to a fix secret shared exponent $z \in \mathbb{Z}_q$:
   $((g^r)^z, (h^r RV_i)^z) = (g^{rz}, h^{rz} RV_i^z)$.

2. The blinded pseudonym is jointly decrypted to the blinded reference RV_i^z using the distributed decryption protocol of the threshold ElGamal cryptosystem.

Now, RV_i^z represents a deterministic fingerprint produced with a key z. It is used to perform a lookup that reidentifies implicit attributes, by blindly comparing reference values with a blind reference set that is associated to the attribute. Especially,

[10] Every pseudonym is effectively encoded as two elements of $\mathbb{G}_q$, whereas the second element is directly derived from a reference value. This second element is directly manipulated by the presented mechanisms.

[11] Otherwise, the use of a fake share would lead to an incorrectly blinded value, which would interfere with blind matching purposes. In generally, such a security mechanism is part of every threshold operation.

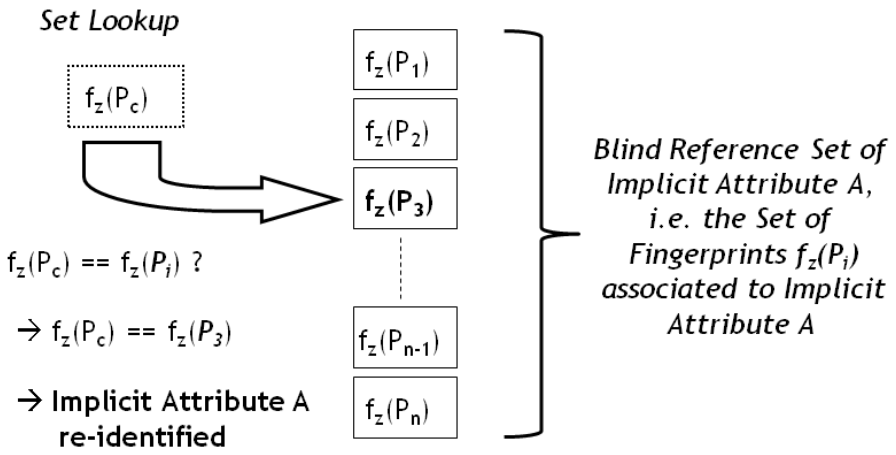

Figure 4.7: Lookup

the presented mechanism supports the re-identification of a recorded transaction pseudonym in several levels of granularity. Hereby, the granularity only depends on the chosen authorization or reference sets. By setting up several different sets and consecutively performing lookups, a multilevel linkability check of a chosen pseudonym is implemented[12]. A lookup is also depicted in Figure 4.7.

4.2.5 Complete Disclosure of Pseudonyms

As a complement to the operations for linking and partial re-identification of transaction pseudonyms, we describe the operations for the complete disclosure of pseudonyms in the following. The given approach can be instantiated such that linkability brokers as well as a single law enforcement authority may execute a complete disclosure. In case of the linkability brokers, the disclosure works as follows:

- Firstly, the linkability brokers cooperatively decrypt a transaction pseudonym, which is recorded in a data repository. This yields the plaintext of the distinct reference value encoded in the pseudonym.
- Next, the linkability brokers select the corresponding entry on the registration list[13]. Then, they cooperatively decrypt the deposited ciphertext to reveal the real-world identity.

[12] Due to the underlying set-based representation, each level of granularity corresponds to a degree of anonymity, cf. Section 5.2.2. In the same section, the concept of a *disclosure policy* is introduced. Its purpose is to specify how consecutive linkability checks shall be executed.

[13] If the access to the registration list is restricted, LBs are unable to completely disclose a transaction pseudonym. In this case, they have to cooperate with the RA in order to access the matching encrypted identity. Thus, the RA may implement a further security mechanism, cf. Section 7.2.1.

The disclosure functionality for the law enforcement authority works in a comparable way. Basically, we assume that the law enforcement authority is in possession of the same private key as the linkability brokers, by initially having played the role of the trusted dealer in the key generation process (cf. section 4.1.2). Then, the disclosure proceeds as follows:

- Firstly, the law enforcement authority decrypts a transaction pseudonym, which is recorded in a data repository. This yields the plaintext of the distinct reference value encoded in the pseudonym.
- Secondly, the authority selects the corresponding entry on the registration list[14]. Then, it decrypts the deposited ciphertext in order to disclose the real-world identity.

4.3 Hybrid Encryption Technique for Expressive Policies

In this section, we introduce a novel hybrid encryption technique that is able to handle expressive policies. In our context, the notion of an expressive policy refers to the capability to efficiently support static attributes as well as one continuous dynamic attribute in combination in conjunctive encryption policies. In this section, again, attributes refer to properties of users. Yet, it is important to note that this section describes a technical approach for handling attributes that is different to the concept of implicit attributes, which were described in the last sections.

We propose to efficiently combine ciphertext-policy attribute-based encryption [17] and location-based encryption [201, 54], which allows for realizing logical encryption policies, while we leverage symmetric AES encryption to efficiently encrypt the payload. Current state-of-the-art encryption techniques are unable to support such encryption capabilities, which consider continuous dynamic attributes that may change in an unpredictable manner (cf. Section 3.3.2).

The next section describes the underlying construction principle, followed by a description of the main primitives. Then, the protocols and mechanisms are explained in detail.

4.3.1 Construction Principle

Realizing end-to-end encryption in pervasive computing settings and applications is a challenging task: traditional asymmetric encryption schemes, e.g. RSA, and PKI concepts are not practical for securing communication with dynamic groups or unknown receivers, since unknown entities cannot be addressed and also certificate verification is a huge obstacle. More recent asymmetric encryption techniques propose to generalize the role of the receivers' identities [192] and thus can enable a more flexible specification of receivers and content. In this approach, called

[14] Since a law enforcement authority is dedicated to completely disclose pseudonyms, we implicitly assume that this authority has full access to the registration list.

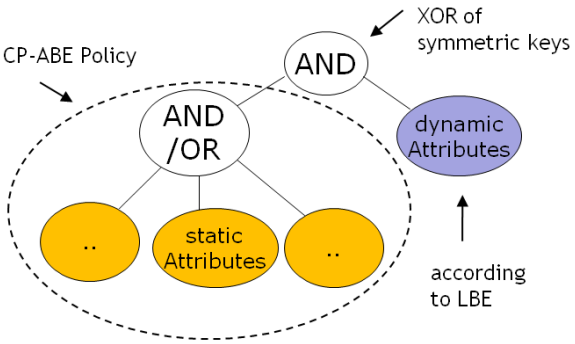

Figure 4.8: Overview of hybrid encryption technique

attribute-based encryption, key-related concepts refer to attributes, which can represent properties of receivers and/or messages.

Yet, handling continuous dynamic attributes is thus far only possible among the unpractical assumption of an online key generator, which we want to avoid in our design. Also, due to the inherent use of computationally demanding pairing-based cryptography, the practical applicability of existing techniques remains highly challenging in scenarios with mobile and resource-constrained devices.

To overcome these issues, we propose to leverage ciphertext-policy attribute-based encryption (CP-ABE) [17] in combination with location-based encryption (LBE) [201, 54] and symmetric AES encryption.

Especially, we propose to make use of CP-ABE to handle static attributes within an encryption policy, while the principle of location-based encryption is employed to derive a symmetric key from a dynamic attribute, e.g. a GPS position. In order to save the computation of pairings, we leverage CP-ABE in a hybrid mode, this means, we split the encryption of the payload from the encryption of the session key. The session key is then additionally bound to the location-based encryption. Thus, in order to decrypt, both the CP-ABE policy (static attributes) and the LBE constraint (a dynamic attribute) have to be satisfied. Figure 4.8 shows this construction principle in overview. Practically, this approach means that we combine an offline key generation for static attributes with a light-weight online key generation for dynamic attributes. Together with relying on AES encryption for the payload, the approach[15] is rendered suitable even for mobile and resource-constrained devices that are the end point of an end-to-end encrypted communication.

[15]Note that our approach considers attribute-based encryption mostly as a black box. The given descriptions thus mostly abstract from the concrete (pairing-related) algorithms of CP-ABE.

4.3.2 Main Primitives

In this section, we describe the main building blocks, that contribute to the design of the presented hybrid encryption technique.

Ciphertext-Policy Attribute-Based Encryption

Attribute-based encryption (ABE) [192] is an encryption technique that generalizes the functional role of identities and keys. In traditional asymmetric encryption schemes, identities relate to distinct public key / private key tuples. In ABE, the concepts of public and private keys are replaced by *sets of attributes*[16], which abstract from actual user properties. Moreover, ABE is certificateless and the cryptographic credentials are issued by a central trusted party called *attribute authority*, which is in possession of a global *master key* for key generation. Since users are associated with sets of attributes, they might try to trade some attributes and related private key components to gain more decryption powers. However, ABE systems are *collusion resistant* [17], i.e. keys of different users are incompatible due to the cryptographic construction.

Like identity-based encryption [27], ABE cryptographically builds upon pairings, i.e. bilinear maps that provide an extra structure on special elliptic curves. While pairings enable attribute-based encryption, they are very computationally demanding. From a practical point of view, the goal is to minimize pairing-related operations, in order to enable use even on resource-constrained devices.

Ciphertext-policy attribute-based encryption (CP-ABE) [17] is a special form of attribute-based encryption, which associates a set of attributes used in the encryption process with logical access structures, also called *attribute policies*. Due to the use of secret sharing [202], the access structures are trees with nodes that represent t-out-of-n combinations of attribute child nodes, naturally including conjunctions (AND) as well as disjunctions (OR).

In CP-ABE, the encryption algorithm takes as input a message and an attribute policy. The algorithm encrypts the message and produces a ciphertext, such that only a receiver possessing a set of attributes that satisfies the attribute policy is able to decrypt that message. In order to avoid the computation of parings and thus enable more practical applications, CP-ABE can be used in *hybrid mode*: a message itself is encrypted with a random symmetric secret key. Only this *session key* is then CP-AB encrypted under a policy. In the following, we assume that the ciphertext also encodes the policy.

An example of an CP-ABE policy and its application to encryption in hybrid mode is given in Figure 4.9. The figure shows an attribute policy containing attributes that are taken from the first response domain. During the encryption under this policy, the session key S is Shamir secret shared according to the operation specified in the nodes of the policy, from the root node down to the leafs. Given an AND node, the key or the share of the key is distributed to child nodes according to an

[16] In the following, we denote the concept that replaces a private key as *private attribute set*.

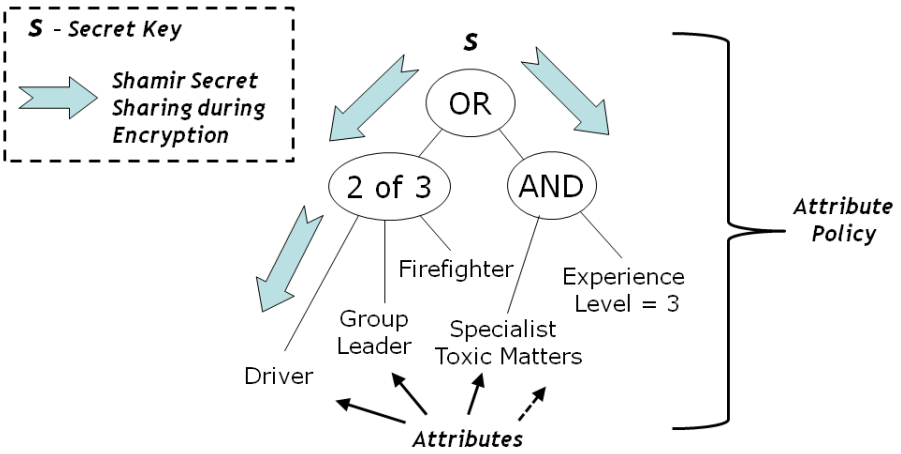

Figure 4.9: Example of CP-ABE policy

n-out-of-n secret sharing. For the decryption operation, this effectively means that all the shares associated to child nodes have to be available, for the reconstruction to succeed. Given an OR node, the key or the share of the key is distributed according to an 1-out-of-n secret sharing, i.e. only one share is required to reconstruct the secret in the level above. During the encryption process, shares of S are thus consecutively dealt out from the root node down to the leaf nodes. Every leaf node is associated to an attribute. The share dealt out to a leaf node is finally encrypted according to attribute-based encryption principles. Thus, for the decryption to succeed, a user requires a set of attributes that at least satisfies the policy. Without at least this set, the shares at the leaf nodes cannot be decrypted. Thus, the secret key S cannot be reconstructed, and consecutively, the message cannot be decrypted.

For the purpose of symmetric encryption, we propose to make use of the advanced encryption standard (AES) [33]. AES supports key sizes of 128, 192 and 256 bits. Throughout this thesis, our descriptions refer to the use of AES-128[17].

Location-Based Encryption

The concept of location-based encryption (LBE) was proposed by Scott and Denning [201, 54]. It aims at securing mobile communication by limiting the area inside which the intended recipient can decrypt a message[18]. .

In order to implement this location-based security constraint, LBE adds a layer of security to a symmetric encryption of a message: the targeted recipient's geographic location L is combined with the session key, in order to produce a location-locked

[17] In recent cryptanalysis research, weaknesses in the AES were identified. In [26, 25], a key recovery attack on AES-128 with computational complexity $2^{126.1}$ is described. Yet, the complexity of this attack is still impractical, the AES-128 is still considered secure.

[18] Yet, further attributes beyond location, e.g. velocity, can also be handled by LBE concepts.

key. This location-locked key is then sent along with the encrypted message. As a result, the ciphertext can only be decrypted if the session key can be recovered from the location-locked key. In turn, LBE requires that this decryption is only possible if the receiver's device is physically presented at location L, or respectively inside an geographic area associated with L.

This process is called location verification, it hinges on a tamper-resistant GPS receiver inside the recipient's mobile device. In LBE, the sender has to transmit parameters which define the area where decryption is permitted and may specify further dynamic constraints like time periods or receiver velocity that have to be verified upon decryption [5].

In general, a location-based encryption technique requires an efficient mapping from location areas to symmetric keys, which is called a *location lock*. The location lock is secured by including an additional key as an input parameter in order to derive symmetric keys.

4.4 Setting and Main Mechanisms for Hybrid Encryption

We introduce the basic protocols of the novel hybrid encryption technique in the following. We describe the encryption and the decryption scheme. Also, we detail the underlying key management approach.

4.4.1 Parties

The parties relevant to the setting of the hybrid encryption technique are derived from the underlying CP-ABE and LBE. For brevity of presentation, we only consider the following two authorities and entities explicitly in our setting:

- Attribute authority AA: the AA is responsible for creating the private credentials (attributes) used for decryption. Especially, it issues a private attribute set $\{A\}_R$ to every receiver.
- Receiver R: this entity receives encrypted messages on her communication device. The device is initialized for decryption with the receiver's private attribute set $\{A\}_R$ and K_{LL}, the key for the location lock function. Also, the device has a tamper-resistant GPS receiver that is leveraged in the following schemes.

4.4.2 Encryption and Decryption Schemes

This section introduces the main schemes of the novel hybrid encryption technique for expressive policies. The technique is hybrid, as it combines CP-ABE with LBE and AES on the level of symmetric keys. In the following description, we refer to location attributes as dynamic attributes only.

We use the following notation:

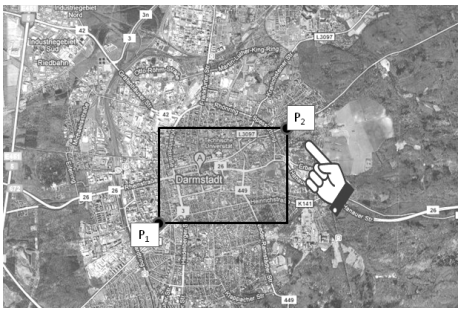

Figure 4.10: Selection of GPS coordinates

- $L^{(P_1,P_2)}$ specifies an geographic area with the shape of an rectangle, defined by GPS coordinates $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ (cf. Figure 4.10, which exemplarily shows definition of GPS coordinates on a digital map.). In the following, we also denote $L^{(P_1,P_2)}$ simply as L.

- $E_{AP}^{L^{(P_1,P_2)}}(M)$ denotes the encryption of a message M under a logical conjunction of a CP-ABE attribute policy AP and a LBE location area attribute $L^{(P_1,P_2)}$.

- $D_{\{A\}_R}^{P_R}(CT)$ denotes the decryption of a ciphertext CT initiated by a receiver R, using his private attribute set $\{A\}_R$, while being positioned at GPS coordinate $P_R = (x_R, y_R)$.

It is possible that one of the two main parts of a policy remains undefined:

- in case the CP-ABE part AP is not specified, encryption is reduced to location-based encryption;

- in case the LBE location area attribute $L^{(P_1,P_2)}$ is not specified, encryption is reduced to ciphertext-policy attribute-based encryption.

The combined approach is introduced next. Here, decryption succeeds if R's attribute set $\{A\}_R$ satisfies the attribute policy AP and R is positioned within $L^{(P_1,P_2)}$, i.e. if $x_2 \geq x_R \geq x_1$ and $y_2 \geq y_R \geq y_1$ hold. Figure 4.11 shows the basic operations of the encryption technique in overview.

Our hybrid encryption employs a keyed *location lock mapping* $f_{LL}(L^{(P_1,P_2)}, K_{LL})$, according to the following principle: GPS coordinates P_1, P_2 and K_{LL} are concatenated. Then, the resulting string $s_{LL^{(P_1,P_2)}} = x_1||y_1||x_2||y_2||K_{LL}$ is hashed, $h(s_{LL^{(P_1,P_2)}})$, to a 128 bit string[19], the location lock value.

[19]Here, we implicitly assume 128 bit security for symmetric keys. Thus, MD5 [186] is a hash function of choice.

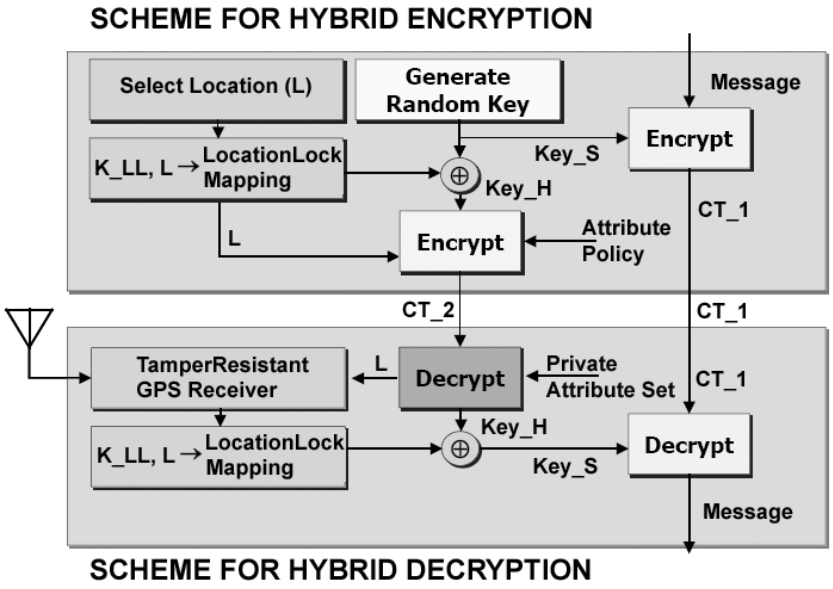

Figure 4.11: Schemes for encryption and decryption

Scheme for Hybrid Encryption

The *hybrid encryption scheme* works as follows (cf. Figure 4.11):

1. A random session key Key_S is generated.
2. The message is symmetrically encrypted under Key_S, producing ciphertext CT_1.
3. The location lock value is computed from the selected location area L and key K_{LL}.
4. Key_S is XORed with the location lock value, generating a hybrid key Key_H.
5. Key_H is concatenated with an encoding of the location area L, producing the string $L||Key_H$. This string is CP-AB encrypted under an attribute policy AP, producing ciphertext CT_2
6. CT_1 concatenated with CT_2 represent the ciphertext CT. CT is transferred to a receiver R.

Scheme for Hybrid Decryption

The *scheme for hybrid decryption* works as follows (cf. Figure 4.11):

1. After reception of $CT = CT_1||CT_2$, receiver R tries to decrypt CT_2, using his private attribute set $\{A\}_R$. On successful decryption, the location area L and Key_H are recovered.

2. R's current GPS position P_R is computed by means of a tamper-resistant GPS receiver and verified to be inside the location area L. On success, the location lock value is computed, taking L and key K_{LL} as input parameters.

3. The location lock value is then XORed with the recovered Key_H, in order to reconstruct Key_S.

4. Key_S is used to symmetrically decrypt CT_1 to M.

4.4.3 Management and Generation of Private Keys

The proposed hybrid encryption technique entails an important design aspect: key management, including the generation of private keys.

Since the present approach combines two existing encryption techniques, it inherits some properties from CP-ABE, other characteristics derive from LBE. Especially, the hybrid encryption technique hinges on a tamper-resistant GPS receiver. The GPS receiver triggers the creation of keys that need to satisfy location-depended constraints in the encryption.

Figure 4.12 shows the design space for the generation of private keys as well as our chosen approach. Basically, in our setting, private key generation (PKG) is possible online, offline and embedded in tamper-resistant hardware [207]. Online PKG refers to a server that is permanently reachable and produces and communicates private keys or attributes on request. In the offline mode, all keys are generated in a preceding phase and handed out to the receiver.

An embedded (online) generation of private keys refers to a local implementation of the key provision mechanisms based on tamper-resistant hardware on the receivers' device. In this case, a device itself creates a private key required for

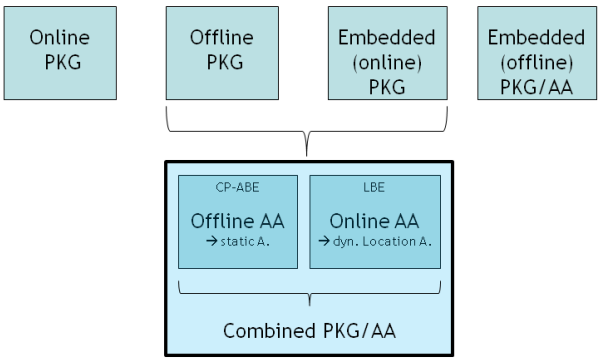

Figure 4.12: Generation of private keys: design space and chosen approach

message decryption. CP-ABE requires a master key for private key generation, which is, among practical considerations, of high risk, since this global trapdoor is then highly distributed. Furthermore, in an embedded (offline) key generation mode, all possible keys/attributes are generated in a preceding phase, then registered in a tamper-resistant storage module of the receiver's device. If a particular key/attribute is required for decryption, the tamper-resistant hardware can temporarily provide the key to the execution environment of the decryption operation (cf. [232, 32, 238]).

In our work, we propose to realize the hybrid encryption technique with the following combination of online and offline key generation mechanisms: static attributes are generated offline by an CP-ABE attribute authority (AA) and distributed to receivers before use, dynamic location attributes are generated by an embedded online LBE key generator which is realized on the device. Practically, this approach means that a global secret, i.e. K_{LL}, the key for the location lock, is required for securing one-to-many encryptions. Even though a global secret is distributed on every device, it can only by used to generate dynamic attributes. Static attributes cannot be generated on the device. Since the decryption based on static attributes is executed in the first step, a maliciously generated dynamic attribute cannot allow decrypting additional ciphertexts in case that insufficient static attributes are available. Yet, K_{LL} also provides protection against outside adversaries in case that only location attributes are used for encryption. Thus, the chosen approaches reconciles misuse potential and functionality to a high degree, under practical assumptions. The chosen approach moves a major part of trust into the organizational level of using security mechanisms, i.e. the offline issuing of private attributes and K_{LL}.

4.5 Summary

In this chapter, we contributed two novel security techniques:

- Firstly, we introduced pseudonyms with implicit attributes, our novel approach to multilevel linkable transaction pseudonyms. Our proposal extends earlier work of Juels and Pappu [125] on encryption-based transaction pseudonyms. By making use of threshold ElGamal encryption, PRNGs and secure multiparty computation mechanisms according to the mix-and-match framework [118], we achieve multilevel linkability of transaction pseudonym for users, organizations and law enforcement authorities.

- Secondly, we proposed a novel hybrid encryption technique for expressive policies. We designed this technique as an efficient combination of attribute-based encryption, location-based encryption as well as AES encryption. The proposal allows handling continuous dynamic attributes in combination with static attributes in order to support encryption under expressive policies. In order to achieve this, we also devised novel mechanisms for the combined offline and online generation of attributes and associated keys.

Both techniques are major building blocks for our integrated approach to multilaterally secure pervasive cooperation, which is introduced in Chapter 5. Further applications and security evaluations of our proposals will be given in Chapter 7.

5 Integrated Approach within Reference Scenario

In this chapter, we describe the main concepts of our novel approach to multilaterally secure pervasive cooperation. The approach is presented within the reference scenario of location-aware first response. According to the goals of thesis, this chapter thus introduces the basic principles and concepts for realizing

- multilaterally secure auditing, providing a fair balance of privacy protection and accountability.
- end-to-end secure pervasive communication, i.e. one-to-many communication with mobile, nameless and possibly unknown receivers as well as dynamic groups of receivers,

The security techniques introduced in Chapter 4 are crucial building blocks for realizing these mechanisms (cf. Figure 1.4). This chapter describes a novel integrated architecture that results from the implementation of the aforementioned principles and mechanisms. In particular, we introduce the technical setting, the involved parties as well as their interactions.

The remainder of this chapter is structured as follows. Firstly, in Section 5.1, we introduce to our approach in overview. In Section 5.2, we describe the two main underlying principles. This is followed by the communication network model, in Section 5.3 and the adversary model, in Section 5.4. After that, an overview on the system is given in Section 5.5. This includes functional, temporal and logical views on the resulting architecture. Finally, the chapter is summarized in Section 5.6.

5.1 Overview

In this section, we firstly give a high-level description of how mobile and central users (cf. Section 2.3.3) and additional parties may securely interact in order to coordinate a first response. We also describe how our main security goals are achieved while efficiently enabling the targeted cooperation.

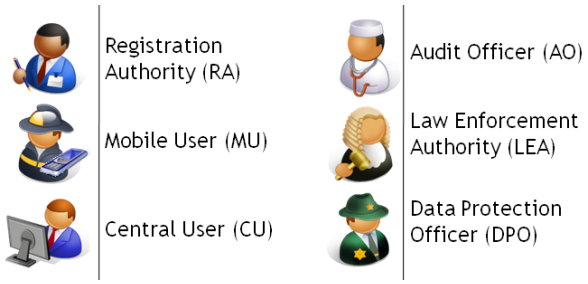

Figure 5.1: Parties in overview

5.1.1 Parties

In the following, we make recurrent use of the icons shown in Figure 5.1. The depicted parties are shown in several further figures and have the following functions, denotation and relations to earlier mentioned parties:

- a *registration authority* is involved in setup processes and registers mobile users to the system. It also provides information to the auditing process that is dependent on registration information. The registration authority corresponds to the registration authority mentioned in Section 4.2.1 and to the attribute authority mentioned in Section 4.4.1.

- A *mobile user* is involved in rescue missions, as a regular first responder or as a specialist, who joins incident handling on request. A mobile user subsumes the roles of a user, as introduced in Section 4.2.1, and of a receiver (cf. Section 4.4.1).

- A *central user* represents the emergency management stuff in a command and control center. The central user has decision making and communication tasks during a rescue mission.

- An *audit officer* represents the interests of organizations responsible for emergency responses and is involved in the analysis of liability issues caused by rescue missions. Within the present approach, an audit officer is involved in cooperative analysis of location logs. An audit officer corresponds to the role of an linkability broker, as described in Section 4.2.1.

- A *data protection officer* represents and defends privacy interests of mobile users in the auditing and also supports transparency of this process. A data officer also corresponds to the role of an linkability broker (cf. Section 4.2.1).

- A *law enforcement authority* represents and enforces legal interest. This authority can globally re-identify mobile users within the system. It corresponds to the role of the law enforcement authority, according to Section 4.2.1.

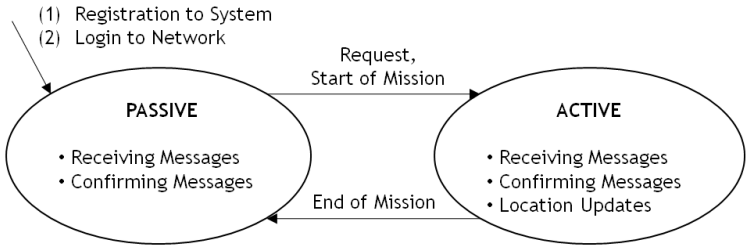

Figure 5.2: States of mobile users

We will refer to these parties in the following sections as well as in various figures. In particular, in Section 5.5.1 we will detail the roles of the parties within the integrated architecture.

5.1.2 Core Interactions

In this section, we introduce the core interactions of our approach. The interactions are clustered in three temporal phases of *before*, *during* and *after* a first response or rescue mission:

- *Before* being able to participate in rescue efforts, every mobile user, whether first responder or external specialist, has to be registered to our system. In a registration, the communication device is personalized.

- *During* rescue missions, she has to be logged in the available digital emergency communication network via her personal communication device. Being registered and logged in to the network is what we define as *passive* state. In this state, a mobile user is able to receive messages that are sent by a central user, located in a command and control center.
  For example, the central user may request specialists that are in close vicinity to an incident site to participate in a response. Upon reading this request, a mobile user individually confirms her availability by sending back an acknowledgement message[1].
  Upon an actual engagement within a rescue mission, the mobile user's state is denoted as *active*. While being active, the user continuously sends location updates, i.e. messages containing current time and GPS position along with an identifier to the command and control center[2].

[1] The design rationale of our approach is explained in the following Section 5.1.3. In this example, beyond confirming availability, an acknowledgement is also needed to satisfy the `documentation of readers` requirement, cf. Section 2.4.3.

