Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology

(Version v0.29 July 31, 2007)

Andreas Pfitzmann
TU Dresden
pfitza@inf.tu-dresden.de

Marit Hansen
ULD Kiel
marit.hansen@datenschutzzentrum.de

Archive of this Document

http://dud.inf.tu-dresden.de/Anon_Terminology.shtml (v0.5 and all succeeding versions)

Starting with v0.20, color is essential to understand the figures and part of the translations.

Abstract

Based on the nomenclature of the early papers in the field, we propose a terminology which is both expressive and precise. More particularly, we define *anonymity*, *unlinkability*, *undetectability*, *unobservability*, *pseudonymity* (*pseudonyms* and *digital pseudonyms*, and their attributes), and *identity management*. In addition, we describe the relationships between these terms, give a rationale why we define them as we do, and sketch the main mechanisms to provide for the properties defined.

Table of contents

Table of figures

List of abbreviations

DC-net	Dining Cryptographers network
iff	if and only if
IHW	Information Hiding Workshop
IMS	Identity Management System
IOI	Item Of Interest
ISO	International Standardization Organization
MMORPG	Massively Multiplayer Online Role Playing Games
MUD	Multi User Dungeon
PE-IMS	Privacy-Enhancing Identity Management System
PETs	Privacy-Enhancing Technologies
PGP	Pretty Good Privacy
w.r.t.	with respect to

Change History

v0.1	July 28, 2000	Andreas Pfitzmann, pfitza@inf.tu-dresden.de
v0.2	Aug. 25, 2000	Marit Köhntopp, marit@koehntopp.de
v0.3	Sep. 01, 2000	Andreas Pfitzmann, Marit Köhntopp
v0.4	Sep. 13, 2000	Andreas Pfitzmann, Marit Köhntopp: Changes in sections Anonymity, Unobservability, Pseudonymity
v0.5	Oct. 03, 2000	Adam Shostack, adam@zeroknowledge.com, Andreas Pfitzmann, Marit Köhntopp: Changed definitions, unlinkable pseudonym
v0.6	Nov. 26, 2000	Andreas Pfitzmann, Marit Köhntopp: Changed order, role-relationship pseudonym, references
v0.7	Dec. 07, 2000	Marit Köhntopp, Andreas Pfitzmann
v0.8	Dec. 10, 2000	Andreas Pfitzmann, Marit Köhntopp: Relationship to Information Hiding Terminology
v0.9	April 01, 2001	Andreas Pfitzmann, Marit Köhntopp: IHW review comments
v0.10	April 09, 2001	Andreas Pfitzmann, Marit Köhntopp: Clarifying remarks
v0.11	May 18, 2001	Marit Köhntopp, Andreas Pfitzmann
v0.12	June 17, 2001	Marit Köhntopp, Andreas Pfitzmann: Annotations from IHW discussion
v0.13	Oct. 21, 2002	Andreas Pfitzmann: Some footnotes added in response to comments by David-Olivier Jaquet-Chiffelle, jld@hta-bi.bfh.ch
v0.14	May 27, 2003	Marit Hansen, marit.hansen@t-online.de, Andreas Pfitzmann: Minor corrections and clarifying remarks
v0.15	June 03, 2004	Andreas Pfitzmann, Marit Hansen: Incorporation of comments by Claudia Diaz; Extension of title and addition of identity management terminology
v0.16	June 23, 2004	Andreas Pfitzmann, Marit Hansen: Incorporation of lots of comments by Giles Hogben, Thomas Kriegelstein, David-Olivier Jaquet-Chiffelle, and Wim Schreurs; relation between anonymity sets and identifiability sets clarified
v0.17	July 15, 2004	Andreas Pfitzmann, Marit Hansen: Triggered by questions of Giles Hogben, some footnotes added concerning quantification of terms; Sandra Steinbrecher caused a clarification in defining pseudonymity
v0.18	July 22, 2004	Andreas Pfitzmann, Marit Hansen: Incorporation of comments by Mike Bergmann, Katrin Borcea, Simone Fischer-Hübner, Giles Hogben, Stefan Köpsell, Martin Rost, Sandra Steinbrecher, and Marc Wilikens
v0.19	Aug. 19, 2004	Andreas Pfitzmann, Marit Hansen: Incorporation of comments by Adolf Flüeli; footnotes added explaining pseudonym = nym and identity of individual generalized to identity of entity
v0.20	Sep. 02, 2004	Andreas Pfitzmann, Marit Hansen: Incorporation of comments by Jozef Vyskoc; figures added to ease reading
v0.21	Sep. 03, 2004	Andreas Pfitzmann, Marit Hansen: Incorporation of comments at the PRIME meeting and by Thomas Kriegelstein; two figures added
v0.22	July 28, 2005	Andreas Pfitzmann, Marit Hansen: Extension of title, adding a footnote suggested by Jozef Vyskoc, some clarifying remarks by Jan Camenisch (on pseudonyms and credentials), by Giles Hogben (on identities), by Vashek Matyas (on the definition of unobservability, on pseudonym, and on authentication), by Daniel Cvrcek (on knowledge and attackers), by Wassim Haddad (to avoid ambiguity of wording in two cases), by Alf Zugenmair (on subjects), by Claudia Diaz (on robustness of anonymity), and by Katrin Borcea-Pfitzmann and Elke Franz (on evolvement of (partial) identities over time)
v0.23	Aug. 25, 2005	Andreas Pfitzmann, Marit Hansen: New first page; adding list of abbreviations and index, translation of essential terms to German, definitions of misinformation and disinformation, clarification of liability broker vs. value broker; some clarifying remarks suggested by Thomas

	Kriegelstein on credentials, identity, complete identity, system, subject, digital pseudonyms, and by Sebastian Clauß on unlinkability
v0.24 Nov. 21, 2005	Andreas Pfitzmann, Marit Hansen: Incorporating clarification of whether organizations are subjects or entities; suggestion of the concept of linkability brokers by Thomas Kriegelstein; clarification on civil identity proposed by Neil Mitchison; corrections of 2 typos found by Rolf Wendolsky; Stefanos Gritzalis, Christos Kalloniatis: Translation of essential terms to Greek
v0.25 Dec. 06, 2005	Andreas Pfitzmann, Marit Hansen: Clarification of how to consider the possible change of attributes in time; Giovanni Baruzzi: Translation of essential terms to Italian
v0.26 Dec. 13, 2005	Yves Deswarte: Translation of essential terms to French
v0.27 Feb. 20, 2006	Vashek Matyas, Zdenek Riha, Alena Honigova: Translation of essential terms to Czech; Stefanos Gritzalis, Christos Kalloniatis: Improved translation of essential terms to Greek; Giovanni Baruzzi, Giuseppe Palumbo: Improved translation of essential terms to Italian
v0.28 May 29, 2006	Andreas Pfitzmann, Marit Hansen: Abbreviation ID deleted, “consolidated proposal”, new def. “undetectability”, changed defs. “unobservability” and “pseudonym(ous)”; “relationship anonymity set” and “unobservability sets” clarified; Sections 6, 8, and 10.2 renamed; Appendix “Relationships between some terms used” added – all that triggered by discussions with Katrin Borcea-Pfitzmann, Sebastian Clauß, Giles Hogben, Thomas Kriegelstein, Stefan Schiffner, Sandra Steinbrecher; a few Italian terms corrected
v0.29 July 31, 2007	Sandra Steinbrecher constructed – for one might-be interpretation of the attacker model – a counterexample against “sender anonymity ⇒ relationship anonymity” and “recipient anonymity ⇒ relationship anonymity” in Section 7: “If many senders send a message each, enjoying perfect sender anonymity, but all these messages go to the same recipient, no relationship anonymity is given, since each of these senders knows the recipient(s) of his/her message. And vice versa: If many recipients receive a message each, enjoying perfect recipient anonymity, but all these messages come from the same sender, no relationship anonymity is given, since each of these recipients knows the sender of his/her message received.” This is not what we (Andreas Pfitzmann, Marit Hansen) meant – it teaches us to slightly revise the definition of relationship anonymity: Each sender does, of course, not enjoy sender anonymity against him/herself nor does any of the recipients enjoy recipient anonymity against him/herself. Therefore, the implications cited above are – as we may say after careful discussion: of course – only valid w.r.t. outsiders, i.e., attackers being neither the sender nor one of the recipients of the messages under consideration. Andreas Pfitzmann, Marit Hansen: the mixture of “absolute” and “relative” definitions of anonymity, unlinkability, undetectability, and unobservability unified by distinguishing from the very beginning between two defs. for each property: one with the original name and the other followed by “delta“; incorporating comments by Katrin Borcea-Pfitzmann, Sebastian Clauß, Maritta Heisel, Thomas Kriegelstein, Katja Liesebach, Stefanie Pötzsch, Sandra Steinbrecher, and Thomas Santen

1 Introduction

Early papers from the 1980ies already deal with anonymity, unlinkability, unobservability, and pseudonymity and introduce these terms within the respective context of proposed measures. We show relationships between these terms and thereby develop a consistent terminology. Then we contrast these definitions with newer approaches, e.g., from ISO IS 15408. Finally, we extend this terminology to identity management. Identity management is a much younger and much less defined field – so a really consolidated proposal for terminology for this field does not exist. But nevertheless, after development and broad discussion since 2004, we believe this terminology to be the most consolidated one in this rapidly emerging field.

We hope that the adoption of this terminology might help to achieve better progress in the field by avoiding that each researcher invents a language of his/her own from scratch. Of course, each paper will need additional vocabulary, which might be added consistently to the terms defined here.

This document is organized as follows: First the setting used is described. Then definitions of anonymity, unlinkability, undetectability, and unobservability are given and the relationships between the respective terms are outlined. Afterwards, known mechanisms to achieve anonymity and unobservability are listed. The next sections deal with pseudonymity, i.e., pseudonyms, their properties, and the corresponding mechanisms. Thereafter, this is applied to privacy-enhancing identity management. An overview of main definitions and their negations follows. Finally, concluding remarks are given. To make the document readable to as large an audience as possible, we did put information which can be skipped in a first reading or which is only useful to part of our readership, e.g., those knowing information theory, in footnotes.

2 Setting

We develop this terminology in the usual setting that *senders* send *messages* to *recipients* using a *communication network*, i.e., *stations*[1] send and receive messages using *communication lines*[2]. For other settings, e.g., users querying a database, customers shopping in an e-commerce shop, the same terminology can be derived by abstracting away the special names “sender”, “recipient”, and “message”. But for ease of explanation, we use the specific setting here, cf. Fig. 1. Only if what we have to say is valid in a broader context without requiring further explanations, we speak more generally about *acting entities* called *actors* (such as senders) and *entities acted upon* called *actees* (such as recipients).[3]

Irrespective whether we speak of senders and recipients or whether we generalize to actors and actees, we regard a *subject* as a possibly acting entity such as, e.g., a human being (i.e., a natural person), a legal person, or a computer. An organization not acting as a legal person we

[1] To keep the setting as simple as possible, usually, we do not distinguish between *human senders* and the *stations* which are used to send messages. Putting it the other way round, usually, we assume that each station is controlled by exactly one human being, its owner. If a differentiation between human communication and computer communication is necessary or if the assumption that each station is controlled by exactly one human being is wrong, the setting has to be more complex. We then use *sender* and *recipient* for human beings and *message* for their communication. For computers and their communications, we use *stations* sending *bit strings*. If we have to look even deeper than bits which are “abstractions” of physical signals, we call the representation of bit strings *signals*.

[2] Communication “lines” are not necessarily wires or optical fibers, but may be just free space in case of radio networks.

[3] Note that these terms intended to generalize the setting are by no means fixed yet. In a communication it is easy to define the counterparts *sender* and *recipient(s)*, and so are *actors* and *actees* counterparts. An *actee* could be a subject or object addressed by an *actor*.

neither see as a single subject nor as a single entity, but as (possibly structured) sets of subjects or entities. Otherwise, the distinction between “subjects” and “sets of subjects” would completely blur.[4]

If we make our setting more concrete, we may call it a *system*. For our purposes, a system has the following relevant properties:

1. The system has a surrounding, i.e., parts of the world are “outside” the system. Together, the system and its surrounding form the universe.
2. The state of the system may change by actions within the system.

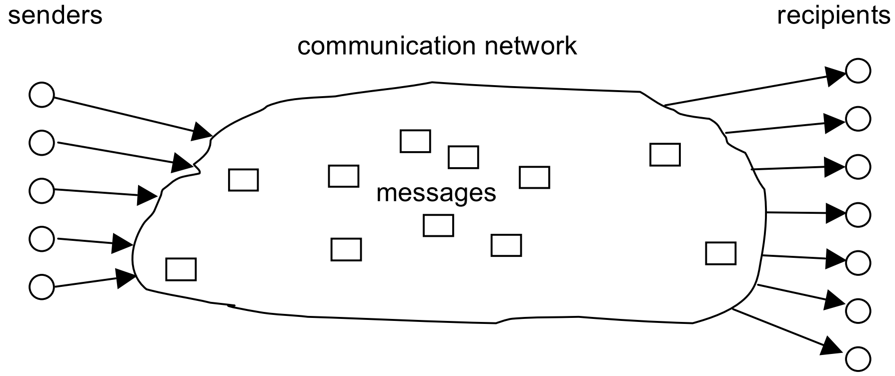


Fig. 1: Setting

All statements are made from the perspective[5] of an *attacker*[6,7] who may be interested in monitoring what communication is occurring, what patterns of communication exist, or even in manipulating the communication. The attacker may be an outsider[8] tapping communication lines or an insider[9] able to participate in normal communications and controlling at least some stations, cf. Fig. 2. We assume that the attacker uses all information available to him to infer (probabilities of) his *items of interest* (IOIs), e.g., who did send or receive which messages. Related to the IOIs are attributes because they may be items of interest themselves or their observation may give information on IOIs: An *attribute* is a quality or characteristic of an entity or an action. Mainly we are interested in attributes of subjects. Examples for attributes in this setting are “sending a message” or “receiving a message”.

[4] Having a clear distinction between subjects and sets of subjects is very useful to sensibly define group pseudonyms in Section 9.

[5] The *perspective* describes the *set of all possible observations*. In the following, a property holds “from an attacker’s perspective” iff it holds for all possible observations of that perspective.

[6] “Attacker” is the historical name of the set of entities working against some protection goal like anonymity. To underline that conflicts of interests are commonplace, “adversary” is used as a synonym for “attacker” in part of the more recent literature on security.

[7] The attacker’s perspective depends on the information the attacker has available. If we assume some limits on how much processing the attacker might be able to do, the information available to the attacker will not only depend on the attacker’s perspective, but on the attacker’s processing (abilities), too.

[8] An outsider is a non-empty set of entities being part of the surrounding of the system considered.

[9] An insider is a non-empty set of entities being part of the system considered.

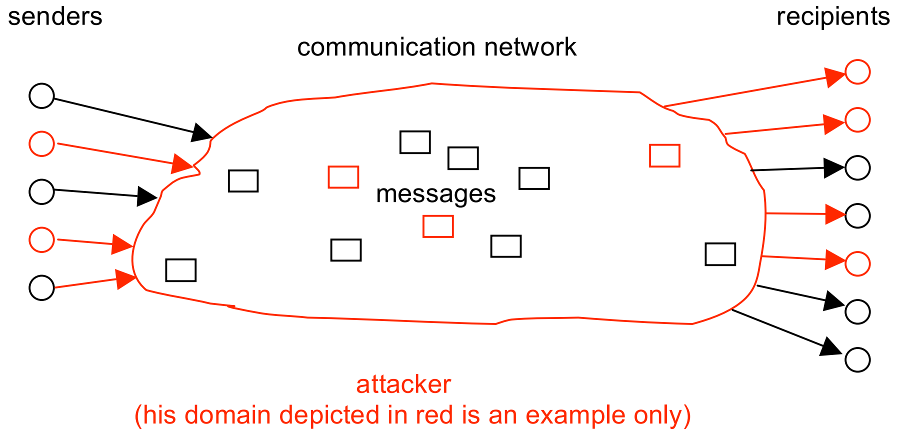


Fig. 2: Example of an attacker's domain within the setting

Throughout the Sections 3 to 12 we assume that the attacker is not able to get information on the sender or recipient from the message content.[10] Therefore, we do not mention the message content in these sections. For most applications it is unreasonable to assume that the attacker forgets something. Thus, normally the knowledge[11] of the attacker only increases.

3 Anonymity

To enable anonymity of a subject, there always has to be an appropriate set of subjects with potentially the same attributes[12]. This leads to a first kind of a definition:

***Anonymity* of a subject means that the subject is not identifiable[13] within a set of subjects, the *anonymity set*.[14]**

The *anonymity set* is the set of all possible subjects[15]. With respect to actors, the anonymity set consists of the subjects who might cause an action. With respect to actees, the anonymity set consists of the subjects who might be acted upon. Therefore, a sender may be anonymous

[10] Of course, encryption of messages provides protection of the content against attackers observing the communication lines and end-to-end encryption even provides protection of the content against all stations passed, e.g. for the purpose of forwarding and/or routing. But message content can neither be hidden from the sender nor from the recipient(s) of the message.

[11] As usual in the field of security and privacy, "knowledge" can be described by probabilities of IOIs. More knowledge then means more accurate probabilities, i.e. the probabilities the attacker assumes to be true are closer to the "true" probabilities.

[12] Since sending and receiving of particular messages are special cases of "attributes" of senders and recipients, this is slightly more general than the setting in Section 2. This generality is very fortunate to stay close to the everyday meaning of "anonymity" which is not only used w.r.t. subjects active in a particular context, e.g. senders and recipients of messages, but w.r.t. subjects passive in a particular context as well, e.g. subjects the records within a database relate to.

[13] "not identifiable within" means "not uniquely characterized within".

[14] From [ISO99]: "[Anonymity] ensures that a user may use a resource or service without disclosing the user's identity. The requirements for anonymity provide protection of the user identity. Anonymity is not intended to protect the subject identity. [...] Anonymity requires that other users or subjects are unable to determine the identity of a user bound to a subject or operation." Compared with this explanation, our definition is more general as it is not restricted to identifying users, but any subjects.

[15] I.e., the "usual suspects" :-) The set of possible subjects depends on the knowledge of the attacker. Thus, anonymity is relative with respect to the attacker.

