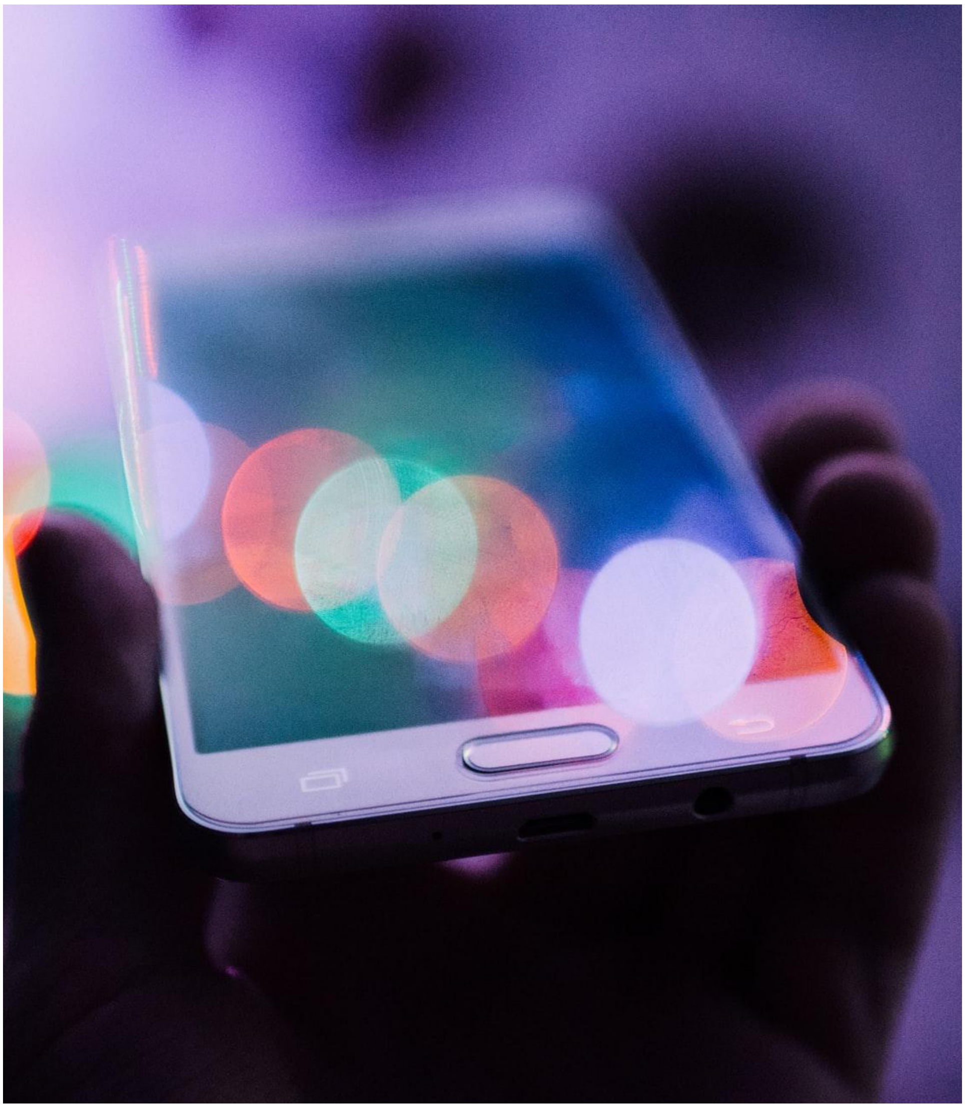
Financial Inclusion DPGs

Digital Public Infrastructures

Final Report

June, 2021



Financial Inclusion DPGs
Digital Public Infrastructures
Final Report

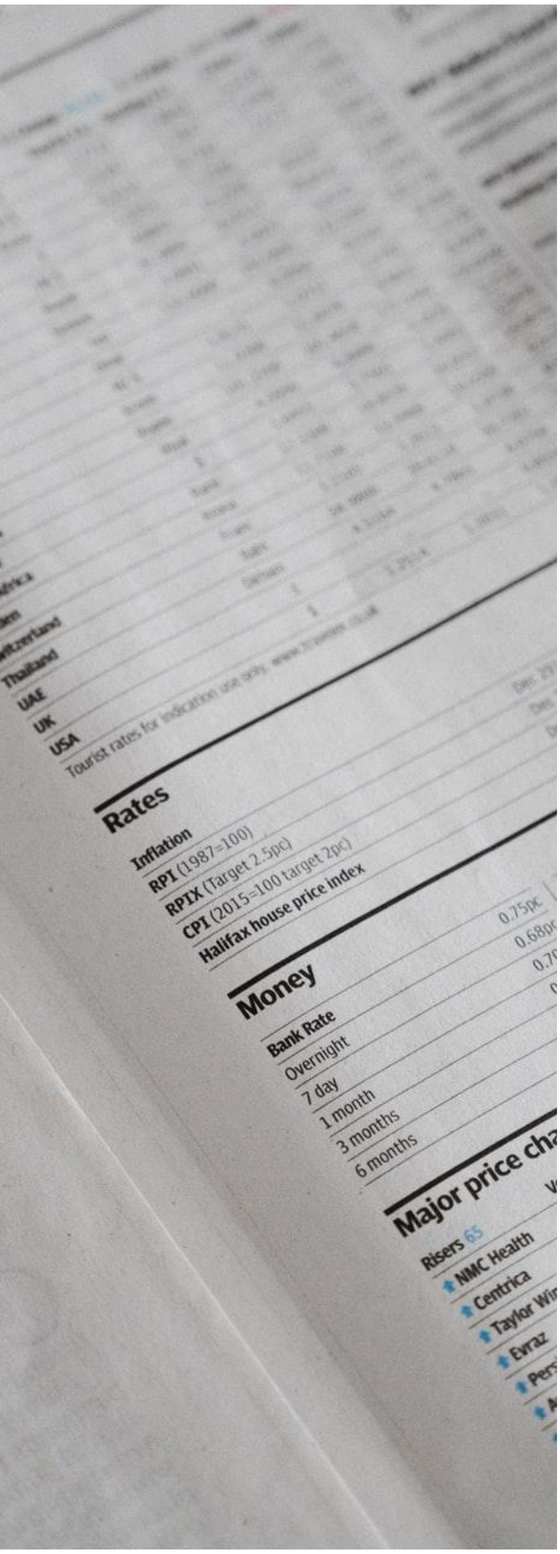
June 2021

The Digital Public Goods Alliance is a multi-stakeholder initiative which aims to accelerate the attainment of the sustainable development goals in low- and middle-income countries by facilitating the discovery, development, use of, and investment in digital public goods. The Secretariat of the Digital Public Goods Alliance is co-hosted by the Norwegian Agency for Development Cooperation (Norad) and UNICEF and governed by an Interim Strategy Group consisting of: iSPIRT; The Government of Norway; The Government of Sierra Leone; and UNICEF.
Many staff, Community of Practice Members and allies of the DPGA generously contributed ideas to this paper.

This final report represents the opinions of the DPGA, and does not represent an endorsement by the individuals and organizations who contributed to this report.

Table of Contents

Executive Summary



Financial inclusion is a key step towards enabling attainment of numerous Sustainable Development Goals while also specifically driving greater economic growth. As the global community corrals around finding solutions that will assist countries in their efforts to build back better after the COVID-19 pandemic, fostering greater financial inclusion will be key.

In September 2020, the Digital Public Goods Alliance (DPGA) convened a Community of Practice (CoP) for Financial Inclusion. All CoPs are a means of leveraging the knowledge and expertise of practitioners operating in relevant sectors. The DPGA convenes CoPs to support the discovery, assessment and advancement of high-potential digital public goods within a specific priority area. In particular, the CoP for Financial Inclusion brought together experts to identify and assess solutions related to digital public infrastructure (DPIs).

This report is the product of that assessment and reviews digital solutions specifically for their relevance to facilitating inclusive financial workflows at scale and enabling other solutions as DPIs, in addition to their ability to meet the DPG Standard. As a result of this work, six digital public goods are being highlighted by the DPGA based on their ability to meet the criteria. Those digital public goods are: Apache Fineract, Mifos, Mojaloop, MOSIP, OpenCRVS, and X-Road.

This report provides a detailed overview of the assessment process used by the DPGA to review and highlight these DPI/DPGs in addition to how each digital public good was able to meet the criteria.

If harnessed correctly, technology has the ability to accelerate greater financial inclusion. The DPGA believes that leveraging these six solutions can play a critical role in making that happen. The aim of this assessment is to provide valuable insight that can support individuals, governments, and organisations seeking to understand open source digital solutions related to financial inclusion that can help enable digital transformation.

Introduction

This report details an assessment undertaken in June 2021 as part of the Digital Public Goods Alliance's Financial Inclusion (CoP), whose efforts have focused on identifying and highlighting digital public goods that are relevant to facilitating inclusive financial workflows at scale and enabling other solutions as digital public infrastructure.