[2] Additional sensor data may be attached to location updates. If an user is appropriately equipped, she may act as a mobile sensor and thus monitor levels of air pollution, or provide vital data for individual health monitoring. Generally, additional sensor information can support decision making processes in the command and control center in various ways, see e.g. [145, 47].

The described state transition between passive and actives states of mobile users is also depicted in Figure 5.2.
Received location updates are securely stored in the control center and thus create location audit logs, which enable post-hoc auditing of rescue missions.

- *After* the end of a rescue mission, a location audit log can be cooperatively analyzed, in order to react upon reported incidents (cf. Section 2.4.4). Audit officers together with a data protection officer may re-identify mobile user in a stepwise process. In the dispute resolution also affected mobile users and a law enforcement authority may participate.

In this chapter, the interactions will be detailed in Section 5.5.2 and Section 5.5.3.

5.1.3 Design of Security Mechanisms

Having introduced core interactions relevant to our approach, we next explain the design rationale of the mechanisms which implement the main associated security goals. An overview of our design is given in Figure 5.3. In particular, according to our requirements elicitation in Section 2.4, we aim for end-to-end secure communication as well as a fair balance of location privacy protection and accountability:

- Our reference scenario requires targeted, location-dependent *end-to-end secure communication*, which enables mobile users that are unknown by identity to participate in rescue missions without initially providing location information:
  - Since the identities of the receivers are unknown to the sender, the selection of mobile users has to be realized on a level of abstraction different to identity. We propose to leverage attributes, i.e. properties a user fulfills, to specify receivers. In particular, a group of mobile users can be expressed as a logical combination of attributes. The proposed combination has been devised based on the results of a user study that involved real emergency workers (cf. Section 7.3.2); it includes attributes related to organizations, roles, specializations as well as the current location of a user in conjunction.
  - In order to achieve end-to-end confidentiality, an encryption mechanism has to be able to deal with dynamic attributes. To deal with this challenge, we propose to employ the hybrid encryption technique for expressive policies, as presented in Section 4.3. Thus, requests and messages are encrypted under expressive policies according to the chosen attributes.
  - After the encryption, messages are broadcasted via an available communication network. Received messages are locally evaluated on mobile devices; this implements an implicit addressing mechanism which additionally protects the location privacy of receivers.

  - In order to prevent replay attacks and to support non-repudiation of senders, we leverage message authentication codes together with unique message IDs. In addition, acknowledgements allow determining and documenting the readers of a message.
  - In sum, we denote the described communication method as *end-to-end secure attribute-based messaging* (ABM).

- In order to achieve *location privacy protection*, we follow the principle of data minimization, i.e. the use of data related to the identities of mobile users is minimized. In particular, we apply this principle to the collection and to the processing of data[3]:
  - We propose that the collection of location data is restricted to the active state, i.e. during rescue missions. Since location information is sent by the users, the update frequency is personally adjustable. This implements an individual control functionality.
  - Instead of using static identifiers, we propose to use (linkable) transaction pseudonyms in the location updates. The pseudonyms are created according to the principles of pseudonyms with implicit attributes (cf. Section 4.1). Thus, location updates are unlinkable w.r.t. the identifiers.
  - We design the analysis capabilities for location updates as a privacy-respecting audit. In particular, the audit logs are already pseudonymized upon creation.

- The resulting pseudonymized location audit logs support *accountability* of real-world actions:
  - Following the principle of data minimization, accountability w.r.t. to mobile users is restricted to the duration of first response missions.
  - In order to prevent misuse by single authorities, we design accountability mechanisms as a cooperative analysis of location logs; the mechanisms harness linkability measures of the employed pseudonym construction. An analysis supports a distribution of powers; we introduce a data protection officer as a representative of and additional support for affected users. Location audit log are a special kind of audit logs. In order to cope with them, we propose location-based auditing mechanisms.
  - We propose that the re-identification of pseudonymous users is controlled by means of a disclosure policy. It allows specifying levels of disclosure both in terms of semantics and anonymity measures.
  - In order to support the requirements of different application contexts, the approach can flexibly be instantiated with and without law enforcement capabilities.

[3] As introduced above, this is also true for the addressing of users, which makes use of attributes instead of identities

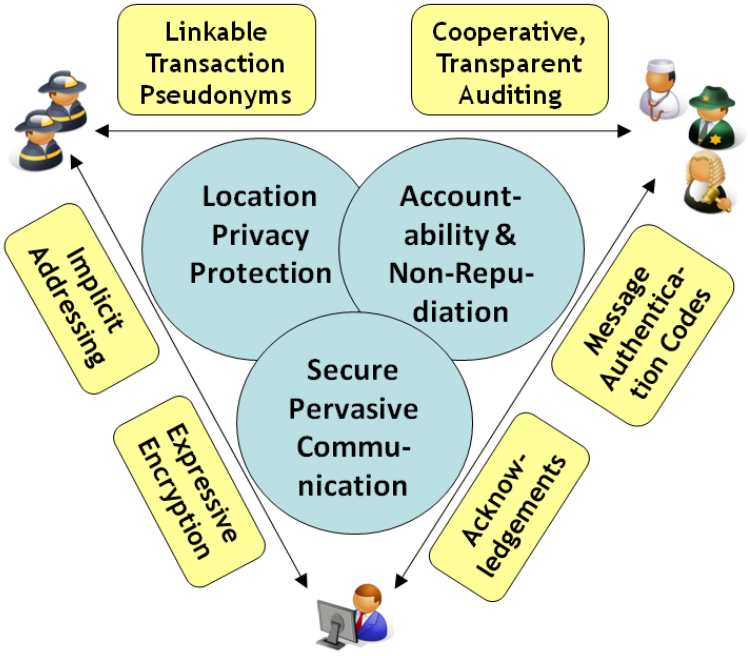

Figure 5.3: Overview of security design

- The individual access to an audit log is part of a fair balance of privacy protection and accountability. In order to realize it, we propose an access control mechanism, that is based on authenticating transaction pseudonyms.
- Transparency of an executed audit is also given to affected users. Transparency implements a second level of accountability, w.r.t. the actions of authorities involved in the auditing. Users can access transparency information, again based on transaction pseudonyms that are used as reference points in an access control mechanism.
- In sum, the described concept is called *multilaterally secure location-based auditing*.

In the remainder of this chapter, we describe the main concepts for the realization of our approach. In particular, this outlines of how the techniques presented in Chapter 4 are instantiated in order to fulfill our security requirements. A more detailed description of the mechanisms is given in Chapter 6.

5.2 Basic Principles

Having presented an overview, this section describes more details of our proposal. Technically, our approach to multilaterally secure pervasive cooperation builds upon

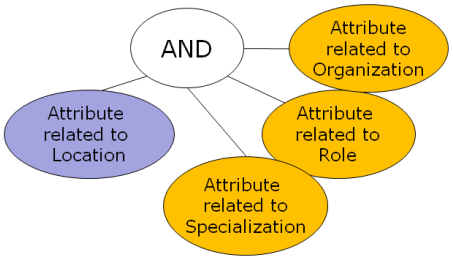

Figure 5.4: Structure of logical messaging policy

two basic principles:

1. mobile users are made implicitly addressable via attributes (including location), i.e. the selection of cooperation partners is executed on a level of abstraction that is different to identity,

2. mobile users regularly provide location updates together with linkable transaction pseudonyms, in order to enable a real-world auditing that is based on pseudonymous location traces.

We describe our realization of these principles next.

5.2.1 Make Users Implicitly Addressable via Attributes

As motivated in Section 2.3.3, reaching the right actors at the right time is of high practical importance for the coordination of incident responses. However, in the beginning of a response mission, the communication structures are often little established. In particular, a sender in a certain messaging task does not immediately known with which actual parties and entities to communicate. Rather, the sender can elaborate *which kind* of organizations, roles and specializations are appropriate and *where* the receivers should be present, to allow for a fast engagement [223, 151].

Thus, we propose that a sender, i.e. a central user, may specify the group of intended readers of a message on a level of abstraction different to identity. Instead, the sender leverages a specific logical combination of receivers' properties. Especially, we propose to use the *logical attributes* as depicted in Figure 5.4 in conjunction. It consists of attributes related to an organization, a role, a specialization or a location, i.e. a place where the receiver is currently present. Such a combination is what we call a *logical messaging policy*. It is used to specify the group of readers of a message that is to be sent to the outside world and the incident site.

Communication mechanisms that support a flexible specification of readers via an attribute-based description are denoted as attribute-based messaging (ABM) in the research literature [23, 232, 241, 24, 237]. ABM concepts allow implementing a communication approach that handles all major communication patterns, as given in Section 2.4.2; ABM thus also minimizes learning efforts for the senders.

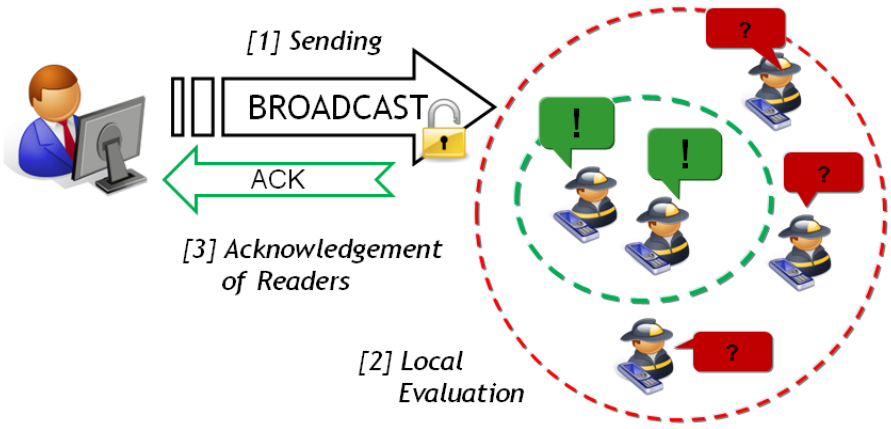

Figure 5.5: Steps of end-to-end secure attribute-based messaging

In the present work, we propose to realize end-to-end secure attribute-based messaging according to the following main steps:

- Firstly, the sender selects the group of intended readers by specifying a conjunction of attributes that readers have to fulfill, encrypts the message under the resulting *logical messaging policy* using the encryption scheme of Section 4.4 and broadcasts it to all mobile users that are logged in the communication network.
- Secondly, every receiver locally evaluates every received message on her communication device. The encryption mechanism assures that she can only decrypt a message and thus only read it if she satisfied the specified attribute combination.
- Thirdly, every reader of a message sends an acknowledgement to the sender, i.e. she confirms that she read the message. Thus, the sender does not know the actual group of readers of a message when sending it, but only after receiving the acknowledgements.

Our approach, as introduced, leverages a variant of an implicit addressing mechanism [177, 176], which makes use of attributes for addressing mobile users, in order to retain a functionality for targeted communication. Thus, within the approach, a mobile user is associated with a set of attributes that she satisfies. The attributes in use can be classified into two classes: static and dynamic. The values of static attributes do not change over time, e.g. a mobile user belongs to the same organization and has the same role as long this is not changed due to external reasons. Dynamic attributes possibly exhibit a frequent value change, e.g. the current location of first responder changes as she moves. The present proposal handles dynamic and static attributes on the encryption level[4]; the proposal is described next.

[4]One-to-many communication is crucial for first response scenarios. Typically, it is supported on the

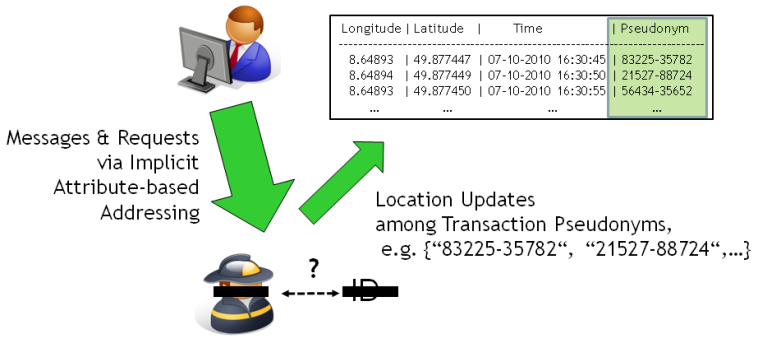

Figure 5.6: Activation of mobile users

In order to realize an end-to-end secure ABM functionality, we can also build on existing digital emergency communication networks. As such, the network provides basic security services for emergency communication; it also implies the existence of secured mobile devices on the receiver side.

However, realizing the end-to-end encryption leads to new challenges: traditional asymmetric encryption schemes and PKI concepts are not practical for communication with unknown receivers (cf. Section 3.3.2). In addition, existing encryption techniques do not provide the required flexibility and means for handling dynamic attributes with continuous values, e.g. location. To overcome these issues, we leverage the novel hybrid encryption technique for expressive policies (cf. Section 4.3), in order to achieve end-to-end encryption in the messaging. This technique, developed in the present work, supports a cryptographic realization of flexible *cryptographic attribute policies*; it also considers dynamic attributes with continuous values.

In the emergency response domain, the use of augmented digital maps is inherent [47]. An integration of the selection of location attributes into a digital map was proposed by real users to support an intuitive use (cf. Figure 4.10 and Section 7.3.2). It requires an expressive encryption, for incorporating location into the end-to-end encryption. Due to the local evaluation of policies, receivers can be addressed depending on their current location, without requiring them to continuously provide location information.

5.2.2 Provide Pseudonymous yet Linkable Location Updates

Once activated, a mobile user regularly provides location updates to the command and control center. Each location update contains the current position of the user, i.e. GPS coordinates computed on the user's device, the current time, and an identifier. Instead of using a static identifier, a user provides a linkable transaction pseudonym in every location update. Such a transaction pseudonym is derived according to the

network layer. E.g. in TETRA networks (cf. Section 2.3.3), multicast communication mechanisms are described. However, these mechanisms do not specify the end-to-end encryption [141].

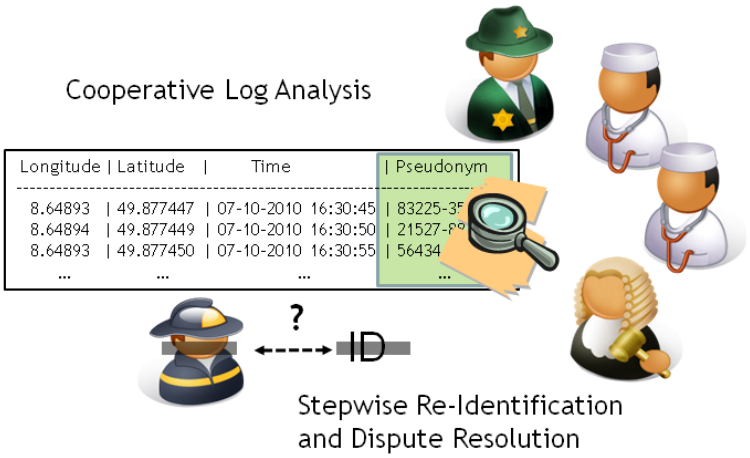

Figure 5.7: Cooperative log analysis

techniques of pseudonyms with implicit attributes, as proposed in Section 4.1. Every location update is securely stored in a so called location audit log. The process of the activation of mobile users and the subsequent provision and storage of location updates is shown in Figure 5.6.

Audit logs can be analyzed by authorized parties in a cooperative manner[5] (as illustrated in Figure 5.7), after missions, in order to deal with real world liability issues. In this context, we propose to implement multilateral security, i.e. a fair balance of security interests, based on the following main properties:

- In the log analysis, attributes that are implicitly encoded in the transaction pseudonyms can be evaluated cooperatively, which allows for a stepwise re-identification of users associated to the pseudonyms. This mechanism minimizes the disclosure of identity-related information and thus preserves user privacy.
- Mobile users are empowered to access the data which is stored in the audit along with a pseudonym, since individual access rights are encoded into the pseudonyms. This is used to implement mechanisms for individual access.
- Transparency of the log analysis is given, i.e. affected mobile users can verify the appropriateness of the log analysis. This is based on pseudonym-dependent selective access to the transparency log, which extends the audit log. Additionally, a data protection officer is involved in the cooperative analysis and report to the users.
- A law enforcement functionality is supported: a law enforcement authority may globally revoke pseudonymity of all involved mobile users. This is im-

[5] In Section 4.2, the parties involved in this task are called linkability brokers.

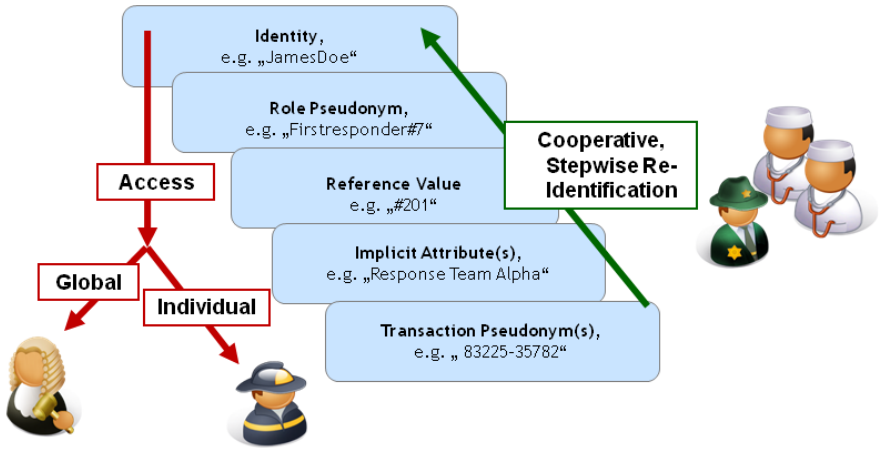

Figure 5.8: Levels of access in auditing

plemented by means of a global decryption capability of the encryption-based transaction pseudonyms. Yet, the present approach can also be instantiated without the law enforcement functionality. This issue is discussed in Section 7.2.1.

The given flexibility w.r.t. the levels of access and re-identification is exemplified in Figure 5.8. The approach provides a multilevel re-identification functionality, it thus supports a dispute resolution processes of reported incidents. Main aspects are explained next.

Audit officers (AOs), together with a data protection officer (DPO) may cooperatively link entries of the log, in order to create a *trace*. A trace consists of several transaction pseudonyms of a single mobile user, without revealing the user's identity. It can visualized in a location-based representation (cf. Section 6.5.2). After its creation, the officers may stepwise re-identify traces (or single log entries), by re-identifying implicit attributes of a trace or a single pseudonym.

The rules and conditions, which we denote as *disclosure policy*, for the actual detection of inappropriate behavior and misuse within the audit log analysis must be defined within the organizational and legal context of the application. We propose that the rules are defined according to the need-to-know principle [6], i.e. to execute a step-wise analysis of the log with highest possible anonymity restrictions. This means that a stepwise re-identification starts on a coarse level, e.g. it is first checked which organization a trace is associated with. In consecutive re-identification steps, the accuracy is increased, a trace can be verified against sub-units within the organization. In Figure 5.8, the example of the "Response Team Alpha" as a possible level of re-identification is shown. Yet, the individual levels do not need to relate to distinct organizations, but can flexibly be defined, since the underlying mechanism leverages a set-based representation. Thus, each of these levels also corresponds to

a degree of anonymity, given by the size of the chosen set.

In case that a complete disclosure is determined, a pseudonym is cooperatively decrypted. As a result, the encoded reference value is recovered. Based on registration information, it can be linked to a role pseudonym (cf. Figure 4.3). By additionally decrypting associated identity information, the real world identity can finally be completely re-identified.

Each action within the log analysis requires a cooperative decision: the audit officers as well as the data protection officer have to jointly agree on the execution of the action. In this process, the DPO acts as a representative of all mobile users and thus protects their privacy interests, since he is able to refuse inappropriate actions. Technically, the cooperative decisions require that a threshold of t officers have to agree. We propose to instantiate the mechanism with $t - 1$ AOs and one DPO. Yet, the approach can flexibly support a wide range of distributions of power, and may also exclude the global access for law enforcement (cf. Section 7.2.1).

5.3 Communication Network Model

This section introduces the communication network model. We assume that two distinct types of networks and communication channels are available within our setting:

- a digital emergency communication network enables communication between the command and control center and mobile users,
- an authenticated broadcast channel with memory enables the cooperative audit log analysis. According to the literature, such a channel is also called a bulletin board [118].

The latter one corresponds to the communication model which is introduced in Section 4.1.2. The parties that participate in the audit log analysis are equipped with smart cards. A smart card is used to authenticate to the bulletin board and to provide a partial result as input to the distributed computations (cf. Figure 4.1).

In order to enable communication between a control center and the outside world, each mobile user is in possession of a *personal communication device*. Each device has a unique identification number. By means of the device, a user can log into the digital network, given that a mutual authentication between the network and the device succeeds. The network access of the device can be revoked by a network administrator.

Further application level security services are in the end user domain and thus enabled through a registration process: every user receives keys and credentials according to her real world properties, i.e. attributes. The received credentials represent a mobile user's digital identity within the first response application context. Thus, by taking part in the registration, the personal communication becomes a *personalized communication device*, that enables secured two-way communication. The device is able to decrypt messages according to the hybrid encryption technique

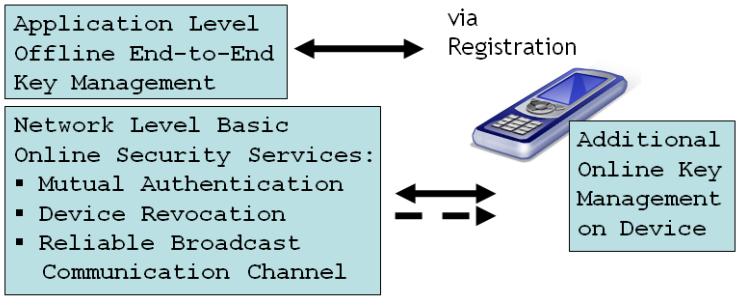

Figure 5.9: Security services of emergency communication network

for expressive policies, as introduced in Section 4.3. We assume that it provides a tamper-resistant GPS receiver. It also implements the online key management procedure of the encryption technique (cf. Section 4.4.3). The security services of the emergency network and the communication device are summarized in Figure 5.9.

5.4 Adversary Model

In the following, we describe our adversary model. This concretizes the notions of end-to-end security and multilateral security within the present work. The adversary model considers two distinct classes of adversaries:

- an *outside adversary* tries to corrupt and interfere with the secured communication between a command and control center and the outside world,
- an *inside adversary* tries to interfere with the targeted balance between privacy protection and accountability.

The capabilities that we ascribe to each adversary are defined next.

5.4.1 Properties of Outside Adversary

For the *outside adversary model*, we consider a limited version of the Dolev-Yao threat model [55]. In the Dolev-Yao model, the adversary has control of all communication channels, being able to eavesdrop messages in transit, destroy, replay and insert messages into the communication channel. However, the adversary is not able to break any cryptographic mechanisms without obtaining the required cryptographic keys. Especially, a Dolev-Yao adversary does not have cryptanalysis capabilities, i.e. is unable to circumvent complexity theoretic assumptions of security mechanisms.

Precisely, we restrict the Dolev-Yao model by removing the ability of the adversary to destroy messages in transit. The deletion of such messages in a computer network scenario leads to denial of service attacks. Although such type of attacks

could be physically plausible in some scenarios using radio jamming techniques, we disregard such attacks. Moreover, we do not allow the adversary to interfere with registration processes.

5.4.2 Properties of Inside Adversary

In order to clarify the meaning of an adversary in our context of multilateral security, we distinguish between *opponents* and *inside adversaries*:

- Firsthand, within the system, specific parties are *mutual opponents* w.r.t. the fulfillment of their own security goals. For example, a mobile user's privacy interests oppose to the accountability interests of audit officers. Thus, from the perspective of one party, the opponent has conflicting security goals. Yet, such (mutual) opponents are (both) authorized for their specific tasks, and thus not considered as adversaries w.r.t. the goal of multilateral security.
- Differently, an *inside adversary* tries to manipulate the results of actions with malicious intent and without authorization. For example, such an adversary, *DPO* or *AO*, may try to corrupt parties in order to trace a mobile user. Such a corruption may also turn an opponent into an inside adversary.

We assume that an inside adversary may corrupt up to $t - 1$ audit officers. In addition, an inside adversary may not interfere with registration processes, cannot circumvent complexity theoretic assumptions of security mechanisms or change the content of logs and bulletin boards.

5.4.3 Further Types of Adversaries

We are aware that further types of adversaries can be devised. E.g. the consideration of adversaries that may interfere with registration processes would require rethinking these mechanisms. This could possibly impact the main security design. Yet, dealing with these adversaries is out of the scope of this thesis and considered future work.

5.5 System Overview

The main principles introduced in the previous sections manifest in an integrated architecture (also briefly denoted as system), which is depicted in overview in Figure 5.10. This section defines the involved parties and modules. Also, it provides temporal and logical views of the system.

5.5.1 Parties and Modules

Conforming with Figure 1.3 and concretizing the number of instantiations involved, we specify the parties[6] within the integrated system as follows

[6]The icons used to visualize the parties throughout this thesis have been shown in Figure 5.1.

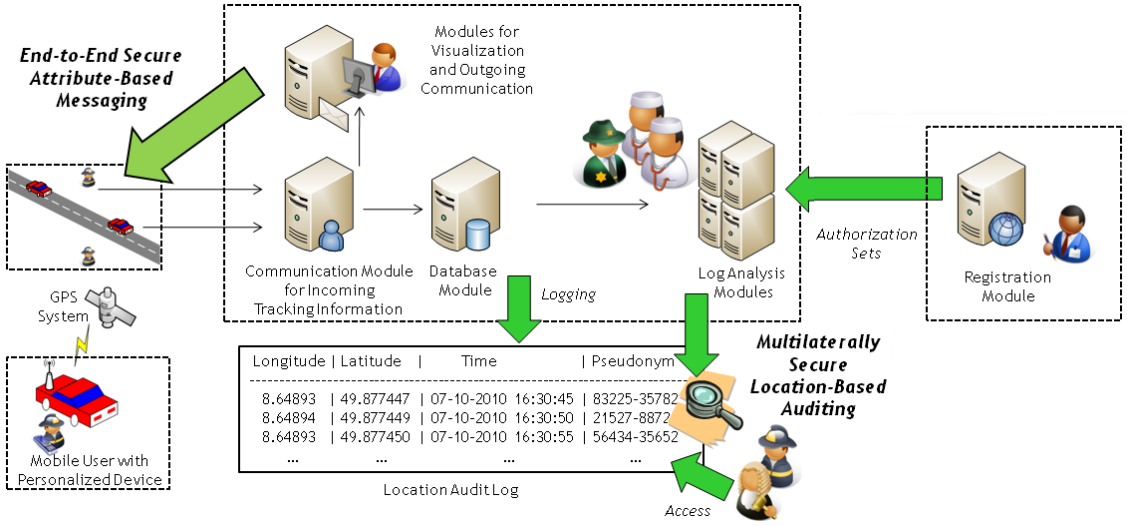

Figure 5.10: Integrated architecture in overview

- a registration authority (RA),
- a law enforcement authority (LEA),
- a set of $t-1$ audit officers (AOs), where t[7] is an odd integer of at least 3,
- a data protection officer (DPO),
- an arbitrarily large number of mobile users (MUs), which is made up of first responders and specialist,
- a central user (CU)[8].

In order to execute operations and protocols, the parties are supported by and make use of the following main modules, that implement system functionality:

- The RA is equipped with a registration module, which supports the creation and storage of a registration list as well as the definition of authorization sets, which are used in the auditing. Also, a verifiable mixnet (cf. Section 4.1.2) is implemented in the registration module.
- The CU is supported by modules for visualization of the emergency situation and communication with the outside world. The communication module implements the mechanisms for end-to-end secure attribute-based messaging.

[7]The parameter t defines the threshold of parties that need to cooperate in order to execute certain distributed computations, cf. Section 4.1.2, Section 5.2.2 and Section 6.1.

[8]We represent the group of people working inside a control center by a single entity, cf. Section 2.3.3.

- Location updates of *MUs* are handled by a communication module for incoming tracking information and by a database module, that securely stores the received data, which results in a location audit log.
- The *AOs* and the *DPO* are supported by modules for the log analysis, which enable a multilaterally secure location-based auditing.

5.5.2 Phases

The complete approach can be divided into several phases. The temporal alignment of the phases[9]. and the involved parties are shown in Figure 5.11. The phases are described next.

- *Setup Phase:* In this phase, system parameters for the cryptosystems and cryptographic master keys used for registration, communication and auditing are created.
- *Registration Phase:* Each mobile user personalizes her communication device, by receiving credentials according to her properties; she is thus enabled for pseudonym generation and secure communication. Also, each user and her registration informations are added to a registration list.
- *Activation and Group Communication Phase:* After being registered and logged in the emergency communication network, mobile users can be requested to join rescue missions by a central user, using end-to-end secure attribute-based messaging. Also, further group communications are enabled by this mechanism.
- *Location Tracking Phase:* Upon activation, during a rescue mission, a mobile user regularly provides location updates under transaction pseudonyms to the control center. This is referred to as location tracking phase. The frequency of location updates depends on the preference of the user. The transaction pseudonyms are created locally on the personal device. Location updates are securely stored in a location audit log in the command and control center.
- *Location Auditing Phase:* In this phase, entries of the log are jointly processed by audit and data protection officers for organizational and legal liability reasons. Upon convincing detection of inappropriate actions, implicit attributes of pseudonyms can be re-identified. The created traces support dispute resolutions, in which mobile users may also exercise an *individual access* to the log, in order to repudiate false accusations by providing evidence of exoneration. If a log analysis leads to to court proceedings, a *law enforcement* authority can re-identify any log entries that may support returning a verdict.

[9] In most cases, previous phases are necessary for the next phase to proceed, e.g. cryptographic keys have to be generated before they can be used, users have to be registered before they can act, and data has to be recorded in logs before the auditing can start. In case of activation and group communication as well as location tracking, phases are overlapping.