(*sender anonymity*) only within a set of potential senders, his/her *sender anonymity set*, which itself may be a subset of all subjects worldwide who may send a message from time to time. The same for the recipient means that a recipient may be anonymous (*recipient anonymity*) only within a set of potential recipients, his/her *recipient anonymity set*, cf. Fig. 3. Both anonymity sets may be disjoint, be the same, or they may overlap. The anonymity sets may vary over time.[16]

Anonymity of a set of subjects within an (potentially larger) anonymity set means that all these individual subjects are not identifiable within this anonymity set.[17]

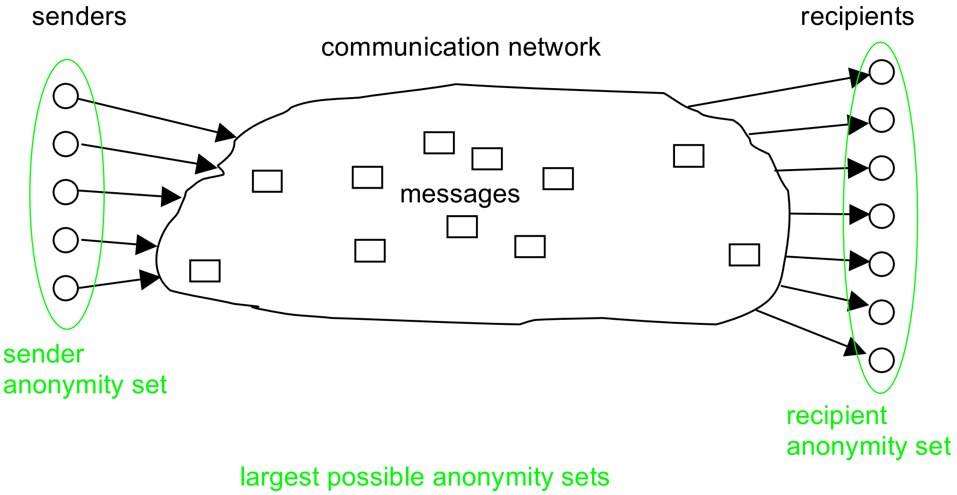


Fig. 3: Anonymity sets within the setting

The definition given above for anonymity basically defines anonymity as a binary property: Either a subject is anonymous or not. To reflect the possibility to quantify anonymity in our definition and to underline that all statements are made from the perspective of an attacker (cf. Fig. 4), it is appropriate to work with a slightly more complicated definition in the following:

Anonymity* of a subject from an attacker's perspective means that the attacker cannot sufficiently identify the subject within a set of subjects, the *anonymity set.

In this revised definition, "sufficiently" underlines both that there is a possibility to quantify anonymity and that for some applications, there might be a need to define a threshold where anonymity begins.

If we do not focus on the anonymity of one individual subject, but on the anonymity provided by a system to all of its users together, called *global anonymity*, we can state: All other things being equal, global anonymity is the stronger, the larger the respective anonymity set is and the more

[16] Since we assume that the attacker does not forget anything he knows, the anonymity set cannot increase w.r.t. a particular IOI. Especially subjects joining the system in a later stage, do not belong to the anonymity set from the point of view of an attacker observing the system in an earlier stage. (Please note that if the attacker cannot decide whether the joining subjects were present earlier, the anonymity set does not increase either: It just stays the same.) Due to linkability, cf. below, the anonymity set normally can only decrease.

[17] In this definition, "set of subjects" is just taken to describe that the anonymity property holds for all elements of the set. Another possible definition would be to consider the anonymity property for the set as a whole. Then a semantically quite different definition could read: Anonymity of a set *S* of subjects within a larger anonymity set *A* means that it is not distinguishable whether the subject whose anonymity is at stake (and which clearly is within *A*) is within *S* or not.

evenly distributed the sending or receiving, respectively, of the subjects within that set is.[18,19] For a fixed anonymity set, *global anonymity* is *maximal* iff all subjects within the anonymity set are equally likely. Since subjects[20] may behave quite distinct from each other (and trying to persuade them to behave more equally may both fail and be not compatible with basic human rights), achieving maximal anonymity or even something close to it usually is impossible. Strong or even maximal global anonymity does not imply strong anonymity or even maximal anonymity of each particular subject[21]: Even if global anonymity is strong, one (or a few) individuals might be quite likely, so their anonymity is weak. W.r.t. these “likely suspects”, nothing is changed if the anonymity set is made larger and sending and receiving of the other subjects are, e.g., distributed evenly. That way, arbitrarily strong global anonymity can be achieved without doing anything for the “likely suspects” [ClSc06]. So there is need to define anonymity measures not only for the system as a whole, but for individual subjects or small sets of subjects.

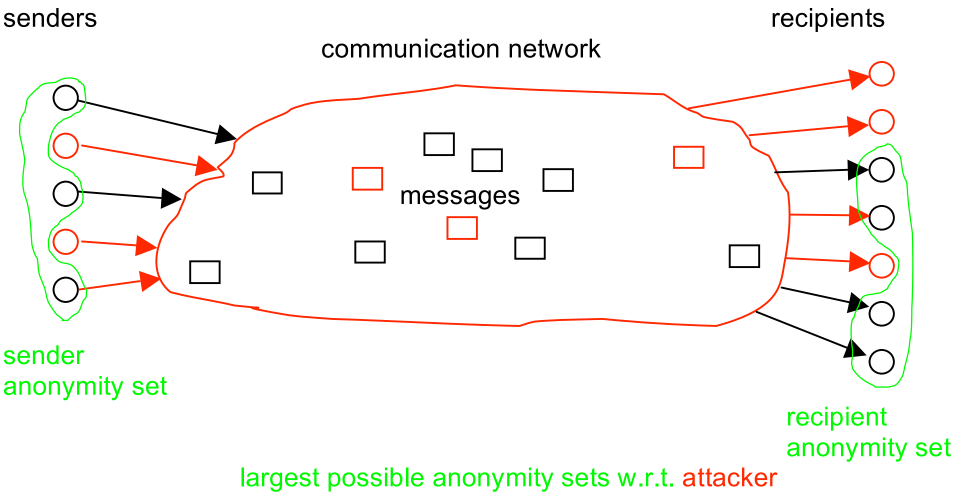


Fig. 4: Anonymity sets w.r.t. attacker within the setting

From the above discussion follows that anonymity in general as well as the anonymity of each particular subject is a concept which is very much context dependent (on, e.g., subjects population, attributes, time frame, etc). In order to quantify anonymity within concrete situations, one would have to describe the system in sufficient detail which is practically not (always) possible for large open systems (but maybe for some small data bases for instance). Besides the *quantity of anonymity* provided within a particular setting, there is another aspect of anonymity: its robustness. *Robustness of anonymity* characterizes how stable the quantity of anonymity is

[18] The *entropy* of a message source as defined by Claude E. Shannon [Shan48] might be an appropriate measure to quantify anonymity – just take who is the sender/recipient as the “message” in Shannon’s definition. For readers interested in formalizing what we informally say: “No change of probabilities” means “no change of knowledge” and vice versa. “No change of probabilities” (or what is equivalent: “no change of knowledge”) implies “no change of entropy”, whereas “no change of entropy” neither implies “no change of probabilities” nor “no change of knowledge”. In an easy to remember notation: No change of probabilities = no change of knowledge ⇒ no change of entropy.

[19] The definition of anonymity is an analog to the definition of “perfect secrecy” by Claude E. Shannon [Shan49], whose definition takes into account that no security mechanism whatsoever can take away knowledge from the attacker which he already has.

[20] Who are – hopefully – in the same anonymity set.

[21] What maximal anonymity of one individual subject means is unclear. On the one hand, if her probability approaches zero, her Shannon entropy (as a measure for anonymity) gets larger and larger. On the other hand, if her probability gets zero, she is outside the anonymity set.

against changes in the particular setting, e.g., a stronger attacker or different probability distributions. We might use *quality of anonymity* as a term comprising both quantity and robustness of anonymity. To keep this text as simple as possible, we will mainly discuss the quantity of anonymity in the following, using the wording "strength of anonymity".

The above definitions of anonymity and the mentioned measures of quantifying anonymity are fine to characterize the status of a subject in a world as is. If we want to describe *changes* to the anonymity of a subject if the world is changed somewhat, e.g., the subject uses the communication network differently or uses a modified communication network, we need another definition of anonymity capturing the delta. The simplest way to express this delta is by the observations of "the" attacker.

An *anonymity delta* (regarding a subject's anonymity) from an attacker's perspective specifies the difference between the subject's anonymity taking into account the attacker's observations (i.e., the attacker's a-posteriori knowledge) and the subject's anonymity given the attacker's a-priori knowledge only.[22]

Since anonymity cannot increase[16,19], having *no anonymity delta* means that anonymity stays the same.[23] To be able to express this conveniently, we use wordings like "perfect preservation of a subject's anonymity" to express that the anonymity delta is minimal, i.e., anonymity of the subject is exactly the same after the attacker's observations (a-posteriori knowledge of the attacker) as it is concerning his a-priori knowledge.[24]

As we can (and should) quantify anonymity in concrete situations, so we can (and should) quantify the anonymity delta.[25]

4 Unlinkability

Unlinkability only has a meaning after the system in which we want to describe anonymity properties has been defined and the entities interested in linking (the attacker) have been characterized. Then:

***Unlinkability* of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these IOIs are related or not.**[26,27]

[22] In some publications, the a-priori knowledge of the attacker is called "background knowledge" and the a-posteriori knowledge of the attacker is called "new knowledge".

[23] This means that if the attacker has no a-priori knowledge about the particular subject, having *no anonymity delta* implies anonymity. But if the attacker has an a-priori knowledge covering all actions of the particular subject, having no anonymity delta does not imply any anonymity at all. If there is no anonymity from the very beginning, even preserving it completely does not yield any anonymity.

[24] It might be worthwhile to generalize "preservation of anonymity of single subjects" to "preservation of anonymity of sets of subjects", in the limiting case all subjects in an anonymity set.

[25] This can be done by just defining:
quantity(anonymity delta) := quantity(anonymity_a-posteriori) – quantity(anonymity_a-priori)
If anonymity_a-posteriori and anonymity_a-priori are the same, their quantification is the same and therefore the difference of these quantifications is 0. If anonymity can only decrease (which usually is quite a reasonable assumption), the maximum of quantity(anonymity delta) is 0.

[26] From [ISO99]: "[Unlinkability] ensures that a user may make multiple uses of resources or services without others being able to link these uses together. [...] Unlinkability requires that users and/or subjects are unable to determine whether the same user caused certain specific

Linkability is the negation of unlinkability:

Linkability **of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker can sufficiently distinguish whether these IOIs are related or not.**

E.g., in a scenario with at least two senders, two messages sent by subjects within the same anonymity set are unlinkable for an attacker if for him, the probability that these two messages are sent by the same sender is sufficiently close to 1/(number of senders). In case of unicast the same is true for recipients, in case of multicast it is slightly more complicated.

An unlinkability delta **of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective specifies the difference between the unlinkability of these IOIs taking into account the attacker's observations and the unlinkability of these IOIs given the attacker's a-priori knowledge only.**

Since we assume that the attacker does not forget anything, having *no unlinkability delta* means that the probability of those items being related from the attacker's perspective stays exactly the same before (a-priori knowledge) and after the attacker's observations (a-posteriori knowledge of the attacker).[28,29] To be able to express this conveniently, we use wordings like "perfect preservation of unlinkability w.r.t. specific items" to express that the unlinkability delta is minimal.[30]

E.g., the unlinkability delta of two messages is sufficiently small (minimal) for an attacker if the probability describing his a-posteriori knowledge that these two messages are sent by the same sender and/or received by the same recipient is sufficiently (exactly) the same as the probability imposed by his a-priori knowledge.[31]

operations in the system." In contrast to this definition, the meaning of unlinkability in this text is less focused on the user, but deals with unlinkability of "items" and therefore takes a general approach.

[27] As the entropy of a message source might be an appropriate measure to quantify anonymity (and thereafter "anonymity" might be used as a quantity), we may use definitions to quantify unlinkability (and thereafter "unlinkability" might be used as a quantity as well). Quantifications of unlinkability can be either probabilities or entropies, or whatever is useful in a particular context.

[28] If the attacker has no a-priori knowledge about the particular IOIs, having *no unlinkability delta* implies unlinkability. But if the attacker has a-priori knowledge covering the relationships of all IOIs, having no unlinkability delta does not imply any unlinkability at all. If there is no unlinkability from the very beginning, even preserving it completely does not yield any unlinkability.

[29] Normally, the attacker's knowledge cannot decrease (analogously to Shannon's definition of "perfect secrecy", see above). An exception of this rule is the scenario where the use of *misinformation* (inaccurate or erroneous information, provided usually without conscious effort at misleading, deceiving, or persuading one way or another [Wils93]) or *disinformation* (deliberately false or distorted information given out in order to mislead or deceive [Wils93]) leads to a growing uncertainty of the attacker which information is correct. A related, but different aspect is that information may become wrong (i.e., outdated) simply because the state of the world changes over time. Since data protection is not only about to protect the current state, but the past and history of a data subject as well, we will not make use of this different aspect in the rest of this paper.

[30] It might be worthwhile to generalize "preservation of unlinkability of two IOIs" to "preservation of unlinkability of sets of IOIs", in the limiting case all IOIs in the system.

[31] Please note that unlinkability of two (or more) messages of course may depend on whether their content is protected against the attacker considered. In particular, messages may be unlinkable if we assume that the attacker is not able to get information on the sender or recipient

Roughly speaking, no unlinkability delta of items means that the ability of the attacker to relate these items does not increase by observing the system or by possibly interacting with it.

5 Anonymity in terms of unlinkability

To describe anonymity in terms of unlinkability, we have to augment the definitions of anonymity given in Section 3 by making explicit the attributes anonymity relates to. This is best explained by looking at an example in detail. In our setting, cf. Section 2, we choose the attribute "having sent a message" as the example. Then we have:

A sender *s* is anonymous w.r.t. sending, iff *s* is anonymous within the set of potential senders, i.e., within the sender anonymity set.

This mainly is a re-phrasing of the definition in Section 2. If we make the message under consideration explicit, the definition reads:

A sender *s* sends a message *m* anonymously, iff *s* is anonymous within the set of potential senders of *m*, the sender anonymity set of *m*.

This can be generalized to sets of messages easily:

A sender *s* sends a set of messages *M* anonymously, iff *s* is anonymous within the set of potential senders of *M*, the sender anonymity set of *M*.

If the attacker's focus is not on the sender, but on the message, we can define:

A message *m* is sent anonymously, iff *m* can have been sent by each potential sender, i.e., by any subject within the sender anonymity set of *m*.

Again, this can be generalized to sets of messages easily:

A set of messages *M* is sent anonymously, iff *M* can have been sent by each set of potential senders, i.e., by any set of subjects within the cross product of the sender anonymity sets of each message *m* within *M*.

from the message content, cf. Section 2. Yet with access to their content even without deep semantical analysis the attacker can notice certain characteristics which link them together – e.g. similarities in structure, style, use of some words or phrases, consistent appearance of some grammatical errors, etc. In a sense, content of messages may play a role as "side channel" in a similar way as in cryptanalysis – i.e. content of messages may leak some information on their linkability.

Of course, all 5 definitions would work for receiving of messages accordingly. For more complicated settings with more operations than these two, appropriate sets of definitions can be developed.

Now we are prepared to describe anonymity in terms of unlinkability.

We do this by using our setting, cf. Section 2. So we consider sending and receiving of messages as attributes; the items of interest (IOIs) are “who has sent or received which message”. Then, *anonymity* of a subject w.r.t. an attribute may be defined as unlinkability of this subject and this attribute.[32]

So we have: *Sender anonymity* of a subject means that to this potentially sending subject, each message is unlinkable.[33]

Correspondingly, *recipient anonymity* of a subject means that to this potentially receiving subject, each message is unlinkable.

Relationship anonymity of a pair of subjects, the potentially sending subject and the potentially receiving subject, means that to this potentially communicating pair of subjects, each message is unlinkable. In other words, sender and recipient (or each recipient in case of multicast) are unlinkable. As sender anonymity of a message cannot hold against the sender of this message himself nor can recipient anonymity hold against any of the recipients w.r.t. himself, relationship anonymity is considered w.r.t. outsiders only, i.e., attackers being neither the sender nor one of the recipients of the messages under consideration.

Thus, relationship anonymity is a weaker[34] property than each of sender anonymity and recipient anonymity: The attacker might know who sends which messages or he might know who receives which messages (and in some cases even who sends which messages *and* who receives which messages). But as long as for the attacker each message sent and each message received are unlinkable, he cannot link the respective senders to recipients and vice versa, i.e., relationship anonymity holds. The *relationship anonymity set* can be defined to be the cross product of two

[32] Unlinkability is a sufficient condition of anonymity, but it is not a necessary condition. Thus, failing unlinkability w.r.t. some attribute(s) does not necessarily eliminate anonymity as defined in Section 3; in specific cases (i.e. depending on the attribute(s)) even the strength of anonymity may not be affected.

[33] The property unlinkability might be more “fine-grained” than anonymity, since there are many more relations where unlinkability might be an issue than just the relation “anonymity” between subjects and IOIs. Therefore, the attacker might get to know information on linkability while not necessarily reducing anonymity of the particular subject – depending on the defined measures. An example might be that the attacker, in spite of being able to link, e.g. by timing, all encrypted messages of a transactions, does not learn who is doing this transaction.

[34] First the easy direction: For all attackers it holds: Sender anonymity implies relationship anonymity, and recipient anonymity implies relationship anonymity (This is true if anonymity is taken as a binary property: Either it holds or it does not hold. If we consider quantities of anonymity, the validity of the implication possibly depends on the particular definitions of how to quantify sender anonymity and recipient anonymity on the one hand, and how to quantify relationship anonymity on the other.). Then the more complicated direction: There exists at least one attacker model, where relationship anonymity does neither imply sender anonymity nor recipient anonymity. Consider an attacker who neither controls any senders nor any recipients of messages, but all lines and – maybe – some other stations. If w.r.t. this attacker relationship anonymity holds, you can neither argue that against him sender anonymity holds nor that recipient anonymity holds. The classical MIX-net (cf. Section 8) without dummy traffic is one implementation with just this property: The attacker sees who sends messages when and who receives messages when, but cannot figure out who sends messages to whom.

potentially distinct sets, the set of potential senders and the set of potential recipients[35] or – if it is possible to exclude some of these pairs – a subset of this cross product. So the relationship anonymity set is the set of all possible sender-recipient(s)-pairs.[36] If we take the perspective of a subject sending (or receiving) a particular message, the relationship anonymity set becomes the set of all potential recipients (senders) of that particular message. So fixing one factor of the cross product gives a recipient anonymity set or a sender anonymity set.