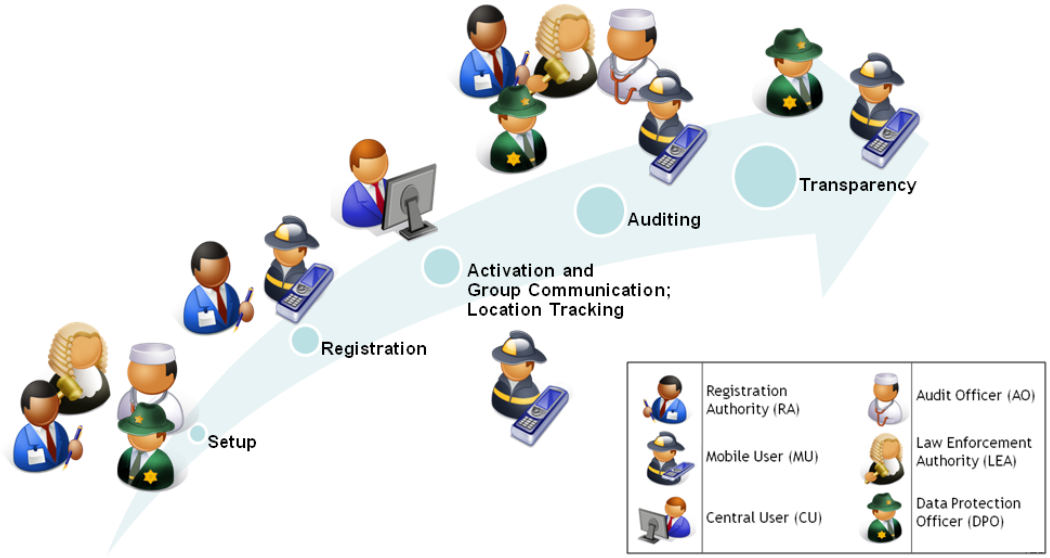

Figure 5.11: Phases and involved parties

- *Transparency Phase:* In this phase, the appropriateness of the actions of the audit officers in the log analysis phase can be verified by mobile users. This is done by checking the transcripts created in the log analysis that are stored on the broadcast channels with memory. Additionally, transparency information can be exchanged between the data protection officer and mobile users.

5.5.3 Interactions

Having introduced a temporal view in the last section, this section gives a logical view of the interactions within the system. During the operation and use of the system, the present parties interact and cooperate in several ways. Figure 5.12 depicts the main interactions. The numbers refer to the following list of interactions:

1. Generation of System Parameters and Public Keys
2. Generation and Distribution of Private Keys
3. Registration of Mobile Users
4. Provision of Attributes for Use in Communication
5. Provision of Location Updates
6. Group Communication
7. Provision of Authorization Sets

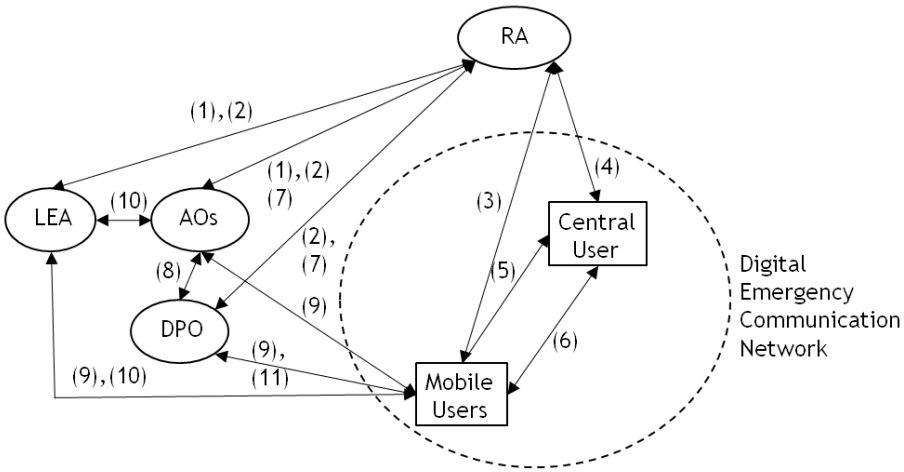

Figure 5.12: Interactions between parties

8. Cooperative Audit
9. Individual Log Access
10. Law Enforcement
11. Exchange of Transparency Information

This section defined who interacts and cooperates in which logical procedures. The mechanisms that implement these procedures will be presented in detail in the next chapter.

5.6 Summary

In this chapter, we introduced our novel approach to multilaterally secure pervasive cooperation in overview. In the context of the whole thesis, this chapter has an integrating function. It connected the application scenario of location-aware first response to a system model, we introduced the main principles to implement security and the resulting integrated architecture.

Our integrated approach addresses the shortcomings of existing work as follows:

- In order to enable secure communication with unknown receivers, we propose to make mobile users implicitly addressable via attributes. In particular, we applied the hybrid encryption technique for expressive policies (presented in Chapter 4) such that location privacy of receivers is protected as well as the appropriateness to users is supported. We thus contributed the principles and basics of a novel attribute-based addressing and messaging mechanism; it harnesses attributes related to organizations, roles, specializations as well as the

current location of a user in conjunction. We thus also added a concept for attribute combinations that are both practical and appropriate to real users to the literature.

- In order to achieve a fair balance of location privacy protection and accountability, we propose that mobile users regularly provide location updates together with linkable transaction pseudonyms. In particular, we leverage pseudonyms with implicit attributes (cf. Chapter 4) for this task; stored location updates constitute audit logs that are pseudonymized already upon creation. In order to complement this proposal, we contributed novel mechanisms for real-world auditing. This setting has not been addressed by the previous work in the area of pseudonymous auditing. In addition, we contributed pseudonymous location traces as a particular form of evidence. On a technical level, our proposal combines cooperative auditing with transparency mechanisms in order to constitute a second level of accountability w.r.t. the actions of involved authorities. Existing research has not proposed such capabilities in combination. We thus extended the concept of pseudonymous auditing to multilaterally secure auditing.

In order to complement the description of our integrated proposal, we also provided the underlying communication network model and a novel adversary model that captures the characteristics of multilateral security in our cooperative setting.

In this chapter, the introduced approach was presented in terms of parties, modules, phases and interactions. Beyond that, further technical and organizational mechanisms are associated to our proposal. They will be introduced in detail in Chapter 6.

6 Mechanisms

In this chapter, we describe the mechanisms that implement the procedures introduced in the last chapter in detail. This includes setup, registration, communication, location tracking as well as auditing mechanisms.

The presentation in this chapter is structured according to the chronological sequence: firstly, the system setup as well as the mechanisms and procedures for managing and registering the digital identities of mobile users are described, in Section 6.1. This is followed by a description of the registration mechanisms in Section 6.2. Section 6.3 then describes the messaging mechanisms, including examples. In Section 6.4 we describe, how location tracking information is provided to the command and control center. The mechanisms for multilaterally secure auditing are given in Section 6.5, including an example. Finally, the chapter is summarized in Section 6.6.

6.1 Setup

In this phase, system parameters and cryptographic keys, both related to auditing and messaging functionalities, are created and distributed, if necessary. The parties involved in the setup are the registration authority (RA), the law enforcement authority (LEA), the data protection officer (DPO) and a set of audit officers (AOs).

This phase proceeds as follows. In order to setup auditing functionalities, the following steps are executed:

1. The RA chooses the parameters t and n. Hereby, t is the threshold that specifies the number of authorities that need to cooperate, is an odd integer of at least 3, and $n = 2t - 1$[1].

2. The RA creates the ElGamal system parameters.

[1] The parameters n and t have a direct influence on the underlying threshold ElGamal cryptosystem. As introduced in Section 4.1.2, it can tolerate a maximum of $t - 1$ corrupt authorities, yet still requires a majority of t participating authorities. The total number of authorities n has to be (at least) $n = t - 1 + t = 2t - 1$, thus $t - 1$ is a minority of authorities. Cf. Section 4.1.2, Section 5.2.2 and Section 5.5.1.

3. The LEA generates an ElGamal key pair (SK_{LB}, PK_{LB}). Then, the LEA executes an (t, n)-secret sharing [202] on the SK_{LB}, hereby dealing out one share to the DPO, one share to each of the $t-1$ AOs, and keeps the remaining $n-t$ shares.

4. The AOs, the DPO and the LEA authority jointly create a shared key z, using the distributed key generation protocol according to Pedersen [172]. As in the case of the private key, each AO and the DPO receive one share, while the LEA receives any further share. The key will be used within blinding operations for re-identification of transaction pseudonyms.

In order to setup messaging functionalities, the following steps are executed:

1. The RA creates the system parameters for the hybrid encryption technique, including CP-ABE system parameters.

2. The RA generates keys for the hybrid encryption technique. In order to do so, it executes the setup algorithm[2] of the underlying CP-ABE cryptosystem, thus the RA generates the public parameters PK and the master key MK. The MK is kept secret by the RA. Thus, the RA is enabled to play the role of the AA of the CP-ABE part of the hybrid encryption technique.

6.2 Registration

The registration is an organizational mechanism that defines which mobile users belong to the system and may thus participate in cooperative incident responses. In the registration phase, mobile users interact with the registration authority in order to personalize their communication devices according to their digital identity, by receiving cryptographic keys and being included in a registration list.

The following section describes how digital identities are represented within the present approach. Then, the process of the registration itself is given.

6.2.1 Representation of Digital Identities

In order to be addressable in communications, to be able to provide pseudonymous location updates and also to be re-identifiable in a log analysis, it is necessary that properties of mobile user are digitally represented within the system. Supporting the use of real world properties of real world entities as digital identifiers in computer networks and applications is commonly denoted as digital identity management [170]. Generally, a digital identity abstracts from a real world person or user, implementing a unique digital representation of that entity. Also, such a digital identity details relationships to other entities or parties and contains associated access rights and credentials w.r.t. certain application contexts [246].

[2] The setup algorithm is the key generation procedure for the attribute authority (AA) of a CP-ABE system.

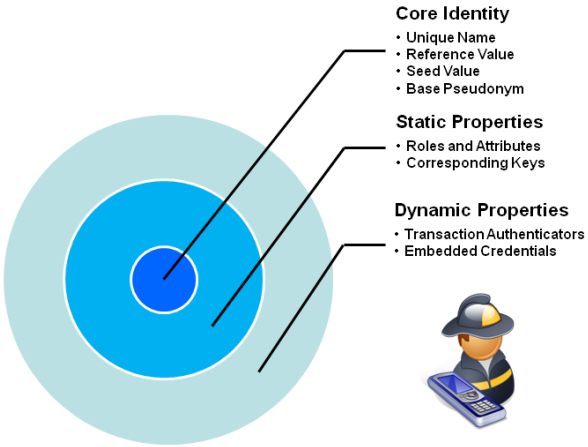

Figure 6.1: Representation of digital identities

In the present approach, mobile users are registered to the system according to a specific digital identity profile that is described next. Figure 6.1 depicts how such a *digital identity for multilaterally secure pervasive cooperation* is organized. It consists of three logical layers, thus it comprises the following identity-related informations:

1. *the core identity:* the unique representation of an real world identity, i.e. a mobile user, consisting of a unique base identifier and related informations,

2. *static user properties:* organizational roles and specializations or relevant skills, i.e. all static attributes relevant to emergency communications,

3. *dynamic user properties:* location-dependent and thus dynamic attributes and associated embedded credentials[3] as well as access rights to audit logs, i.e. transaction authenticators.

In our approach, every layer is associated with keying material and credentials that a mobile user receives for implementing the targeted security goals:

- In order to reconcile privacy protection and accountability, a base pseudonym $P_{U_i,B}$ is issued and further derived informations are registered, to enable the pseudonymous provision of location updates and the selective analysis of audit logs,

- in order to enable end-to-end secure communication via attribute-based messaging, a private attribute set $\{A\}_{U_i}$, containing static attributes, is issued, and the generation of dynamic attributes is supported.

[3] According to Section 4.4.3, we denote the local generation of keys and credentials on a device as *embedded*. Thus, the term *associated embedded credentials* refers to keys that are generated according to dynamic attributes.

#201	Responder#13	E_{PK_LB}("JohnDoe"),	Org. = Firefighters, Role = Group Leader, Spec. = Negotiations
#047	Responder#17	E_{PK_LB}("JaneDoe"),	Org. = Firefighters, Role = Emergency Driver, Spec. = Cartography
#092	Specialist#38	E_{PK_LB}("JeffDoe"),	Org. = Civil Defense, Role = Consultant, Spec. = Toxic Matters
....	....	....	....
Reference	*Role Pseudonym*	*Encrypted Identity*	*Attributes*

Figure 6.2: Sample registration list

A personal communication device, that is carried by and associated to any mobile user, as specified in Section 5.3, provides the digital container, platform and technical trust anchor of this approach. It is personalized in the registration process, which is described next.

6.2.2 Registration Process

During the the registration process, an integrity-protected registration list is created by the *RA*. The list contains one entry per mobile user that is registered to the system. An example of such a list is depicted in Figure 6.2. As shown, each list entry contains identity-related informations including a unique reference value, a unique role pseudonym, an encryption of the real world identity as well as associated static attributes[4]. The underlying registration which creates such a list has two main parts. We describe them next.

The first main part of the registration proceeds according to the registration procedure introduced in Section 4.2.2, i.e. this procedure is instantiated in our application context of first response. During this part, the *RA* issues a base pseudonym to each mobile user, that enables her to derive transaction pseudonyms locally on her device. In order to register, the user provides her mobile device for personalization to the *RA*. In case the user has no such device, she receives a new one[5]. Then, this part of the registration process consists of the following main steps:

1. For each user, a new entry in the integrity protected registration list created is by the *RA*. An encryption of the users' real world identity is added to that entry.

[4]Additional keys issued to the users are neglected in the figure.
[5]For example, this is the case if a new external specialist or volunteer registers.

2. The user receives a distinct role pseudonym, which associates the user with her organizational role in the emergency response context. Also, the user receives a distinct reference value, which we denote A_{U_i}. Both, the role pseudonym and the reference value are added to the respective entry of the registration list.

3. Then, the user receives a base pseudonym, which is a non-deterministic encryption of the reference value: $P_{U_i,B} = E_{PK_{LB}}(A_{U_i})$. It is registered to the mobile device.

4. The random factor $r_{i,B}$ used in the encryption of the reference value is stored on the user's device.

5. The user generates an unique seed s_{U_i} and registers it to the PRNG of her mobile device[6].

In the second part of the registration process, a user receives attributes for use in end-to-end secure attribute-based messaging. System-wide attributes with same semantics have the same string representation. The attribute-related registration proceeds as follows:

1. Upon proof of eligibility given by the user, the RA creates a set of cryptographic attributes, by executing the key generation according to the CP-ABE system within the hybrid encryption technique. This set contains attributes according to organization as well as role memberships and specializations that a mobile user satisfies.

2. The resulting set of attributes, $\{A\}_{U_i}$, is transferred to the user's device.

3. In turn, the unique identification number of the mobile device is added to the user's entry in the registration list.

4. The user receives a key for symmetric encryption of replies, K^{RS}_{Ack}, and registers two keys for mutual message authentication[7] with sender S, denoted K^{R}_{MAC} and K^{S}_{MAC}.

5. Additionally, the user receives a symmetric keys, denoted K_{LL}, for securing the location lock function of the hybrid encryption technique.

Having participated in the registration, a mobile user is enabled to participate in cooperative rescue missions.

[6]Figure 4.4 shows the functions of seed and base pseudonym in the generation of transaction pseudonyms.

[7]The keys are part of message authentication codes (MACs).

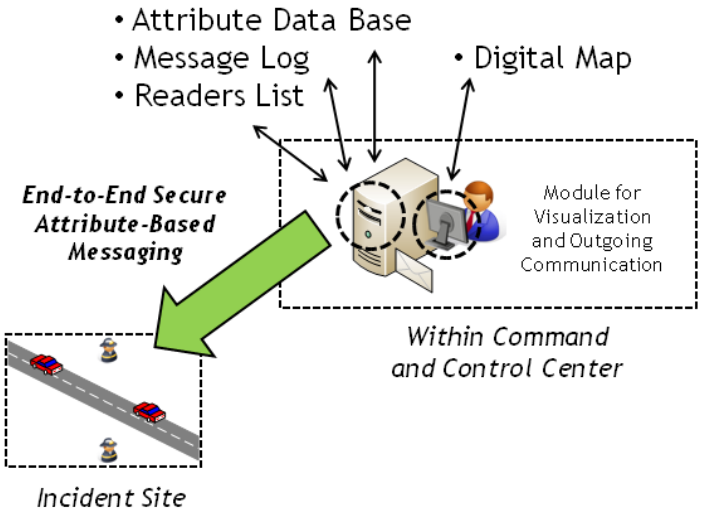

Figure 6.3: Implementation of ABM within integrated system

6.3 Activation and Group Communication

For this phase, we assume that mobile users have been registered to the system before and are in the passive state. As detailed in section 5.1, this means they have joined the digital emergency network via their personalized communication devices, and are thus able to receive messages that are sent by the central user. The communication mechanism for this kind of group communication is denoted *end-to-end secure attribute-based messaging*. The following sections provide a detailed description of our approach.

6.3.1 Overview

Within the integrated system (cf. Section 5.5), the communication mechanism of end-to-end secure attribute-based messaging is mainly implemented in the module for outgoing communication and on the personalized communication devices. The module for outgoing communication also provides

- a digital map (DM), that helps selecting location attributes,
- a central attribute data base (ADB), that stores all defined static attributes,
- a message log (ML), that stores outgoing messages,
- a readers list (RL), that is used to document the group of readers of a message.

Log and list are append-only. Figure 6.3 shows the components in overview.

In the present approach, the realization of end-to-end secure ABM hinges on two main conceptual layers:

- On the *logical messaging policy layer*, a sender may specify logical messaging policies, in order to select receivers in the communication via an ABM system on a level of abstraction different to identity.

- The *access control layer* provides security mechanisms that enforce the constraints specified by the logical messaging policies, by employing encryption techniques and tamper-resistant access control support mechanisms.

In the following, sending a single message by means of the provided communication functionality is called a *messaging act*.

6.3.2 Logical Messaging Policy Layer:

In any messaging act, a sender

- has to choose between two communication modes: *direction communication / requests* and *depositions*. The first one refers to the communication patterns `CP1`–`CP3`, the latter one to `CP4` (cf. Section 2.4.2);

- specifies the logical messaging policy. Therefore, the sender firstly selects attributes that represent organizations (e.g. Police), roles (e.g. Group Leader) and specializations (e.g. Specialist Toxic Matters), from the central attribute database, secondly, selects a location attribute by selecting a geographic area on a digital map. This is executed by selecting two points P_1, P_2 that define a rectangle (cf. Figure 4.10). According to the spatial position on a digital map, each point refers to a GPS position that is thus specified.

The basic structure of logical messaging policies, as shown in Figure 5.4, is a logical conjunction of one attribute related to location, one attribute related to a specialization, one attribute related to a role as well as one attribute related to an organization. Thus, a specified logical messaging policy consists of at least one and at most four of the given attributes.

6.3.3 Access Control Layer

End-to-end secure attribute-based messaging makes use of an efficient end-to-end encryption mechanism in order to guarantee end-to-end confidentiality against outside adversaries. Especially, we build upon the novel hybrid encryption technique (cf. Section 4.3) that is proposed within this thesis. It is the main mechanism for implementing the access control layer. Yet, the selection of the communication pattern has an effect on this access control layer:

- for direct communications (`CP1`, `CP3`) and requests (`CP2`), the enforcement requires making use of the hybrid encryption technique,

- depositions (`CP4`) can be handled with CP-ABE (cf. Section 4.3.2) alone.

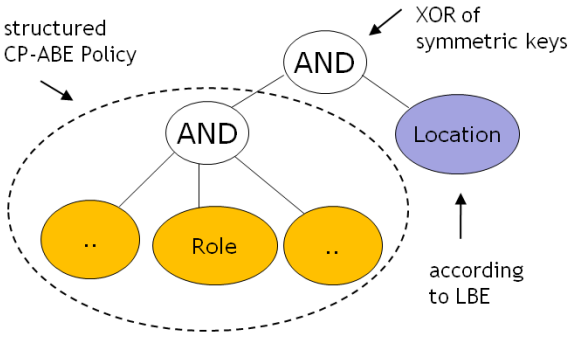

Figure 6.4: Mapping of messaging policies to hybrid encryption

In the latter case, the specification of sending policy does not contain a continuous location attribute. This allows for a direct mapping to CP-ABE policies[8]. If a deposition is chosen, also no broadcast of messages is executed. Rather, the deposited message is internally stored on the ML for parties that join the rescue missions at a later point in time.

The following descriptions focus on the realization of `CP1-CP3`. In this case, logical messaging policies are mapped to the hybrid encryption technique as follows, also shown in Figure 6.4: the attributes related to organizations, roles and specializations are mapped to a structured CP-ABE policy. This structured policy adheres to the structure of the messaging policy, i.e. it is a conjunction. The attribute related to location is basically handled as introduced in Section 4.4.2. In particular, a key is securely derived from GPS coordinates and then XORed with a symmetric session key.

6.3.4 Protocol for End-to-End Secure Messaging

This section provides a schematic view of messaging acts, in order to complement the description.

In order to send a message, the sender has to specify a logical messaging policy by selecting static attributes and a location attribute on the digital map DM, and composes the message content. Basically, a messaging act furthermore consists of a broadcast of an end-to-end encrypted message M_{E2E} and answer back steps. The end-to-end encryption incorporates a unique message ID, ID_M, to prevent replay attacks, symmetric non-repudiation is supported by message authentication codes (MACs). Messages sent out and acknowledged readers are documented on message log (ML) and readers list (RL). Optionally, readers can reply and answer a read messages.

[8] Yet, this kind of encryption can be executed in the same technical setting given by our hybrid encryption approach, i.e. the hybrid encryption technique reduces to CP-ABE in that case.

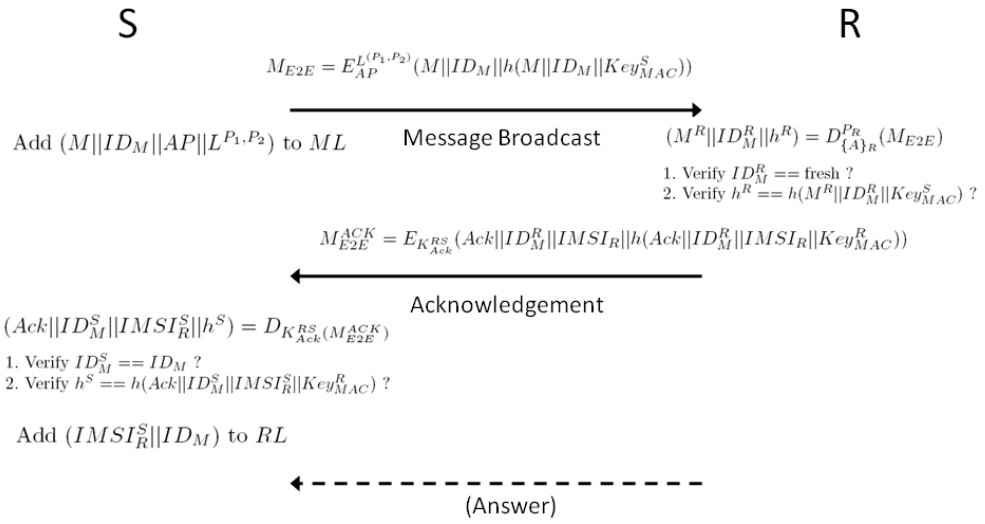

Figure 6.5: Protocol for end-to-end secure attribute-based messaging

In Section 5.2.1, our approach to attribute-based messaging has been introduced to consist of the main steps *sending*, *local evaluation* and *acknowledgement*[9]. The protocol that implements these steps and which is underlying every messaging act is depicted in Figure 6.5. In this figure, the left side represents the sender in a control center, the right side the mobile users that receive message. Here, $||$ represents string concatenation. In detail, the protocol proceeds as follows:

- The sender concatenates: a message content m, a unique message ID, which we denote as ID_M, and a MAC on the former two contents. This MAC is realized via hashing the concatenated content and a symmetric key. Then, an encryption according to the specified logical messaging policy is executed. The so encrypted message M_{E2E} is broadcasted via the digital emergency communication network. Also, the message is added to the message list ML.

- Upon receiving the message, every mobile user tries to decrypt the message. This succeeds, if the policy is satisfied. Decryption provides the received message content M^R, the received message ID IM_M^R as well as the received MAC value h^R. Every user verifies whether the message ID is fresh, i.e. that it has not been used before[10]. Also, it verifies the MAC by recomputing it and comparing the value.

[9] Optionally, a reader can answer a message. This step can be implemented mostly analogously to acknowledgements. Further details, e.g. a set of reference strings for indicating different levels of priority of a message, are considered future work.

[10] In order to verify that a message ID has not been used before, a receiver has to store every received message ID locally on her device. The received MACs are also stored to support a later analysis.

- In case both verifications succeed, a receiver becomes a reader of the message. She acknowledges that she is able to read a fresh and integrity protected message. In order to so, she concatenates the string "Ack", the received message ID, her unique device identification number and a MAC on the previous content. Together, this is symmetrically encrypted and sent to the command and control center as acknowledgement message.

- The sender decrypts every received acknowledgement message. Decryption provides the "Ack" string, the value of a message ID ID_M^S, a devices identification number $IMSI_R^S$ and a MAC value h^S. The sender identifies the messaging act via the ID_M^S and verifies the MAC value. If this succeeds, a reference to the reader and the message is added to the RL, in order to document the group of readers of a message.

6.3.5 Examples

As introduced, end-to-end secure attribute-based messaging is a very flexible communication mechanism. In this section, we give concrete examples of messaging policies and elaborate on their relevance to the first response application context, in order to show how ABM can be applied effectively. In Figure 6.6, six distinct examples are given. In every example the rightmost string shall represent a location attribute selected on a digital map. Here, textual representations instead of GPS positions, e.g. "Near Disaster Area", are used to convey the functions in the application context.

- *Example 1:* This policy can be used in order to communicate tactical information relevant to a rescue mission. The role attribute *group leader* is used to address mobile users with command and control responsibilities in the field. This reflects that command and control is actually exercised locally in the first response domain.

- *Example 2:* Based on a policy as given in this example, specialist that may immediately be required can be contacted. In this case, the sender can select a location attribute that specifies a region which allows for a fast transfer to the incident site.

- *Example 3:* This policy maps to a situation, which requires large numbers of helpers with a special skill. Such helpers are normally not directly associated to an emergency services organization, but are rather available and organized as volunteers. In the message content, they can e.g. be requested to show up at a certain point, where a local organizer will arrange further instructions.

- *Example 4:* Medics with special skills are often required in order to quickly react in emergency situations. With such kind of messaging policy, they can efficiently be contacted to allow for a fast engagement.

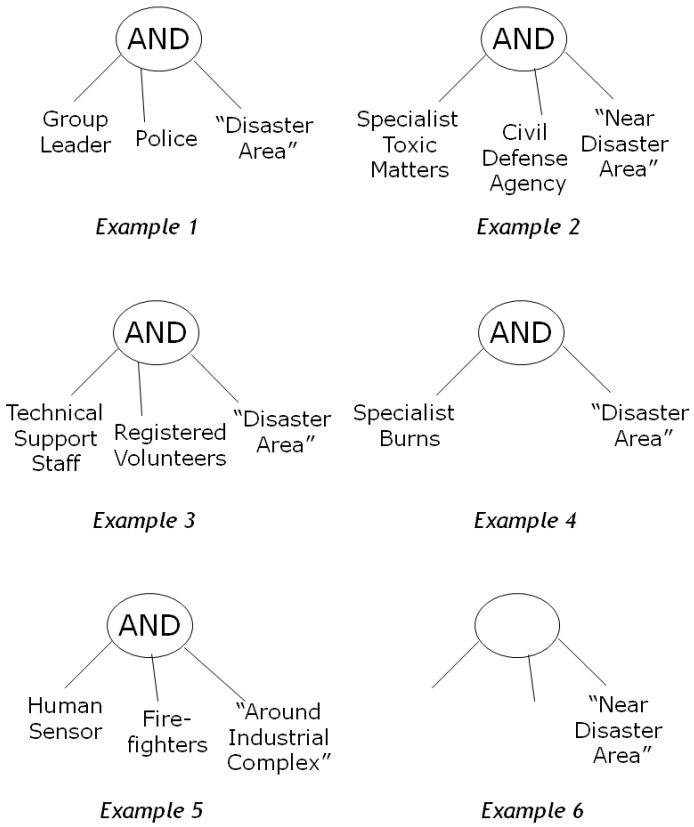

Figure 6.6: Examples of logical messaging policies

- *Example 5:* Reports and informations on the local situation are often valuable to decision makers in a control center. This kind of policy can be used to harness mobile users as human sensors, i.e. requesting them to send in reports or digital photos that document local effects if a disaster. It thus implements a kind of query on human sensors.
- *Example 6:* In case that only the location addressing is used, a pure geo-casting functionality can be realized. This can for example be used to send out urgent warnings to all mobile users involved in a rescue mission.

6.4 Location Tracking

After a mobile user has changed her state to active, i.e. upon the start of her participation in a rescue mission, the user provides location updates to the command and control center, i.e. messages including information on the current location of the user. The computation of this location information is GPS-based, i.e. the communication device locally estimates latitude and longitude values of the user's geographic position based on the global positioning system. Every update is send along with a transaction pseudonym. The frequency of updates is chosen accordingly to the preference of the user, e.g. every 10 seconds.