6 Undetectability and unobservability

In contrast to anonymity and unlinkability, where not the IOI, but only its relationship to subjects or other IOIs is protected, for undetectability, the IOIs are protected as such.[37]

***Undetectability* of an item of interest (IOI) from an attacker's perspective means that the attacker cannot sufficiently distinguish whether it exists or not.**[38,39]

If we consider messages as IOIs, this means that messages are not sufficiently discernible from, e.g., "random noise".[40]

Undetectability is maximal iff whether an IOI exists or not is completely indistinguishable. We call this perfect undetectability.

***An undetectability delta* of an item of interest (IOI) from an attacker's perspective specifies the difference between the undetectability of the IOI taking into account the attacker's observations and the undetectability of the IOI given the attacker's a-priori knowledge only.**

[35] In case of multicast, the set of potential recipients is the power set of all potential recipients.

[36] For measures to quantify relationship anonymity, if they shall be comparable with quantifying sender and recipient anonymity, you have to compensate for the multiplication of possibilities in forming the cross product. For the simplest metric (we do not advocate to use) just counting the size of the set, you have to take the square root of the size of the set of possible sender-recipient(s)-pairs.

[37] Undetectability can be regarded as a possible and desirable property of steganographic systems (see Section 8 "Known mechanisms for anonymity, undetectability, and unobservability"). Therefore it matches the information hiding terminology [Pfit96, ZFKP98]. In contrast, anonymity, dealing with the relationship of discernible IOIs to *subjects*, does not directly fit into that terminology, but independently represents a different dimension of properties.

[38] What we call "undetectability" starting with Version v0.28 of this document, has been called "unobservability" before. From [ISO99]: "[Unobservability] ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used. [...] Unobservability requires that users and/or subjects cannot determine whether an operation is being performed." As seen before, our approach is less user-focused and insofar more general. With the communication setting and the attacker model chosen in this text, our definition of unobservability shows the method how to achieve it: preventing distinguishability of IOIs. Thus, the ISO definition might be applied to a different setting where attackers are prevented from observation by other means, e.g., by encapsulating the area of interest against third parties.

[39] In some applications (e.g. steganography), it might be useful to quantify undetectability to have some measure how much uncertainty about an IOI remains after the attacker's observations. Again, we may use probabilities or entropy, or whatever is useful in a particular context.

[40] A slightly more precise formulation might be that messages are not discernible from no message. A quantification of this property might measure the number of indistinguishable IOIs and/or the probabilities of distinguishing these IOIs.

The undetectability delta is minimal iff whether an IOI exists or not is indistinguishable to exactly the same degree whether the attacker takes his observations into account or not. We call this “perfect preservation of undetectability”.

Undetectability of an IOI clearly is only possible w.r.t. subjects being not involved in the IOI (e.g., neither being the sender nor one of the recipients of a message). Therefore, if we just speak about undetectability without spelling out a set of IOIs, it goes without saying that this is a statement comprising only those IOIs the attacker is not involved in.

As the definition of undetectability stands, it has nothing to do with anonymity – it does not mention any relationship between IOIs and subjects. Even more, for subjects being involved in an IOI, undetectability of this IOI is clearly impossible.[41] Therefore, early papers describing new mechanisms for undetectability designed the mechanisms in a way that if a subject necessarily could detect an IOI, the other subject(s) involved in that IOI enjoyed anonymity at least. Undetectability by uninvolved subjects together with anonymity even if IOIs can be detected has been called unobservability:

Unobservability **of an item of interest (IOI) means**

- **undetectability of the IOI against all subjects uninvolved in it and**
- **anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI.**

As we had anonymity sets of subjects with respect to anonymity, we have *unobservability sets* of subjects with respect to unobservability, cf. Fig. 5.[42]

Sender unobservability then means that it is sufficiently undetectable whether any sender within the unobservability set sends. Sender unobservability is perfect iff it is completely undetectable whether any sender within the unobservability set sends.

Recipient unobservability then means that it is sufficiently undetectable whether any recipient within the unobservability set receives. Recipient unobservability is perfect iff it is completely undetectable whether any recipient within the unobservability set receives.

Relationship unobservability then means that it is sufficiently undetectable whether anything is sent out of a set of could-be senders to a set of could-be recipients. In other words, it is sufficiently undetectable whether within the relationship unobservability set of all possible sender-recipient(s)-pairs, a message is sent in any relationship. Relationship unobservability is perfect iff it is completely undetectable whether anything is sent out of a set of could-be senders to a set of could-be recipients.

All other things being equal, unobservability is the stronger, the larger the respective unobservability set is, cf. Fig. 6.

[41] Remembering that we had this before in the context of relationship anonymity (cf. Section 5), we could describe relationship anonymity (against outsiders) as undetectability of the communication relationship.

[42] Mainly, unobservability deals with IOIs instead of subjects only. Though, like anonymity sets, unobservability sets consist of all subjects who might possibly cause these IOIs, i.e. send and/or receive messages.

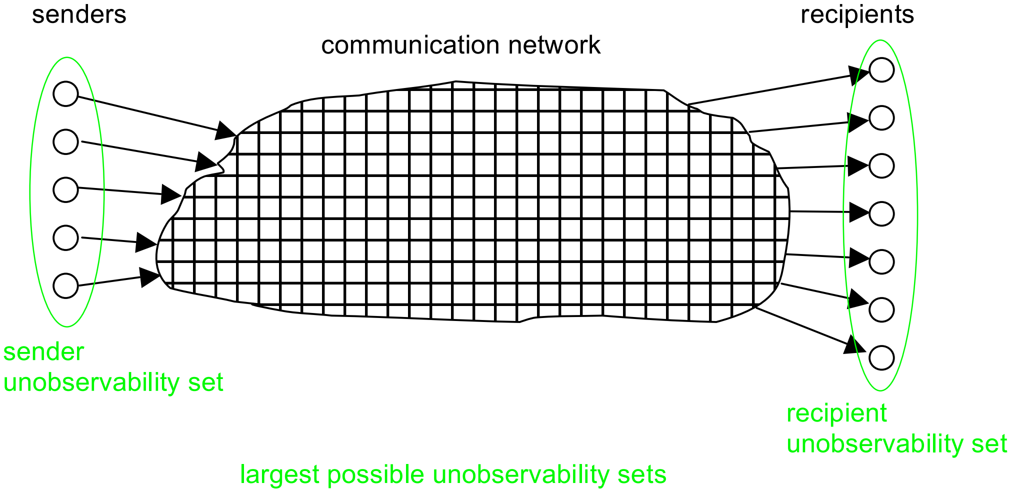


Fig. 5: Unobservability sets within the setting

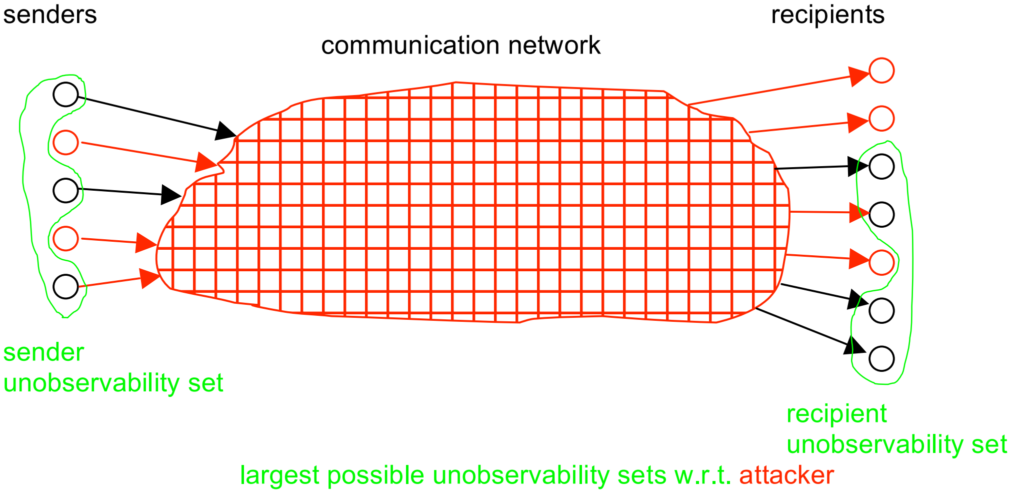


Fig. 6: Unobservability sets w.r.t. attacker within the setting

***An unobservability delta* of an item of interest (IOI) means**

- **undetectability delta of the IOI against all subjects uninvolved in it and**
- **anonymity delta of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI.**

A *minimal unobservability delta* of IOIs means a minimal undetectability delta of these IOIs against all subjects uninvolved in these IOIs and a minimal anonymity delta against those subjects involved in IOIs. To be able to express this conveniently, we use wordings like “perfect preservation of unobservability” to express that the unobservability delta is minimal.

7 Relationships between terms

With respect to the same attacker, unobservability reveals always only a subset of the information anonymity reveals.[43] We might use the shorthand notation

unobservability ⇒ anonymity

for that (⇒ reads “implies”). Using the same argument and notation, we have

sender unobservability ⇒ sender anonymity
recipient unobservability ⇒ recipient anonymity
relationship unobservability ⇒ relationship anonymity

As noted above, we have

sender anonymity ⇒ relationship anonymity
recipient anonymity ⇒ relationship anonymity

sender unobservability ⇒ relationship unobservability
recipient unobservability ⇒ relationship unobservability

With respect to the same attacker, unobservability reveals always only a subset of the information undetectability reveals

unobservability ⇒ undetectability

[43] [ReRu98] propose a continuum for describing the strength of anonymity. They give names: “absolute privacy” (the attacker cannot perceive the presence of communication, i.e., unobservability) – “beyond suspicion” – “probable innocence” – “possible innocence” – “exposed” – “provably exposed” (the attacker can prove the sender, recipient, or their relationship to others). Although we think that the terms “privacy” and “innocence” are misleading, the spectrum is quite useful.

8 Known mechanisms for anonymity, undetectability, and unobservability

Before it makes sense to speak about any particular mechanisms[44] for anonymity, undetectability, and unobservability in communications, let us first remark that all of them assume that stations of users do not emit signals the attacker considered is able to use for identification of stations or their behavior or even for identification of users or their behavior. So if you travel around taking with you a mobile phone sending more or less continuously signals to update its location information within a cellular radio network, don't be surprised if you are tracked using its signals. If you use a computer emitting lots of radiation due to a lack of shielding, don't be surprised if observers using high-tech equipment know quite a bit about what's happening within your machine. If you use a computer, PDA, or smartphone without sophisticated access control, don't be surprised if Trojan horses send your secrets to anybody interested whenever you are online – or via electromagnetic emanations even if you think you are completely offline.

DC-net [Chau85, Chau88] and MIX-net [Chau81] are mechanisms to achieve sender anonymity and relationship anonymity, respectively, both against strong attackers. If we add dummy traffic, both provide for the corresponding unobservability [PfPW91].[45]

Broadcast [Chau85, PfWa86, Waid90] and private information retrieval [CoBi95] are mechanisms to achieve recipient anonymity against strong attackers. If we add dummy traffic, both provide for recipient unobservability.

This may be summarized: A mechanism to achieve some kind of anonymity appropriately combined with dummy traffic yields the corresponding kind of unobservability.

Of course, dummy traffic[46] alone can be used to make the number and/or length of sent messages undetectable by everybody except for the recipients; respectively, dummy traffic can be used to make the number and/or length of received messages undetectable by everybody except for the senders.

As a side remark, we mention steganography and spread spectrum as two other well-known undetectability mechanisms.

The usual concept to achieve undetectability of IOIs at some layer[47], e.g., sending meaningful messages, is to achieve statistical independence of all discernible phenomena at some lower implementation layer. An example is sending dummy messages at some lower layer to achieve, e.g., a constant rate flow of messages looking – by means of encryption – randomly for all parties except the sender and the recipient(s).

[44] Mechanisms are part of the system in general and the communication network in particular, cf. Section 2.

[45] If dummy traffic is used to pad sending and/or receiving on the sender's and/or recipient's line to a constant rate traffic, MIX-nets can even provide sender and/or recipient anonymity and unobservability.

[46] Misinformation and disinformation may be regarded as semantic dummy traffic, i.e., communication from which an attacker cannot decide which are real requests with real data or which are fake ones. Assuming the authenticity of misinformation or disinformation may lead to privacy problems for (innocent) bystanders.

[47] Modern computer and communication networks are implemented in layers of functionality, where each upper layer uses the services of the lower layers to provide a more comfortable service, cf. e.g. [Tane96].

9 Pseudonymity

Having anonymity of human beings, unlinkability, and maybe unobservability is superb w.r.t. data minimization, but would prevent any useful two-way communication. For many applications, we need appropriate kinds of identifiers:

A *pseudonym*[48] is an identifier[49] of a subject[50] other than one of the subject's real names[51].

We can generalize pseudonyms to be identifiers of *sets* of subjects – see below –, but we do not need this in our setting.

The subject which the pseudonym refers to is the *holder* of the pseudonym[52].

A subject is *pseudonymous* if a pseudonym[53] is used[54] as identifier instead of one of its real names.[55,56]

[48] "Pseudonym" comes from Greek "pseudonumon" meaning "falsely named" (pseudo: false; onuma: name). Thus, it means a name other than the "real name". To avoid the connotation of "pseudo" = false, some authors call pseudonyms as defined in this paper simply *nyms*. This is nice and short, but we stick with the usual wording, i.e. pseudonym, pseudonymity, etc. However the reader should not be surprised to read nym, nymity, etc. in other texts.

[49] A name or another bit string. Identifiers which are generated using random data only, i.e., fully independent of the subject and related attributes, do not contain side information on the identified subject, whereas non-random identifiers may do. E.g., nicknames chosen by a user may contain information on heroes he admires; a sequence number may contain information on the time the pseudonym was issued; an e-mail address or phone number contains information how to reach the user.

[50] In our setting: sender or recipient.

[51] "Real name" is the antonym to pseudonym. There may be multiple real names over life time, in particular the legal names, i.e. for a human being the names which appear on the birth certificate or on other official identity documents issued by the State; for a legal person the name under which it operates and which is registered in official registers (e.g., commercial register or register of associations). A human being's real name typically comprises their given name and a family name.
Note that from a mere technological perspective it cannot always be determined whether an identifier of a subject is a pseudonym or a real name.

[52] We prefer the term "holder" over "owner" of a pseudonym because it seems to make no sense to "own" identifiers, e.g., bit strings. Furthermore, the term "holder" sounds more neutral than the term "owner", which is associated with an assumed autonomy of the subject's will. The holder may be a natural person (in this case we have the usual meaning and all data protection regulations apply), a legal person, or even only a computer.

[53] Fundamentally, pseudonyms are nothing else than another kind of attributes. But whereas in building an IT system, its designer can strongly support the holders of pseudonyms to keep the pseudonyms under their control, this is not equally possible w.r.t. attributes in general. Therefore, it is useful to give this kind of attribute a distinct name: pseudonym.

[54] For pseudonyms chosen by the user (in contrast to pseudonyms assigned to the user by others), primarily, the holder of the pseudonym is using it. Secondarily, all others he communicated to using the pseudonym can utilize it for linking. Each of them can, of course, divulge the pseudonym and all data related to it to other entities. So finally, the attacker will utilize the pseudonym to link all data related to this pseudonym he gets to know being related. Hopefully, the appropriate use of pseudonyms primarily by the holder (cf. Pseudonymity w.r.t. linkability, Section 11, and Identity management, Section 13) and secondarily by others will keep the sensitivity of the linkable data sets to a minimum.

Defining the process of preparing for the use of pseudonyms, e.g., by establishing certain rules how and under which conditions to identify holders of pseudonyms by so-called *identity brokers*[57] or how to prevent uncovered claims by so-called *liability brokers* (cf. Section 11), leads to the more general notion of pseudonymity[58]:

***Pseudonymity* is the use of pseudonyms as identifiers.**[59,60]

So *sender pseudonymity* is defined as the sender being pseudonymous, *recipient pseudonymity* is defined as the recipient being pseudonymous, cf. Fig. 7.[61]

[55] We can also speak of "pseudonymous usage" (i.e. use of a pseudonym instead of the real name(s)) and of "pseudonymous data" (i.e. data belonging to a subject where a pseudonym is used instead of its real name(s)).

[56] Please note that despite the terms “anonymous” and “pseudonymous” are sharing most of their characters, their semantics is quite different: Anonymous says something about a subject with respect to identifiability, pseudonymous only says something about employing a mechanism, i.e., using pseudonyms. Whether this mechanism helps in a particular setting to achieve something close to anonymity, is a completely different question. On the level of subjects, “anonymous” should be contrasted with “(privacy-enhancingly) identity managed”, cf. Section 13.4. But since “anonymous” can be defined precisely whereas “(privacy-enhancingly) identity managed” is at least at present hard to define equally precise, we prefer to follow the historical path of research dealing with the more precise mechanism (pseudonym, pseudonymity) first.

[57] *Identity brokers* have for the pseudonyms they are the identity broker for the information who is their respective holder. Therefore, identity brokers can be implemented as a special kind of certification authorities for pseudonyms. Since anonymity can be described as a particular kind of unlinkability, cf. Section 5, the concept of identity broker can be generalized to linkability broker. A *linkability broker* is a (trusted) third party that, adhering to agreed rules, enables linking IOIs for those entities being entitled to get to know the linking.

[58] Concerning the natural use of the English language, one might use “pseudonymization” instead of “pseudonymity”. But at least in Germany, the data protection officers gave “pseudonymization” the meaning that you have first person-related data having some kinds of identifier for the civil identity (cf. footnote 63 for some clarification of “civil identity”): “replacing a person’s name and other identifying characteristics with a label, in order to preclude identification of the data subject or to render such identification substantially difficult” (§ 6a German Federal Data Protection Act). Therefore, we use a different term (coined by David Chaum: “pseudonymity”) to describe the process where from the very beginning, only the holder is able to link to his/her civil identity.

[59] From [ISO99]: “[Pseudonymity] ensures that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use. [...] Pseudonymity requires that a set of users and/or subjects are unable to determine the identity of a user bound to a subject or operation, but that this user is still accountable for its actions.” This view on pseudonymity covers only the use of digital pseudonyms. Therefore, our definition of pseudonymity is much broader as it does not necessarily require disclosure of the user’s identity and accountability. Pseudonymity alone – as it is used in the real world and in technological contexts – does not tell anything about the strengths of anonymity, authentication or accountability; these strengths depend on several properties, cf. below.

[60] Quantifying pseudonymity would primarily mean quantifying the state of using a pseudonym according to its different dimensions (cf. the next two Sections 10 and 11), i.e., quantifying the authentication and accountability gained and quantifying the anonymity left over (e.g. using entropy as the measure). Roughly speaking, well-employed pseudonymity could mean in e-commerce appropriately fine-grained authentication and accountability to counter identity theft or to prevent uncovered claims using e.g. the techniques described in [BüPf90], combined with much anonymity retained. Poorly employed pseudonymity would mean giving away anonymity without preventing uncovered claims.

[61] Providing sender pseudonymity and recipient pseudonymity is the basic interface communication networks have to provide to enhance privacy for two-way communications.

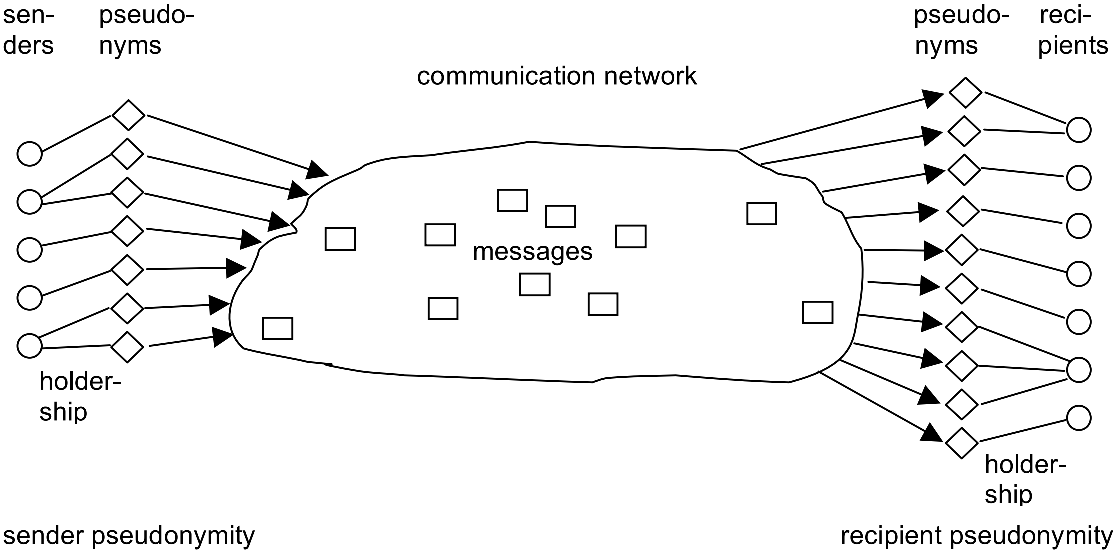


Fig. 7: Pseudonymity

In our usual setting, we assume that each pseudonym refers to exactly one specific holder, invariant over time.

Specific kinds of pseudonyms may extend this setting: A *group pseudonym* refers to a set of holders, i.e., it may refer to multiple holders; a *transferable pseudonym* can be transferred from one holder to another subject becoming its holder.

Such a *group pseudonym* may induce an anonymity set: Using the information provided by the pseudonym only, an attacker cannot decide whether an action was performed by a specific subject within the set. [62]

Transferable pseudonyms can, if the attacker cannot completely monitor all transfers of holdership, serve the same purpose, without decreasing accountability as seen by an authority monitoring all transfers of holdership.

An interesting combination might be transferable group pseudonyms – but this is left for further study.

[62] Please note that the mere fact that a pseudonym has several holders does not yield a group pseudonym: For instance, creating the same pseudonym may happen by chance and even without the holders being aware of this fact, particularly if they choose the pseudonyms and prefer pseudonyms which are easy to remember. But the context of each use of the pseudonym (e.g. used by which subject – usually denoted by another pseudonym – in which kind of transaction) then usually will denote a single holder of this pseudonym.

10 Pseudonymity with respect to accountability and authorization

10.1 Digital pseudonyms to authenticate messages

A *digital pseudonym* is a bit string which, to be meaningful in a certain context, is

- unique as identifier (at least with very high probability) and
- suitable to be used to authenticate the holder's IOIs relatively to his/her digital pseudonym, e.g., to authenticate his/her messages sent.

Using digital pseudonyms, accountability can be realized with pseudonyms – or more precisely: with respect to pseudonyms.

10.2 Accountability for digital pseudonyms

To authenticate IOIs relative to pseudonyms usually is not enough to achieve accountability for IOIs.

Therefore, in many situations, it might make sense to either

- attach funds to digital pseudonyms to cover claims or to
- let identity brokers authenticate digital pseudonyms (i.e., check the civil identity of the holder[63] of the pseudonym and then issue a digitally signed statement that this particular identity broker has proof of the identity of the holder of this digital pseudonym and is willing to divulge that proof under well-defined circumstances) or
- both.

If sufficient funds attached to a digital pseudonym are reserved and/or the digitally signed statement of a trusted identity broker is checked before entering into a transaction with the holder of that pseudonym, accountability can be realized in spite of anonymity.

10.3 Transferring authenticated attributes and authorizations between pseudonyms

To transfer *attributes including their authentication by third parties* (called "credentials" by David Chaum [Chau85]) – all kinds of *authorizations* are special cases – between digital pseudonyms of one and the same holder, it is always possible to prove that these pseudonyms have the same holder.

But as David Chaum pointed out, it is much more anonymity-preserving to maintain the unlinkability of the digital pseudonyms involved as much as possible by transferring the credential from one pseudonym to the other without proving the sameness of the holder. How this can be done is described in [Chau90, CaLy04].

We will come back to the just described property "convertibility" of digital pseudonyms in Section 12.

[63] If the holder of the pseudonym is a natural person or a legal person, civil identity has the usual meaning, i.e. the identity attributed to an individual by a State (e.g. represented by the social security number or the combination of name, date of birth, and location of birth etc.). If the holder is, e.g., a computer, it remains to be defined what "civil identity" should mean. It could mean, for example, exact type and serial number of the computer (or essential components of it) or even include the natural person or legal person responsible for its operation.

11 Pseudonymity with respect to linkability

Whereas anonymity and accountability are the extremes with respect to linkability to subjects, pseudonymity is the entire field between and including these extremes. Thus, pseudonymity comprises all degrees of linkability to a subject. Ongoing use of the same pseudonym allows the holder to establish or consolidate a reputation[64]. Some kinds of pseudonyms enable dealing with claims in case of abuse of unlinkability to holders: Firstly, third parties (identity brokers, cf. Section 10.2) may have the possibility to reveal the civil identity of the holder in order to provide means for investigation or prosecution. To improve the robustness of anonymity, chains of identity brokers may be used [Chau81]. Secondly, third parties may act as liability brokers of the holder to clear a debt or settle a claim. [BüPf90] presents the particular case of value brokers.

There are many properties of pseudonyms which may be of importance in specific application contexts. In order to describe the properties of pseudonyms with respect to anonymity, we limit our view to two aspects and give some typical examples:

11.1 Knowledge of the linking between the pseudonym and its holder

The knowledge of the linking may not be a constant, but change over time for some or even all people. Normally, for non-transferable pseudonyms the knowledge of the linking cannot decrease.[65] Typical kinds of such pseudonyms are:

a) *public pseudonym*:
The linking between a public pseudonym and its holder may be publicly known even from the very beginning. E.g., the linking could be listed in public directories such as the entry of a phone number in combination with its owner.

b) *initially non-public pseudonym*:
The linking between an initially non-public pseudonym and its holder may be known by certain parties, but is not public at least initially. E.g., a bank account where the bank can look up the linking may serve as a non-public pseudonym. For some specific non-public pseudonyms, certification authorities acting as identity brokers could reveal the civil identity of the holder in case of abuse.

c) *initially unlinked pseudonym*:
The linking between an initially unlinked pseudonym and its holder is – at least initially – not known to anybody with the possible exception of the holder himself/herself. Examples for unlinked pseudonyms are (non-public) biometrics like DNA information unless stored in databases including the linking to the holders.

Public pseudonyms and initially unlinked pseudonyms can be seen as extremes of the described pseudonym aspect whereas initially non-public pseudonyms characterize the continuum in between.

Anonymity is the stronger, the less is known about the linking to a subject. The strength of anonymity decreases with increasing knowledge of the pseudonym linking. In particular, under the assumption that no gained knowledge on the linking of a pseudonym will be forgotten and that the pseudonym cannot be transferred to other subjects, a public pseudonym never can become

[64] Establishing and/or consolidating a reputation under a pseudonym is, of course, insecure if the pseudonym does not enable to authenticate messages, i.e., if the pseudonym is not a digital pseudonym, cf. Section 10.1. Then, at any moment, another subject might use this pseudonym possibly invalidating the reputation, both for the holder of the pseudonym and all others having to do with this pseudonym.

[65] With the exception of misinformation or disinformation which may blur the attacker's knowledge (see above).

an unlinked pseudonym. In each specific case, the strength of anonymity depends on the knowledge of certain parties about the linking relative to the chosen attacker model.

If the pseudonym is transferable, the linking to its holder can change. Considering an unobserved transfer of a pseudonym to another subject, a formerly public pseudonym can become non-public again.

11.2 Linkability due to the use of a pseudonym in different contexts

With respect to the degree of linkability, various kinds of pseudonyms may be distinguished according to the kind of context for their usage:

a) *person pseudonym*:
A person pseudonym is a substitute for the holder's name which is regarded as representation for the holder's civil identity. It may be used in many different contexts, e.g., a number of an identity card, the social security number, DNA, a nickname, the pseudonym of an actor, or a mobile phone number.

b) *role pseudonym*:
The use of role pseudonyms is limited to specific roles[66], e.g., a customer pseudonym or an Internet account used for many instantiations of the same role "Internet user". The same role pseudonym may be used with different communication partners. Roles might be assigned by other parties, e.g., a company, but they might be chosen by the subject himself/herself as well.

c) *relationship pseudonym*:
For each communication partner, a different relationship pseudonym is used. The same relationship pseudonym may be used in different roles for communicating with the same partner. Examples are distinct nicknames for each communication partner.[67]

d) *role-relationship pseudonym*:
For each role and for each communication partner, a different role-relationship pseudonym is used. This means that the communication partner does not necessarily know, whether two pseudonyms used in different roles belong to the same holder. On the other hand, two different communication partners who interact with a user in the same role, do not know from the pseudonym alone whether it is the same user.[68]

e) *transaction pseudonym*[69]:
For each transaction, a transaction pseudonym unlinkable to any other transaction pseudonyms and at least initially unlinkable to any other IOI is used, e.g., randomly generated transaction numbers for online-banking. Therefore, transaction pseudonyms can be used to realize as strong anonymity as possible.[70]

[66] Cf. Section 13.3 for a more precise characterization of "role".

[67] In case of group communication, the relationship pseudonyms may be used between more than two partners.

[68] As with relationship pseudonyms, in case of group communication, the role-relationship pseudonyms may be used between more than two partners.

[69] Apart from "transaction pseudonym" some employ the term "one-time-use pseudonym", taking the naming from "one-time pad".

[70] In fact, the strongest anonymity is given when there is no identifying information at all, i.e., information that would allow linking of anonymous entities, thus transforming the anonymous transaction into a pseudonymous one. If the transaction pseudonym is used exactly once, we have the same strength of anonymity as if no pseudonym is used at all. Another possibility to achieve strong anonymity is to prove the holdership of the pseudonym or specific attributes (e.g., with zero-knowledge proofs) without revealing the information about the pseudonym or more detailed attributes themselves. Then, no identifiable or linkable information is disclosed.

The strength of the anonymity of these pseudonyms can be represented as the lattice that is illustrated in the following diagram, cf. Fig. 8. The arrows point in direction of increasing anonymity, i.e., A → B stands for "B enables stronger anonymity than A".[71]

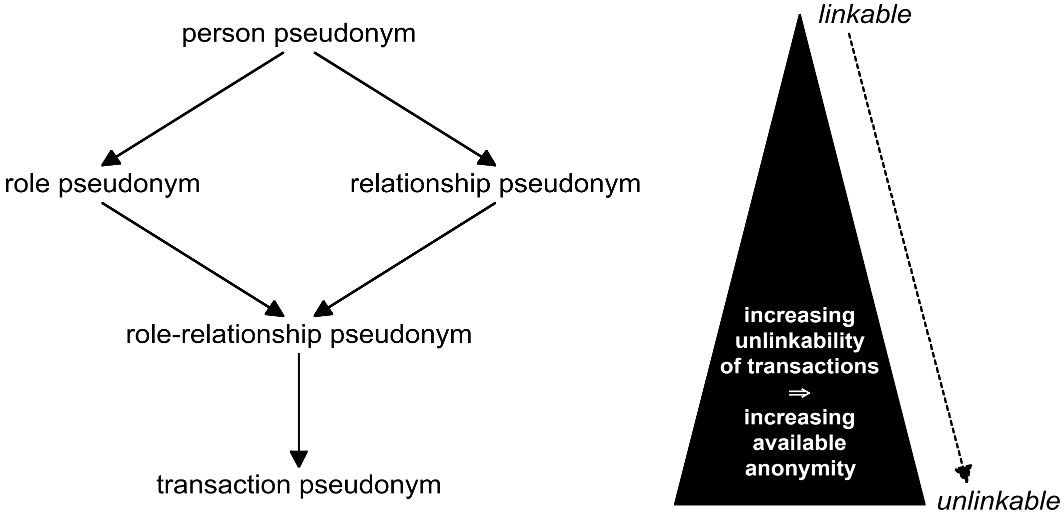

person pseudonym
role pseudonym
relationship pseudonym
role-relationship pseudonym
transaction pseudonym
linkable
increasing unlinkability of transactions
⇒
increasing available anonymity
unlinkable

Fig. 8: Lattice of pseudonyms according to their use in different contexts

In general, anonymity of both role pseudonyms and relationship pseudonyms is stronger than anonymity of person pseudonyms. The strength of anonymity increases with the application of role-relationship pseudonyms, the use of which is restricted to both the same role and the same relationship.[72] Ultimate strength of anonymity is obtained with transaction pseudonyms, provided that no other information, e.g., from the context or from the pseudonym itself (cf. footnote 49), enabling linking is available.

Anonymity is the stronger, ...

- ... the less personal data of the pseudonym holder can be linked to the pseudonym;
- ... the less often and the less context-spanning pseudonyms are used and therefore the less data about the holder can be linked;
- ... the more often independently chosen, i.e., from an observer's perspective unlinkable, pseudonyms are used for new actions.

The amount of information of linked data can be reduced by different subjects using the same pseudonym (e.g., one after the other when pseudonyms are transferred or simultaneously with specifically created group pseudonyms[73]) or by misinformation or disinformation, cf. footnote 29.

[71] "→" is not the same as "⇒" of Section 7, which stands for the implication concerning anonymity and unobservability.

[72] If a role-relationship pseudonym is used for roles comprising many kinds of activities, the danger arises that after a while, it becomes a person pseudonym in the sense of: "A person pseudonym is a substitute for the holder's name which is regarded as representation for the holder's civil identity." This is even more true both for role pseudonyms and relationship pseudonyms.

[73] The group of pseudonym holders acts as an inner anonymity set within a, depending on context information, potentially even larger outer anonymity set.

12 Known mechanisms and other properties of pseudonyms

A digital pseudonym could be realized as a public key to test digital signatures where the holder of the pseudonym can prove holdership by forming a digital signature which is created using the corresponding private key [Chau81]. The most prominent example for digital pseudonyms are public keys generated by the user himself/herself, e.g., using PGP[74].

A *public key certificate* bears a digital signature of a so-called *certification authority* and provides some assurance to the binding of a public key to another pseudonym, usually held by the same subject. In case that pseudonym is the civil identity (the real name) of a subject, such a certificate is called an *identity certificate*. An *attribute certificate* is a digital certificate which contains further information (*attributes*) and clearly refers to a specific public key certificate. Independent of certificates, attributes may be used as identifiers of sets of subjects as well. Normally, attributes refer to sets of subjects (i.e., the anonymity set), not to one specific subject.
There are several other properties of pseudonyms related to their use which shall only be briefly mentioned, but not discussed in detail in this text. They comprise different degrees of, e.g.,

- limitation to a fixed number of pseudonyms per subject[75] [Chau81, Chau85, Chau90],
- guaranteed uniqueness[76] [Chau81, StSy00],
- transferability to other subjects,
- authenticity of the linking between a pseudonym and its holder (possibilities of verification/falsification or indication/repudiation),
- provability that two or more pseudonyms have the same holder[77],
- convertibility, i.e., transferability of attributes of one pseudonym to another[78] [Chau85, Chau90],
- possibility and frequency of pseudonym changeover,
- re-usability and, possibly, a limitation in number of uses,
- validity (e.g., guaranteed durability and/or expiry date, restriction to a specific application),
- possibility of revocation or blocking,
- participation of users or other parties in forming the pseudonyms, or
- information content about attributes in the pseudonym itself.

In addition, there may be some properties for specific applications (e.g., an addressable pseudonym serves as a communication address which enables to contact its holder) or due to the participation of third parties (e.g., in order to circulate the pseudonyms, to reveal civil identities in case of abuse, or to cover claims).