The provision of location information consists of the following steps:

1. *Pseudonym Generation:* Each user U_i derives from her base pseudonym $P_{U_i,B}$ an ordered set of transaction pseudonyms $\{P_{U_i,j}\}$. In order to do so, firstly, the seeded PRNG of the communication device is used to produce an ordered set of random factors $\{r_{i,j}\}$. Then, the random factor inside the base pseudonym is updated with a random factor from the set, i.e. a re-encryption is performed: $P_{U_i,1} = P_{U_i,B} * (g^{r_{i,1}}, h^{r_{i,1}})$, $P_{U_{i,j+1}} = P_{U_i,j} * (g^{r_{i,j+1}}, h^{r_{i,j+1}})$[11].
2. *Location Updates:* In the active state, each user provides location information along with transaction pseudonyms from the set $\{P_{U_i,j}\}$. According to the preferences of each user, location updates are sent in a specified interval of time. Each time, the pseudonym $P_{U_i,j}$ is changed to $P_{U_i,j+1}$. Changing a transaction pseudonym, based on re-encryption, does not change the reference value encoded in the pseudonym.
3. *Storage:* The location updates are securely stored after reception in the command and control center, thus a location audit log is created. Its entries are in the form *pseudonym - time - location*. The *pseudonym* field records the value of a transaction pseudonym.

In the given description, we abstract from additional security mechanisms, i.e. signing and encrypting the location. For this purpose, standard mechanisms can be applied, especially the update only needs to be encrypted for a single party in the command and control center.

[11] The described method is also shown in Figure 4.4.

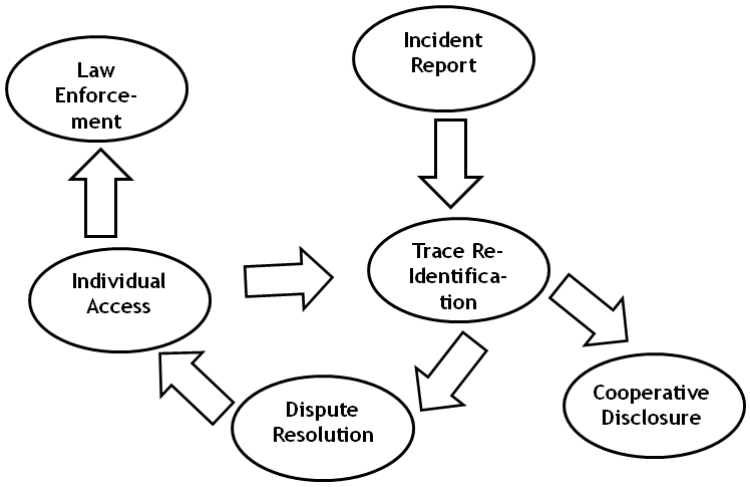

Figure 6.7: Process and steps of auditing

6.5 Multilaterally Secure Auditing

While providing location updates, as described above, proceeds automated once it is triggered, an ex-post audit is a more complex socio-technical process, involving cooperative decisions, execution of technical protocols as well as dispute resolution steps. The following sections describe both the technical mechanisms, which make use of the operations associated to pseudonyms with implicit attributes, as introduced in Section 4.1, as well the embedding in an integrated process. Firstly, an overview of the proposed process is given, followed by further descriptions of the involved mechanisms. This als includes descriptions of the associated transparency mechanisms.

6.5.1 Overview

The proposed approach to multilaterally secure auditing consist of several main steps, that are shown in Figure 6.7. It results from extending and modifying the basic process of pseudonymous auditing due to Sobirey et al. [209, 67] (cf. Figure 3.2). In particular, our proposal reflects that

- real-world audits based on collected location information require starting points for the analysis to commence. We introduce incident reports for this purpose;
- the support of partial re-identifications in the auditing mechanisms manifest in dispute resolution steps on the process level;
- transparency measures complement the audit, they are partly realized as additional ex-post log access and analysis steps[12].

[12]In the following, the transparency mechanisms are described separately in Section 6.5.5.

The main steps proceed as follows:

- *Incident Report:* A log analysis is started upon a possible case of misuse is reported. We call this an incident report. It contains the description of a possible malicious incident associated with a time and a location. Incident reports can e.g. be given by eye witnesses after a rescue mission.
- *Trace Re-Identification:* Upon receiving an incident report, the authorities authorized for auditing begin to analyze an existing location audit log. The entries of the log are initially unlinkable w.r.t. their identifiers, since they are indexed by transaction pseudonyms. Based on the linking procedures supported by the underlying pseudonym technique, i.e. secure multiparty computation protocols, transaction pseudonyms can be linked to each other, in order to create a trace. Linking two transaction pseudonyms means that they represent the same mobile user, yet without disclosing which user is actually represented. Created traces (or single transaction pseudonyms) can be partially re-identified. This means that implicit attributes of a trace, possibly related to organizational or team structures, can be detected, again without disclosing the real world identity of the represented user.
- *Dispute Resolution:* Having re-identified an implicit attribute of a trace implies that a mobile user has been present at a certain location and time, as represented by the trace. This information is used to find out further details about the case of misuse that was reported. Therefore, a responsible person is asked whether she can resolve the dispute, whether the reported incident took place, or to provide further relevant information.
- *Individual Access:* In the dispute resolution step, a mobile user may be named to be possibly involved in the reported incident. In this case, the user may react by providing further information on the incident. Also, she may individually access the audit log in order to repudiate false accusations by providing evidences of exoneration. In case that a dispute could not be resolved, i.e. if it could not be by verified whether a misuse took place, or traces could not be associated to an accountable user, additional traces can be created and re-identified. Also, a partial re-identification may be executed on a more fine-grained level.
- *Cooperative Disclosure:* Following a partial re-iden-tification, a complete re-identification can be executed, upon a detection of inappropriate actions document by the log. We call this a cooperative disclosure. In this case, pseudonyms can be completely revoked in order to unveil the encoded reference value. This value refers to an entry of the registration. The encrypted real world identity field can then be decrypted consecutively.
- *Law Enforcement:* This step is optional. If a log analysis leads to court proceedings, i.e. a detected incident has legal relevance, a law enforcement authority can disclose all log entries that may support returning a verdict.

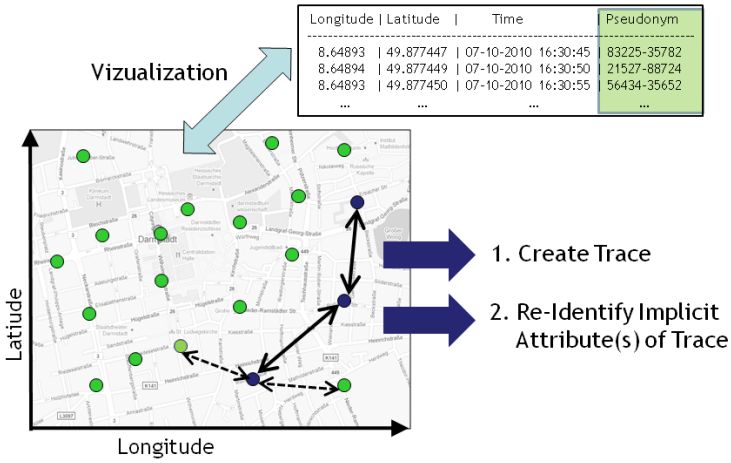

Figure 6.8: Visualization of log analysis

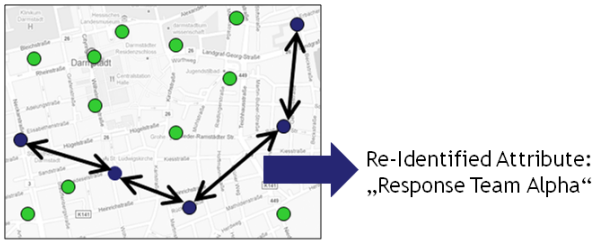

Figure 6.9: Example of re-identified trace

6.5.2 Log Analysis Mechanisms

The presented approach to auditing makes use of transaction pseudonyms as central reference points for implementing security mechanisms. For the log analysis itself, this entails that a pseudonym and the associated time and GPS position can be represented on a digital map, in order to visualize the analysis. An example of such a visualization is given in Figure 6.8. In this Figure, the x-axis of the digital map represents the longitude value of the GPS position, the y-axis the corresponding latitude value. Green points represent entries of the log which have not been considered for analysis operations yet, blue points and associated arrows with a continuous line represent a trace that has already been created. Arrows with a dashed line indicate sample possibilities for continuing the trace creation. An established trace can be re-identified w.r.t. attributes that are implicitly associated with a pseudonym via registration information. An example of a re-identified trace is shown in Figure 6.9.

The procedures employed within a log analysis, as specified in Section 6.5.2, are

based on secure multiparty computation protocols, i.e. computations on encrypted data, which is possible since pseudonyms are created as re-encryptions of ElGamal ciphertexts. The linking and re-identification procedures are jointly executed by the audit officers and the data protection officer. This requires that each officer agrees to the execution by providing the partial input to the broadcast channel, which is also called a bulletin board and implemented by a bulletin board server. The bulletin board server synchronizes the distributed computations, i.e. it aggregates the partial results of every officer. Also, it creates a transcript of every executed procedure. The transcript includes pseudonym-based references to log entries, wherein pseudonyms are denoted as P_m, P_n in case of two pseudonyms that are linked, and as $\{P_m, P_n, ..\}$, in case a trace is considered. Also, the transcript refers to the operation that has been executed (linking, re-identification, disclosure) and a result of the operation, where applicable. Thus, a transcript includes the following content:

- Log entries indexed by P_m, P_n have been considered for linking. Linking result: true / false.
- Log entries indexed by $\{P_m, P_n, ..\}$ have been considered for re-identification w.r.t. attribute A. Re-identification result: true / false.
- Log entries indexed by $\{P_m, P_n, ..\}$ have been considered for disclosure.

These transcripts created by a log analysis constitute a transparency log. Associated transparency mechanisms are described in Section 6.5.5.

6.5.3 Disclosure Policy and Provision of Authorization Sets

Within the log analysis, officers jointly re-identify every created trace w.r.t. to an implicit attribute A. This supports that only minimal identity-related informations need to be disclosed in the course of an audit. Yet, the actual conditions and rules according to which attributes may be re-identified, i.e. the disclosure policy (cf. Section 5.2.2), have to be defined within the application context. The present approach supports a step-wise disclosure based on implicit attributes. A disclosure policy can basically be defined by means of organizational structures, which allows adhering to the need-to-know principle [6], i.e. to start a step-wise analysis on a coarse level.

For example, the disclosure policy may state that the first re-identification shall be executed w.r.t. to an organizational attribute, e.g. "Police". The consecutive re-identification steps may then test whether roles within an organization are satisfied (e.g. the attribute "First Responder"), or check against existing team structures (e.g. the already given example of the attribute "Response Team Alpha"). Every implicit attribute refers to an authorization set, that needs to be defined by the registration authority. The definition of an authorization set proceeds according to the mechanisms introduced in Section 6.5.2. In order to do so, the RA firstly selects the base pseudonyms of the relevant entries of the registration list and then anonymizes them by means of a verifiable mixnet. The resulting authorization set

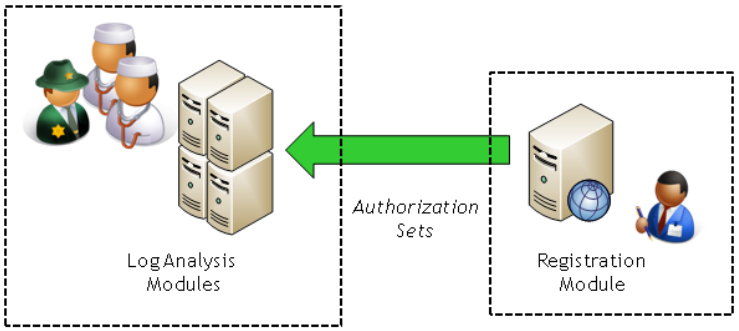

Figure 6.10: Provision of authorization sets

is then provided to the officers, which derive a blind reference set from it. This provision is also shown in Figure 6.10. Blind reference sets can be reused, i.e. multiple re-identifications w.r.t. to the same represented attribute can be executed.

Technically, implicit attributes have a set-based representation. This allows formulating the disclosure policy additionally in terms of anonymity, since anonymity is defined according to the size of the anonymity set. For example, a disclosure policy might state that a re-identification step has to be based on an anonymity set with cardinality of 20.

6.5.4 Mechanism for Individual Log Access

In order to resolve disputes, a mobile user U_i may access data recorded in the log that relate to herself. In order to do, she selects an entry k of the log by handing out authentication information in form of an aggregated random factor $r_{i,A} = \sum_{j=1}^{j=k} r_{i,j}$ and the base pseudonym $P_{U_i,B}$ to the access control mechanism of the log, i.e. the policy decision point. After verifying, whether the pseudonym indexing the log entry k matches the reconstructed transaction pseudonym $P_{U_i,k}$, the user receives a tuple *time - location*. This may additionally by certified by the audit officers. The user can use the tuple to repudiate location- and time-dependent accusations against her. The protocol for individual log access is also given in Figure 6.11.

6.5.5 Transparency Mechanisms

Transparency mechanisms implement a second level of accountability within our approach, i.e. audit officers can be made accountable for violating the disclosure policy within an audit log analysis. Our transparency mechanisms have two components:

- Firstly, a data protection officer is involved in the auditing and has to agree in order to execute any operation within an log analysis. Thus, the *DPO* can

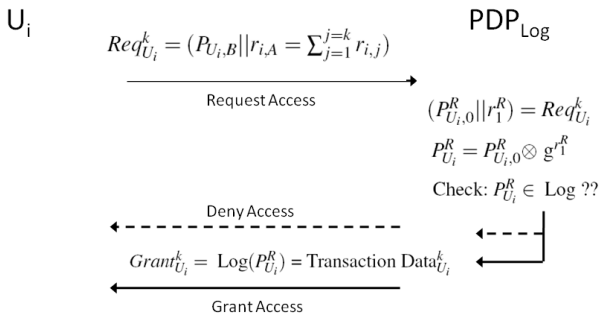

Figure 6.11: Protocol for individual log access

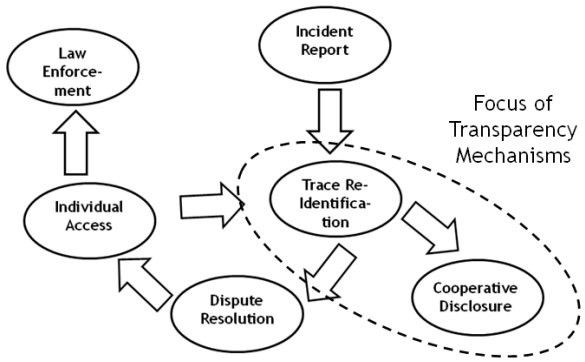

Figure 6.12: Transparency within auditing process

provide details on the analysis and on the decision process to every requesting user.

- Secondly, the transcripts created by a log analysis constitute a transparency log. This log can be accessed by a user to decide whether the investigations have been executed according to the disclosure policy.

Figure 6.12 shows the scope of the latter mechanism within the complete auditing process.

In order to implement it, we propose that an affected user may selectively access the transparency log, in order to verify all entries indexed by pseudonyms that relate to herself. As in the case of individual log access, transaction pseudonyms are the reference points for implementing an selective access mechanism, this time to the transparency logs. In order to access the transparency log, a user provides her base pseudonym $P_{U_i,B}$, her chosen seed value and the index of her last generated transaction pseudonym to the access control mechanism of the transparency log. The access control mechanism firstly reconstructs every transaction pseudonym the

user has provided within an location update by iteratively reencrypting the base pseudonym. Then it selects every entry of the transparency log that contains a transaction pseudonym that is present in the afore created list of used transaction pseudonyms. The entries of the transparency log are handed out to the user. They document the auditing actions that have been induced on log entries that relate to the user herself.

6.5.6 Scenario and Application Example

Having described the mechanisms for auditing, we now provide a descriptive example that shall illustrate how the presented approach can actually be employed in practice. Again, the example takes place in an emergency response context.

We assume the scenario that a large airport is affected by a large scale emergency. Several airplanes have caught fire due to an accident. The burning is spreading over to the terminal buildings. Since the fire brigade of the airport is unable to handle the situation on its own, additional forces from nearby fire departments are requested. Also, a local fire department sends a group of 50 mobile first responders to support the rescue missions. Arriving at the airport, the first responders register to the system.

During the course of the successful rescue mission, their movements and positions are continuously sent to the control center and stored in the audit log. After successfully managing the emergency, a group of airport officers is appointed to analyze a specific incident which has been reported to them by an anonymous eye witness: it is mentioned that a group of 4 firefighters suddenly disappeared from an important task to extinguish fire in an office wing, located in the vicinity of a jeweler in the shopping area. The store reports that expensive items have disappeared, and several offices have been destroyed due to the lack of man power. Analyzing the log, the officers manage to identify traces of 5 pseudonymous users that move away from the office wing in question (by linking log entries). Moreover, the 5 traces can be re-identified to belong to a local fire department (by re-identifying implicit attributes). On request, the responsible local commander asserts that a group of his first responders decided to change a mission task, due to the observation of strange knocking sounds nearby. While, in that case, the commanders information suffices to resolve the dispute on the incident in question, the concerned firefighters could have also used the individual log access functionality, in order to document the actions during the mission.

6.6 Summary

This chapter provided the details of the mechanisms relevant to our integrated approach to multilaterally secure pervasive cooperation. Continuing our scenario-oriented presentation, the mechanisms were illustrated in the context of location-aware first response. In particular, our presentation included setup, registration,

communication, location tracking as well as auditing and transparency mechanisms. We contributed:

- a novel representation of digital identities which supports mobile users to be addressable in communications, to be able to provide pseudonymous location updates, to be re-identifiable in a log analysis and to individually access log content. The proposed representation is organized in three logical layers; on the user's side, a personal communication device provides the digital container, platform and technical trust anchor of this approach.
- a trusted registration process; registered users are enabled to participate in cooperative rescue missions. The registration complements our digital identity representation as the main organizational trust anchor of our work.
- a protocol for end-to-end secure attribute-based messaging; the proposal supports protection against replay attacks, non-repudiation of senders and documentation of readers. In addition, we provided novel use cases for ABM concepts. This included the capability to query human sensors, which we thus added to the literature.
- a novel auditing process; in contrast to previous work, a stepwise process is introduced. It is more closely designed according to human-oriented dispute resolutions. As part of this process, means for individual access to audit log content were provided. We showed how to implement a policy decision point that leverages transaction pseudonyms as central reference points. In addition, we gave a descriptive application example of real-world auditing capabilities. Differently to existing work, our proposal can flexibly be instantiated with and without law enforcement capabilities.
- transparency mechanisms that make use both of a data protection officer as well as of transparency logs; such logs can be accessed despite the fact that affected users are pseudonymous.

Having now completed the description of our novel concepts and mechanisms, we will evaluate our proposals in Chapter 7.

7 Evaluation and Discussion

This thesis addresses IT security and privacy aspects of cooperative pervasive systems. It aims to develop concepts and mechanisms for what we denote as *multilaterally secure pervasive cooperation*. Yet, evaluating the achieved state of security of a pervasive system is a challenging task. Showing that our devised mechanisms fulfill the protection goals that were elicited in Section 2.4 thus requires to consider different conceptual and technological layers interwoven within the proposed approach. In order to support the claim that our goal is reached by the contributions presented in this thesis, this chapter evaluates and answers the following main questions:

- Are the proposed mechanisms technically feasible? Can they be realized within the setting they are presented in, under realistic assumptions?
- Are the proposed mechanisms secure? Do they fulfill the protection goals as stated?
- Are the proposed mechanisms appropriate to potential users? Under which circumstances could they be used in practice?

In order to answer these question, we built proof of concept implementations and conducted practical experiments with the prototypes. In addition, we conducted a security analysis of the mechanisms. Both are presented in this chapter. The security of our pseudonym construction is additionally supported by an independent security evaluation conducted by an external expert. Moreover, we report on experiments with potential real users, based on a preliminary ABM prototype, that supported the design process. In order to assess limits and circumstances for a practical use of pseudonymized location traces in dispute resolutions, we conducted simulated court cases as part of a juridical simulation study. Additionally, in this chapter, we will elaborate on the applicability of our contributions to further settings and relevant application contexts beyond emergency response.

The remainder of this chapter is organized as follows. Section 7.1 sketches the prototypes. Section 7.2 analyzes the main mechanisms w.r.t. the fulfillment of the security requirements. Appropriateness considerations are presented in Section 7.3. The general applicability of our concepts is discussed in Section 7.4. We summarize this chapter in Section 7.5.

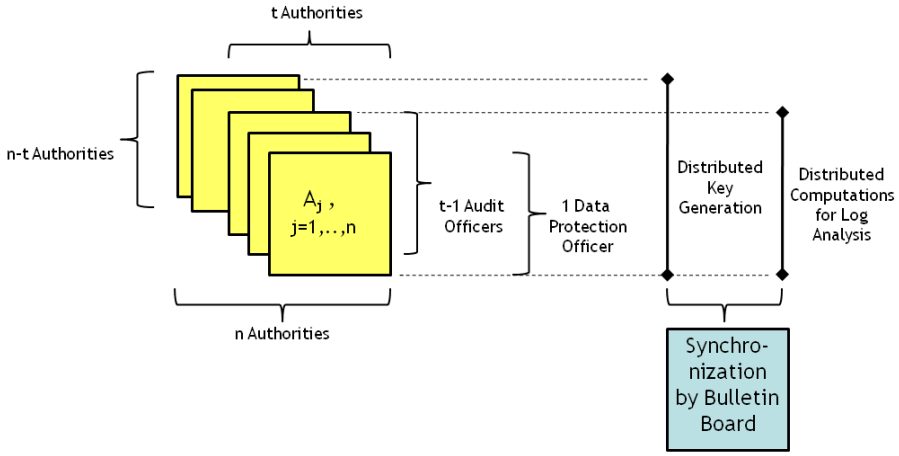

Figure 7.1: Architecture for distributed cryptographic mechanisms

7.1 Technical Feasibility

As part of this work, prototype implementations of the core mechanisms proposed in this thesis have been developed. Implementing a certain approach is a good way to find out the obstacles of theoretical concepts and thus to develop a deeper understand of the material. In particular, our prototypes serve as proof of concept and thus support the claim that our contributions are technically feasible within realistic settings. Beside descriptions of the prototype implementations, we also report on relevant issues related to resource consumptions of our mechanisms.

7.1.1 Prototype of Auditing Mechanisms

In this section, we briefly describe the prototype implementation of multilevel linkable transaction pseudonyms and the auditing mechanisms which build upon them. The description includes a simple application example, which shows some of the main processes realized within the prototype.

The proposed mechanisms have been implemented in the Java programming language, which offers APIs for the development of IT security and cryptography-related software: the Java Cryptography Architecture (JCA) and the Java Cryptography Extension (JCE). Additionally, in some parts of our work, we leverage the FlexiProvider toolkit[1], which provides cryptographic base mechanisms suitable for applications that are implemented according to the JCA.

The prototype supports the generation of pseudonyms and pseudonymized location updates as well as the storage in audit logs and the consecutive analysis of log content. For the generation of location updates and thus the definition of entries in audit logs, we follow a simulation-based approach. I.e. we developed a module that

[1] See WWW.FLEXIPROVIDER.DE

generates the traces of mobile users. A view of the architecture supporting the distributed cryptographic mechanism for the audit log analysis is given in Figure 7.1. In our work, we follow the proposal found in the research literature that the communication channels underlying the schemes are represented by a bulletin board, i.e. a software module that stores and synchronizes the partial inputs of the authorities [118] (cf. Section 4.1.2, Figure 4.1 and Section 6.5.2). The prototype can flexibly handle different distributions of power w.r.t. the threshold parameters t and n and different strengths of encryption, which have a direct effect on the bitlength of every transaction pseudonym. In order to illustrate the functionality of the prototype, we describe a simple and reduced example in the following[2].

Example

In the given example, the initial setup phase (cf. Section 6.1) is skipped, and a security level of 32 bit[3] is chosen. This is necessary for the pseudonyms to remain reasonably displayable on the given sheet of paper, since the chosen level of security has an effect on the length of pseudonyms that will be shown in a numerical representation[4].

The example consists of three steps.

- Firstly, in Figure 7.2, the creation of a registration list is shown. Here, we deliberately use only two real world names, Bernhard Wolf and Georg Schweer, in order to draw the reader's attention to these two entries. For the other entries of the registration, we make use of the wild-card names Person03 to Person10.
- Next, an excerpt of audit log content that was created in the same setting is given in Figure 7.3. It especially shows the concept of transaction pseudonyms. Here, only three location updates are shown. Every entry relates to the same user. Yet, each entry of the log is associated to a different transaction pseudonym.
- To conclude the example in a meaningful manner, in Figure 7.4 the result of a pseudonym disclosure is shown[5]. Here, the role reference is discovered. By relating it to the registration list, the name of the accountable mobile user, in this case Berhard Wolf, can be completely recovered.

The depicted example has been part of a simulated court case in a juridical simulation study [205]. This issue will be discussed in Section 7.3.1.

[2]The example does not include partial re-identifications, which are nevertheless supported by the prototype.

[3]The security level relates to ElGamal security, not to symmetric security.

[4]Choosing a higher security level would result in a longer numerical representation of the pseudonyms. Displaying a pseudonym that was created according to a security level of 64 bit e.g. results in a numerical representation as follows: 5138434074120674335-6719133392833443198.

[5]During a log analysis, further entries stored on a bulletin board have been created. To keep the example simple, they are not displayed.

```
_____________________________
PHASE 2: [REGISTRATION]
Registering User Identities and Base Pseudonyms...
_____________________________
_____________________________
Retrieving Pre-Configured User Data...
_____________________________
Processing User Data...
_____________________________
Adding: BernhardWolf as FirstResponder01 with Reference 100
Adding: GeorgSchwer as FirstResponder02 with Reference 200
Adding: Person03 as FirstResponder03 with Reference 300
Adding: Person04 as FirstResponder04 with Reference 400
Adding: Person05 as Paramedic01 with Reference 500
Adding: Person06 as Paramedic02 with Reference 600
Adding: Person07 as Paramedic03 with Reference 700
Adding: Person08 as Driver01 with Reference 800
Adding: Person09 as Driver02 with Reference 900
Adding: Person10 as Driver03 with Reference 1000

_____________________________________________-
REGISTRATION LIST
(Index - Name - RolePseudonym - RoleReference - Base Pseudonym)
_____________________________________________-
[01] : BernhardWolf - RP: FirstResponder01 - RR  100 - BP: 2327035730-3970910689
[02] : GeorgSchwer  - RP: FirstResponder02 - RR  200 - BP: 3270964552-3741210949
[03] : Person03     - RP: FirstResponder03 - RR  300 - BP: 113144732-1699819696
[04] : Person04     - RP: FirstResponder04 - RR  400 - BP: 3709931940-2188511534
[05] : Person05     - RP: Paramedic01      - RR  500 - BP: 771281733-3970351984
[06] : Person06     - RP: Paramedic02      - RR  600 - BP: 3123205367-439359092
[07] : Person07     - RP: Paramedic03      - RR  700 - BP: 2423575764-2908341115
[08] : Person08     - RP: Driver01         - RR  800 - BP: 447471167-3429229704
[09] : Person09     - RP: Driver02         - RR  900 - BP: 117147067-2519668730
[10] : Person10     - RP: Driver03         - RR 1000 - BP: 3237584808-1415347053

_____________________________
[REGISTRATION] successfully completed!
_____________________________
```

Figure 7.2: Example: registration

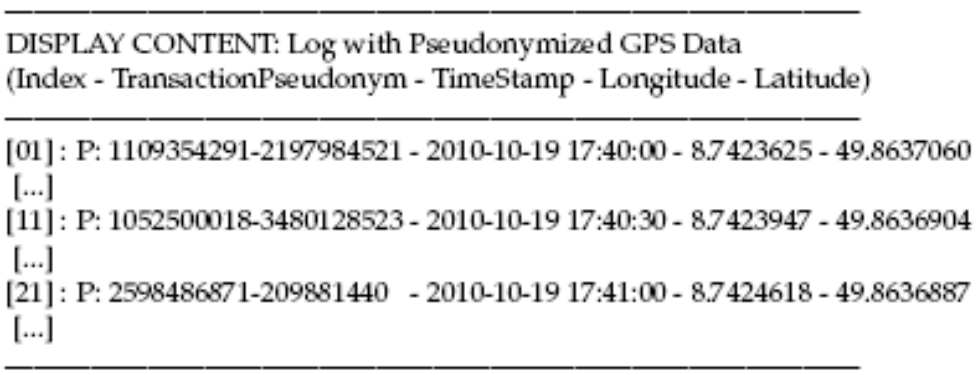

Figure 7.3: Example: excerpt of audit log content

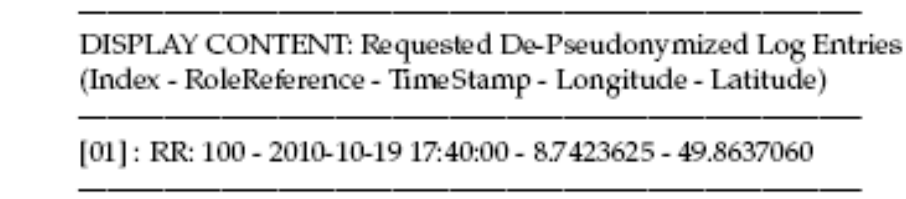

Figure 7.4: Example: disclosure of a pseudonym

7.1.2 Storage Overhead induced by Transaction Pseudonyms

In this section, we elaborate on the issue of storage overhead that arises due to the use of pseudonyms with implicit attributes.

Due to the proposed construction, a transaction pseudonym is represented as two elements of the algebraic group underlying the ElGamal system. Every value thus refers to one group element, and the bit length of the group element is directly depending on the chosen security level. As argued before, in order to keep the previous example presentable within this thesis, we have chosen a security level of 32 bit. In this setup, a single transaction pseudonym is represented by two numerical values, e.g. 1109354291 and 2197984521 (cf. Figure 7.3).