Some of the properties can easily be realized by extending a digital pseudonym by attributes of some kind, e.g., a communication address, and specifying the appropriate semantics. The binding of attributes to a pseudonym can be documented in an attribute certificate produced either by the holder himself/herself or by a certification authority. The non-transferability of the attribute certificate can be somewhat enforced, e.g., by biometrical means, by combining it with individual hardware (e.g., chipcards), or by confronting the holder with legal consequences.

[74] In using PGP, each user may create an unlimited number of key pairs by himself/herself (at this moment, such a key pair is an initially unlinked pseudonym), bind each of them to an e-mail address, self-certify each public key by using his/her digital signature or asking another introducer to do so, and circulate it.

[75] For pseudonyms issued by an agency that guarantees the limitation of at most one pseudonym per individual, the term “is-a-person pseudonym” is used.

[76] E.g., “globally unique pseudonyms”.

[77] For digital pseudonyms having only one holder each and assuming that no holders cooperate to provide wrong “proofs”, this can be proved trivially by signing e.g. the statement “<Pseudonym1> and <Pseudonym2> have the same holder.” digitally with respect to both these pseudonyms. Putting it the other way round: Proving that pseudonyms have the same holder is all but trivial.

[78] This is a property of convertible credentials.

13 Identity management

13.1 Setting

To adequately address privacy-enhancing identity management, we have to extend our setting:

- It is not realistic to assume that an attacker might not get information on the sender or recipient of messages from the message content and/or the sending or receiving context (time, location information, etc.) of the message. We have to consider that the attacker is able to use these attributes for linking messages and, correspondingly, the pseudonyms used with them.
- In addition, it is not just human beings, legal persons, or simply computers sending messages and using pseudonyms at their discretion as they like at the moment, but they use application programs, which strongly influence the sending and receiving of messages and may even strongly determine the usage of pseudonyms.

13.2 Identity and identifiability

Identity can be explained as an exclusive perception of life, integration into a social group, and continuity, which is bound to a body and shaped by society. This concept of identity[79] distinguishes between "I" and "Me" [Mead34]: "I" is the instance that is accessible only by the individual self, perceived as an instance of liberty and initiative. "Me" is supposed to stand for the social attributes, defining a human identity that is accessible by communications and that is an inner instance of control and consistency.[80]

Corresponding to the anonymity set introduced in the beginning of this text, we can work with an "identifiability set"[81] [Hild03] to define "identifiability" and "identity"[82]:

***Identifiability* of a subject from an attacker's perspective means that the attacker can sufficiently identify the subject within a set of subjects, the *identifiability set*.**

Fig. 9 contrasts anonymity set and identifiability set.

[79] Here (and in Section 13 throughout), we have human beings in mind, which is the main motivation for privacy. From a structural point of view, *identity* can be attached to any *subject*, be it a human being, a legal person, or even a computer. This makes the terminology more general, but may lose some motivation at first sight. Therefore, we start in our explanation with identity of human beings, but implicitly generalize to subjects thereafter. This means: In a second reading of this paper, you may replace "individual" by "subject" (introduced as "possibly acting entity" at the beginning of Section 2) throughout as it was used in the definitions of the Sections 2 through 12. It may be discussed whether the definitions can be further generalized and apply for any "entity", regardless of subject or not.

[80] For more information see [ICPP03].

[81] The *identifiability set* is a set of possible subjects.

[82] This definition is compatible with the definitions given in: Giles Hogben, Marc Wilikens, Ioannis Vakalis: On the Ontology of Digital Identification, in: Robert Meersman, Zahir Tari (Eds.): On the Move to Meaningful Internet Systems 2003: OTM 2003 Workshops, LNCS 2889, Springer, Berlin 2003, 579-593; and it is very close to that given by David-Olivier Jaquet-Chiffelle in http://www.calt.insead.edu/fidis/workshop/workshop-wp2-december2003/presentation/VIP/vip_id_def2_files/frame.htm: "An identity is any subset of attributes of a person which uniquely characterizes this person within a community."

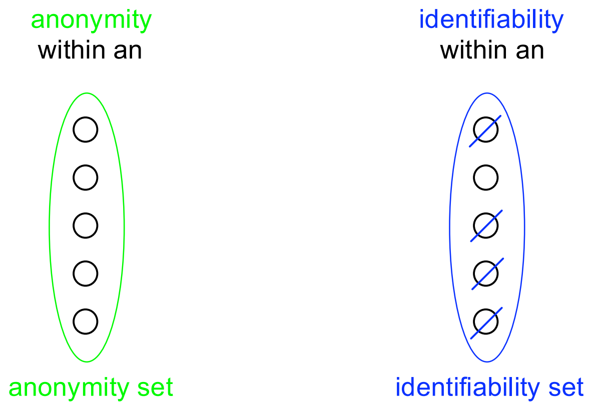


Fig. 9: Anonymity set vs. identifiability set

All other things being equal, identifiability is the stronger, the larger the respective identifiability set is. Conversely, the remaining anonymity is the stronger, the smaller the respective identifiability set is.

An *identity* is any subset of attributes of an individual which sufficiently identifies this individual within any set of individuals.[83] **So usually there is no such thing as "the identity", but several of them.**

Of course, attribute values or even attributes themselves may change over time. Therefore, if the attacker has no access to the change history of each particular attribute, the fact whether a particular subset of attributes of an individual is an identity or not may change over time as well. If the attacker has access to the change history of each particular attribute, any subset forming an identity will form an identity from his perspective irrespective how attribute values change.[84]

13.3 Identity-related terms

Role

In sociology, a "role" or "social role" is a set of connected actions, as conceptualized by actors in a social situation (i.e., situation-dependent identity attributes). It is mostly defined as an expected behavior (i.e., sequences of actions) in a given individual social context.

Partial identity

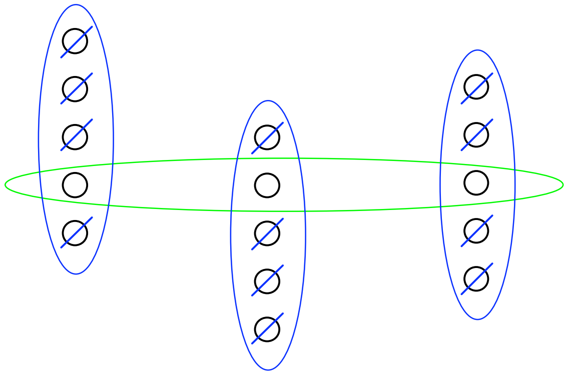
Each identity of a person comprises many partial identities of which each represents the person in a specific context or role. A partial identity is a subset of attributes of a complete identity, where a *complete identity* is the union[85] of all attributes of all identities of this person[86]. On a technical

[83] An equivalent, but slightly longer definition of identity would be: An *identity* is any subset of attributes of an individual which distinguishes this individual from all other individuals within any set of individuals.

[84] Any reasonable attacker will not just try to figure out attribute values per se, but the point in time (or even the time frame) they are valid (in), since this change history helps a lot in linking and thus inferring further attribute values. Therefore, it may clarify one's mind to define each "attribute" in a way that its value cannot get invalid. So instead of the attribute "location" of a particular individual, take the set of attributes "location at time x". Depending on the inferences you are interested in, refining that set as a list ordered concerning "location" or "time" may be helpful.

[85] If attributes are defined such that they don't get invalid (cf. footnote 84), "union" can have the usual meaning within set theory.

level, these attributes are data. Of course, attribute values or even attributes themselves of a partial identity may change over time.
A *pseudonym* might be an identifier for a partial identity.[87]
Whereas we assume that an "identity" uniquely characterizes an individual (without limitation to particular identifiability sets), a partial identity may not do, thereby enabling different quantities of anonymity. But we may find for each partial identity appropriately small identifiability sets[88], where the partial identity uniquely characterizes an individual, cf. Fig. 10.[89]
As with identities, depending on whether the attacker has access to the change history of each particular attribute or not, the identifiability set of a partial identity may change over time if the values of its attributes change.



anonymity set of a partial identity given that the set of all possible subjects (the a-priori anonymity set, cf. footnote 89, case 1.) can be partitioned into the three disjoint identifiability sets of the partial identity shown

Fig. 10: Relation between anonymity set and identifiability set

Digital identity
Digital identity denotes attribution of attributes to a person, which are immediately operationally accessible by technical means. More to the point, the identifier of a digital partial identity[90] can be a simple e-mail address in a news group or a mailing list. Its owner will attain a certain reputation. More generally we might consider the whole identity as a combination from "I" and "Me" where the "Me" can be divided into an implicit and an explicit part: Digital identity is the digital part from the explicated "Me". Digital identity should denote all those personally related data that can be stored and automatically interlinked by a computer-based application.

[86] We have to admit that usually nobody, including the person concerned, will know "all" attributes or "all" identities. Nevertheless we hope that the notion "complete identity" will ease the understanding of "identity" and "partial identity".
[87] If it is possible to transfer attributes of one pseudonym to another (as convertibility of credentials provides for, cf. Section 12), this means transferring a partial identity to this other pseudonym.
[88] For identifiability sets of cardinality 1, this is trivial, but it may hold for "interesting" identifiability sets of larger cardinality as well.
[89] The relation between *anonymity set* and *identifiability set* can be seen in two ways:

1. Within an a-priori anonymity set, we can consider a-posteriori identifiability sets as subsets of the anonymity set. Then the largest identifiability sets allowing identification characterize the a-posteriori anonymity, which is zero iff the largest identifiability set allowing identification equals the a-priori anonymity set.
2. Within an a-priori identifiability set, its subsets which are the a-posteriori anonymity sets characterize the a-posteriori anonymity. It is zero iff all a-posteriori anonymity sets have cardinality 1.

[90] A *digital partial identity* is the same as a *partial digital identity*. In the following, we skip "partial" if the meaning is clear from the context.

Virtual identity
Virtual identity is sometimes used in the same meaning as digital identity or digital partial identity, but because of the connotation with “unreal, non-existent, seeming” the term is mainly applied to characters in a MUD (Multi User Dungeon), MMORPG (Massively Multiplayer Online Role Playing Games) or to avatars.

13.4 Identity management-related terms

Identity management
Identity management means managing various partial identities (usually denoted by pseudonyms) of an individual, i.e., administration of identity attributes including the development and choice of the partial identity and pseudonym to be (re-)used in a specific context or role.

Establishment of *reputation* is possible when the individual re-uses partial identities. A prerequisite to choose the appropriate partial identity is to recognize the situation the person is acting in.

Privacy-enhancing identity management[91]
Given the restrictions of a set of applications, identity management is called *privacy-enhancing* if it sufficiently preserves unlinkability (as seen by an attacker) between the partial identities of an individual required by the applications.[92]
Identity management is called *perfectly privacy-enhancing* if it perfectly preserves unlinkability between the partial identities, i.e., by choosing the pseudonyms (and their authorizations, cf. Section 10.3) denoting the partial identities carefully, it maintains unlinkability between these partial identities towards an attacker to the same degree as giving the attacker the attributes with all pseudonyms omitted.

Privacy-enhancing identity management enabling application design
An application is designed in a privacy-enhancing identity management enabling way if neither the pattern of sending/receiving messages nor the attributes given to entities (i.e., human beings, organizations, computers) reduce unlinkability more than is strictly necessary to achieve the purposes of the application.

Identity management system (IMS)[93]
An identity management system in its broadest sense refers to technology-based administration of identity attributes including the development and choice of the partial identity and pseudonym to be (re-)used in a specific context or role.[94]

[91] Given the terminology defined in Sections 2 to 5, privacy-enhancing identity management is *unlinkability-preserving* identity management. So, maybe, the term “privacy-preserving identity management” would be more appropriate. But to be compatible to the earlier papers in this field, we stick to privacy-enhancing identity management.

[92] Note that due to our setting, this definition focuses on the main property of Privacy-Enhancing Technologies (PETs), namely data minimization: This property means to limit as much as possible the release of personal data and for those released, preserve as much unlinkability as possible. We are aware of the limitation of this definition: In the real world it is not always desired to achieve utmost unlinkability. We believe that the user as the data subject should be empowered to decide on the release of data and on the degree of linkage of his or her personal data within the boundaries of legal regulations, i.e., in an advanced setting the privacy-enhancing application design should also take into account the support of “user-controlled release” as well as “user-controlled linkage”.

[93] Some publications use the abbreviations IdMS or IDMS instead.

[94] We can distinguish between identity management system and identity management application: The term “identity management system” is seen as an infrastructure, in which “identity management applications” as components, i.e., software installed on computers, are co-ordinated.

Privacy-enhancing identity management system (PE-IMS)
A Privacy-Enhancing IMS is an IMS that, given the restrictions of a set of applications, sufficiently preserves unlinkability (as seen by an attacker) between the partial identities and corresponding pseudonyms of an individual.

User-controlled identity management system
A user-controlled identity management system is an IMS that makes the flow of identity attributes explicit and gives its user a large degree of control [CPHH02]. The guiding principle is “notice and choice”.

Combining user-controlled IMS with PE-IMS means user-controlled linkability of personal data, i.e., achieving user-control based on thorough data minimization.[95]
According to respective situation and context, such a system supports the user in making an informed choice of pseudonyms, representing his or her partial identities. A user-controlled PE-IMS supports the user in managing his or her partial identities, i.e., to use different pseudonyms with associated identity attributes according to different contexts, different roles the user is acting in and according to different interaction partners. It acts as a central gateway for all interactions between different applications, like browsing the web, buying in Internet shops, or carrying out administrative tasks with governmental authorities [HBCC04].

14 Overview of main definitions and their negations

Anonymity of a subject from an attacker’s perspective means that the attacker cannot sufficiently identify the subject within a set of subjects, the *anonymity set*.	*Identifiability* of a subject from an attacker’s perspective means that the attacker can sufficiently identify the subject within a set of subjects, the *identifiability set*.
Unlinkability of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker’s perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these IOIs are related or not.	*Linkability* of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker’s perspective means that within the system (comprising these and possibly other items), the attacker can sufficiently distinguish whether these IOIs are related or not.
Undetectability of an item of interest (IOI) from an attacker’s perspective means that the attacker cannot sufficiently distinguish whether it exists or not.	*Detectability* of an item of interest (IOI) from an attacker’s perspective means that the attacker can sufficiently distinguish whether it exists or not.
Unobservability of an item of interest (IOI) means • undetectability of the IOI against all subjects uninvolved in it and • anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI.	*Observability* of an item of interest (IOI) means <many possibilities to define the semantics>.

[95] And by default unlinkability of different user actions so that interaction partners involved in different actions by the same user cannot combine the personal data disseminated during these actions.

15 Concluding remarks

This text is a proposal for consolidating terminology in the field “anonymity/identifiability, (un)linkability, (un)detectability, (un)observability, pseudonymity, and identity management”. The authors hope to get further feedback to improve this text and to come to a more precise and comprehensive terminology. Everybody is invited to participate in the process of defining an essential set of terms.

References

BüPf90 Holger Bürk, Andreas Pfitzmann: Value Exchange Systems Enabling Security and Unobservability; Computers & Security 9/8 (1990) 715-721.

CaLy04 Jan Camenisch and Anna Lysyanskaya: Signature Schemes and Anonymous Credentials from Bilinear Maps; Crypto 2004, LNCS 3152, Springer, Berlin 2004, 56-72.

Chau81 David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM 24/2 (1981) 84-88.

Chau85 David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985) 1030-1044.

Chau88 David Chaum: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability; Journal of Cryptology 1/1 (1988) 65-75.

Chau90 David Chaum: Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms; Auscrypt ‘90, LNCS 453, Springer, Berlin 1990, 246-264.

ClSc06 Sebastian Clauß, Stefan Schiffner: Structuring Anonymity Metrics; in: A. Goto (Ed.), DIM ’06, Proceedings of the 2006 ACM Workshop on Digital Identity Management, Fairfax, USA, Nov. 2006, 55-62.

CoBi95 David A. Cooper, Kenneth P. Birman: Preserving Privacy in a Network of Mobile Computers; 1995 IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press, Los Alamitos 1995, 26-38.

CPHH02 Sebastian Clauß, Andreas Pfitzmann, Marit Hansen, Els Van Herreweghen: Privacy-Enhancing Identity Management; The IPTS Report 67 (September 2002) 8-16.

HBCC04 Marit Hansen, Peter Berlich, Jan Camenisch, Sebastian Clauß, Andreas Pfitzmann, Michael Waidner: Privacy-Enhancing Identity Management; Information Security Technical Report (ISTR) Volume 9, Issue 1 (2004), Elsevier, UK, 35-44, http://dx.doi.org/10.1016/S1363-4127(04)00014-7.

Hild03 Mireille Hildebrandt (Vrije Universiteit Brussels): presentation at the FIDIS workshop 2nd December, 2003; slides: http://www.calt.insead.edu/fidis/workshop/workshop-wp2-december2003/presentation/VUB/VUB_fidis_wp2_workshop_dec2003.ppt.

ICPP03 Independent Centre for Privacy Protection & Studio Notarile Genghini: Identity Management Systems (IMS): Identification and Comparison Study; commissioned by the Joint Research Centre Seville, Spain, September 2003, http://www.datenschutzzentrum.de/projekte/idmanage/study.htm.

ISO99 ISO IS 15408, 1999, http://www.commoncriteria.org/.

Mead34 George H. Mead: Mind, Self and Society, Chicago Press 1934.

Pfit96 Birgit Pfitzmann (collected by): Information Hiding Terminology -- Results of an informal plenary meeting and additional proposals; Information Hiding, LNCS 1174, Springer, Berlin 1996, 347-350.

PfPW91 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: ISDN-MIXes -- Untraceable Communication with Very Small Bandwidth Overhead; 7th IFIP International Conference on Information Security (IFIP/Sec '91), Elsevier, Amsterdam 1991, 245-258.

PfWa86 Andreas Pfitzmann, Michael Waidner: Networks without user observability -- design options; Eurocrypt '85, LNCS 219, Springer, Berlin 1986, 245-253; revised and extended version in: Computers & Security 6/2 (1987) 158-166.

ReRu98 Michael K. Reiter, Aviel D. Rubin: Crowds: Anonymity for Web Transactions, ACM Transactions on Information and System Security 1(1), November 1998, 66-92.

Shan48 Claude E. Shannon: A Mathematical Theory of Communication; The Bell System Technical Journal 27 (1948) 379-423, 623-656.