In a practical application, the security level has to be chosen such that brute-force-attacks on the pseudonymized data is rendered impossible. Given 32 bit symmetric security, there may be at most 2^{32} keys that need to be considered for brute-force decryption. Current security catalogues propose a level according to 100 bit symmetric security [34] for practical applications of legally binding digital signatures.

Security (in bit)	**No. of** Entities	**Frequency** (per min.)	**Duration (in hours)**	**No. of Stored Pseudonyms**	**Storage (in GB)**	**Payload (in GB)**
256	100	2	10	120 000	0.01	< 0.01
256	100	6	10	360 000	0.02	< 0.01
256	500	2	10	600 000	0.04	0.01
256	500	6	10	1 800 000	0.11	0.02
256	100	2	500	6 000 000	0.36	0.06
256	100	6	500	18 000 000	1.07	0.20
256	500	2	500	30 000 000	1.79	0.34
256	500	6	500	90 000 000	5.36	1.01
1024	100	2	10	120 000	0.03	< 0.01
1024	100	6	10	360 000	0.09	< 0.01
1024	500	2	10	600 000	0.14	0.01
1024	500	6	10	1 800 000	0.43	0.02
1024	100	2	500	6 000 000	1.43	0.06
1024	100	6	500	18 000 000	4.29	0.20
1024	500	2	500	30 000 000	7.15	0.34
1024	500	6	500	90 000 000	21.45	1.01

Table 7.1: Storage requirements

Thus, the main storage requirement that is induced by our pseudonym construction is given by two group elements per transaction pseudonym. The bit size of each group element depends on the chosen security level. In case that 1024 bit security for ElGamal is chosen, every transaction pseudonym thus requires about 2 KB of storage. Additionally, the frequency of location updates also largely impacts the storage requirements.

Table 7.1 contains the calculated storage requirements for representative scenarios. The setting is as follows: we present calculations for a medium (256 bit) and a high level (1024 bit) of security. Moreover, we distinguish between average scale (100 entities) and large scale (500 entities) rescue missions. We assume that every entity sends a pseudonymized location update every 30 seconds or 10 seconds. For the duration of missions, we distinguish between single missions of 10 hours as well as a yearly requirement of estimated 500 hours (of location tracking). In the table, the column *No. of Stored Pseudonyms* refers to the total number of transaction pseudonyms (and thus entries of the location audit log) that are created and stored according to the given scenario. The column *Storage* shows the resulting calculated storage needs for the transaction pseudonyms only, taking into account that each pseudonym is represented as two group elements. The storage requirement for the additional payload of timestamps and GPS coordinates is given in the last column, assuming 96 bit of payload per log entry[6].

We conclude that, in sum, our approach has an reasonable overhead that can easily be met by current data storage systems, even considering that every transaction pseudonym may require up to several KB of storage, depending on the underlying group. In particular, the approach can be instantiated over elliptic curve groups, such that a comparable level of security can be achieved at much smaller key sizes, i.e. 160 bit instead of 1024 bit. In this case, the storage requirement roughly corresponds to the 256 bit level of Table 7.1.

For the mobile communication device of mobile users, the storage is even more efficient. Only the index of a transaction pseudonym w.r.t. the output of the PRNG must be stored beyond a transaction lifetime, since every pseudonym can be reconstructed by the user.

7.1.3 Prototype Implementation of ABM

Our approach to end-to-end secure attribute-based messaging and the underlying hybrid encryption technique have been developed in a two-step approach. Firstly, an initial ABM prototype was created in order to enable a cognitive walkthrough with potential end users of this novel communication approach (cf. 7.3.2). The findings contributed to the final design and lead to a second prototype, which is briefly described in the following.

Our ABM prototype implementation consists of several main components. A messaging center represents the tool for the central user that supports the sending of messages. The messages can be received, decrypted and displayed by clients. One variant of the client is tailored for desktop PCs, one for standard mobile devices. The components encompass protype implementations of the encryption technique, which supports the end-to-end encrypted sending and the decryption of a message after reception.

[6]Depending on the implementation of the log, additional storage will be required. We do not take this into account for our calculations.

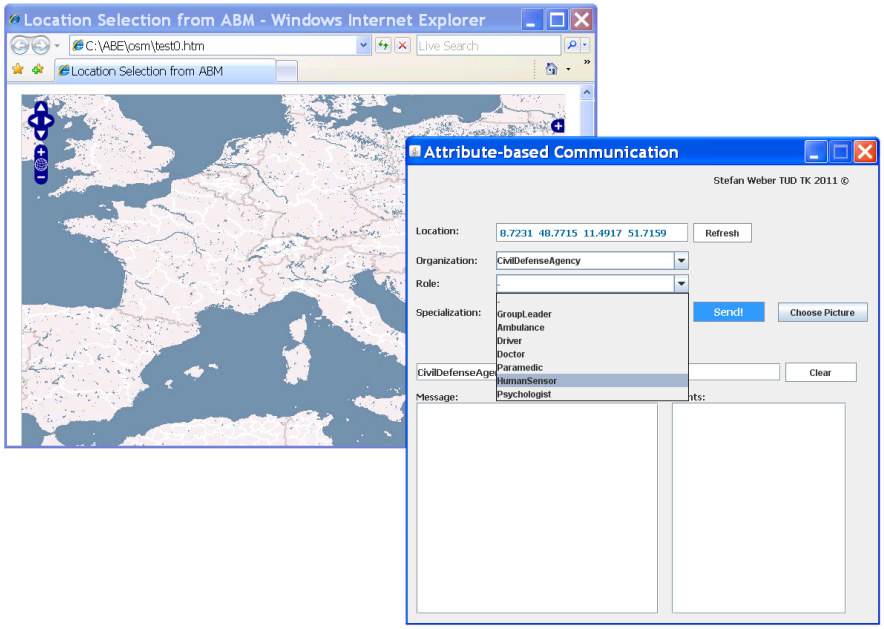

Figure 7.5: View of messaging center

A view of the messaging center is given in Figure 7.5. In consists of two parts, comprising a digital map and an user interface for the definition of static attributes and textual messages. The latter part is based on the programming language Java. Here, the sender may select attributes related to organizations, roles and specializations from pre-defined lists of existing attributes and textually enter the content of a message. The selection of location attributes makes use of a digital map that is displayed in an Internet browser. It harnesses digital maps provided by OpenLayers [7]. Here, the user may specify a location attribute by selecting a geographic region on the digital map. Derived GPS information is then synchronized with the other part of the messaging center, in order to complement the specification of the sending policy. In Figure 7.6, a view of the desktop client if given. Additionally, Figure 7.7 gives an example of a message that could not be decrypted by the receiver, i.e. the policy could not be satisfied.

The underlying encryption technique was implemented in the C programming language. In particular, C was chosen for efficiency reasons, in order to speed up the cryptographic operations in comparison to a Java implementation. For parts of the prototype, the following cryptographic libraries were used:

- Advanced Crypto Software Collection: Ciphertext-Policy Attribute-based Encryption[8]

[7] See HTTP://WWW.OPENLAYERS.ORG/.
[8] See HTTP://ACSC.CSL.SRI.COM/CPABE/.

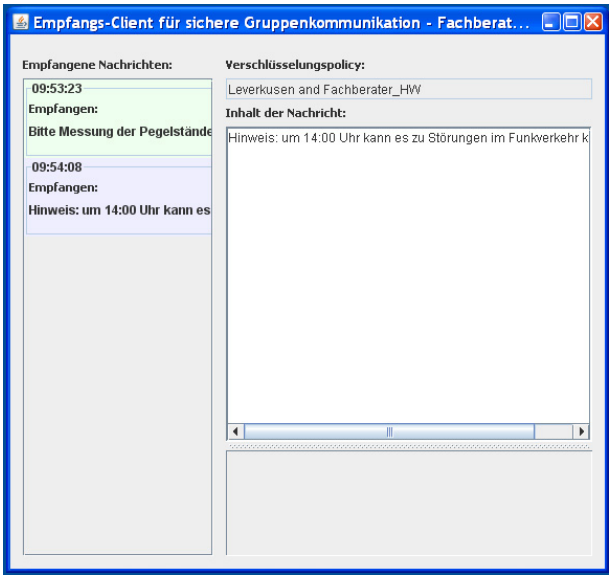

Figure 7.6: View of client for desktop PCs

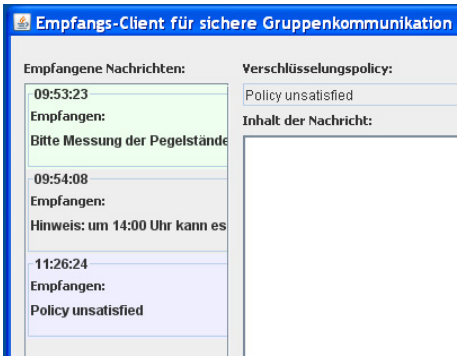

Figure 7.7: Example of unsatisied policy

- PBC Library: The Pairing-Based Cryptography Library[9]
- GNU MP Bignum Library[10]

7.1.4 Resource Consumptions of ABM

In order to assess the resource consumptions of our approach to end-to-end secure attribute-based messaging, a variant of the receiving clients has been developed for standard mobile devices. In particular, we chose a HTC P3600 smart phone as reference platform[11]. This device supports Windows ME 5.0[12] as operating system.

On this platform, we conducted runtime measurements to support the claim that our approach is compatible to resource constrained devices[13]. Here, the main focus of our investigation is whether decryption is possible in real-time on mobile devices. Following proposals in the research literature, our prototype implementation harnesses a 160 bit elliptic curve group. In particular, it was constructed on the curve $y^2 = x^3 + x$ over a 512 bit field. This curve is denoted as pairing group in the following. In pairing groups, the bit security is measured by multiplying the underlying group's field size with the embedding degree of the group [159, 124]. In our experimental setting, we chose a 512 bit base field with an embedding degree of 2, thus the bit security is considered equivalent to 1024 bit RSA security[14]. We consider this setting as appropriate for emergency communications.

We executed 20 experiments in the described setting. We chose messaging policies of maximum complexity w.r.t. pairings, i.e. the policies included three attributes related to CP-ABE. The length of the textual messages varied between 20 and 60 characters. The measured decryption time varied between 2.4 and 2.7 seconds on the chosen platform, which we consider as real-time.

We conclude that our proposal is suitable even for resource-constrained mobile devices. The most time consuming operation is the decryption on a mobile device. On a conceptual as well as on an implementation level, there is further space for optimization of the encryption operations, which we consider as future work.

7.2 Security

In this section, we provide an analysis on the fulfillment of the security requirements that were defined in Section 2.4. Since the requirements are split up in two sets, also the discussion has two main parts.

[9] See HTTP://CRYPTO.STANFORD.EDU/PBC/.

[10] See HTTP://GMPLIB.ORG/.

[11] See HTTP://WWW.HTC.COM/DE/PRODUCT/P3600/SPECIFICATION.HTML.

[12] See WWW.MICROSOFT.COM/WINDOWSMOBILE.

[13] In the literature, complementary runtime measurements and experiments can be found. In [116], Jacobi discusses the applicability of attribute-based encryption to wireless sensor networks. Experiments relevant to vehicular ad hoc network scenarios are reported in [110]. Traynor et al. [218] investigate the application of ABE to conditional access systems such as pay-per-view television.

[14] A table for comparison of bit security levels can be found in [140].

In the first part, we analyze the proposed approach to multilaterally secure auditing, including the underlying pseudonym technique. In the latter part, we address our approach to attribute-based messaging, including the hybrid encryption technique that we build upon.

7.2.1 Security Analysis of Auditing

We next discuss the fulfillment of the security requirements relevant to auditing.

- `SReqA1: Data minimization`: From the users' perspective, individual privacy within the location tracking is protected due to the use of transaction pseudonyms. Additionally, location tracking is restricted to the active state, such that, in sum, *data minimization* w.r.t. identifiers that are directly associated to users is given within our approach.
  However, the approach is tailored within the context of emergency communications, where parties use dedicated digital radio networks with own security infrastructure, e.g. according to the TETRA standard[15]. Thus, complementary security measures are provided by the host network, where further identifiers cannot be avoided. Yet, this is not considered within our adversary model (cf. Section 5.4), only the pseudonymized identifiers are chosen for the auditing. Here, every user is able to adjust the frequency of pseudonym changes and of location updates sent to the control center, thus she is empowered to adjust the temporal granularity of linkability within an audit log.
  Yet, since such a log also supports the user, sending frequent location updates is also aligned with a user's own interests, in the sense of multilateral security.

- `SReqA2: Individual access`: In order to implement an *individual access* functionality, which supports defending against false accusations and thus could actually entail legal effects[16], the underlying approach to pseudonym authentication needs to assure a uniqueness property.
  Especially, it must not be possible for an adversary[17] to provide authentication information for a pseudonym without being the real originator. This is achieved in our construction due to a two-factor authentication process: The users needs to provide both the base pseudonym and the aggregated random factors. An adversary could only try to guess base pseudonym and matching aggregated random factor, since she cannot access the seed to derive correct values, which is generated and stored only locally.

[15] Cf. WWW.TETRAMOU.COM.

[16] The acceptability of GPS tracking information as evidence in court proceedings is also a legal issue. In a trial, it has to be considered if evidence of *having been at a certain location* is acceptable and actually relates to *having committed a certain action*. From a security point of view, this boils down to the question, whether the location tracking infrastructure is trustworthy, which is, in fact, a core assumption of our approach. We provide a further treatment of this issue by describing and discussing simulated legal trials and court cases in Section 7.3.1.

[17] In that case, the adversary could be a further mobile user of the location tracking system who tries to fake evidences.

Moreover, the probability to succeed with such a bruteforce attack can be lowered by requiring a user to authenticate multiple consecutive log entries.

- `SReqA3: Privacy-respecting log analysis / SReqA4: Minimal disclosure`: As proposed, log analysis boils down to creating user traces within a log, harnessing two main operations (cf. Section 6.5.2). This is even possible in pseudonymized logs, since the underlying pseudonym approach supports these operations.
  The properties of the pseudonym construction stem from a semantically secure encryption operation, thus transaction pseudonyms do not leak information about the implicit attributes and the encoded reference value.
  Moreover, no single audit officer is able to decrypt a pseudonym and thus to link a pseudonym to a user. This is achieved since pseudonym creation is performed as encryption operations of a threshold cryptosystem, and registration information is still required for resolution of reference values. Therefore, officers have to cooperate in every step of the log analysis, implementing a distribution of power and operational separation of duty in our system. In sum, a *privacy-respecting log analysis* is given.
  The log analysis is complemented by methods for partial re-identification. The first linking operation offers *minimal disclosure* due to the direct application of plaintext equality tests [118], i.e. it directly exhibits the privacy property of secure multiparty computation.
  Differently, in the proposed set lookup approach, the equality test is executed by means of deterministic fingerprints, thus semantic security is not satisfied for this operation. This approach is required in order to make reference sets reusable, and only additional information from comparing fingerprints could be maliciously derived. Yet, this is within the capabilities that opponents are ascribed to within our adversary model w.r.t. multilateral security, which aims at dispute resolution. In particular, the process of auditing has to comply to a disclosure policy, which encodes the rules for the re-identification of mobile users[18]. The compliance to this policy is assured by means of the transparency mechanisms, see below.
  In addition, for the creation of reference sets, the anonymizing property of the mixnet supports blinding. Technically, the mixnet harnesses semantically secure ElGamal reencryption.

- `SReqA5: Distribution of powers / SeqA7: Law enforcement`: The proposed construction allows flexibly representing several *distributions*

[18] An *inside adversary* (cf. Section 5.4.2) could aim to reduce a user's degree of anonymity by correlating background knowledge and reference sets of several consecutive steps of partial re-identification. The resulting intersection of two or several reference sets (and thus anonymity sets) is possibly smaller than each of the sets. In the literature, comparable attacks on anonymity techniques are known as *intersection attack* [16, 247, 130]. We address this issue only by means of the disclosure policy, i.e. we explicitly allow certain kinds of consecutive re-identification steps. In particular, we consider the definition of intersection-attack-resistant disclosure policies as future work.

of powers. In particular, this flexibility builds on the use of a (t, n) threshold ElGamal cryptosystem as well as the distributed computation of linking operations.
In Chapter 5, we proposed a basic setting, which can flexibly be tailored to different application needs. Due to its flexibility, the complete approach can e.g. also be instantiated without a data protection officer. Firsthand, the approach can also tolerate the failure of at maximum $n - t$ authorities, which may be due to unavailability or due to corruption. Additionally, the robustness of the scheme stems from its ability to tolerate attacks against officers or failures of them, without corrupting the whole system. Technically, this builds on the property of Shamir secret sharing that any number of shares below the threshold yield no partial information about the key.
However, we require the registration phase to be trustworthy, since it depends on a single registration authority RA, which is contrary to the distributed design of the rest of the schemes.
Also, the *law enforcement* authority LEA represents a single TTP. However, the scheme can be instantiated without LEA, if not required in a certain application context. In that case, the initial generation of SK_{LB} is executed according to the distributed key generation protocol of Pedersen [172].
In addition, the power of the officers to completely disclose pseudonyms is restricted to re-identifying at most the reference value. Only in cooperation with the RA, the matching encrypted identity on the registration list can be retrieved.
Effectively, the RA thus implements an additional access control mechanism here. By encrypting the registration list under a second public key of the LEA instead of PK_{LB}, an additional distribution of powers can be implemented.
Variants in the encryption of the registration list can also be used to impose higher computational cost on the final disclosure step, if necessary.

- `SReqA6: Transparency`: The multilateral security property of the overall approach makes use of the principle of *accountability by auditability* on several levels: mobile users can partly be held accountable for real-world actions according to their presence and absence at certain locations during missions, due to the existence of location audit logs. Additionally, audit officers can be held accountable for their actions during the log analysis process, partly due to existence of transcripts of the cooperative log analysis. This second level of accountability is denoted as *transparency*.
  Especially, anyone who can read the transparency log can audit the log analysis process. Such a verifier can control whether the analysis has been executed according to the disclosure policy. Thus, this particular transparency mechanism requires individual efforts for controlling the transparency log in order to be enforced. Individual access to the transparency log itself is controlled by a generalization of the mechanism for individual access. Its security depends on the choice of unique seeds and the correct creation of base pseudonyms

within the registration process. Yet, we assume that the complete registration is trustworthy.
As a variant, transparency logs can be made accessible to larger groups of verifiers, in order to support a transparency mechanism with shared responsibilities for controlling the log.
A complementary support measure for transparency is given due the existence of a data protection officer. The *DPO* can individually give out information on the log analysis process, constituting a further social and organizational level of security.

Security Requirement	Main Security Mechanism
SReqA1: Data minimization	Unlinkable transaction pseudonyms (based on semantically-secure encryption) Restricted data collection Adjustable frequency
SReqA2: Individual access	Two-factor pseudonym authentication
SReqA3: Privacy-respecting log analysis	Separation of duty (based on trusted registration authority) Privacy-respecting trace creation (based on privacy property of SMPC)
SReqA4: Minimal disclosure	(Reusable) partial re-identification (based on set lookup) Anonymization by mixnet (based on semantically-secure encryption) Disclosure policy (enforced by transparency mechanisms)
SReqA5: Distribution of powers	SMPC / threshold cryptography (based on secret sharing of keys) Flexible instantiability, incl. *DPO* (based on key distribution)
SReqA6: Transparency	Individual access to transparency log (based on pseudonym authentication) Data protection officer
SReqA7: Law enforcement	Global decryption capability (based on trusted key generation) Variant without law enforcement (based on distributed key generation)

Table 7.2: Audit security requirements and mechanisms

In Table 7.2, we present the security requirements and the associated security mechanisms in overview. In particular, in our approach the fulfillment of protection

goals reduces to cryptographic assumptions, is based on partially trusted processes / authorities and is achieved by means of cooperative protocols and schemes.

7.2.2 Trust Requirements relevant to Auditing

Having analyzed the fulfillment of the protection goals, we next provide a complementary view of the security of the presented concepts by listing the trust requirements. Especially, we describe which parties within the auditing approach need to be trusted not to violate the ascribed behavior to which extent. Each listed trust requirement describes and refers to a risk that has to be addressed, in order to accomplish a trustworthy implementation and operation of a system [62].

Our discussion excludes *mobile users*, since the major issue is that real world actions during a rescue mission cannot easily be judged to be inappropriate. The presented approach shall support an ex-post handling of liability issues. Software modules are also only considered on an abstract level.

We identified the following trust requirements:

- The *registration authority* has to be trusted to enforce a correct registration phase, and to provide correct authorizations sets.

- The *mixnet* that is used by the *RA* is verifiable and thus does not need to be fully trusted. In particular, it can guarantee anonymization if at least one of the mix servers is honest and correctly executes the mixing phase[19]. Thus at least one mix server has to be trusted; otherwise a denial of service attack against the creation of blind reference sets (cf. Section 4.2.4) can be launched.

- A quorum of *officers* (i.e. a set of at least t officers, including *AOs* and the *DPO*) have to be trusted to execute an audit according to a specified disclosure policy, in order to achieve a dispute resolution. At least t out of n officers are required to execute steps involving shared keys. Yet, violations can be detected, based on the transparency mechanism, and even in case of collusion and direct decryption of a pseudonym, only the reference value and not the real world identity of affected mobile users is disclosed.

- The *bulletin board*, the *audit log* and the *registration list* have to be trusted to operate and store data correctly. A reliable communication subsystem is crucial for the whole auditing process.

We conclude that denial of service attacks represent the greatest risks within the approach. While such attacks are beyond the scope of this work, they could additionally be handled on conceptual, implementation as well as organizational levels (cf. Section 5.4.3).

[19] In particular, this requires reencrypting the ciphertexts with random values and randomly permuting the batch of all ciphertexts (cf. Section 4.1.2).

7.2.3 Independent Security Review of Pseudonymization Technique

The security evaluation of mechanisms can involve a certification of the achieved level of security, given by a third party. A common way is to rely on standardized evaluation procedures, e.g. according to common criteria. While such a certification is actually required in some application contexts, e.g. public security and emergency response, it is only reasonable for fully developed ICT products. It is rather inapplicable to scientific prototypes.

Yet, in order to support the present security evaluation, a main contribution of this thesis, the pseudonymization approach, has been assessed by an expert of the independent German trust provider TÜViT[20]. The expert acknowledged the correctness and trustworthiness of our approach, but imposed operational conditions for a real world usage [205, 206].

We will discuss this issue more closely in Section 7.3.1.

7.2.4 Discussion of Hybrid Encryption Technique

In the following two sections, we assess the security provided by our proposed approach to end-to-end secure attribute-based messaging. Firstly, we discuss the novel hybrid encryption technique. Then, then fulfillment of the security requirements relevant to emergency communication (cf. Section 2.4.3) is investigated.

According to Section 4.3.1 and Section 4.4.3, the proposed design of the hybrid encryption technique follows two main goals: achieving efficiency in handling continuous dynamic attributes and minimizing trust requirements in attribute authorities at the same time. We recap our design decisions and discuss the resulting level of security.

At first, handling dynamic attributes requires means for providing keys on mobile devices. An *online AA* (or online PKG) could principally solve the problem, but does not scale. An *offline AA* only allows handling dynamic attributes by preregistering all possible attributes to a local trusted activator. This is inefficient for continuous attributes. An *embedded AA* could be implemented locally on tamper-resistant hardware. However, it locally requires the master key and could generate all attributes of all users, such that the key escrow risk associated to a compromise is extremely high. Within our approach, we propose to conceptually split the role of the single *AA* (cf. Figure 4.12): an *offline CP-ABE AA* issues all static attributes in a registration phase, while an *embedded LBE AA* handles dynamic location attributes, based on tamper-resistant hardware.

W.r.t. to encryption security, the hybrid technique is designed such that the location-based encryption (LBE) parts adds a further level of security to the symmetric session key that is used for message encryption. In our approach, the XOR operation encrypts the initially generated session key comparable to an one-time pad [203]. Hence, decryption is only possible if the required CP-ABE attributes are available

[20] TÜViT (see WWW.TUVIT.DE) is specialized in evaluating the trustworthiness of IT security modules as well as their operational embedding.

to decrypt the outer asymmetric encryption layer and the location lock value can be generated correctly in order to recover the session key.

In most cases, messaging policies include a conjunction of location and further CP-ABE attributes (cf. Figure 6.6). Then, this approach retains encryption of messages even in case the *embedded LBE AA* is compromised.

Moreover, in case the CP-ABE attributes are compromised, a message is still protected by the additional location-dependent encryption layer. Thus, the hybrid encryption technique allows realizing end-to-end encryption while being able to handle expressive policies.

In addition, our proposal minimizes the use of pairings in the end-to-end encryption. This design broadens the applicability of the encryption technique to a range of mobile devices. In turn, the hybrid encryption technique looses full cryptographic collusion resistance w.r.t. the expressive policy. Yet, a collusion between receivers or adversaries that try trading CP-ABE attributes, e.g. in order to gain access to messages of further organizations, fails.

The hybrid encryption assumes tamper-resistant hardware, especially a tamper-resistant GPS receiver. In the emergency response application context, this assumption is practically fulfilled, e.g. by given TETRA mobile communication devices.

The application logic required to implement the location lock mapping and the location verification procedure is small, such that means to guarantee correctness based on certification procedures can easily be applied. Together with a secure software stack supported by a TPM chip of the mobile device [32], additional practical security guarantees could be given.

In some cases, a device may be unable to compute its current GPS position, e.g. inside closed buildings. To circumvent functional problems, we propose to internally rely on the last computed (and thus computable) GPS position in such cases.

7.2.5 Security Analysis of Communication Mechanisms

In this section, we discuss the fulfillment of the security requirements relevant to emergency communication.

- `SReq1: Basic security`: The basic security mechanisms of mutual authentication, message integrity and availability are given by the security architecture of the emergency communication network (cf. 5.3).
  Since the ABM scheme is realized on the end-to-end encryption layer, they apply to it, too. Especially, device revocation is possible by means of the network, without relying on additional cryptographic mechanisms on the application level.

- `SReq2: End-to-end confidentiality w/o online PKG`: End-to-end encryption in the messaging is given due to and implemented by the use of the proposed hybrid encryption technique on the end-to-end encryption layer. In particular, the enforcement of the LBE part of expressive policies hinges on tamper-resistant GPS receivers. In addition, computational security reduces

to the same computational assumptions as in CP-ABE. For more details, we refer to [17].
Collusion resistance is given as discussed in Section 7.2.4.

- `SReq3: Protection against replay attacks`: Replay attacks are handled on the end-to-end encryption layer: after decryption, the receiver verifies the freshness of the included message ID. The receiver rejects messages that contain an ID that she already decrypted. This mechanism requires that the message ID is unique due to its generation.

- `SReq4: Non-repudiation of senders`: Non-repudiation of senders is assured due to two mechanisms.
  Firstly, each message sent is added to the message log ML, for additional security digitally signed by the sender S. This record can later be analyzed.
  Secondly, each message includes a MAC, such that it can be linked to the sender, given that the registration information is correct.

- `SReq5: Documentation of readers`: Readers, i.e. the subset of all receivers of a message that satisfied the logical messaging policy, are documented via the readers list RL. In order to achieve this, readers have to send acknowledgements to the control center. The fulfillment of this requirement thus hinges on the compliance to the protocol for end-to-end secure attribute-based messaging (cf. Figure 6.5)[21].
  Unique mobile subscriber identities, $IMSI_R$, can be resolved to real world identities of readers, by linking them to information present on the registration list $RegL$.

- `SReq6: Efficiency of security mechanisms`: Efficiency of the proposed ABM scheme has computational and organizational factors.
  Regarding computational efficiency, our approach has a low pairing complexity. Firsthand, this is achieved by the design of the messaging policies (cf. Figure 5.4) as well as by the proposed hybrid encryption mode. In particular, the session key decryption requires one XOR operation for the LBE part. In order to decrypt the CP-ABE part of the policy, two pairing operations for every attribute that is matched by one of a receiver's attributes are required[22]. Yet, messaging policies are designed such that at most 6 pairing operations are required. Thus, the hybrid policy encryption technique together with the policy design render the decryption practically in real time on resource-constrained devices (cf. Section 7.1.4).
  From the organizational perspective, no online PKE is required, such that the

[21] For additional security, the software modules implementing the protocol can be certified by a trust provider.

[22] In case the approach would be extended to policies with additional internal AND-/OR-levels, one exponentiation operation would be required for each internal node from an attribute in the leaf to the root node of the CP-ABE policy part.

number of interactions that are required for the end-to-end key management are reduced to a single registration phase.

- `SReq7: Appropriateness to users`: Appropriateness to users is supported by the following factors.
  Firstly, our ABM approach allows for a single, combined realization of all necessary communication patterns `CP1–CP4` (cf. Section 2.4.2). It thus minimizes learning efforts.
  Secondly, our approach integrates continuous location attributes into the selection of receivers, which are intuitive selectors for senders.
  Thirdly, more generally, the approach has been designed based on insights that were derived from experiments with potential real users. We discuss this issue more closely in Section 7.3.2.

- `SReq8: Location privacy protection of receivers`: From the receivers' perspective, the given approach allows for an acceptable integration into personal lives, since privacy protection is given due to the following mechanisms.
  Firstly, every registered mobile user can be efficiently contacted and requested via an implicit addressing method that includes location. In particular, in our proposal this is possible without continuously disclosing identifying information along with location updates beforehand. Instead, the implicit addressing is based on broadcasts and local enforcement (by means of the hybrid encryption technique) on the mobile device[23].
  Secondly, upon activation unlinkable transaction pseudonyms provide privacy protection, as discussed in Section 7.2.1.

In Table 7.3, we list the security requirements and the associated security mechanisms in overview. The fulfillment of protection goals reduces to cryptographic assumptions and trusted processes. Moreover, the implementation of functionalities for implicit addressing on mobile devices (which in turn require trusted hardware) is a key mechanism to achieve privacy protection. In addition, our design is also based on experiences with real users. This issue is discussed in more detail in the following sections.

7.3 Appropriateness

In this section, we elaborate on the appropriateness and practicality of our work to realistic application scenarios. Firstly, we present results of a study that addressed the acceptability of pseudonymized location traces as evidence in legal disputes. Then, in Section 7.3.2, we describe experiments with a preliminary ABM prototype involving potential real users, that contributed to the final design.

[23]The privacy protection achieved by broadcast- and implicit addressing-based communication mechanisms is also denoted as *receiver anonymity* in the literature, cf. [177].

Security Requirement	Main Security Mechanism
SReq1: Basic security	Mutual authentication Message integrity Availability Device revocation (all given by underlying network)
SReq2: End-to-end confidentiality w/o online PKG	Hybrid encryption technique (based on offline and embedded PKG) (based on tamper-resistant GPS receiver) Collusion resistance (based on CP-ABE)
SReq3: Protection against replay attacks	Message ID (based on unique generation of IDs)
SReq4: Non-repudiation of senders	Message authentication codes (based on key distribution) Message log
SReq5: Documentation of readers	Acknowledgements (based on compliance to protocol) Message authentication codes (based on key distribution) Readers list (based on correct registration information)
SReq6: Efficiency of security mechanisms	Policy design Hybrid encryption mode (based on encryption technique) Offline key generation (based on registration)
SReq7: Appropriateness to users	Single communication mechanism Intuitive location selection Design tailored to end users (based on experiments)
SReq8: Location privacy protection of receivers	Broadcast Implicit addressing (based on local enforcement on device)

Table 7.3: Communication security requirements and mechanisms

7.3.1 Using Pseudonymized Location Traces in Legal Disputes

As part of this research, the acceptability of pseudonymized location traces in legal disputes has been evaluated. A legal dispute represents a highly demanding scenario, thus it is also appropriate to draw conclusions about application scenarios with less demands, as targeted by our work.

A major goal of the investigation that we report on in the following was to assess technologies that produce digital evidence in a realistic, yet safe environment, while both the technology and the juridical regulations are still configurable. As stated by Bratus et al., a critical issue in such settings is that "computer-generated evidence comes from an entity that cannot take an oath ensuring its intent of providing the truth" [30]. Thus, we aimed to identify the limiting factors towards the legal acceptability of digital evidence, in particular w.r.t. our approach to pseudonymous auditing presented in this thesis.

Setting

The present investigation was part of an interdisciplinary study. In particular, we conducted simulated court cases as part of a juridical simulation [185, 189], which included German layers, a judge and IT security experts. This so-called simulation study[24] was prepared and conducted at the Center for Advanced Security Research Darmstadt (CASED)[25] in 2010.

An impression of the course of a simulated court case is given in Figure 7.8. The study was organized by members of the PROVET group[26] from Universität Kassel, under the auspices of Prof. Alexander Roßnagel.

Assumptions

In the legal assessment some assumptions[27] were made, which are described next.

The application of the pseudonymization technique was considered in the technical and organizational context of digital emergency communication networks[28]. Especially, TETRA networks were considered. These networks are specifically tailored for mission-critical settings and thus satisfy stringent security and reliability requirements [141]. This is also true for the involved mobile communication devices, which are equipped with tamper-resistant GPS receivers.

Additionally, we assume that the devices may contain further associated functionalities, which are described in the next section. To enable mobile users to provide pseudonymized location information, a prior registration is required, in order to enable correct generation and re-identification of pseudonyms. The registration

[24] The underlying methodology is described by Roßnagel in [188].
[25] See HTTP://WWW.CASED.DE/.
[26] PROVET is the *Projektgruppe verfassungsverträgliche Technikgestaltung*, i.e. the project group for legally compliant technology design, see HTTP://PROVET.UNI-KASSEL.DE.
[27] These assumptions are in accordance to the assumptions that were stated throughout this thesis.
[28] In particular, this is a instantiation of the setting that is described in Chapter 5.

Figure 7.8: Impression of court case simulated at CASED

thus implements an organizational trust anchor and is assumed to having occurred correctly and trustworthy.

Court Case

In the study, we defined two representative court cases[29]. Every case describes a scenario and an associated legal dispute. We next sketch one of the cases[30].

In the given case, it is assumed that a first responder has been present at the location of a certain incident. The incident involved a famous person, and the responder allegedly took a digital picture documenting the scene with a camera integrated in his mobile device. The photo was sold by him to a newspaper, yet he did not receive the payment. Instead, the newspaper claimed that the picture was taken by an internal editor. The picture itself contained no GPS data attached, yet the first responder accessed the entries of the pseudonymized location audit log that shall help to document his presence. In a simulated legal trial, the judge had to decide whether provided re-identified GPS traces can be accepted as evidence.

Based on our prototype (cf. Section 7.1.1), we generated scenario-related evidence. The associated location traces are also shown in Figure 7.9 and Figure 7.10. These traces illustrate the (simulated) movement of the responder in a period of time relevant to the incident that was addressed by the court case.

[29] The simulation study covered 10 court cases, cf. [189]. We focus on the cases relevant to this thesis.

[30] Our other court case was less complex, in particular it was assumed that no additional functionalities were associated to the mobile devices. We focus on the description of the more complex court case, since it highlighted certain practical aspects that we elaborate on in the remainder of this section.

Figure 7.9: Sample location trace used as evidence, marked with dots

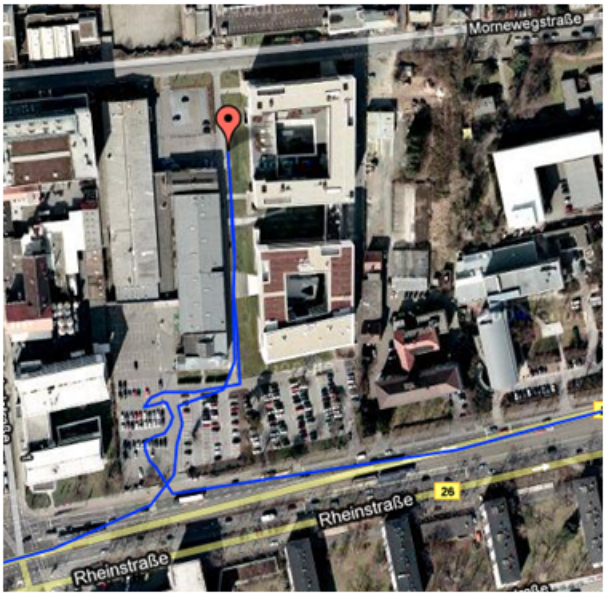

Figure 7.10: Sample location trace used as evidence, marked with blue line

Identified Limiting Factors

Within the study, a judge, who was supported by an IT security expert[31], investigated which conditions have to be met to consider de-pseudonymized location traces as legally acceptable evidence.

The main statement given is that the employed mechanisms were acknowledged to be secure, but the legal acceptability is not improved in comparison to traditional, non-digital evidence, e.g. human eye witnesses or testimonies. Yet, several factors were identified that can have a direct effect on the legal acceptability. We briefly elaborate on these factors in the following.

- *Date of registration:* the date of registration needs to be available to the court.
- *Role of registration authority:* the registration authority should not be part of an organization involved in the incident, in the given case a fire department. Such an internal registration authority would be considered a deficit in a real case.
- *Strength of encryption:* cryptographic parameters have to be chosen such that pseudonymity is protected against brute force re-identification attacks. The strength used in the sample settings was considered inappropriate for practical purposes, yet considered adequate to illustrate the functionality.
- *Association of user and device:* due to the approach, evidence was given that the registered device has been present at a certain location and time. Yet, this information does not indicate which legal person has actually carried the device. Further mechanisms to complement the association of user and device are thus required[32].

Conclusion

The identified factors indicate that special care has to be taken in order to turn theoretically secure approaches for generating digital evidence into practically secure and multilaterally acceptable systems. As argued, the main factors relate to the concrete setting and the particular instantiation of our approach; also several organizational factors have to be considered. In particular, the binding of device and user has to be free of doubt in order to generate legally acceptable digital evidence. This issue requires further research efforts that are beyond the scope of this thesis.

[31] This was the same expert that was introduced in Section 7.2.3.

[32] This issue could be approached by a biometric binding of device and user's identity [165], if a high reliability of the mechanism is given. Alternatively, electronic tags with a physical binding to the user, as they are used e.g. in the field of electronic monitoring of law offenders [219], could be applied. Yet, this type of solution raises additional acceptance issues. In particular, in our scenario a responder would have to be willing to continuously wear a RFID-enabled wristband or bracelet in order to support the binding of device and user. Comparable solutions are currently under investigation e.g. in health-care scenarios [115].

A general conclusion of the study is that the impact of digital evidence (with location traces being just one example) on a court decision is mostly dependent on the individual case. Especially, its impact has always to be considered in relation to further available non-digital evidence. In case that e.g. human witnesses can report on an incident, nowadays judges clearly prefer these. In case that such traditional piece of evidence is not available to a court, the trustworthiness of digital evidence is thoroughly assessed. In particular, in order to exclude manipulations of available digital evidence, one has to assess the relation of the interests and the costs associated to malicious behavior. In the court case that we reported on, this issue is e.g. reflected by the imposed constraint that a registration authority should be independent, in order to mitigate conflicts of interests.

In general, novel technologies have to be established over a long period of time, in order to be considered acceptable by judges and experts; the relevancy within legal disputes is thus also a question of habituation. In particular, the unknown side effects that are often inherent in immature technologies have to be minimized within the assessment of digital evidence. Foremost, this requires gaining experience.

In turn, we conclude that an application in contexts such as our targeted dispute resolution setting can prepare the subsequent usage of our proposal also in legally binding court cases.

7.3.2 Supporting Appropriateness of ABM to End Users

The design of our ABM approach draws from experiences and discussions with potential real users, i.e. first responders, decision makers and trainers from German police and fire departments as well as relief organizations[33]. It is beyond the scope of this thesis to provide a distinct, in-depth usability evaluation of the final prototype, yet, we discuss the user study as well the impact on our design decisions.

Iterative Design Process

The design of our proposal to end-to-end secure attribute-based messaging followed an iterative approach (cf. Section 2.4.1):

- We presented our initial proposal of an attribute-based messaging scheme and system for end-to-end confidential emergency communication both to the IT security research community (in [232]) and to the first response research community (in [231]).

- The associated prototype was used to initiate discussions and to conduct a user study with potential real users, based on a cognitive walkthrough[34] [21] of typical emergency communication scenarios.
  The study was supported by and executed together with an usability expert of

[33] This investigation was part of the research project SoKNOS, WWW.SOKNOS.DE.

[34] A cognitive walkthrough, an usability evaluation method, builds on practical user experiments with a system.

Fraunhofer IESE[35]. The experiments helped to understand how potential real users prefer to interact by and with an emergency communication system and ABM concepts, in particular.

- The findings of the study (cf. [251]) contributed to Section 2.4.1 and to our final ABM design and concept, as published in [237] and presented in this thesis.

In the following sections, we introduce the setting of the user study and describe the experiments that were executed by the participants. Furthermore, we summarize the received user feedback and the drawn conclusions.

Setting

Our study was part of an end user evaluation session of the project SoKNOS. During this session, potential real users and domain experts (cf. [250]) were confronted with prototypes of several novel mechanisms and concepts in the area of ICT-supported emergency management.

For our part, we recruited a set of 8 domain experts among the participants of the evaluation session. In particular, the population included:

- three emergency workers of German fire brigades,
- two decision makers of German fire brigades,
- one lecturer of the *Deutsche Hochschule der Polizei (DHPol)*[36],
- one decision maker of a German police authority,
- one executive manager of a software company that develops geographic information systems (GIS) supporting emergency management.

Each participant was given a printout of the documentation of the study[37] [233] as well as a brief oral introduction to the concept of attribute-based messaging and its proposed application to the area of emergency communication by a moderator. The participants were seated at a table. A computer screen on the table and a keyboard and a mouse were provided as input devices. The documentation of the experiments and discussions was supported by a minute writer.

Experiments

We requested the domain experts to participate in a particular cognitive walkthrough of emergency communication scenarios. Each participant was confronted with an

[35] The *Fraunhofer Institute for Experimental Software Engineering*, (HTTP://WWW.IESE.FRAUNHOFER.DE/), was a research partner in the project SoKNOS, which hosted the user study.

[36] The DHPol is an internal German state university for police executives.

[37] The documentation had also been electronically distributed several days before the user study among all potential participants.

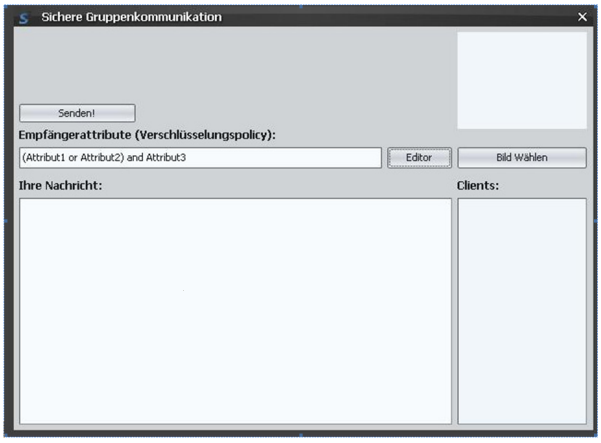

Figure 7.11: View of ABM prototype used for experiments

Figure 7.12: View of editor supporting policy definition

ABM prototype (cf. Figure 7.11) that supported a flexible definition of sending policies. In the proposed setting, the messaging policies were not restricted to a certain logical structure. Instead, arbitrary conjunctions and disjunctions could be used to specify readers. For the definition of policies, the participants were also supported by an editor (see Figure 7.12) that helped to define nested policies.

After the introduction, the participants were asked by a moderator to execute several messaging acts and define appropriate policies. Afterwards, the users could elaborate on the mental and cognitive processes and difficulties and formulate wishes on the design.

In particular, the experiments included

- executing messaging acts suitable for pre defined situations,
- defining a messaging act that was known to be common due to personal experience,
- defining a complex, yet still realistic messaging act.

After executing the tasks, the participants were requested

- to answer questions on their ability to handle the selection of readers by means of attribute combinations,
- to elaborate on the comprehensibility of the proposed communication concept,
- to identify elementary as well as difficult operations,
- to compare the proposal with known means for emergency communication,
- to state personal preferences for the usage of an ABM system.

Feedback

In the following, we present selected quotes that were given by the participants (cf. [251]):

- "This is a charming way of addressing communication partners that are not known by identity."
- "The approach is in accordance to our existing role- and task-based ICT."
- "ABM is very useful to communicate with external specialists."
- "Selecting location attributes directly on a digital map would be favorable".

Conclusions

The overall approach was recognized as a generalization of the concept of messaging lists, that is common in emergency communication[38]. Thus, ABM was considered as applicable to the targeted setting and understandable by the available group of experts.

In general, attribute-based messaging was considered to be easy learnable, given that messaging acts can be handled by policies that are easy definable. Using disjunctions and conjunctions within one policy was considered too complex and too difficult. Thus, for the design of messaging policies, a compromise of expressiveness and complexity was favored. Additionally, a selection of location attributes directly within a digital map was an articulated end user wish, in order to support an intuitive use. Instead of using the proposed editor for defining policies, drop-down boxes with lists of attributes were preferred.

The received proposals were incorporated into the final design of our attribute-based messaging approach, as presented in this thesis. In this design, also the resource constraints imposed by the mobile devices that commonly used for emergency communication had to be considered.

[38] Our conclusions relate to German emergency workers.

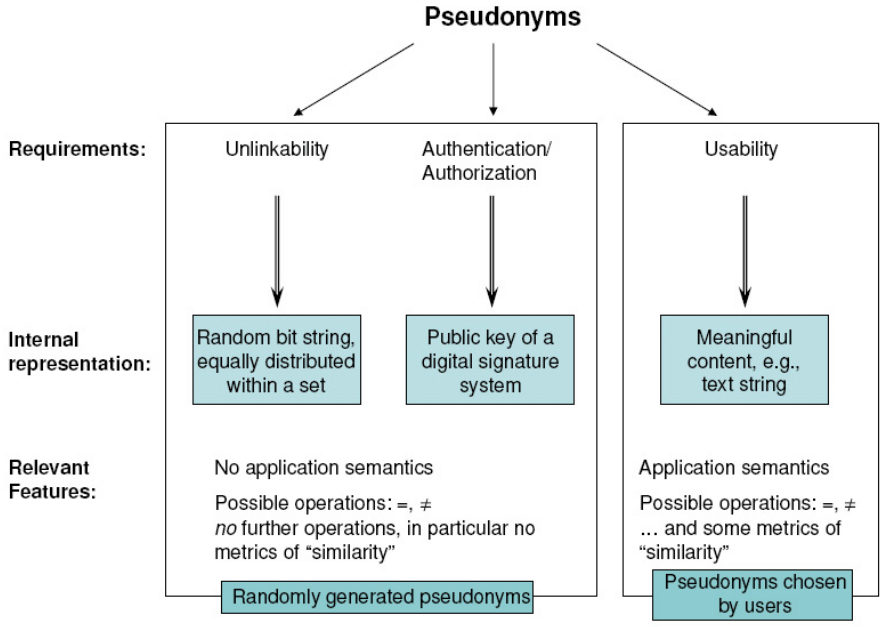

Figure 7.13: Types of pseudonyms according to [28]

7.4 Applicability

In the last sections, we supported our claim that the mechanisms proposed in this thesis are technically feasible, secure and appropriate to certain application settings. In the following sections, we elaborate on the general applicability of the presented concepts.

7.4.1 Pseudonyms with Implicit Attributes

Pseudonyms with implicit attributes are a novel approach to multilevel linkable transaction pseudonyms. Especially, this proposal provides several degrees for flexibly handling the pseudonym-to-identity-mapping.

In [28], Borcea-Pfitzmann et al. distinguish several types of pseudonyms based on unlinkability, authentication / authorization and usability. This classification is shown in Figure 7.13. Generally, transaction pseudonyms are basic tools for implementing unlinkability of user actions; they are thus relevant to many applications that take into account user privacy issues. In addition, many applications also inherently require mechanisms for the authentication and authorization of pseudonymous users.

In the present work, we proposed mechanisms for a cooperative partial re-identification of transaction pseudonyms, with applications to audit log analysis. In ad-

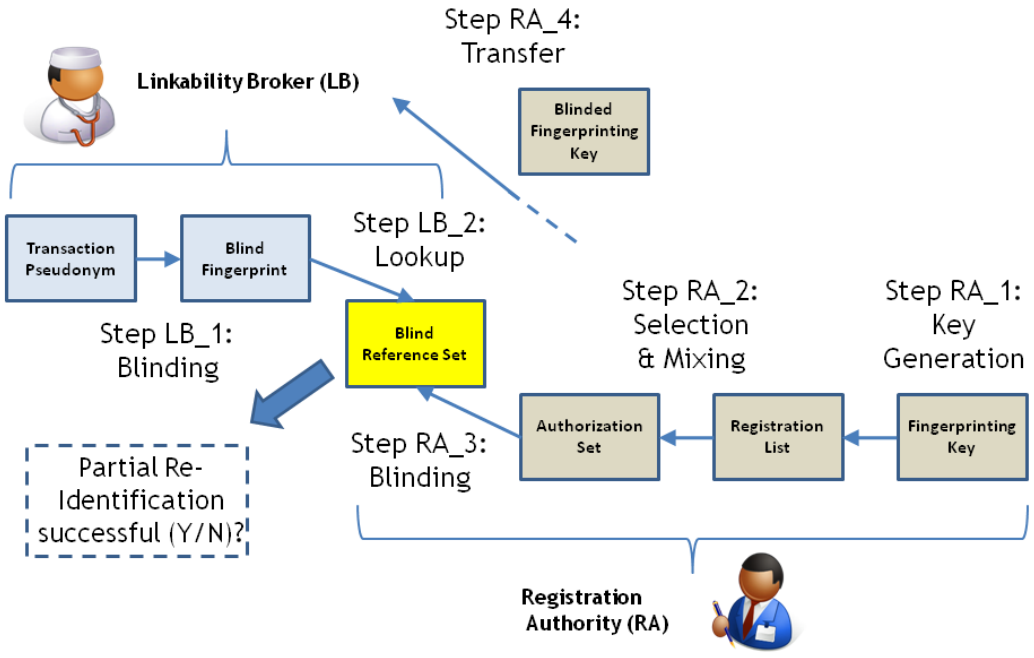

Figure 7.14: Partial re-identification in single authority setting

dition, our proposal is also applicable to authentication[39] and access control. Yet, cooperative authentication can represent, differently to our auditing setting, an impractical overhead in many settings. In [237], we proposed a technique that also supports the partial re-identification *by a single party*. It is described in the next section.

Single Authority Partial Re-Identification

In the following, our novel single authority re-identification method is instantiated in the same setting as given by the multi authority case (cf. Section 4.1). In particular, we make use of a single linkability broker (LB) instead of multiple LBs. Some additional interactions both with the registration authority (RA) and with the authorities that are in possession of the private ElGamal key s are required. The main steps of the re-identification technique are shown in Figure 7.14.

In step RA_1, the RA creates a fingerprinting key $z \in_R \mathbb{Z}_q$ in order to initialize the mechanism.

In step RA_2, the RA selects all base pseudonyms in the registration list that match the semantic of a chosen (implicit) attribute, e.g. it selects all base pseudonyms belonging to the attribute *specialist for X* and mixes them in order to set up an *authorization set*.

[39] Authentication is yet a (further) type of linkability.

In step RA_3, the authorization set is blinded as follows, in order to produce a *blind reference set*:

- Firstly, by raising the first component of each pseudonym $((g^r), (h^r RV_i))$ within the authorization set to the power of z: $(g^r)^z = (g^{rz})$, in order to derive a partly processed pseudonym $((g^{rz}), (h^r RV_i))$.
- Secondly, by decrypting each of the partly processed pseudonyms (using s) to blind deterministic fingerprints $g^{-z} RV_i$. This succeeds, since $(g^{rz})^s = g^{rsz} = g^{rs} * g^z = h^r * g^z$, which can be used to cancel out the first factor of $(h^r RV_i)$ via an algebraic division, hereby computing $g^{-z} RV_i$.

The blind reference sets together with the attached semantic in terms of the implicit attribute are provided to the single linkability broker.

In step RA_4, the linkability broker receives $zs \in \mathbb{Z}_q$, which is used as a *blinded* fingerprinting key. Note that the LB learns nothing about z or s due to this.

The steps RA_1 to RA_4 can be executed in a prior preparation phase, thus we consider them as *offline* operations. In particular, step RA_1 and step RA_4 only have to be executed once, while step RA_3 and RA_4 have to executed for every blind reference set that shall be created.

The following steps can be performed *online*, i.e. in real time during the operation of a system that implements our mechanism.

In step LB_1, in order to re-identify an implicit attribute of a chosen transaction pseudonym $(g^r, h^r RV_?)$, i.e. to test whether the information encoded in the pseudonym is implicitly attached to the semantics of the attribute in question or not, the LB

- raises the first component of the pseudonym to the power of zs: $(g^r)^{zs} = (g^{rzs})$,
- performs an algebraic division in order to produce a blind fingerprint: $(h^r ID_?)/(g^{rzs}) = g^{-z} ID_?$,

In step LB_2, the linkability broker

- executes a fingerprint lookup on the chosen blind reference set, i.e. it compares whether the produced blind deterministic fingerprint is part of this set.
- On success, i.e. if the fingerprint is part of the set, the transaction pseudonym has been partially re-identified w.r.t. the implicit attribute in question. Otherwise, the linkability broker may proceed with a lookup on a different blind reference set.

Application to Authentication and Authorization

Based on the introduced mechanism for single authority partial re-identification, authentication and authorization of transaction pseudonyms can be realized.

In this case, a blind reference set technically represents one rule of an access control policy, analogously to the case of role- or attribute-based access control proposals [193, 249]. Thus, our approach can be applied to settings that require both unlinkability and authentication, e.g. as a cryptographic tool for identity management approaches [238], electronic citizen cards and several further applications. More generally, it is applicable to settings and applications that aim at reconciling unlinkability and linkability by means of pseudonyms. This is e.g. relevant to privacy-preserving reputation establishment [238, 153]. Our proposal is especially suitable for settings with resource constraints, such as RFID applications. In [125], an elaboration on suitable elliptic curve setups is presented.

7.4.2 Multilaterally Secure Auditing

Within this thesis, we presented our novel approach to multilaterally secure auditing especially within the setting of location-based auditing. In particular, we described how to support real-world auditing that were motivated by first response scenarios. In addition, the proposed concepts can also be applied to a range of further application scenarios. We summarize them in Table 7.4.

Application Scenario	**Examples and Features**
Traditional audit log settings	In operating systems, e.g. UNIX
Real-time intrusion detection on pseudonymous data sets	Based on single authority re-identification mechanism
Pseudonym-based transparency mechanisms	Supporting unlinkable transparency logs and individual access to personal data
Context-aware systems	Supporting alert generation on pseudonymized sensor data
Real-time command and control	Real-time attribute re-identification of units

Table 7.4: Application scenarios of multilaterally secure auditing

In particular, traditional audit log settings, e.g. in operating systems can be addressed. The application of real-time intrusion detection on pseudonymous data sets can be supported, harnessing the single authority re-identification mechanism. The presented pseudonym-based transparency mechanisms can be applied to a range of further applications that require means for transparency, cf. [98]. Means for access to personal data are also considered as transparency tools [70]. Our proposed mechanisms for pseudonym-based individual access can e.g. be applied to identity-management systems [238].

A related application scenario is that of context-aware systems, i.e. pervasive computing applications that entail some kind of proactive system behavior [11]. On a technical level, this partly requires that alerts can be generated, e.g. on acquired sensor data.

In the application example of first responder tracking, vital data or air pollution can locally be sensed and also be sent to a control center. The monitoring system can generate alerts if certain thresholds are exceeded, e.g. if physical parameters indicate injuries. Staff members can react upon such warnings. Adapting our approach can provide protection in form of transaction pseudonyms on the identifier level, leaving the content level for real-time alert generation. Also, real-time command and control can be supported based on partial re-identification of attributes.

7.4.3 Hybrid Encryption Technique

The novel hybrid encryption technique represents a practical approach for integrating context information into encryption policies.

Application Scenario	Examples and Features
Context-based encryption	Requires deterministic lock function for particular type of context information
Application to further encryption schemes	Supports hybrid mode encryption e.g. applicable to IBE

Table 7.5: Application scenarios of hybrid encryption technique

In this thesis, it has been proposed with a focus on GPS-based location information. Yet, different types of context information can be included, given that a deterministic lock function can be realized. Securing context-based content distribution mechanisms is thus a primary field of application. The underlying construction principle of combining symmetric keys is also applicable to further encryption schemes that operate in hybrid encryption mode. E.g. it can directly be transferred to identity-based encryption (IBE) schemes [86]. Table 7.5 summarizes the mentioned application scenarios.

7.4.4 End-To-End Secure ABM

End-to-end secure attribute-based messaging supports targeted one-to-many communication with communication partners that are not known by identity.

In the research literature, smart metering and smart grids [127] as well as vehicular networks [110] and health care environments [160], which are considered as particular instances of dynamic organizations, can be identified as relevant fields of applications for ABM concepts. In [155], also social messaging applications are proposed. We summarize the mentioned application scenarios in Table 7.6.

7.5 Summary

In this chapter, we evaluated the main concepts and mechanisms presented by this thesis. Our evaluation proceeded as follows:

Application Scenario	Examples and Features
Smart grids	Communication with unknown identities within utility companies and of mobile users
Smart metering	Message warehousing service
Vehicular networks	Communication with unknown and moving vehicles
Health care	Dynamic organizations with frequent changes of people's roles and permissions
Social messaging	Location-based messaging with privacy protection

Table 7.6: Application scenarios of end-to-end secure ABM

- As proof of concept, we built prototypes for auditing and attribute-based messaging, including prototype implementations of underlying pseudonymization and encryption techniques, in order to show the technical feasibility.
- The prototypes were used to conduct experiments that addressed resource constraints. We provided practical arguments that the overheads w.r.t. to storage requirements for multilaterally secure location-based auditing and w.r.t. the runtime of end-to-end secure ABM on mobile devices are reasonable.
- We analyzed in detail the achieved level of security of our proposals. Where applicable, we reduced the security to computational and organizational assumptions or to the existence of a tamper-resistant hardware component. In addition, an independent security review of our pseudonymization technique acknowledged the correctness and trustworthiness of our proposal. We also described variants for flexibly instantiating our auditing concepts with and without law enforcement capabilities, as well as with different distributions of powers.
- We participated in a legal simulation study in order to assess the acceptability of location traces as evidence. We thus contributed novel insights on the issue of location accountability to the literature. In particular, within the study we identified the main factors for leveraging pseudonymous location traces as legally acceptable evidence. In addition, we compared the legal acceptability to traditional, non-digital evidence such as human eye witnesses.
- In order to assure the appropriateness of our ABM mechanisms to end users, we conducted a user study. It made use of an initial ABM prototype. Based on the results of this study, we contributed to the understanding of a practical ABM usage; our insights are particularly relevant to the first response domain. Also, they contributed to our proposal presented in this thesis.

In addition to the evaluation summarized above, we elaborated on the general applicability of our presented concepts. In particular, we identified further fields of application, e.g. in traditional audit settings such as in operating systems as well as in a range of communication scenarios. Moreover, we contributed a novel method for single authority partial re-identification of transaction pseudonyms. Based on this extension, our pseudonymization technique can also be applied to design access control mechanisms that are compatible with pseudonymous users.

Having evaluated our proposed concepts and mechanisms for multilaterally secure pervasive cooperation, only the final chapter, Chapter 8, is yet to come.

8 Summary

Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. [...] But they are sufficiently pervasive that we must design our protocols around their limitations.
C. Kaufman, R. Perlman and M. Speciner, in [129]

With pervasive computing becoming reality, also privacy and IT security become more important issues to the individual than ever before. Today, the public perception of pervasive computing is often dominated by negative connotations.