Shan49 Claude E. Shannon: Communication Theory of Secrecy Systems; The Bell System Technical Journal 28/4 (1949) 656-715.

StSy00 Stuart Stubblebine, Paul Syverson: Authentic Attributes with Fine-Grained Anonymity Protection; Financial Cryptography 2000, LNCS Series, Springer, Berlin 2000.

Tane96 Andrew S. Tanenbaum: Computer Networks; 3rd ed., Prentice-Hall, 1996.

Waid90 Michael Waidner: Unconditional Sender and Recipient Untraceability in spite of Active Attacks; Eurocrypt '89, LNCS 434, Springer, Berlin 1990, 302-319.

Wils93 Kenneth G. Wilson: The Columbia Guide to Standard American English; Columbia University Press, New York 1993.

ZFKP98 J. Zöllner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke, G. Wolf: Modeling the security of steganographic systems; 2nd Workshop on Information Hiding, LNCS 1525, Springer, Berlin 1998, 345-355.

Relationships between some terms used

For some terms used in this document, the following “is”-relation (subclass hierarchy) holds:

items of interest (IOI) <are>
- entity
  - subject
    - actor
    - actee
    - human being (= natural person = individual)
    - legal person
    - computer
      - sender of a message
      - recipient of a message
    - insider
    - outsider
  - object
- message
- actions
  - sending of message
  - receiving of message
- identifier
  - name
  - pseudonym
    - digital pseudonym

In addition, we would like to have a notation for a “may have”-relation. Thereby, we give the most general relation. In the example below, “subject” may have “digital pseudonym” implies that “objects” may have no “digital pseudonym”.

Subject <may have>
- digital pseudonym

{If, e.g., in the area of ontologies, there is some other standard notation for this, please let us know.}

Index

Translation of essential terms

To Czech

Vashek Matyas, Masaryk Univ. Brno, Czech republic
matyas@fi.muni.cz

Zdenek Riha, Masaryk Univ. Brno, Czech republic
zriha@fi.muni.cz

Alena Honigova
alena_honigova@itse.cz

abuse	zneužít, zneužití
accountability	prokazatelná odpovědnost
accountability in spite of anonymity	prokazatelná odpovědnost i přes anonymitu
accountability with respect to a pseudonym	prokazatelná odpovědnost vzhledem k pseudonymu
actee	<Your input needed>
acting entity	jednající entita
action	jednání, čin, akce
actor	<Your input needed>
addressable pseudonym	adresovatelný pseudonym
anonymity	anonymita
anonymity delta	<Your input needed>

anonymity set	anonymitní množina
anonymous	anonymní
a-posteriori knowledge	a posteriori (znalost po události)
application design	návrh aplikace
a-priori knowledge	a priori (znalost před událostí)
attacker	útočník
attacker model	model útočníka
attribute	atribut
attribute authentication by third parties	atributová autentizace za pomoci třetí strany
attribute certificate	atributový certifikát
attribute values	hodnoty atributů
authentication	autentizace
authorization	<Your input needed>
avatar	zosobnění
background knowledge	znalost prostředí / pozadí
biometrics	biometrika
bit string	<Your input needed>
blocking	blokující, blokování
broadcast	vysílání, broadcast
certification authority	certifikační autorita
chains of identity brokers	řetězce zprostředkovatelů identity
change history	historie změn
civil identity	občanská totožnost/identita
communication network	komunikační síť
communication relationship	komunikační vztahy<<<please change to singular>>>
complete identity	úplná totožnost/identita
computer	počítač
context	kontext
convertibility	převoditelnost
convertibility of digital pseudonyms	převoditelnost digitálních pseudonymů
cover claims	pokrýt nároky
credential	autorizační atributy
customer pseudonym	pseudonym zákazníka
data minimization	minimalizace dat
data protection regulations	předpisy pro ochranu (osobních) dat
data subject	dotčený (subjekt dat)
DC-net	DC-síť
delta	<Your input needed>
detectability	<Your input needed>
digital identity	digitální identita
digital partial identity	digitální částečná identita
digital pseudonym	digitální pseudonym
digital signature	digitální podpis
disinformation	dezinformace (záměrná)
distinguish	odlišit
dummy traffic	nevýznamný / umělý provoz
encryption	(za)šifrování
end-to-end encryption	šifrování mezi koncovými uzly (end-to-end)
entity	entita
entropy	entropie
forget	zapomenout
globally unique pseudonym	globálně jedinečný pseudonym
group communication	skupinová komunikace
group pseudonym	skupinový pseudonym
holder	držitel

holder of the pseudonym	držitel pseudonymu
human being	lidská bytost
I	já
identifiability	identifikovatelnost
identifiability set	identifikovatelnostní množina
identifiable	identifikovatelný
identifier	identifikátor
identifier of a subject	identifikátor subjektu
identity	identita, totožnost
identity broker	zprostředkovatel identity
identity card	občanský průkaz, identifikační průkaz
identity certificate	certifikát identity
identity management	správa identit
identity management application	aplikace pro správu identity
identity management system	systém správy identit
identity theft	krádež identity
imply	implikovat, znamenat
IMS	IMS
indistinguishability	nerozlišitelnost
indistinguishable	nerozlišitelný
individual	individuální
initially non-public pseudonym	zpočátku neveřejný pseudonym
initially unlinked pseudonym	zpočátku nespojený pseudonym
insider	vnitřní činitel
introducer	předkladatel, uvaděč
is-a-person pseudonym	pseudonym je-osobou
items of interest	předměty zájmu
key	klíč
knowledge	znalost
largest possible anonymity set	největší možná anonymitní množina
lattice	mřížka
legal person	právnická osoba
liability broker	zprostředkovatel odpovědnosti
linkability	spojitelnost
linkability between the pseudonym and its holder	spojitelnost mezi pseudonymem a jeho držitelem
linkability broker	zprostředkovatel spojitelnosti
Me	o mně (“Me”)
mechanisms	mechanizmy
mechanisms for anonymity	mechanizmy pro anonymitu
mechanisms for unobservability	mechanizmy pro nepozorovatelnost
message	zpráva
message content	obsah zprávy
misinformation	nesprávná / mylná informace
MIX-net	mixovací síť
mobile phone number	číslo mobilního telefonu
multicast	<Your input needed>
name	jméno
natural person	fyzická osoba
new knowledge	nová znalost
non-public pseudonym	neveřejný pseudonym
notice and choice	oznámení a volba
nym	-nym
nymity	-nymita
observation	pozorování
one-time pad	jednorázové heslo

one-time-use pseudonym	jednorázový pseudonym
organization	organizace
outsider	vnější činitel
owner	vlastník
partial digital identity	částečná digitální identita
partial identity	částečná identita
perfect secrecy	dokonalé utajení
person pseudonym	pseudonym osoby
perspective	perspektiva, úhel pohledu
precise	přesný
privacy	soukromí
privacy-enhancing application design	návrh aplikace zvyšující ochranu soukromí
privacy-enhancing identity management system	systém správy identity zvyšující ochranu soukromí
Privacy-Enhancing Technologies	technologie zvyšující ochranu soukromí
private information retrieval	vyhledávání/získávání soukromých informací
private key	soukromý / privátní klíč
probabilities	pravděpodobnosti
property	vlastnost
pseudonym	pseudonym
pseudonymity	pseudonymita
pseudonymization	pseudonymizace
pseudonymous	pseudonymní (pod pseudonymem)
public key	veřejný klíč
public key certificate	certifikát veřejného klíče
public pseudonym	veřejný pseudonym
quality of anonymity	úroveň / kvalita anonymity
quantify pseudonymity	kvantifikovat pseudonymitu
quantify unlinkability	kvantifikovat nespojitelnost
quantify unobservability	kvantifikovat nepozorovatelnost
quantity of anonymity	kvantifikovat anonymitu
real name	skutečné jméno
recipient	příjemce
recipient anonymity	anonymita příjemce
recipient anonymity set	anonymitní množina příjemců
recipient pseudonymity	pseudonymita příjemce
recipient unobservability	nepozorovatelnost příjemce
recipient unobservability set	nepozorovatelnostní množina příjemců
relationship anonymity	anonymita vztahu
relationship anonymity set	anonymitní množina vztahu
relationship pseudonym	pseudonym vztahu
relationship unobservability	nepozorovatelnost vztahu
relationship unobservability set	nepozorovatelnostní množina vztahu
reputation	pověst, reputace
revocation	odvolání
robustness of anonymity	robustnost anonymity
role	role
role pseudonym	pseudonym role
role-relationship pseudonym	pseudonym role-vztah
semantic dummy traffic	sémantický umělý provoz
sender	odesilatel
sender anonymity	anonymita odesilatele
sender anonymity set	anonymitní množina odesilatelů
sender pseudonymity	pseudonymita odesilatele
sender unobservability	nepozorovatelnostní množina
sender unobservability set	nepozorovatelnostní množina odesilatelů

sender-recipient-pairs	dvojice odesilatel-příjemce
set	množina
set of subjects	množina subjektů
setting	nastavení
side channel	postranní kanál
signal	<Your input needed>
social role	sociální role
social security number	číslo sociálního zabezpečení
spread spectrum	rozložené spektrum
state	stav
station	<Your input needed>
steganographic systems	steganografické systémy
steganography	steganografie
strength of anonymity	síla/odolnost anonymity
subject	subjekt
surrounding	okolní
system	systém
transaction pseudonym	transakční pseudonym
transfer of holdership	změna držení (vlastnictví)
transferability	převoditelnost
transferable group pseudonym	převoditelný pseudonym skupiny
transferable pseudonym	převoditelný pseudonym
undetectability	nedetekovatelnost
undetectability delta	<Your input needed>
unicast	<Your input needed>
uniqueness	jedinečnost
universe	universum
unlinkability	nespojitelnost
unlinkability delta	<Your input needed>
unobservability	nepozorovatelnost
unobservability delta	<Your input needed>
unobservability set	nepozorovatelnostní množina
user-controlled identity management system	<Your input needed>
user-controlled linkage	uživatelem řízené spojení
user-controlled release	uživatelem řízené zveřejnění
usual suspects	obvyklí podezřelí
value broker	zprostředkovatel hodnoty
virtual identity	virtuální identita
zero-knowledge proof	důkaz s nulovým rozšířením znalosti

To French

Dr. Yves Deswarte, LAAS-CNRS
Yves.Deswarte@laas.fr

Here is the color code I used:

- I indicate in black those terms that should be easily accepted.
- In blue are neologisms that I propose, i.e., they are not (currently) French words or expressions, but I think that most French people would understand them. So they'd be generally preferable to existing French expressions that would be ambiguous or too long. (But some rigorous French people do not accept easily neologisms).
- In red are the terms or expressions that translate (as well as I can) the English terms or expressions, but are not exactly equivalent. Other

French speakers may prefer other expressions or find better translations.

- In some cases (e.g., for pseudonymity or linkability), I indicated my proposal (in blue since it is a neologism) and an "official" expression in red (e.g., from the official French version of the Common Criteria). In other cases I indicated several possibilities in red, when I could not decide which I feel better (I'd chose probably one or the other one according to the context).

I'd recommend other French speaking partners to check at least those blue and red expressions.

abuse	abus
accountability	responsabilité
accountability in spite of anonymity	responsabilité malgré l'anonymat
accountability with respect to a pseudonym	responsabilité par rapport à un pseudonyme
actee	<Your input needed>
acting entity	agent
action	action
actor	<Your input needed>
addressable pseudonym	pseudonyme adressable
anonymity	anonymat
anonymity delta	<Your input needed>
anonymity set	ensemble d'anonymat
anonymous	anonyme
a-posteriori knowledge	connaissance a posteriori
application design	conception d'application
a-priori knowledge	connaissance a priori
attacker	attaquant
attacker model	modèle d'attaquant
attribute	attribut
attribute authentication by third parties	authentification d'attribut par tierces parties
attribute certificate	certificat d'attribut
attribute values	valeurs d'attributs
authentication	authentification
authorization	<Your input needed>
avatar	avatar
background knowledge	connaissance de fond
biometrics	biométrie
bit string	<Your input needed>
blocking	blocage
broadcast	diffusion
certification authority	autorité de certification
chains of identity brokers	chaînes de courtiers d'identité
change history	historique des modifications
civil identity	identité civile
communication network	réseau de communication
communication relationship	relations de communication<<<please change to singular>>>
complete identity	identité complète
computer	ordinateur
context	contexte
convertibility	convertibilité
convertibility of digital pseudonyms	convertibilité de pseudonymes numériques
cover claims	couvrir des dommages
credential	garantie
customer pseudonym	pseudonyme du client

data minimization	minimisation des données
data protection regulations	règlementation sur la protection des données
data subject	sujet auquel se rapportent les données
DC-net	réseau-DC
delta	<Your input needed>
detectability	<Your input needed>
digital identity	identité numérique
digital partial identity	identité numérique partielle
digital pseudonym	pseudonyme numérique
digital signature	signature numérique
disinformation	fausse information
distinguish	distinguer
dummy traffic	traffic factice
encryption	chiffrement
end-to-end encryption	chiffrement de bout-en-bout
entity	entité
entropy	entropie
forget	oublier
globally unique pseudonym	pseudonyme globalement unique
group communication	communication de groupe
group pseudonym	pseudonyme de groupe
holder	détenteur
holder of the pseudonym	détenteur du pseudonyme
human being	être humain
I	Je
identifiability	identifiabilité
identifiability set	ensemble d'identifiabilité
identifiable	identifiable
identifier	identificateur
identifier of a subject	identificateur d'un sujet
identity	identité
identity broker	courtier d'identité
identity card	carte d'identité
identity certificate	certificat d'identité
identity management	gestion des identités
identity management application	application de gestion des identités
identity management system	système de gestion des identités
identity theft	vol d'identité
imply	impliquer
IMS	SGI
indistinguishability	indistingabilité
indistinguishable	indistingable
individual	individuel
initially non-public pseudonym	pseudonyme initialement non-public
initially unlinked pseudonym	pseudonyme initialement non-relié
insider	[quelqu'un] de l'intérieur
introducer	introducteur
is-a-person pseudonym	pseudonyme est-une-personne
items of interest	éléments d'intrêt
key	clé
knowledge	connaissance
largest possible anonymity set	le plus grand ensemble d'anonymat possible
lattice	treillis
legal person	personne morale
liability broker	garant
linkability	associabilité, possibilité d'établir un lien

linkability between the pseudonym and its holder	associabilité entre le pseudonyme et son détenteur, possibilité d'établir un lien entre le pseudonyme et son détenteur
linkability broker	autorité de liaison
Me	Moi
mechanisms	mécanismes
mechanisms for anonymity	mécanismes d'anonymat
mechanisms for unobservability	mécanismes d'inobservabilité
message	message
message content	contenu du message
misinformation	mauvaise information
MIX-net	réseau de MIX
mobile phone number	numéro de téléphone portable
multicast	<Your input needed>
name	nom
natural person	personne réelle
new knowledge	connaissance nouvelle
non-public pseudonym	pseudonyme non-public
notice and choice	notification et choix
nym	nyme
nymity	nymité
observation	observation
one-time pad	masque jetable
one-time-use pseudonym	pseudonyme jetable (ou pseudonyme à usage unique)
organization	organisation
outsider	[quelqu'un] de l'extérieur
owner	propriétaire
partial digital identity	identité numérique partielle
partial identity	identité partielle
perfect secrecy	secret parfait
person pseudonym	pseudonyme de personne
perspective	point de vue
precise	précis
privacy	[protection de la] vie privée, intimité
privacy-enhancing application design	conception d'application préservant la vie privée
privacy-enhancing identity management system	système de gestion des identités préservant la vie privée
Privacy-Enhancing Technologies	Technologies de Protection de la Vie Privée
private information retrieval	récupération d'information
private key	clé privée
probabilities	probabilités
property	propriété
pseudonym	pseudonyme
pseudonymity	pseudonymat, possibilité d'agir sous un pseudonyme
pseudonymization	pseudonymisation
pseudonymous	pseudonymique
public key	clé publique
public key certificate	certificat à clé publique
public pseudonym	pseudonyme public
quality of anonymity	qualité d'anonymat
quantify pseudonymity	quantifier le pseudonymat
quantify unlinkability	quantifier l'inassociabilité, quantifier la difficulté à établir un lien

quantify unobservability	quantifier l'inobservabilité
quantity of anonymity	quantifier l'anonymat
real name	nom réel
recipient	recepteur
recipient anonymity	anonymat de réception
recipient anonymity set	ensemble d'anonymat de réception
recipient pseudonymity	pseudonymat de réception
recipient unobservability	inobservabilité de réception
recipient unobservability set	ensemble d'inobservabilité de réception
relationship anonymity	anonymat de relation
relationship anonymity set	<Your input needed>
relationship pseudonym	pseudonymat de relation
relationship unobservability	inobservabilité de relation
relationship unobservability set	<Your input needed>
reputation	réputation
revocation	révocation
robustness of anonymity	robustesse d'anonymat
role	rôle
role pseudonym	pseudonyme de rôle
role-relationship pseudonym	pseudonyme de rôle et de relation
semantic dummy traffic	trafic sémantique factice
sender	émetteur
sender anonymity	anonymat d'émission
sender anonymity set	ensemble d'anonymat d'émission
sender pseudonymity	pseudonymat d'émission
sender unobservability	inobservabilité d'émission
sender unobservability set	ensemble d'inobservabilité d'émission
sender-recipient-pairs	paires d'émetteurs-récepteurs
set	ensemble
set of subjects	ensemble de sujets
setting	configuration
side channel	canal de fuite
signal	<Your input needed>
social role	rôle social
social security number	numéro de sécurité sociale
spread spectrum	étalement de spectre
state	état
station	<Your input needed>
steganographic systems	systèmes stéganographiques
steganography	stéganographie
strength of anonymity	force d'anonymat
subject	sujet
surrounding	environnement
system	système
transaction pseudonym	pseudonyme de transaction
transfer of holdership	transfert de détention
transferability	transférabilité
transferable group pseudonym	pseudonyme de groupe transférable
transferable pseudonym	pseudonyme transférable
undetectability	<Your input needed>
undetectability delta	<Your input needed>
unicast	<Your input needed>
uniqueness	unicité
universe	univers
unlinkability	inassociabilité, impossibilité d'établir un lien
unlinkability delta	<Your input needed>

unobservability	inobservabilité
unobservability delta	<Your input needed>
unobservability set	ensemble d'inobservabilité
user-controlled identity management system	<Your input needed>
user-controlled linkage	établissement de lien sous le contrôle de l'utilisateur
user-controlled release	divulgation sous le contrôle de l'utilisateur
usual suspects	suspects habituels
value broker	courtier de valeurs
virtual identity	identité virtuelle
zero-knowledge proof	preuve sans divulgation de connaissance