With this thesis, we demonstrated that carefully devised protection mechanisms can rather become enablers for multilaterally acceptable and thus trustworthy digital interactions and cooperations. We denoted this topic as *multilaterally secure pervasive cooperation*.

We summarize the main contributions of this thesis in the next section.

8.1 Contributions

This thesis aimed at enabling two crucial functionalities of cooperative pervasive systems: real-world auditing in and by pervasive location tracking systems as well as end-to-end secure communication between a sender and mobile, unknown receivers.

Motivated by the application scenario of ICT-enhanced emergency response, we developed a novel integrated approach as well as the supporting security techniques and mechanisms that aim at mitigating acceptance issues of pervasive computing systems in highly demanding real-world application contexts. In particular, we targeted settings in which highly demanding and conflicting IT security and privacy requirements had to be fulfilled.

Firstly, this thesis contributed the following security techniques and mechanisms:

- *Pseudonyms with implicit attributes* are a novel approach to multilevel linkable transaction pseudonyms. We extended earlier work of Juels and Pappu [125] on encryption-based transaction pseudonyms, by developing new mechanisms for controlled pseudonym linkability. This included mechanisms for

cooperative, stepwise re-identification as well as individual authentication of pseudonyms. Our proposal makes use of efficient techniques for secure multiparty computation and cryptographically secure PRNGs.

- *Multilaterally secure location-based auditing* is a novel consideration of auditing mechanism suitable for real-world actions. It harnesses our novel pseudonym mechanisms in order to support a fair balance of privacy protection and accountability. In contrast to previous work, a cooperative log analysis was introduced that is oriented more closely on stepwise, human-oriented dispute resolution processes. Within the approach, transparency mechanisms constituted a second level of accountability; in addition, means that enable individuals in repudiating false accusation were presented. Our approach can be flexibly instantiated, including law enforcement capabilities and data protection officers that support individual users.

- A *hybrid encryption technique for expressive policies* was introduced. It supports encryption policies that include a continuous dynamic attribute by leveraging an efficient combination of ciphertext-policy attribute-based encryption, location-based encryption and symmetric encryption according to AES. The technique was also devised to meet the requirements of resource-constrained mobile devices.

- *End-to-end secure attribute-based messaging* constitutes a novel communication mechanism for end-to-end encrypted one-to-many messaging. It is suitable even for settings with mobile receivers that are unknown by identity and that form dynamic groups. Based on our hybrid encryption technique, we described how to flexibly support important communication patterns, including location addressing and notifications of a priori unknown recipients, e.g. external specialists; the proposal also allows querying human sensors. Harnessing a novel mechanism for the implicit addressing of communication partners, also location privacy protection of receivers is given. In addition, the approach was tailored according to the needs of potential end users within the emergency response domain.

The techniques and mechanisms constituted the major building blocks of our *novel approach to multilaterally secure pervasive cooperation*. In particular, we also provided an integrated architecture that was tailored towards *location-aware first response*. By doing so, we considered location, which represents a primary type of context information that is leveraged by many pervasive applications, as the central integrating concept for pervasive interactions and cooperations. In our design, both communication during rescue missions as well as real-world auditing in the ex-post phase of an emergency are inherently conceived as being location-based.

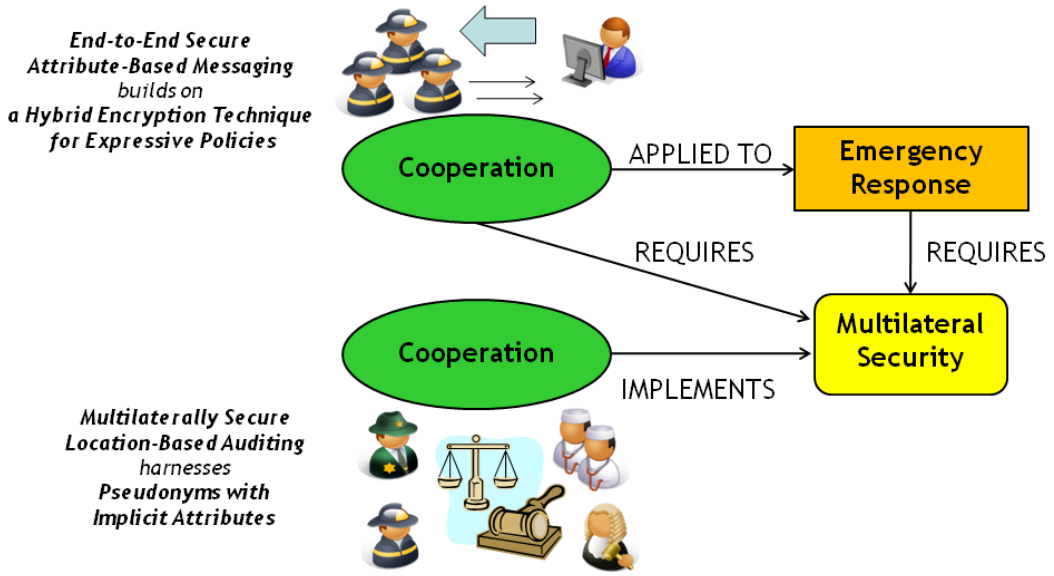

Figure 8.1: Multilaterally secure pervasive cooperation

8.2 Conclusion

This thesis presented novel design proposals towards the realization of privacy-respecting and moreover multilaterally secure cooperative pervasive systems. In particular, we depicted how cooperation based on pervasive ICT can support settings that inherently require multilateral security. On the other hand, we also described how cooperation can be a key mechanism to implement multilateral security (cf. Figure 8.1).

On a technical level, we showed that data minimization, in particular the replacement of person-related identifiers must not lead to a confinement of system functionality, if protection mechanisms are carefully designed.

Hence, modern cryptographic mechanisms are required in many parts of a pervasive system. Nowadays, standard mobile devices already provide technical platforms that are suitable to host highly complex protection mechanisms, in case the mechanisms are efficiently designed.

Location privacy protection has become an important issue to many individuals. We evaluated the complementary aspect of *location accountability* by means of an interdisciplinary study and thus added novel practical insights on this issue to the ongoing scientific discussion.

Unquestionable, the degree of protection provided by the contributions of this thesis comes at a cost. The cost comprises *design and evaluation efforts, hardware as well as operating expense and storage needs*. Also, the *availability of cooperating authorities* and *individual participation for controlling transparency logs* is crucial. Yet, we have shown that theses factors come at a reasonable cost. In particular, *trusted registration*

processes are required. However, a registration is required for most ICT applications, anyway. We notice that moving a major part of trust into the organizational level is an inherent issue of securing cooperative systems.

While a profound theoretical and technical knowledge is required to devise security mechanisms, additional care has to be taken in order to support a practical use. While explicit user interfaces tend to disappear within pervasive system, many additional interfaces to the real world emerge. In particular, also legal considerations and individual acceptance factors need to be considered to assure that pervasive systems can "weave themselves into the fabric of everyday life until they are indistinguishable from it" [243]. Yet, "disappearing computers" [216] still entail (digital) traces. Arguing and demonstrating that, nevertheless, a fairly balanced use of sensitive data is possible, the present thesis made a step towards the realization of multilaterally secure and thus multilaterally acceptable pervasive systems.

8.3 Outlook

Having summarized and concluded on our main contributions, we suggest directions for future research.

Extended pseudonym constructions

The presented approach to *pseudonyms with implicit attributes* already provides flexible degrees of linkability for several parties. However, harnessing additional properties of the underlying cryptographic primitives can allow realizing extended functionalities. By exploiting homomorphic encryption, the pseudonym technique could be extended towards including a statistical function, and thus to realize *countable accountable pseudonyms*. Such pseudonyms may have applications in novel accounting and pay-per-transaction methods.

More generally, as already sketched in Section 7.4.1, the present work can be the basis to define pseudonym-based access control mechanisms. Generalizations of our blind reference sets may represent access control policies, comparable to existing role- or attribute-based access control proposals. In case of application to privacy policies, it seems interesting to investigate whether user-understandable policies should be defined in terms of anonymity, in terms of attribute semantics, or based on a combination of both.

Integration with reputation

Establishing reputation histories while protecting privacy requires to reconcile unlinkability and linkability [152, 153]. Technically, this issue is comparable to the tradeoff of location privacy protection and accountability that was addressed by this thesis. Through reputation mechanisms, users can be supported to select reputable interaction partners, based on aggregated historical trust and reputation values and

recommendations. In order to compute reputation scores, it is necessary to establish interaction histories, i.e. aggregating experiences over past transactions. Based on an extended application of secure multiparty computation techniques, not only on the pseudonym level, also reputation values could be assessed. Based on SMPC, the correctness of the output and privacy of the inputs could be guaranteed, without relying on a single, external trusted party.

Further mechanisms for multilateral security

This thesis provides a starting point for research on multilateral security in the context of pervasive systems. Following this line of research, the next steps can be to identify additional and complementary building blocks and mechanisms that constitute design alternatives towards the realization of privacy-respecting and moreover multilaterally secure pervasive systems.

This may include a broader investigation of accountability and its impact as incentive for achieving a fairly balanced state of protection. Especially, a combination of multiple accountability mechanisms may constitute more effective incentive mechanisms, especially w.r.t. the handling of sensitive data in pervasive systems. Here, the principles of audit and transparency logs that allow for an ex-post penalization of unwelcome behavior could be complemented by giving rewards for welcome behavior. This could naturally include the consideration of reputation and economical factors.

Extended mechanisms for secure communication

With *end-to-end secure attribute-based messaging*, we contributed a novel mechanism that enables communication in settings, where receivers are unknown by identity; this is typically found in many cooperative pervasive computing applications. The following directions for future research concern to broaden the applicability of ABM mechanisms.

In the setting of this thesis, we assume that the sender of a message is not constrained by limited input capabilities or small display sizes. As a next step, research may focus on enabling one-to-many communication in settings in which the sender herself has only a mobile communication device. Complementary, further existing network infrastructures can be considered as communication backbone for attribute-based messaging. For example, online social networking platforms may be harnessed to implement some sort of social attribute-based communication mechanisms.

Erklärung[1]

Hiermit erkläre ich, die vorgelegte Arbeit zur Erlangung des akademischen Grades "Dr. rer. nat." mit dem Titel *Multilaterally Secure Pervasive Cooperation* selbstständig und ausschließlich unter Verwendung der angegebenen Hilfsmittel erstellt zu haben. Ich habe bisher noch keinen Promotionsversuch unternommen.

Darmstadt, 30. September 2011 Stefan G. Weber

[1] gemäß §9 Abs. 1 der Promotionsordnung der TU Darmstadt

Wissenschaftlicher Werdegang des Verfassers[2]

10/2000 – 07/2006	Studium der Informatik Nebenfächer: Rechtswissenschaften und Psychologie Technische Universität Darmstadt Abschluss: Diplom-Informatiker Diplomarbeitsthema: *A Coercion-Resistant Cryptographic Voting Protocol - Evaluation and Prototype Implementation*
11/2006 – 12/2009	Wiss. Mitarbeiter am Fachbereich Informatik Technische Universität Darmstadt
seit 01/2010	Stipendiat im Center for Advanced Security Research Darmstadt (CASED) Technische Universität Darmstadt

[2] gemäß §20 Abs. 3 der Promotionsordnung der TU Darmstadt

Bibliography

[1] G. D. Abowd and E. D. Mynatt. Charting Past, Present, and Future Research in Ubiquitous Computing. *ACM Transactions on Computer-Human Interaction*, 7(1):29–58, 2000.

[2] A. Acquisti, S. D. C. di Vimercati, S. Gritzalis, and C. Lambrinoudakis, editors. *Digital Privacy: Theory, Technologies and Practices*. Taylor & Frances, 2007.

[3] N. R. Adam, V. Atluri, S. A. Chun, J. Ellenberger, B. Shafiq, J. Vaidya, and H. Xiong. Secure Information Sharing and Analysis for Effective Emergency Management. In *Digital Government Research Conference (DG.O '08)*, pages 407–408. Digital Government Society of North America, 2008.

[4] E. Aitenbichler. A Focus on Location Context. In *Handbook of Research on Ubiquitous Computing Technology for Real Time Enterprises*, pages 257–281. IGI Global Publisher, 2008.

[5] A. Al-Fuqaha and O. Al-Ibrahim. Geo-Encryption Protocol for Mobile Networks. *Computer Communications*, 30(11-12):2510–2517, 2007.

[6] R. J. Anderson. *Security Engineering: a Guide to Building Dependable Distributed Systems*. John Wiley & Sons, 2008.

[7] C. A. Ardagna. *Privacy and Security in Distributed and Pervasive Systems*. PhD thesis, Universita' degli Studi di Milano, 2008.

[8] Ausschuss für Bildung, Forschung und Technikfolgenabschätzung. Zukunftsreport Ubiquitous Computing. http://dipbt.bundestag.de/dip21/btd/17/004/1700405.pdf, 2009.

[9] M. Backes, P. Druschel, A. Haeberlen, and D. Unruh. CSAR: A Practical and Provable Technique to Make Randomized Systems Accountable. In *Network and Distributed System Security Symposium (NDSS '09)*. The Internet Society, 2009.

[10] S. A. Bagues, A. Zeidler, F. Valdivielso, and I. R. Matias. Sentry@Home - Leveraging the Smart Home for Privacy in Pervasive Computing. *International Journal of Smart Home*, 1(2), July 2007.

[11] M. Baldauf, S. Dustdar, and F. Rosenberg. A Survey on Context-Aware Systems. *International Journal of Ad Hoc and Ubiquitous Computing*, 2(43):263–277, 2007.

[12] G. Bell and P. Dourish. Yesterday's Tomorrows: Notes on Ubiquitous Computing's Dominant Vision. *Personal Ubiquitous Computing*, 11:133–143, January 2007.

[13] V. Bellotti and A. Sellen. Design for Privacy in Ubiquitous Computing Environments. In *European Conference on Computer Supported Cooperative Work (ECCSW'93)*, pages 75–92, 1993.

[14] A. R. Beresford. *Location Privacy in Ubiquitous Computing*. PhD thesis, University of Cambridge, Computer Laboratory, 2005.

[15] A. R. Beresford and F. Stajano. Location Privacy in Pervasive Computing. *IEEE Pervasive Computing*, 02(1):46–55, 2003.

[16] O. Berthold and H. Langos. Dummy Traffic against Long Term Intersection Attacks. In *Privacy Enhancing Technologies (PET '02)*. Springer, 2002.

[17] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-Policy Attribute-Based Encryption. In *IEEE Symposium on Security and Privacy (SP '07)*, pages 321–334. IEEE CS, 2007.

[18] P. Bhaskar and S. I. Ahamed. Privacy in Pervasive Computing and Open Issues. In *Conference on Availability, Reliability and Security (ARES '07)*, pages 147–154. IEEE CS, 2007.

[19] J. Biskup and U. Flegel. Threshold-Based Identity Recovery for Privacy Enhanced Applications. In *ACM Conference on Computer and Communications Security (CCS '00)*, pages 71–79. ACM, 2000.

[20] J. Biskup and U. Flegel. Transaction-Based Pseudonyms in Audit Data for Privacy Respecting Intrusion Detection. In *Recent Advances in Intrusion Detection, International Workshop (RAID '00)*, pages 28–48. Springer, 2000.

[21] M. H. Blackmon. Cognitive Walkthrough. In W. S. Bainbridge, editor, *Encyclopedia of Human-Computer Interaction - Volume 1*, pages 104–107. Berkshire Publishing Group, 2004.

[22] M. Blum, A. De Santis, S. Micali, and G. Persiano. Noninteractive Zero-Knowledge. *SIAM Journal on Computing*, 20:1084–1118, December 1991.

[23] R. Bobba, O. Fatemieh, F. Khan, C. A. Gunter, and H. Khurana. Using Attribute-Based Access Control to Enable Attribute-Based Messaging. In *Annual Computer Security Applications Conference (ACSAC '06)*, pages 403–413. IEEE CS, 2006.

[24] R. Bobba, O. Fatemieh, F. Khan, A. Khan, C. A. Gunter, H. Khurana, and P. Manoj. Attribute-Based Messaging: Access Control and Confidentiality. *ACM Transactions on Information Systems Security (TISSEC)*, 13:31:1–31:35, December 2010.

[25] A. Bogdanov and D. Khovratovich. Key Recovery for the Full AES. In *Advances in Cryptology - AsiaCrypt '11*, to appear.

[26] A. Bogdanov, D. Khovratovich, and C. Rechberger. Biclique Cryptanalysis of the Full AES. Cryptology ePrint Archive, Report 2011/449, 2011.

[27] D. Boneh and M. K. Franklin. Identity-Based Encryption from the Weil Pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003.

[28] K. Borcea-Pfitzmann, E. Franz, and A. Pfitzmann. Usable Presentation of Secure Pseudonyms. In *Workshop on Digital Identity Management (DIM '05)*, pages 70–76. ACM Press, 2005.

[29] D. Bradler. *Peer-to-Peer Concepts for Emergency First Response*. PhD thesis, Technische Universität Darmstadt, 2010.

[30] S. Bratus, A. Lembree, and A. Shubina. Software on the Witness Stand: What Should It Take for Us to Trust It? In *Conference on Trust and Trustworthy Computing (TRUST '10)*, pages 396–416. Springer, 2010.

[31] A. D. Brucker and D. Hutter. Information Flow in Disaster Management Systems. In *Conference on Availability, Reliability and Security (ARES '10)*, pages 156–163. IEEE CS, 2010.

[32] A. D. Brucker, H. Petritsch, and S. G. Weber. Attribute-Based Encryption with Break-Glass. In *Workshop in Information Security Theory and Practice (WISTP'10)*, pages 237–244. Springer, 2010.

[33] D. A. Buell. The Advanced Encryption Standard. In H. Bidgoli, editor, *Handbook of Information Security - Volume 2*, pages 498–507. John Wiley and Sons, 2006.

[34] Bundesnetzagentur. Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung. Bundesanzeiger Nr. 17, Seite 383, 01.02.2011, 2011. `http://www.bundesnetzagentur.de/`.

[35] L. Buttyan and J.-P. Hubaux. *Security and Cooperation in Wireless Networks - Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing*. Cambridge University Press, 2007.

[36] J. Camenisch, T. Groß, and T. S. Heydt-Benjamin. Rethinking Accountable Privacy Supporting Services. In *Workshop on Digital Identity Management (DIM '08)*, pages 1–8. ACM Press, 2008.

[37] J. Camp and K. Connelly. Beyond Consent: Privacy in Ubiquitous Computing (Ubicomp). In *Digital Privacy: Theory, Technologies and Practices*, pages 327–343. Taylor & Frances, 2007.

[38] L. Carver and M. Turoff. Human-Computer Interaction: the Human and Computer as a Team in Emergency Management Information Systems. *Communication of the ACM*, 50(3):33–38, 2007.

[39] J. Cas. Privacy in Pervasive Computing Environments - A Contradiction in Terms? *IEEE Technology and Society Magazine*, 24(1):24– 33, 2005.

[40] D. Catalano, R. Cramer, I. Damgard, G. D. Crescenzo, D. Pointcheval, and T. Takagi. *Contemporary Cryptology*. Birkhäuser, 2005.

[41] E. Cayirci and C. Rong. *Security in Wireless Ad Hoc and Sensor Networks*. John Wiley and Sons, 2009.

[42] D. Chadwick, G. Lunt, and G. Zhao. Secure Role Based Messaging. In *IFIP Conference on Communications and Multimedia Security (CMS '04)*, pages 303–316, 2004.

[43] D. Chaum. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM*, 24(2):84–88, 1981.

[44] D. Chaum. Security without Identification: Transaction Systems to Make Big Brother Obsolete. *Communications of the ACM*, 28(10):1030–1044, 1985.

[45] D. Chaum, A. Fiat, and M. Naor. Untraceable Electronic Cash. In *Advances in Cryptology - CRYPTO '88*, pages 319–327, 1988.

[46] D. Chaum and T. P. Pedersen. Wallet Databases with Observers. In *Advances in Cryptology - CRYPTO '92*, pages 89–105. Springer, 1993.

[47] Committee on Planning for Catastrophe, editor. *Successful Response Starts With A Map: Improving Geospatial Support for Disaster Management*. National Academy Press, 2007.

[48] S. Consolvo, P. Roessler, B. E. Shelton, A. LaMarca, B. Schilit, and S. Bly. Technology for Care Networks of Elders. *IEEE Pervasive Computing*, 3:22–29, 2004.

[49] V. Coroama. The Smart Tachograph - Individual Accounting of Traffic Costs and its Implications. In *Conference on Pervasive Computing (PERVASIVE '06)*, pages 135–152. Springer, 2006.

[50] V. Coroama, J. Bohn, and F. Mattern. Living in a Smart Environment - Implications for the Coming Ubiquitous Information Society. In *Conference on Systems, Man and Cybernetics (SMC '04)*, pages 5633 – 5638. IEEE CS, 2004.

[51] R. Cramer, I. Damgard, and B. Schoenmakers. Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In *Advances in Cryptology - CRYPTO 94*, pages 174–187. Springer, 1994.

[52] L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. http://www.w3.org/TR/P3P/, 200?

[53] C. Delakouridis, L. Kazatzopoulos, G. F. Marias, and P. Georgiadis. Share The Secret: Enabling Location Privacy in Ubiquitous Environments. In *Workshop on Location- and Context-Awareness (LoCA '05)*, pages 289–305. Springer, 2005.

[54] D. E. Denning and L. Scott. Geo-Encryption - Using GPS to Enhance Data Security. GPS World, 2003.

[55] D. Dolev and A. C. Yao. On the Security of Public Key Protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, Mar 1983.

[56] B. Dragovic. *CASPEr: Containment-Aware Security for Pervasive Computing Environments*. PhD thesis, University of Cambridge, 2006.

[57] S. Dritsas, D. Gritzalis, and C. Lambrinoudakis. Protecting Privacy and Anonymity in Pervasive Computing: Trends and Perspectives. *Telematics and Informatics*, 23(3):196–210, 2006.

[58] M. Duckham and L. Kulik. Location Privacy and Location-Aware Computing. In *Dynamic & Mobile GIS: Investigating Change in Space and Time*, pages 34–51. CRC Press, 2006.

[59] P. A. Ehlert. Intelligent User Interfaces: Introduction and Survey. Research Report DKS03-01 / ICE 01, 2003.

[60] T. ElGamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.

[61] C. Endres, A. Wurz, M. Hoffmann, and A. Behring. A Task-Based Messaging Approach to Facilitate Staff Work. In *International Conference on Information Systems for Crisis Response and Management (ISCRAM '10)*, 2010.

[62] N. Ferguson and B. Schneier. *Practical Cryptography*. Wiley Publishing, Inc., 2003.

[63] B. Ferris, K. Watkins, and A. Borning. Location-Aware Tools for Improving Public Transit Usability. *IEEE Pervasive Computing*, 9:13–19, 2010.

[64] A. Fiat and A. Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In *Advances in Cryptology - CRYPTO 86*, pages 186–194. Springer, August 1986.

[65] C. Fischer and H. Gellersen. Location and Navigation Support for Emergency Responders: A Survey. *IEEE Pervasive Computing*, 9:38–47, 2010.

[66] S. Fischer-Hübner. *IDA (Intrusion Detection and Avoidance System): Ein einbruchsentdeckendes und einbruchsvermeidendes System (in German).* Reihe Informatik. Shaker, 1993.

[67] S. Fischer-Hübner. *IT-Security and Privacy - Design and Use of Privacy-Enhancing Security Mechanisms*. Springer, 2001.

[68] S. Fischer-Hübner. Pseudonymity. In *Encyclopedia of Database Systems*, page 2207. Springer, 2009.

[69] S. Fischer-Hübner and K. Brunnstein. Combining Verified and Adaptive System Components Towards More Secure System Architectures. In *Workshop on Computer Architectures to Support Security and Persistance of Information*. Springer, 1990.

[70] S. Fischer-Hübner, C. J. Hoofnagle, K. Rannenberg, M. Waidner, I. Krontiris, and M. Marhöfer. Online Privacy: Towards Informational Self-Determination on the Internet (Dagstuhl Perspectives Workshop 11061). *Dagstuhl Reports*, 1(2):1–15, 2011.

[71] U. Flegel. *Privacy-Respecting Intrusion Detection*. Springer, 2007.

[72] F. Flentge, S. G. Weber, A. Behring, and T. Ziegert. Designing Context-Aware HCI for Collaborative Emergency Management. In *Int'l Workshop on HCI for Emergencies in conjunction with CHI '08*, 2008.

[73] C. Floerkemeier and M. Lampe. Issues with RFID Usage in Ubiquitous Computing Applications. In *Conference on Pervasive Computing (PERVASIVE '04)*, pages 188–193. Springer, 2004.

[74] C. Floerkemeier, R. Schneider, and M. Langheinrich. Scanning with a Purpose - Supporting the Fair Information Principles in RFID Protocols. In *Symposium on Ubiquitous Computing Systems (UCS '04)*, pages 214–231. Springer, 2004.

[75] F. O. for Information Security (BSI), editor. *Pervasive Computing: Trends and Impacts*. SecuMedia, 2006.

[76] A. P. Fournaris. Trust Ensuring Crisis Management Hardware Module. *Information Security Journal: A Global Perspective*, 19(2):74–83, 2010.

[77] U. L. für Datenschutz Schleswig-Holstein (ULD) and I. für Wirtschaftsinformatik der HU Berlin, editors. *Technikfolgen-Abschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung*. 2006.

[78] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes. On Non-Cooperative Location Privacy: a Game-Theoretic Analysis. In *ACM Conference on Computer and Communications Security (CCS '09)*, pages 324–337. ACM Press, 2009.

[79] M. Friedewald and O. Raabe. Ubiquitous Computing: An Overview of Technology Impacts. *Telematics and Informatics*, 28(2):55–65, 2011.

[80] M. Friedewald, E. Vildjiounaiteb, Y. Puniec, and D. Wright. Privacy, Identity and Security in Ambient Intelligence: A Scenario Analysis. *Telematics and Informatics*, 24(1):15–29, 2007.

[81] L. Fritsch and T. Scherner. A Multilaterally Secure, Privacy-Friendly Location-Based Service for Disaster Management and Civil Protection. In *International Conference on Networking (ICN '05)*, pages 1130–1137. Springer, 2005.

[82] J. Furukawa and K. Sako. An Efficient Scheme for Proving a Shuffle. In *Advances in Cryptology - CRYPTO 01*, pages 368–387. Springer, 2001.

[83] S. Garfinkel. Adopting Fair Information Practices to low-cost RFID Systems. In *Workshop on Socially Informed Design of Privacy-Enhancing Solutions in Ubiquitous Computing in conjunction with UbiComp '02*, 2002.

[84] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Secure Distributed Key Generation for Discrete-Log Based Cryptosystems. In *Advances in Cryptology - EUROCRYPT '99*, pages 295–310. Springer, 1999.

[85] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Secure Applications of Pedersen's Distributed Key Generation Protocol. In *Topics in Cryptology- CT-RSA '03*, pages 373–390. Springer, 2003.

[86] C. Gentry. IBE (Identity-Based Encryption). In H. Bidgoli, editor, *Handbook of Information Security - Volume 2*, pages 575–592. John Wiley and Sons, 2006.

[87] S. Goldwasser, S. Micali, and C. Rackoff. The Knowledge Complexity of Interactive Proof-Systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.

[88] D. Gollmann. *Computer Security, 2nd Edition*. John Wiley & Sons, 2006.

[89] A. Görlach, A. Heinemann, W. W. Terpstra, and M. Mühlhäuser. Location Privacy. In A. Boukerche, editor, *Handbook of Algorithms for Wireless Networking and Mobile Computing*, Computer and Information Science Series, pages 393–411. Chapman & Hall, 2005.

[90] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In *ACM Conference on Computer and Communications Security (CCS '06)*, pages 89–98. ACM Press, 2006.

[91] A. Greenfield, editor. *Everyware - The Dawning Age of Ubiquitous Computing*. New Riders, 2006.

[92] M. Gruteser and D. Grunwald. Enhancing Location Privacy in Wireless LAN through Disposable Interface Identifiers: a Quantitative Analysis. *Mobile Networks and Applications*, 10(3):315–325, 2005.

[93] M. Gruteser and X. Liu. Protecting Privacy in Continuous Location-Tracking Applications. *IEEE Security & Privacy*, 2(2):28–34, 2004.

[94] S. F. Gürses, B. Berendt, and T. Santen. Multilateral Security Requirements Analysis for Preserving Privacy in Ubiquitous Environments. In *Workshop on Ubiquitous Knowledge Discovery for Users in conjunction with ECML PKDD '06*, pages 51–64, 2006.

[95] S. F. Gürses and T. Santen. Contextualizing Security Goals: A Method for Multilateral Security Requirements Elicitation. In *Sicherheit '06*, pages 42–53, 2006.

[96] M. Hartmann and G. Austaller. Context Models and Context-Awareness. In *Ubiquitous Computing Technology for Real Time Enterprises*, pages 235–256. IGI Global Publisher, 2008.

[97] G. R. Hayes, G. D. Abowd, J. S. Davis, M. Blount, M. Ebling, and E. D. Mynatt. Opportunities for Pervasive Computing in Chronic Cancer Care. In *Conference on Pervasive Computing (PERVASIVE '08)*, pages 262–279. Springer, 2008.

[98] H. Hedbom. A Survey on Transparency Tools for Enhancing Privacy. In *The Future of Identity in the Information Society*, pages 67–82. Springer, 2009.

[99] H. Hedbom and T. Pulls. Unlinking Database Entries: Implementation Issues in Privacy Preserving Secure Logging. In *International Workshop on Security and Communication Networks (IWSCN '10)*, pages 1 –7. IEEE CS, 2010.

[100] H. Hedbom, T. Pulls, P. Hjärtquist, and A. Lavén. Adding Secure Transparency Logging to the PRIME Core. In *Privacy and Identity Management for Life*, pages 299–314. Springer, 2010.