To German

abuse	Missbrauch
accountability	Zurechenbarkeit
accountability in spite of anonymity	Zurechenbarkeit trotz Anonymität
accountability with respect to a pseudonym	Zurechenbarkeit zu einem Pseudonym
actee	derjenige, auf den eine Handlung wirkt
acting entity	handelnde Entität
action	Handlung
actor	Handelnder
addressable pseudonym	adressierbares Pseudonym
anonymity	Anonymität
anonymity delta	Anonymitätsdifferenz
anonymity set	Anonymitätsmenge
anonymous	anonym
a-posteriori knowledge	A-Posteriori-Wissen
application design	Anwendungsentwurf
a-priori knowledge	A-Priori-Wissen
attacker	Angreifer
attacker model	Angreifermodell
attribute	Attribut
attribute authentication by third parties	Attributauthentisierung durch Dritte
attribute certificate	Attributzertifikat
attribute values	Attributwerte
authentication	Authentisierung
authorization	Autorisierung
avatar	Avatar
background knowledge	Hintergrundwissen
biometrics	Biometrie
bit string	Bitkette
blocking	Sperren
broadcast	Verteilung
certification authority	Zertifizierungsinstanz
chains of identity brokers	Ketten von Identitätstreuhändern
change history	Änderungshistorie
civil identity	zivile Identität
communication network	Kommunikationsnetz
communication relationship	Kommunikationsbeziehung
complete identity	vollständige Identität
computer	Rechner
context	Kontext
convertibility	Umrechenbarkeit
convertibility of digital pseudonyms	Umrechenbarkeit digitaler Pseudonyme

cover claims	Forderungen abdecken
credential	Credential
customer pseudonym	Kundenpseudonym
data minimization	Datenminimierung
data protection regulations	Datenschutzregelungen
data subject	Betroffener
DC-net	DC-Netz
delta	Differenz
detectability	Erkennbarkeit
digital identity	digitale Identität
digital partial identity	digitale partielle Identität
digital pseudonym	digitales Pseudonym
digital signature	digitale Signatur
disinformation	Desinformation
distinguish	unterscheiden
dummy traffic	bedeutungsloser Verkehr
encryption	Verschlüsselung
end-to-end encryption	Ende-zu-Ende-Verschlüsselung
entity	Entität
entropy	Entropie
forget	vergessen
globally unique pseudonym	global eindeutiges Pseudonym
group communication	Gruppenkommunikation
group pseudonym	Gruppenpseudonym
holder	Inhaber
holder of the pseudonym	Inhaber des Pseudonyms
human being	Mensch
I	“I”
identifiability	Identifizierbarkeit
identifiability set	Identifizierbarkeitsmenge
identifiable	identifizierbar
identifier	Identifikator
identifier of a subject	Identifikator eines Subjektes
identity	Identität
identity broker	Identitätstreuhänder
identity card	Ausweis
identity certificate	Identitätszertifikat
identity management	Identitätsmanagement
identity management application	Identitätsmanagementanwendung
identity management system	Identitätsmanagementsystem
identity theft	Identitätsdiebstahl
imply	implizieren
IMS	IMS
indistinguishability	Ununterscheidbarkeit
indistinguishable	ununterscheidbar
individual	Individuum
initially non-public pseudonym	initial nicht-öffentliches Pseudonym
initially unlinked pseudonym	initial unverkettetes Pseudonym
insider	Insider
introducer	Introducer, Bekanntmacher
is-a-person pseudonym	Ist-eine-Person-Pseudonym
items of interest	interessierende Dinge
key	Schlüssel
knowledge	Wissen
largest possible anonymity set	größtmögliche Anonymitätsmenge
lattice	Verband

legal person	juristische Person
liability broker	Treuhänder für Verbindlichkeiten
linkability	Verkettbarkeit
linkability between the pseudonym and its holder	Verkettbarkeit zwischen dem Pseudonym und seinem Inhaber
linkability broker	Verkettbarkeitstreuhänder
Me	“Me”
mechanisms	Mechanismen
mechanisms for anonymity	Mechanismen für Anonymität
mechanisms for unobservability	Mechanismen für Unbeobachtbarkeit
message	Nachricht
message content	Nachrichteninhalt
misinformation	Missinformation
MIX-net	MIX-Netz
mobile phone number	Mobiltelefonnummer
multicast	Senden an mehrere Empfänger
name	Name
natural person	natürliche Person
new knowledge	neues Wissen
non-public pseudonym	nicht-öffentliches Pseudonym
notice and choice	“Notice and Choice” (d.h. Information des Betroffenen und Gelegenheit zur eigenen Entscheidung über die Verarbeitung der Daten)
nym	Nym
nymity	Nymity
observation	Beobachtung
one-time pad	One-Time-Pad
one-time-use pseudonym	einmal zu benutzendes Pseudonym
organization	Organisation
outsider	Außenstehender
owner	Eigentümer
partial digital identity	digitale Teilidentität
partial identity	Teilidentität
perfect secrecy	perfekte Geheimhaltung
person pseudonym	Personenpseudonym
perspective	Sicht
precise	präzise
privacy	Privatheit
privacy-enhancing application design	Privatheit fördernder Anwendungsentwurf
privacy-enhancing identity management system	Privatheit förderndes Identitätsmanagementsystem
Privacy-Enhancing Technologies	Privatheit fördernde Technik
private information retrieval	Abfragen und Überlagern
private key	privater Schlüssel
probabilities	Wahrscheinlichkeiten
property	Eigenschaft
pseudonym	Pseudonym
pseudonymity	Pseudonymität
pseudonymization	Pseudonymisierung
pseudonymous	pseudonym
public key	öffentlicher Schlüssel
public key certificate	Zertifikat für den öffentlichen Schlüssel
public pseudonym	öffentliches Pseudonym
quality of anonymity	Anonymitätsqualität
quantify pseudonymity	Pseudonymität quantifizieren

quantify unlinkability	Unverkettbarkeit quantifizieren
quantify unobservability	Unbeobachtbarkeit quantifizieren
quantity of anonymity	Anonymitätsquantität
real name	wirklicher Name
recipient	Empfänger
recipient anonymity	Empfängeranonymität
recipient anonymity set	Empfängeranonymitätsmenge
recipient pseudonymity	Empfängerpseudonymität
recipient unobservability	Empfängerunbeobachtbarkeit
recipient unobservability set	Empfängerunbeobachtbarkeitsmenge
relationship anonymity	Beziehungsanonymität
relationship anonymity set	Beziehungsanonymitätsmenge
relationship pseudonym	Beziehungspseudonym
relationship unobservability	Beziehungsunbeobachtbarkeit
relationship unobservability set	Beziehungsunbeobachtbarkeitsmenge
reputation	Reputation
revocation	Widerruf
robustness of anonymity	Anonymitätsrobustheit
role	Rolle
role pseudonym	Rollenpseudonym
role-relationship pseudonym	Rollenbeziehungspseudonym
semantic dummy traffic	(den Angreifer) irreführender Verkehr
sender	Sender
sender anonymity	Senderanonymität
sender anonymity set	Senderanonymitätsmenge
sender pseudonymity	Senderpseudonymität
sender unobservability	Senderunbeobachtbarkeit
sender unobservability set	Senderunbeobachtbarkeitsmenge
sender-recipient-pairs	Sender-Empfänger-Paare
set	Menge
set of subjects	Subjektmenge
setting	Szenario
side channel	Seitenkanal
signal	Signal
social role	soziale Rolle
social security number	Sozialversicherungsnummer
spread spectrum	Spreizband
state	Zustand
station	Endgerät
steganographic systems	Stegosysteme
steganography	Steganographie
strength of anonymity	Anonymitätsstärke
subject	Subjekt
surrounding	Umgebung
system	System
transaction pseudonym	Transaktionspseudonym
transfer of holdership	Transfer der Inhaberschaft
transferability	Transferierbarkeit
transferable group pseudonym	transferierbares Gruppenpseudonym
transferable pseudonym	transferierbares Pseudonym
undetectability	Unerkennbarkeit
undetectability delta	Unerkennbarkeitsdifferenz
unicast	Senden an einen Empfänger
uniqueness	Eindeutigkeit
universe	Universum
unlinkability	Unverkettbarkeit

unlinkability delta	Unverkettbarkeitsdifferenz
unobservability	Unbeobachtbarkeit
unobservability delta	Unbeobachtbarkeitsdifferenz
unobservability set	Unbeobachtbarkeitsmenge
user-controlled identity management system	nutzergesteuertes Identitätsmanagementsystem
user-controlled linkage	nutzergesteuerte Verkettung
user-controlled release	nutzergesteuerte Freigabe
usual suspects	die üblichen Verdächtigen
value broker	Wertetreuhänder
virtual identity	virtuelle Identität
zero-knowledge proof	Zero-Knowledge-Beweis

To Greek

Prof. Stefanos Gritzalis, University of the Aegean, Greece
sgritz@aegean.gr http://www.icsd.aegean.gr/sgritz

Christos Kalloniatis, Researcher, University of the Aegean, Greece
ch.kalloniatis@ct.aegean.gr

abuse	κατάχρηση
accountability	ευθύνη
accountability in spite of anonymity	ευθύνη ανεξαρτήτως της ύπαρξης ανωνυμίας
accountability with respect to a pseudonym	ευθύνη με βάση το ψευδώνυμου
actee	δρων Παραλήπτης
acting entity	ενεργή Οντότητα
action	ενέργεια
actor	δρων Αποστολέας
addressable pseudonym	αναγνωρίσιμο Ψευδώνυμο
anonymity	ανωνυμία
anonymity delta	διαφοροποίηση της Ανωνυμίας
anonymity set	σύνολο ανωνύμων οντοτήτων
anonymous	ανώνυμος
a-posteriori knowledge	μεταγενέστερη γνώση
application design	σχεδιασμός εφαρμογής
a-priori knowledge	προγενέστερη γνώση
attacker	επιτιθέμενος
attacker model	μοντέλο επιτιθέμενου
attribute	ιδιότητα/ χαρακτηριστικό
attribute authentication by third parties	αυθεντικοποίηση ιδιοτήτων από τρίτες οντότητες
attribute certificate	πιστοποιητικό ιδιότητας-χαρακτηριστικών
attribute values	τιμές ιδιοτήτων
authentication	αυθεντικοποίηση
authorization	εξουσιοδότηση
avatar	αβατάρα
background knowledge	προγενέστερη γνώση
biometrics	βιομετρία
bit string	διαδοχή bits
blocking	δέσμευση
broadcast	εκπομπή
certification authority	αρχή πιστοποίησης
chains of identity brokers	αλυσίδες μεσιτών ταυτοτήτων
change history	ιστορικό αλλαγών

civil identity	πολιτική ταυτότητα
communication network	δίκτυο επικοινωνίας
communication relationship	σχέση επικοινωνίας
complete identity	ολοκληρωμένη ταυτότητα
computer	υπολογιστής
context	περιεχόμενο
convertibility	μετατρεψιμότητα
convertibility of digital pseudonyms	μετατρεψιμότητα ψηφιακών ψευδωνύμων
cover claims	αξιώσεις κάλυψης
credential	διαπιστευτήρια
customer pseudonym	ψευδώνυμο πελάτη
data minimization	ελαχιστοποίηση δεδομένων
data protection regulations	κανονισμοί προστασίας δεδομένων
data subject	ενεργή οντότητα που περιέχει δεδομένα για προστασία
DC-net	DC-net
delta	διαφοροποίηση
detectability	ανιχνευσιμότητα
digital identity	ψηφιακή ταυτότητα
digital partial identity	στοιχείο έμμεσου προσδιορισμού της ταυτότητας
digital pseudonym	ψηφιακό ψευδώνυμο
digital signature	ψηφιακή υπογραφή
disinformation	παραπληροφόρηση
distinguish	διακρίνω
dummy traffic	περιττή κυκλοφορία
encryption	κρυπτογράφηση
end-to-end encryption	κρυπτογράφηση από-άκρο-σε-άκρο
entity	οντότητα
entropy	εντροπία
forget	ξεχνώ
globally unique pseudonym	συνολικά μοναδικό ψευδώνυμο
group communication	ομαδική επικοινωνία
group pseudonym	ομαδικό ψευδώνυμο
holder	κάτοχος
holder of the pseudonym	κάτοχος του ψευδώνυμου
human being	ανθρώπινη οντότητα
I	I
identifiability	αναγνωρισιμότητα
identifiability set	σύνολο αναγνωρίσιμων οντοτήτων
identifiable	αναγνωρίσιμος
identifier	προσδιοριστικό
identifier of a subject	προσδιοριστικό μιας ενεργής οντότητας
identity	ταυτότητα
identity broker	μεσίτης αποκάλυψης ταυτότητας
identity card	έντυπη ταυτότητα
identity certificate	πιστοποιητικό ταυτότητας
identity management	διαχείριση ταυτότητας
identity management application	εφαρμογή διαχείρισης ταυτότητας
identity management system	σύστημα διαχείρισης ταυτότητας
identity theft	κλοπή ταυτότητας
imply	υποδηλώνω
IMS	IMS
indistinguishability	δυσδιακρισία
indistinguishable	δυσδιάκριτος
individual	μεμονωμένος
initially non-public pseudonym	αρχικά μη-δημόσιο ψευδώνυμο

initially unlinked pseudonym	αρχικά μη-συνδέσιμο ψευδώνυμο
insider	εσωτερικός
introducer	εκκινών
is-a-person pseudonym	μοναδικό ψευδώνυμο ανά φυσικό πρόσωπο
items of interest	στοιχεία που ενδιαφέρουν
key	κλειδί
knowledge	γνώση
largest possible anonymity set	το δυνητικά μεγαλύτερο σύνολο ανωνυμίας
lattice	πλέγμα
legal person	νομικό πρόσωπο
liability broker	μεσίτης επίλυσης νομικών ζητημάτων
linkability	συνδεσιμότητα
linkability between the pseudonym and its holder	συνδεσιμότητα μεταξύ ψευδωνύμου και του κατόχου του
linkability broker	μεσίτης επίλυσης ζητημάτων συνδεσιμότητας
Me	εγώ
mechanisms	μηχανισμοί
mechanisms for anonymity	μηχανισμοί για ανωνυμία
mechanisms for unobservability	μηχανισμοί για μη-παρατηρησιμότητα
message	μήνυμα
message content	περιεχόμενο μηνύματος
misinformation	παραπληροφόρηση
MIX-net	MIX-net
mobile phone number	αριθμός κινητού τηλεφώνου
multicast	λήψη από πολλαπλές οντότητες
name	όνομα
natural person	φυσικό πρόσωπο
new knowledge	νέα γνώση
non-public pseudonym	μη-δημόσιο ψευδώνυμο
notice and choice	παρατηρώ και επιλέγω
nym	nym
nymity	nymity
observation	παρατήρηση
one-time pad	συμπληρωματικά δεδομένα μιας χρήσης
one-time-use pseudonym	ψευδώνυμο μιας χρήσης
organization	οργανισμός
outsider	εξωτερικός επιτιθέμενος
owner	ιδιοκτήτης
partial digital identity	στοιχείο έμμεσου προσδιορισμού της ταυτότητας
partial identity	μερική ταυτότητα
perfect secrecy	τέλεια μυστικότητα
person pseudonym	ψευδώνυμο φυσικού προσώπου
perspective	προοπτική, θεώρηση
precise	ακριβής
privacy	ιδιωτικότητα
privacy-enhancing application design	σχεδίαση εφαρμογών ενίσχυσης της ιδιωτικότητας
privacy-enhancing identity management system	σύστημα διαχείρισης ταυτότητας που ενισχύει την ιδιωτικότητα
Privacy-Enhancing Technologies	τεχνολογίες ενίσχυσης της Ιδιωτικότητας
private information retrieval	ανάκτηση ιδιωτικών πληροφοριών
private key	ιδιωτικό κλειδί
probabilities	πιθανότητες
property	ιδιότητα
pseudonym	ψευδώνυμο
pseudonymity	ψευδωνυμία
pseudonymization	η διαδικασία της ψευδωνυμίας

pseudonymous	η κατάσταση ενός χρήστη που χρησιμοποιεί ψευδώνυμο
public key	δημόσιο κλειδί
public key certificate	πιστοποιητικό δημοσίου κλειδιού
public pseudonym	δημόσιο ψευδώνυμο
quality of anonymity	ποιότητα ανωνυμίας
quantify pseudonymity	ποσοτικοποιώ τη ψευδωνυμία
quantify unlinkability	ποσοτικοποιώ τη μη-συνδεσιμότητα
quantify unobservability	ποσοτικοποιώ τη μη- παρατηρησιμότητα
quantity of anonymity	ποσότητα ανωνυμίας
real name	πραγματικό όνομα
recipient	παραλήπτης
recipient anonymity	ανωνυμία του παραλήπτη
recipient anonymity set	σύνολο ανωνύμων παραληπτών
recipient pseudonymity	ψευδωνυμία του παραλήπτη
recipient unobservability	μη- παρατηρησιμότητα του παραλήπτη
recipient unobservability set	σύνολο μη- παρατηρήσιμων παραληπτών
relationship anonymity	ανωνυμία σχέσης
relationship anonymity set	σύνολο ανωνύμων σχέσεων
relationship pseudonym	ψευδωνυμία σχέσης
relationship unobservability	μη-παρατηρησιμότητα σχέσης
relationship unobservability set	σύνολο μη-παρατηρήσιμων σχέσεων
reputation	φήμη
revocation	ανάκληση
robustness of anonymity	ρωμαλεότητα ανωνυμίας
role	ρόλος
role pseudonym	ψευδώνυμο ρόλου
role-relationship pseudonym	ψευδώνυμο ρόλου-σχέσης
semantic dummy traffic	σημασιολογικά περιττή κυκλοφορία
sender	αποστολέας
sender anonymity	ανωνυμία αποστολέα
sender anonymity set	σύνολο ανωνυμιών αποστολέων
sender pseudonymity	ψευδωνυμία του αποστολέα
sender unobservability	μη- παρατηρησιμότητα του αποστολέα
sender unobservability set	σύνολο μη- παρατηρήσιμων αποστολέων
sender-recipient-pairs	ζεύγη αποστολέα-παραλήπτη
set	σύνολο
set of subjects	σύνολο ενεργών οντοτήτων
setting	περιβάλλον
side channel	δίαυλος παράπλευρων πληροφοριών
signal	σήμα
social role	κοινωνικός ρόλος
social security number	αριθμός κοινωνικής ασφάλισης
spread spectrum	φάσμα
state	κατάσταση
station	σταθμός
steganographic systems	συστήματα στεγανογραφίας
steganography	στεγανογραφία
strength of anonymity	ισχύς της ανωνυμίας
subject	ενεργή οντότητα
surrounding	περιβάλλον
system	σύστημα
transaction pseudonym	ψευδώνυμο δοσοληψίας
transfer of holdership	μεταφορά ιδιοκτησίας
transferability	δυνατότητα μεταβίβασης
transferable group pseudonym	μεταβιβάσιμο ομαδικό ψευδώνυμο

transferable pseudonym	μεταβιβάσιμο ψευδώνυμο
undetectability	μη-ανιχνευσιμότητα
undetectability delta	διαφοροποίηση της μη-ανιχνευσιμότητας
unicast	λήψη από μοναδική οντότητα
uniqueness	μοναδικότητα
universe	κόσμος
unlinkability	μη- συνδεσιμότητα
unlinkability delta	διαφοροποίηση της μη-συνδεσιμότητας
unobservability	μη- παρατηρησιμότητα
unobservability delta	διαφοροποίηση της μη-παρατηρησιμότητας
unobservability set	σύνολο μη- παρατηρήσιμων οντοτήτων
user-controlled identity management system	σύστημα διαχείρισης ταυτότητας ελεγχόμενο από το χρήστη
user-controlled linkage	σύστημα σύνδεσης ελεγχόμενο από το χρήστη
user-controlled release	σύστημα αποσύνδεσης ελεγχόμενο από το χρήστη
usual suspects	συνήθεις ύποπτοι
value broker	μεσίτης προσδιορισμού αξίας
virtual identity	εικονική ταυτότητα
zero-knowledge proof	απόδειξη μηδενικής γνώσης