[101] J. Heesen and O. Siemoneit. Opportunities for Privacy and Trust in the Development of Ubiquitous Computing. *International Review of Information Ethics (IRIE)*, 8:47–52, 2007.

[102] S. Helal, B. Winkler, C. Lee, Y. Kaddoura, L. Ran, C. Giraldo, S. Kuchibhotla, and W. Mann. Enabling Location-Aware Pervasive Computing Applications for the Edlerly. In *Conference on Pervasive Computing and Communications (PERCOM '03)*, page 531. IEEE CS, 2003.

[103] U. Hengartner. *Access Control to Information in Pervasive Computing Environments*. PhD thesis, Carnegie Mellon University, 2005.

[104] D. Henrici and P. Müller. Hash-Based Enhancement of Location Privacy for Radio-Frequency Identification Devices Using Varying Identifiers. In *Conference on Pervasive Computing and Communications Workshops (PERCOMW '04)*. IEEE CS, 2004.

[105] D. Henrici and P. Müller. Providing Security and Privacy in RFID Systems Using Triggered Hash Chains. In *Conference on Pervasive Computing and Communications (PERCOM '08)*, pages 50–59. IEEE CS, 2008.

[106] M. Hirt. *Multi-Party Computation: Efficient Protocols, General Adversaries, and Voting*. PhD thesis, ETH Zurich, September 2001.

[107] J.-H. Hoepman. In Things We Trust? Towards Trustability in the Internet of Things. *CoRR*, abs/1109.2637, 2011.

[108] J. I. Hong. *An Architecture for Privacy-Sensitive Ubiquitous Computing*. PhD thesis, University of California at Berkeley, Computer Science Division, Berkeley, 2005.

[109] J. I. Hong, J. D. Ng, S. Lederer, and J. A. Landay. Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems. In *Conference on Designing Interactive Systems (DIS '04)*, pages 91–100. ACM Press, 2004.

[110] D. Huang and M. Verma. ASPE: Attribute-Based Secure Policy Enforcement in Vehicular Ad Hoc Networks. *Ad Hoc Networks*, 7(8):1526–1535, 2009.

[111] G. Iachello. *Privacy and Proportionality*. PhD thesis, Georgia Institute of Technology, 2006.

[112] G. Iachello and G. D. Abowd. Privacy and Proportionality: Adapting Legal Evaluation Techniques to Inform Design in Ubiquitous Computing. In *Conference on Human Factors in Computing Systems (CHI '05)*, pages 91–100. ACM Press, 2005.

[113] G. Iachello and J. Hong. *End-User Privacy in Human-Computer Interaction*. Now Publishers, 2007.

[114] R. Iannella, K. Robinson, and O.-P. Rinta-Koski. Towards a Framework for Crisis Information Management Systems (CIMS). In *14th Annual Conference of The International Emergency Management Society (TIEMS)*, 2007.

[115] IPC of Ontario and HP Canada. RFID and Privacy - Guidance for Health-Care Providers, 2008.

[116] D. Jacobi. *Secure Multi-Purpose Wireless Sensor Networks*. PhD thesis, Technische Universität Darmstadt, to appear.

[117] M. Jakobsson. Cryptographic Privacy Protection Techniques. In H. Bidgoli, editor, *Handbook of Information Security - Volume 3*, pages 300–310. John Wiley and Sons, 2006.

[118] M. Jakobsson and A. Juels. Mix and Match: Secure Function Evaluation via Ciphertexts. In *Advances in Cryptology: ASIACRYPT '00*, pages 162–177. Springer, 2000.

[119] X. Jiang, N. Y. Chen, J. I. Hong, K. Wang, L. Takayama, and J. A. Landay. Siren: Context-Aware Computing for Firefighting. In *Conference on Pervasive Computing (PERVASIVE '04)*, pages 87–105. Springer, 2004.

[120] X. Jiang, J. I. Hong, L. A. Takayama, and J. A. Landay. Ubiquitous Computing for Firefighters: Field Studies and Prototypes of large Displays for Incident Command. In *Conference on Human Factors in Computing Systems (CHI '04)*, pages 679–686. ACM Press, 2004.

[121] C. W. Johnson. Complexity, Structured Chaos and the Importance of Information Management for Mobile Computing in the UK Floods of 2007. In *Workshop on Mobile Information Technology for Emergency Response (Mobile Response '08)*, pages 1–11. Springer, 2008.

[122] O. Jorns, O. Jung, J. Gross, and S. Bessler. A Privacy Enhancement Mechanism for Location Based Service Architectures Using Transaction Pseudonyms. In *Conference on Trust, Privacy and Security in Digital Business (TrustBus '05)*, pages 100–109. Springer, 2005.

[123] O. Jorns, G. Quirchmayr, and O. Jung. A Privacy Enhancing Mechanism Based on Pseudonyms for Identity Protection in Location-Based Services. In *Australasian Symposium on ACSW Frontiers (ACSW '07)*, pages 133–142. Australian Computer Society, 2007.

[124] M. Joye and G. Neven, editors. *Identity-Based Cryptography*. IOS Press, 2009.

[125] A. Juels and R. Pappu. Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. In *Conference on Financial Cryptography (FC '03)*, pages 103–121. Springer, 2003.

[126] A. Kapadia. *Models for Privacy in Ubiquitous Computing Environments*. PhD thesis, University of Illinois at Urbana-Champaign, 2005.

[127] Y. Karabulut, H. Weppner, I. Nassi, A. Nagarajan, Y. Shroff, N. Dubey, and T. Shields. End-to-End Confidentiality for a Message Warehousing Service using Identity-Based Encryption. In *ICDE Workshops*, pages 33–40, 2010.

[128] M. Karyda, S. Gritzalis, J. H. Park, and S. Kokolakis. Privacy and Fair Information Practices in Ubiquitous Environments: Research Challenges and Future Directions. *Internet Research*, 19(2):194–208, 2009.

[129] C. Kaufman, R. Perlman, and M. Speciner. *Network Security: Private Communication in a Public World, 2nd Edition*. Prentice Hall International, 2002.

[130] D. Kesdogan, D. Agrawal, and S. Penz. Limits of Anonymity in Open Environments. In *Workshop on Information Hiding (IH '02)*, pages 53–69. Springer, 2002.

[131] D. Kesdogan, H. Federrath, A. Jerichow, and A. Pfitzmann. Location Management Strategies Increasing Privacy in mobile Communication. In *IFIP International Information Security Conference (SEC'96)*, pages 39–48. Chapman & Hall, 1996.

[132] J. K. Kim, R. Sharman, H. R. Rao, and S. Upadhyaya. Framework for Analyzing Critical Incident Management Systems (CIMS). In *Hawaii International Conference on System Sciences (HICSS '06)*, page 79. IEEE CS, 2006.

[133] F. Koeune. Pseudo-Random Number Generator. In *Encyclopedia of Cryptography and Security*, pages 485–487. 2005.

[134] J. Krumm. A Survey of Computational Location Privacy. *Personal and Ubiquitous Computing*, 13(6):391–399, 2009.

[135] J. Lachner and H. Hellwagner. Information and Communication Systems for Mobile Emergency Response. In *United Information Systems Conference (UNISCON '08)*, pages 213–224. Springer, 2008.

[136] L. Langer, M. Volkamer, S. G. Weber, A. Schmidt, and J. Buchmann. Towards Long-Term Free and Secret Electronic Elections Providing Voter-Verifiability in the Bulletin Board Model. In *International Conference on Theory and Practice of Electronic Governance (ICEGOV '09)*, pages 203–210. ACM Press, 2009.

[137] M. Langheinrich. Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. In *International Conference on Ubiquitous Computing (UbiComp '01)*, pages 273–291. Springer, 2001.

[138] M. Langheinrich. *Personal Privacy in Ubiquitous Computing - Tools and System Support*. PhD thesis, ETH Zurich, Zurich, Switzerland, May 2005.

[139] M. Langheinrich. Privacy in Ubiquitous Computing. In J. Krumm, editor, *Ubiquitous Computing*. CRC Press, 2009.

[140] K. Lauter. The Advantages of Elliptic Curve Cryptography for Wireless Security. *IEEE Wireless Communications*, 11(1):62 – 67, Feb. 2004.

[141] C. Linde. *Aufbau und Technik des digitalen BOS-Funks*. Franzis Verlag, 2008.

[142] Y. Lindell and B. Pinkas. Secure Multiparty Computation for Privacy-Preserving Data Mining. *Journal of Privacy and Confidentiality*, 01(01):59–98, 2009.

[143] J. Löffler and M. Klann, editors. *Mobile Information Technology for Emergency Response (MobileResponse)*. Springer, 2009.

[144] S. Loke. *Context-Aware Pervasive Systems - Architectures for a New Breed of Applications*. Auerbach Publications, 2007.

[145] K. Lorincz, D. J. Malan, T. R. F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton. Sensor Networks for Emergency Response: Challenges and Opportunities. *IEEE Pervasive Computing*, 3(4):16–23, 2004.

[146] Y. Ma, D. V. Kalashnikov, R. Hariharan, S. Mehrotra, N. Venkatasubramanian, N. Ashish, and J. Lickfett. On-Demand Information Portals for Disaster Situations. In *Conference on Intelligence and Security Informatics (ISI '07)*, pages 133–136. IEEE CS, 2007.

[147] P. D. MacKenzie, T. Shrimpton, and M. Jakobsson. Threshold Password-Authenticated Key Exchange. *J. Cryptology*, 19(1):27–66, 2006.

[148] B. S. Manoj and A. H. Baker. Communication Challenges in Emergency Response. *Communications of the ACM*, 50(3):51–53, 2007.

[149] G. F. Marias, C. Delakouridis, L. Kazatzopoulos, and P. Georgiadis. Location Privacy through Secret Sharing Techniques. In *Workshop on Trust, Security and Privacy for Ubiquitous Computing at WOWMOM '05*, pages 614–620. IEEE CS, 2005.

[150] G. F. Marias, L. Kazatzopoulos, C. Delakouridis, and P. Georgiadis. Applying Privacy on the Dissemination of Location Information. *Telematics and Informatics*, 23(3):211–225, 2006.

[151] L. Martin. Identity-Based Encryption: A Closer Look. *ISSA*, (Sep.):22–24, 2005.

[152] L. A. Martucci, S. Ries, and M. Mühlhäuser. Identifiers, Privacy and Trust in the Internet of Services. In *IFIP International Conference on Trust Management (IFIPTM '10)*, 2010.

[153] L. A. Martucci, S. Ries, and M. Mühlhäuser. Sybil-Free Pseudonyms, Privacy and Trust: Identity Management in the Internet of Services. *Journal of Information Processing*, 19:317–331, 2011.

[154] U. M. Maurer. Modelling a Public-Key Infrastructure. In *European Symposium on Research in Computer Security (ESORICS '96)*, pages 325–350. Springer, 1996.

[155] R. Mayrhofer, A. Sommer, and S. Saral. Air-Writing: a Platform for Scalable, Privacy-Preserving, Spatial Group Messaging. In *International Conference on Information Integration and Web-based Applications & Services (iiWAS '10)*, pages 183–191. ACM Press, 2010.

[156] S. Mehrotra, C. Butts, D. Kalashnikov, N. Venkatasubramanian, R. Rao, G. Chockalingam, R. Eguchi, B. Adams, and C. Huyck. Project Rescue: Challenges in Responding to the Unexpected. *SPIE Journal of Electronic Imaging, Displays, and Medical Imaging*, 5304:179–192, January 2004.

[157] A. Meissner, T. Luckenbach, T. Risse, T. Kirste, and H. Kirchner. Design Challenges for an Integrated Disaster Management Communication and Information System. *Workshop on Disaster Recovery Networks (DIREN '02)*, 2002.

[158] A. Meissner, Z. Wang, W. Putz, and J. Grimmer. MIKoBOS - A Mobile Information and Communication System for Emergency Response. In *International Conference on Information Systems for Crisis Response and Management (ISCRAM '06)*, 2006.

[159] A. Menezes. An Introduction to Pairing-Based Cryptography. Notes from Lectures, 2005.

[160] M. C. Mont, P. Bramhall, and K. Harrison. A Flexible Role-Based Secure Messaging Service: Exploiting IBE Technology for Privacy in Health Care. In *Workshop on Database and Expert Systems Applications (DEXA '03)*, pages 432–437. IEEE CS, 2003.

[161] M. Mühlhäuser and I. Gurevych. Introduction to Ubiquitous Computing. In *Handbook of Research on Ubiquitous Computing Technology for Real Time Enterprises*, pages 1–20. IGI Global Publisher, 2008.

[162] M. Mühlhäuser and I. Gurevych, editors. *Ubiquitous Computing Technology for Real Time Enterprises - Handbook of Research*. IGI Global Publisher, 2008.

[163] Y. Murakami. Privacy Issues in the Ubiquitous Information Society and Law in Japan. In *Conference on Systems, Man, and Cybernetics (SMC '04)*, pages 5645–5650. IEEE CS, 2004.

[164] B. W. Murgatroyd. End to End Encryption in Public Safety TETRA Networks. *IE Seminar on Secure GSM and Beyond: End to End Security for mobile Communication*, (Digest No. 2003/10059), 2003.

[165] C. Nickel, M. O. Derawi, P. Bours, and C. Busch. Scenario Test of Accelerometer-Based Biometric Gait Recognition. In *International Workshop on Security and Communication Networks (IWSCN '11)*. IEEE CS, 2011.

[166] M. Ohkubo, K. Suzuki, and S. Kinoshita. Cryptographic Approach to Privacy-Friendly Tags. In *RFID Privacy Workshop*. MIT Press, 2003.

[167] M. Ohkubo, K. Suzuki, and S. Kinoshita. RFID Privacy Issues and Technical Challenges. *Communications of the ACM*, 48(9):66–71, 2005.

[168] S. Ortmann, P. Langendörfer, and M. Maaser. Adapting Pervasive Systems to Multi-User Privacy Requirements. *International Journal of Ad Hoc and Ubiquitous Computing*, 3(4):264–276, 2008.

[169] C. Park, K. Itoh, and K. Kurosawa. Efficient Anonymous Channel and All/Nothing Election Scheme. In *Advances in Cryptology - EUROCRYPT 93*, pages 248–259. Springer, 1993.

[170] J. Pato. Identity Management. In *Encyclopedia of Cryptography and Security*, pages 282–285. Springer, 2005.

[171] C. Patrikakis, P. Karamolegkos, A. Voulodimos, M. H. A. Wahab, N. S. A. M. Taujuddin, C. Hanif, L. Pareschi, D. Riboni, S. G. Weber, A. Heinemann, S. S. Cheung, J. Chaudhari, and J. K. Paruchuri. Security and Privacy in Pervasive Computing. *IEEE Pervasive Computing*, 6(4):73–75, 2007.

[172] T. P. Pedersen. A Threshold Cryptosystem without a Trusted Party (Extended Abstract). In *Advances in Cryptology - EUROCRYPT '91*, pages 522–526. Springer, 1991.

[173] T. P. Pedersen. *Distributed Provers and Verifiable Secret Sharing Based on the Discrete Logarithm Problem*. PhD thesis, University of Aarhus, Department of Computer Science, Denmark, March 1992.

[174] A. Pfitzmann. Multilateral Security: Enabling Technologies and Their Evaluation. In *Conference on Emerging Trends in Information and Communication Security (ETRICS '06)*, pages 1–13. Springer, 2006.

[175] A. Pfitzmann and M. Hansen. A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml, Dec. 2009. v0.32.

[176] A. Pfitzmann, A. Juschka, A.-K. Stande, S. Steinbrecher, and S. Köpsell. Communication Privacy. In *Digital Privacy: Theory, Technologies and Practices*, pages 19–45. Taylor & Frances, 2007.

[177] A. Pfitzmann and M. Waidner. Networks without User Observability. *Computers and Security*, 6:158–166, May 1987.

[178] B. Pfitzmann, M. Waidner, and A. Pfitzmann. Secure and Anonymous Electronic Commerce: Providing Legal Certainty in Open Digital Systems Without Compromising Anonymity. Technical Report IBM Research Report RZ 3232 (93278) 05/22/00, IBM Research Division, 2000.

[179] D. J. Phillips. Beyond Privacy: Confronting Locational Surveillance in Wireless Communication. *Communication Law and Policy*, 8(1):1–23, 2003.

[180] M. Pielot and S. Boll. Tactile Wayfinder: Comparison of Tactile Waypoint Navigation with Commercial Pedestrian Navigation Systems. In *Conference on Pervasive Computing (PERVASIVE '10)*, pages 76–93. Springer, 2010.

[181] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure Attribute-Based Systems. In *ACM Conference on Computer and Communications Security (CCS '06)*, pages 99–112. ACM Press, 2006.

[182] K. Rannenberg. Multilateral Security - a Concept and Examples for Balanced Security. In *Workshop on New Security Paradigms (NSPW '00)*, pages 151–162. ACM Press, 2000.

[183] K. Rannenberg, A. Pfitzmann, and G. Müller. IT Security and Multilateral Security. In *Multilateral Security for Global Communication - Technology, Infrastructure, Economy*, page 21 29, 1999.

[184] A. Redz. On Equality Testing Protocols and their Security. Technical report, KTH Stockholm, 2003.

[185] Referat Kommunikation der TU Darmstadt. Medieninformation: Neue Sicherheitstechnik vor Gericht, 2010.

[186] R. Rivest. The MD5 Message-Digest Algorithm, 1992.

[187] C. M. Roberts. Radio Frequency Identification (RFID). *Computers and Security*, 25(1):18–26, 2006.

[188] A. Roßnagel. Simulationsstudien als Methode der Technikgestaltung. In G. Müller and K.-H. Stapf, editors, *Mehrseitige Sicherheit in der Kommunikationstechnik - Band 2: Erwartung, Akzeptanz, Nutzung*, pages 323–334. 1999.

[189] A. Roßnagel, M. Bedner, and D. Heinson. IT-Sicherheitstechnik vor Gericht. CASED Internal Report, 2011.

[190] A. Roßnagel. Datenschutz in der Welt allgegenwärtigen Rechnens (Privacy in a World of Ubiquitous Computing). *it - Information Technology*, 49(2):83–90, 2007.

[191] J. Ryoo and Y. B. Choi. A Comparison and Classification Framework for Disaster Information Management Systems. *International Journal of Emergency Management (IJEM)*, 3(4):264–279, 2006.

[192] A. Sahai and B. Waters. Fuzzy Identity-Based Encryption. In *Advances in Cryptology - EUROCRYPT '05*, pages 457–473. Springer, 2005.

[193] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. Role-Based Access Control Models. *IEEE Computer*, 29(2):38–47, 1996.

[194] M. Satyanarayanan. Pervasive Computing: Vision and Challenges. *IEEE Personal Communications*, 8(4):10 –17, 2001.

[195] M. Satyanarayanan. Privacy: The Achilles Heel of Pervasive Computing? *IEEE Pervasive Computing*, 2(1):2–3, 2003.

[196] M. Satyanarayanan. When Disaster Strikes. *IEEE Pervasive Computing*, 03(4):2–3, 2004.

[197] B. N. Schilit, N. Adams, and R. Want. Context-Aware Computing Applications. In *Workshop on Mobile Computing Systems and Applications*, pages 85–90. IEEE CS, 1994.

[198] B. N. Schilit and M. M. Theimer. Disseminating Active Map Information to Mobile Hosts. *IEEE Network*, 8(5):22–32, 1994.

[199] S. Schlott. *Privacy- und Sicherheitsaspekte in Ubiquitären Umgebungen*. PhD thesis, Universität Ulm, 2008.

[200] B. Schneier and J. Kelsey. Secure Audit Logs to Support Computer Forensics. *ACM Trans. Inf. Syst. Secur.*, 2(2):159–176, 1999.

[201] L. Scott and D. E. Denning. A Location Based Encryption Technique and Some of Its Applications. In *ION National Technical Meeting 2003*, pages 730–740, 2003.

[202] A. Shamir. How to Share a Secret. *Communications of the ACM*, 22(11):612–613, 1979.

[203] C. E. Shannon. Communication Theory of Secrecy Systems. *The Bell System Technical Journal*, 28:656–715, 1949.

[204] Y. Shen, T. C. Lam, J.-C. Liu, and W. Zhao. On the Confidential Auditing of Distributed Computing Systems. In *International Conference on Distributed Computing Systems (ICDCS'04)*, pages 600–607. IEEE CS, 2004.

[205] Simulationsgericht Darmstadt. Urteil Fall 2 der CASED Simulationsstudie, 2011.

[206] Simulationsgericht Darmstadt. Urteil Fall 6 der CASED Simulationsstudie, 2011.

[207] Y. R. Slim Trabelsi. Enabling Secure Service Discovery with Attribute Based Encryption. Technical Report RR-06-164, Eurecom, 2006.

[208] M. Sobirey and S. Fischer-Hübner. Privacy-Oriented Auditing. In *Procceedings of the 13th Annual Workshop on Design for Protecting the User*. CSR (Centre for Software Reliability), 1996.

[209] M. Sobirey, S. Fischer-Hübner, and K. Rannenberg. Pseudonymous Audit for Privacy Enhanced Intrusion Detection. In *IFIP International Information Security Conference (SEC'97)*, pages 151–163. Chapman & Hall, 1997.

[210] M. Sobirey, B. Richter, and H. König. The Intrusion Detection System AID - Architecture, and Experiences in Automated Audit Analysis. In *Communications and Multimedia Security (CMS '96)*, pages 278–290, 1996.

[211] D. J. Solove. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3), 2006.

[212] A. Soppera and T. Burbridge. Maintaining Privacy in Pervasive Computing Enabling Acceptance of Sensor-Based Services. *BT Technology Journal*, 22:106–118, July 2004.

[213] S. Spiekermann. *User Control in Ubiquitous Computing: Design Alternatives and User Acceptance*. Shaker Verlag, 2008.

[214] F. Stajano. Security Issues in Ubiquitous Computing. In *Handbook of Ambient Intelligence and Smart Environments*, pages 281–314. Springer, 2010.

[215] T. Straub and A. Heinemann. Security for Ubiquitous Computing. In *Handbook of Research on Ubiquitous Computing Technology for Real Time Enterprises*, pages 337–362. IGI Global Publisher, 2008.

[216] N. Streitz. The Disappearing Computer. *Commun. ACM*, 48(3), 2005.

[217] R. C. Stuart. Digital Evidence. In H. Bidgoli, editor, *Handbook of Information Security, Vol. 2*, pages 658–663. John Wiley Sons, 2006.

[218] P. Traynor, K. Butler, W. Enck, and P. McDaniel. Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems. In *Network and Distributed System Security Symposium (NDSS '08)*. The Internet Society, 2008.

[219] E. Troshynski, C. Lee, and P. Dourish. Accountabilities of Presence: Reframing Location-Based Systems. In *Conference on Human Factors in Computing Systems (CHI '08)*, pages 487–496. ACM Press, 2008.

[220] H.-L. Truong, L. Juszczyk, A. Manzoor, and S. Dustdar. ESCAPE - An Adaptive Framework for Managing and Providing Context Information in Emergency Situations. In *European Conference on Smart Sensing and Context (EuroSSC '07)*. Springer, 2007.

[221] G. Tselentis, J. Domingue, A. Galis, A. Gavras, D. Hausheer, S. Krco, V. Lotz, and T. Zahariadis, editors. *Towards the Future Internet - A European Research Perspective*. IOS Press, 2009.

[222] Y. Tsiounis and M. Yung. On the Security of ElGamal Based Encryption. In *Workshop on Practice and Theory in Public Key Cryptography (PKC '98)*, pages 117–134. Springer, 1998.

[223] M. Turoff, M. Chumer, B. Van de Walle, and X. Yao. The Design of a Dynamic Emergency Response Management Information System (dermis). *The Journal of Information Technology Theory and Application (JITTA)*, 5(4):1–35, 2004.

[224] S. U.S. Department of Health, Education and Welfare. *Records, Computers, and the Rights of Citizens.* MIT Press, 1973.

[225] B. Van de Walle and M. Turoff. Introduction to Emergency Response Information Systems: Emerging Trends and Technologies. *Communications of the ACM*, 50:29–31, 2007.

[226] J. Wall, J. K. Ward, L. Castro, J. Favela, M. Perez, C. Gacia-Pena, S. Berkovsky, C. Lueg, G. Verdouw, F. C. Pereira, P. Correia, J. Rodrigues, M. Ferreira, P. Gomes, C. Olaverri-Monreal, D. Bolchini, S. G. Weber, E. Park, and H. S. Nam. Large-Scale Opportunistic Sensing. *IEEE Pervasive Computing*, 10(4):54–58, 2011.

[227] R. Want, K. P. Fishkin, A. Gujar, and B. L. Harrison. Bridging Physical and Virtual Worlds with Eelectronic Tags. In *Conference on Human Factors in Computing Systems (CHI '99)*, pages 370–377. ACM Press, 1999.

[228] S. Warren and L. Brandeis. The Right to Privacy. *Harvard Law Review*, IV(5), 1890.

[229] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters. Building an Encrypted and Searchable Audit Log. In *Network and Distributed System Security Symposium (NDSS '04)*. The Internet Society, 2004.

[230] S. G. Weber. Harnessing Pseudonyms with Implicit Attributes for Privacy-Respecting Mission Log Analysis. In *Conference on Intelligent Networking and Collaborative Systems (INCoS '09)*, pages 119 – 126. IEEE CS, 2009.

[231] S. G. Weber. Secure and Efficient First Response Coordination Based on Attribute-Based Encryption Techniques. ISCRAM '09 Student Poster Session, 2009.

[232] S. G. Weber. Securing First Response Coordination with Dynamic Attribute-Based Encryption. In *Conference on Privacy, Security and Trust (PST '09) in conjunction with World Congress on Privacy, Security, Trust and the Management of e-Business (CONGRESS '09)*, pages 58 – 69. IEEE CS, 2009.

[233] S. G. Weber. Unterlagen zur Evaluation durch Anwendungspartner am 03.12.2009 in Darmstadt, Gegenstand der Evaluation: Plugin für sichere Gruppenkommunikation. SoKNOS Internal Document, 2009.

[234] S. G. Weber. A Hybrid Encryption Technique Supporting Expressive Policies. In *Tagungsband des 13. Kryptotags. Workshop der Fachgruppe "Angewandte Kryptographie" der "Gesellschaft für Informatik e.V."*., page 5, 2010.

[235] S. G. Weber and R. Drüeke. Ubiquitous Computing: Zwischen Privatheit und (Eigen-)Verantwortlichkeit. In *Deutschsprachiges Symposiums des International Center for Information Ethics (ICIE '08): Wandel des Internets - Wandel der Informationsethik? Schwerpunkt: Das Internet ohne Personalcomputer*, 2008.

[236] S. G. Weber, A. Heinemann, and M. Mühlhäuser. Towards an Architecture for Balancing Privacy and Traceability in Ubiquitous Computing Environments. In *Workshop on Privacy and Assurance (WPA '08) at Conference on Availability, Reliability and Security (ARES '08)*, pages 958–964. IEEE CS, 2008.

[237] S. G. Weber, Y. Kalev, S. Ries, and M. Mühlhäuser. MundoMessage: Enabling Trustworthy Ubiquitous Emergency Communication. In *International Conference on Ubiquitous Information Management and Communication (ICUIMC '11)*, pages 29:1–29:10. ACM Press, 2011.

[238] S. G. Weber, L. A. Martucci, S. Ries, and M. Mühlhäuser. Towards Trustworthy Identity and Access Management for the Future Internet. In *4th International Workshop on Trustworthy Internet of People, Things & Services (Trustworthy IoPTS '10) in conjunction with Internet of Things conference (IoT '10)*, 2010.

[239] S. G. Weber and M. Mühlhäuser. Multilaterally Secure Ubiquitous Auditing. In *Intelligent Networking and Collaborative Systems and Applications, SCI 329*, pages 207–233. Springer, 2010.

[240] S. G. Weber, S. Ries, and A. Heinemann. Inherent Tradeoffs in Ubiquitous Computing Services. In *INFORMATIK '07*, pages 364–368. GI, 2007.

[241] S. G. Weber, S. Ries, and M. Mühlhäuser. Concepts and Scheme for Multilaterally Secure, User-Friendly Attribute-Based Messaging. Technical Report TR-13, Telecooperation Research Division, TU Darmstadt, Darmstadt, October 2010. ISSN 1864-0516.

[242] W. Weber, J. M. Rabaey, and E. Aarts, editors. *Ambient Intelligence*. Springer, 2007.

[243] M. Weiser. The Computer for the 21st Century. *Scientific American*, 265(3):94–104, 1991.

[244] M. Weiser. Some Computer Science Issues in Ubiquitous Computing. *Communications of the ACM*, 36(7):75–84, 1993.

[245] A. Westin. *Privacy and Freedom*. Atheneum, New York, 1967.

[246] P. Windley. *Digital Identity*. OReilly, 2005.

[247] M. Wright, M. Adler, B. N. Levine, and C. Shields. An Analysis of the Degradation of Anonymous Protocols. In *Network and Distributed System Security Symposium (NDSS '02)*. The Internet Society, 2002.

[248] A. C. Yao. Protocols for Secure Computations (Extended Abstract). In *Symposium on Foundations of Computer Science (FOCS '82)*, pages 160–164. IEEE CS, 1982.

[249] E. Yuan and J. Tong. Attribute Based Access Control (ABAC) for Web Services. In *Conference on Web Services (ICWS'05)*, pages 561 – 569. IEEE CS, 2005.

[250] T. Ziegert. SoKNOS - ein Forschungsprojekt im Bereich öffentliche Sicherheit. SoKNOS Abschlussbericht, 2010.

[251] T. Ziegert. SoKNOS Evaluationsreport. SoKNOS Project Deliverable D.WP 1.9b, 2010.

[252] A. Zugenmaier and T. Walter. Security in Pervasive Computing: Calling for new Security Principles. In *Conference on Pervasive Services (PerSer '07)*, pages 96–99. IEEE CS, 2007.