To Italian

Dr. Giovanni Baruzzi, Syntlogo GmbH
giovanni.baruzzi@syntlogo.de

Dr. Giuseppe Palumbo, Univ. Modena, Italy
gpalumbo@unimore.it

The terms in this color have been introduced, changed and need peer revision

abuse	abuso
accountability	responsabilità
accountability in spite of anonymity	responsabilità malgrado l'anonimato
accountability with respect to a pseudonym	responsabilità relativa a uno pseudonimo
actee	(seldom) attato. better: soggetto/oggetto
acting entity	entità agente
action	azione
actor	attore
addressable pseudonym	pseudonimo indirizzabile
anonymity	anonimato
anonymity delta	delta di anonimato
anonymity set	insieme anonimo
anonymous	anonimo
a-posteriori knowledge	conoscenza a posteriori
application design	progettazione di applicazioni
a-priori knowledge	conoscenza a priori
attacker	attaccante
attacker model	modello di attacco
attribute	attributo
attribute authentication by third parties	autentica di attributi da parte di terzi
attribute certificate	certificato attributivo
attribute values	valori dell'attributo

authentication	autenticazione
authorization	autorizzazione
avatar	avatar
background knowledge	conouser-controlled identity management system scenze pregresse
biometrics	biometria
bit string	stringa di bit
blocking	blocco
broadcast	broadcast, trasmissione a largo raggio
certification authority	autorità di certificazione
chains of identity brokers	catene di intermediari di certificazione
change history	storia delle variazioni
civil identity	identità civile
communication network	rete di comunicazione
communication relationship	relazione di comunicazione
complete identity	identità completa
computer	calcolatore, computer
context	contesto
convertibility	convertibilità
convertibility of digital pseudonyms	convertibilità di pseudonimi digitali
cover claims	coprire i rischi, copertura di rischi
credential	credenziali
customer pseudonym	pseudonimo cliente
data minimization	minimizzazione dei dati
data protection regulations	normativa sulla protezione dei dati
data subject	soggetto-dati
DC-net	DC-net
delta	delta
detectability	rivelabilità, scopribilità
digital identity	identità digitale
digital partial identity	identità digitale parziale
digital pseudonym	pseudonimo digitale
digital signature	firma digitale
disinformation	informazioni fuorvianti
distinguish	distinguere
dummy traffic	traffico dummy, traffico fasullo
encryption	cifratura
end-to-end encryption	cifratura end-to-end
entity	entità
entropy	entropia
forget	dimenticare
globally unique pseudonym	pseudonimo globalmente unico
group communication	comunicazione di gruppo
group pseudonym	pseudonimo di gruppo
holder	possessore
holder of the pseudonym	possessore dello pseudonimo
human being	essere umano
I	Io
identifiability	identificabilità
identifiability set	insieme di identificabilità
identifiable	identificabile
identifier	identificatore
identifier of a subject	identificatore di un soggetto
identity	identità
identity broker	intermediario di identità
identity card	carta d'identità

identity certificate	certificato d'identità
identity management	gestione delle identità
identity management application	applicazione di gestione delle identità
identity management system	sistema di gestione delle identità
identity theft	furto d'identità
imply	implica
IMS	Identity Management System: sistema di gestione delle identità
indistinguishability	indistinguibilità
indistinguishable	indistinguibile
individual	individuo
initially non-public pseudonym	pseudonimo inizialmente non pubblico
initially unlinked pseudonym	pseudonimo inizialmente non collegato
insider	Insider, entità che agisce dall'interno
introducer	introduttore, utente
is-a-person pseudonym	pseudonimo di persona naturale, pseudonimo individuale
items of interest	elementi di interesse
key	chiave
knowledge	conoscenza
largest possible anonymity set	il più grande degli insiemi anonimi
lattice	reticolo
legal person	persona giuridica
liability broker	intermediario di responsabilità
linkability	collegabilità
linkability between the pseudonym and its holder	collegabilità tra lo pseudonimo e il suo possessore
linkability broker	intermediario di collegabilità
Me	me
mechanisms	meccanismo
mechanisms for anonymity	meccanismo per l'anonimato
mechanisms for unobservability	meccanismi per l'inosservabilità
message	messaggio
message content	contenuto del messaggio
misinformation	informazioni sbagliate
MIX-net	MIX-net
mobile phone number	numero di telefono cellulare
multicast	<Your input needed>
name	nome
natural person	persona naturale
new knowledge	nuova conoscenza
non-public pseudonym	pseudonimo non pubblico
notice and choice	avviso e scelta (principio secondo cui un utente deve essere informato e deve poter scegliere circa il trattamento dei dati)
nym	nym, nomignolo, pseudonimo
nymity	nymity, pseudonomia,
observation	osservazione
one-time pad	blocco appunti monouso
one-time-use pseudonym	pseudonimo monouso
organization	organizzazione
outsider	outsider / osservatore esterno
owner	proprietario
partial digital identity	identità digitale parziale
partial identity	identità parziale
perfect secrecy	segretezza perfetta

person pseudonym	pseudonimo di persona
perspective	prospettiva
precise	preciso
privacy	privacy, riservatezza
privacy-enhancing application design	progetto di applicazioni atte a migliorare la tutela della privacy
privacy-enhancing identity management system	sistema di gestione delle identità atto a migliorare la tutela della privacy
Privacy-Enhancing Technologies	tecnologie per la tutela della privacy
private information retrieval	reperimento di informazioni private
private key	chiave privata
probabilities	probabilità
property	proprietà
pseudonym	pseudonimo
pseudonymity	pseudonomia
pseudonymization	pseudonomizzazione
pseudonymous	pseudonimo (sic!)
public key	chiave pubblica
public key certificate	certificato a chiave pubblica
public pseudonym	pseudonimo pubblico
quality of anonymity	qualità dell'anonimato
quantify pseudonymity	quantificazione della pseudonomia
quantify unlinkability	quantificazione della non-collegabilità
quantify unobservability	quantificazione della inosservabilità
quantity of anonymity	quantità di anonimato
real name	vero nome
recipient	destinatario
recipient anonymity	anonimato del destinatario
recipient anonymity set	insieme anonimo dei destinatari
recipient pseudonymity	pseudonimia del destinatario
recipient unobservability	inosservabilità del destinatario
recipient unobservability set	insieme dell'inosservabilità del destinatario
relationship anonymity	anonimato di relazione
relationship anonymity set	insieme delle relazioni di anonimato
relationship pseudonym	pseudonimo di relazione
relationship unobservability	inosservabilità della relazione
relationship unobservability set	insieme di inosservabilità delle relazioni
reputation	reputazione
revocation	revoca
robustness of anonymity	robustezza dell'anonimato
role	ruolo
role pseudonym	pseudonimo di ruolo
role-relationship pseudonym	pseudonimo di ruolo-relazione
semantic dummy traffic	traffico fasullo semantico
sender	mittente
sender anonymity	anonimato del mittente
sender anonymity set	insieme di anonimato del mittente
sender pseudonymity	pseudonimia del mittente
sender unobservability	inosservabilità del mittente
sender unobservability set	insieme di inosservabilità del mittente
sender-recipient-pairs	coppie mittente-destinatario
set	insieme
set of subjects	insieme di soggetti
setting	scenario
side channel	canale laterale
signal	segnale

social role	ruolo sociale
social security number	"numero della sicurezza sociale", better: codice fiscale
spread spectrum	spettro espanso
state	stato
station	stazione
steganographic systems	sistemi steganografici
steganography	steganografia
strength of anonymity	forza dell’anonimato
subject	soggetto
surrounding	circostante
system	sistema
transaction pseudonym	pseudonimo di transazione
transfer of holdership	trasferimento di possesso
transferability	trasferibilità
transferable group pseudonym	pseudonimo di gruppo trasferibile
transferable pseudonym	pseudonimo trasferibile
undetectability	non individuabilità
undetectability delta	delta di non rivelabilità
unicast	unicast, trasmissione unidirezionale
uniqueness	unicità
universe	universo
unlinkability	non-collegabilità
unlinkability delta	delta di non-collegabilità
unobservability	inosservabilità
unobservability delta	delta di non osservabilità
unobservability set	insieme di inosservabilità
user-controlled identity management system	sistema di gestione delle identità controllato dall’utente
user-controlled linkage	collegamento controllato dall'utente
user-controlled release	rilascio controllato dall'utente
usual suspects	soliti sospetti
value broker	intermediario di valore
virtual identity	identità virtuale
zero-knowledge proof	prova di non conoscenza

To <your mother tongue>
<your name and e-mail address>

abuse	<Your input needed>
accountability	<Your input needed>
accountability in spite of anonymity	<Your input needed>
accountability with respect to a pseudonym	<Your input needed>
actee	<Your input needed>
acting entity	<Your input needed>
action	<Your input needed>
actor	<Your input needed>
addressable pseudonym	<Your input needed>
anonymity	<Your input needed>
anonymity delta	<Your input needed>
anonymity set	<Your input needed>
anonymous	<Your input needed>
a-posteriori knowledge	<Your input needed>
application design	<Your input needed>

a-priori knowledge	<Your input needed>
attacker	<Your input needed>
attacker model	<Your input needed>
attribute	<Your input needed>
attribute authentication by third parties	<Your input needed>
attribute certificate	<Your input needed>
attribute values	<Your input needed>
authentication	<Your input needed>
authorization	<Your input needed>
avatar	<Your input needed>
background knowledge	<Your input needed>
biometrics	<Your input needed>
bit string	<Your input needed>
blocking	<Your input needed>
broadcast	<Your input needed>
certification authority	<Your input needed>
chains of identity brokers	<Your input needed>
change history	<Your input needed>
civil identity	<Your input needed>
communication network	<Your input needed>
communication relationship	<Your input needed>
complete identity	<Your input needed>
computer	<Your input needed>
context	<Your input needed>
convertibility	<Your input needed>
convertibility of digital pseudonyms	<Your input needed>
cover claims	<Your input needed>
credential	<Your input needed>
customer pseudonym	<Your input needed>
data minimization	<Your input needed>
data protection regulations	<Your input needed>
data subject	<Your input needed>
DC-net	<Your input needed>
delta	<Your input needed>
detectability	<Your input needed>
digital identity	<Your input needed>
digital partial identity	<Your input needed>
digital pseudonym	<Your input needed>
digital signature	<Your input needed>
disinformation	<Your input needed>
distinguish	<Your input needed>
dummy traffic	<Your input needed>
encryption	<Your input needed>
end-to-end encryption	<Your input needed>
entity	<Your input needed>
entropy	<Your input needed>
forget	<Your input needed>
globally unique pseudonym	<Your input needed>
group communication	<Your input needed>
group pseudonym	<Your input needed>
holder	<Your input needed>
holder of the pseudonym	<Your input needed>
human being	<Your input needed>
I	<Your input needed>
identifiability	<Your input needed>
identifiability set	<Your input needed>

identifiable	<Your input needed>
identifier	<Your input needed>
identifier of a subject	<Your input needed>
identity	<Your input needed>
identity broker	<Your input needed>
identity card	<Your input needed>
identity certificate	<Your input needed>
identity management	<Your input needed>
identity management application	<Your input needed>
identity management system	<Your input needed>
identity theft	<Your input needed>
imply	<Your input needed>
IMS	<Your input needed>
indistinguishability	<Your input needed>
indistinguishable	<Your input needed>
individual	<Your input needed>
initially non-public pseudonym	<Your input needed>
initially unlinked pseudonym	<Your input needed>
insider	<Your input needed>
introducer	<Your input needed>
is-a-person pseudonym	<Your input needed>
items of interest	<Your input needed>
key	<Your input needed>
knowledge	<Your input needed>
largest possible anonymity set	<Your input needed>
lattice	<Your input needed>
legal person	<Your input needed>
liability broker	<Your input needed>
linkability	<Your input needed>
linkability between the pseudonym and its holder	<Your input needed>
linkability broker	<Your input needed>
Me	<Your input needed>
mechanisms	<Your input needed>
mechanisms for anonymity	<Your input needed>
mechanisms for unobservability	<Your input needed>
message	<Your input needed>
message content	<Your input needed>
misinformation	<Your input needed>
MIX-net	<Your input needed>
mobile phone number	<Your input needed>
multicast	<Your input needed>
name	<Your input needed>
natural person	<Your input needed>
new knowledge	<Your input needed>
non-public pseudonym	<Your input needed>
notice and choice	<Your input needed>
nym	<Your input needed>
nymity	<Your input needed>
observation	<Your input needed>
one-time pad	<Your input needed>
one-time-use pseudonym	<Your input needed>
organization	<Your input needed>
outsider	<Your input needed>
owner	<Your input needed>
partial digital identity	<Your input needed>
partial identity	<Your input needed>

perfect secrecy	<Your input needed>
person pseudonym	<Your input needed>
perspective	<Your input needed>
precise	<Your input needed>
privacy	<Your input needed>
privacy-enhancing application design	<Your input needed>
privacy-enhancing identity management system	<Your input needed>
Privacy-Enhancing Technologies	<Your input needed>
private information retrieval	<Your input needed>
private key	<Your input needed>
probabilities	<Your input needed>
property	<Your input needed>
pseudonym	<Your input needed>
pseudonymity	<Your input needed>
pseudonymization	<Your input needed>
pseudonymous	<Your input needed>
public key	<Your input needed>
public key certificate	<Your input needed>
public pseudonym	<Your input needed>
quality of anonymity	<Your input needed>
quantify pseudonymity	<Your input needed>
quantify unlinkability	<Your input needed>
quantify unobservability	<Your input needed>
quantity of anonymity	<Your input needed>
real name	<Your input needed>
recipient	<Your input needed>
recipient anonymity	<Your input needed>
recipient anonymity set	<Your input needed>
recipient pseudonymity	<Your input needed>
recipient unobservability	<Your input needed>
recipient unobservability set	<Your input needed>
relationship anonymity	<Your input needed>
relationship anonymity set	<Your input needed>
relationship pseudonym	<Your input needed>
relationship unobservability	<Your input needed>
relationship unobservability set	<Your input needed>
reputation	<Your input needed>
revocation	<Your input needed>
robustness of anonymity	<Your input needed>
role	<Your input needed>
role pseudonym	<Your input needed>
role-relationship pseudonym	<Your input needed>
semantic dummy traffic	<Your input needed>
sender	<Your input needed>
sender anonymity	<Your input needed>
sender anonymity set	<Your input needed>
sender pseudonymity	<Your input needed>
sender unobservability	<Your input needed>
sender unobservability set	<Your input needed>
sender-recipient-pairs	<Your input needed>
set	<Your input needed>
set of subjects	<Your input needed>
setting	<Your input needed>
side channel	<Your input needed>
signal	<Your input needed>
social role	<Your input needed>

social security number	<Your input needed>
spread spectrum	<Your input needed>
state	<Your input needed>
station	<Your input needed>
steganographic systems	<Your input needed>
steganography	<Your input needed>
strength of anonymity	<Your input needed>
subject	<Your input needed>
surrounding	<Your input needed>
system	<Your input needed>
transaction pseudonym	<Your input needed>
transfer of holdership	<Your input needed>
transferability	<Your input needed>
transferable group pseudonym	<Your input needed>
transferable pseudonym	<Your input needed>
undetectability	<Your input needed>
undetectability delta	<Your input needed>
unicast	<Your input needed>
uniqueness	<Your input needed>
universe	<Your input needed>
unlinkability	<Your input needed>
unlinkability delta	<Your input needed>
unobservability	<Your input needed>
unobservability delta	<Your input needed>
unobservability set	<Your input needed>
user-controlled identity management system	<Your input needed>
user-controlled linkage	<Your input needed>
user-controlled release	<Your input needed>
usual suspects	<Your input needed>
value broker	<Your input needed>
virtual identity	<Your input needed>
zero-knowledge proof	<Your input needed>