Digital public goods are defined in the UN Secretary General's 2020 Roadmap for Digital Cooperation as, "open source software, open data, open AI models, open standards and open content that adhere to privacy and other applicable laws and best practices, do no harm, and help attain the SDGs."

The Digital Public Goods Alliance's mission is to accelerate the attainment of the sustainable development goals in low- and middle-income countries by facilitating the discovery, development, use of, and investment in digital public goods as defined above.

Understanding the importance of financial inclusion, this report focuses substantially on digital solutions that could also serve as digital public infrastructure (DPI). Insight on how this was determined is provided at length in the assessment section of the methodology.

This report combines both publicly available information and information provided directly by the digital solutions demonstrating their relevance to facilitating inclusive financial workflows at scale and enabling other solutions as digital public infrastructure at the time of writing this report. In addition, the DPGA team has reviewed these digital solutions against the DPG Standard. The methodology section also touches on limitations of this research approach.

The assessment presented in this report includes seven digital public goods identified by the Financial Inclusion CoP, six of which the DPGA is highlighting as digital public infrastructures given their ability to meet the criteria for DPI relevance and the DPG Standard. Those digital public goods are Apache Fineract, Mifos, Mojaloop, MOSIP, OpenCRVS, and X-Road.

How to navigate this report

This report is meant to highlight digital public goods that meet the DPG Standard and are relevant to facilitating inclusive financial workflows at scale and enabling other solutions as DPIs.

The introduction provides insight into what digital public goods are, and the efforts the DPGA has undertaken to ensure this report's highlighting of digital public goods can foster digital transformation in low- and middle-income countries through the adoption of digital solutions.

The methodology section explains the function of the Financial Inclusion Community of Practice, what determines how a potential solution is relevant to facilitating inclusive workflows at scale and enabling other solutions as digital public infrastructure, and the role the DPG Standard plays in defining what is a digital public good.

Based on the criteria set in the methodology, the Highlighted Solutions section provides an overview and assessment of each solution and how they meet the criteria, and final high level considerations that readers of this report may find helpful.

The concluding section indicates how the DPGA intends to continue working with stakeholders, including members of the Financial Inclusion Community of Practice, to continue promoting and advancing relevant open source solutions.

Intended audiences and use of the report

This report is written to support individuals and institutions who work with countries to evaluate, promote and propose open source digital solutions for financial inclusion. As well, this report may be a valuable tool for practitioners, funders, decision-makers and technical assistance providers, exploring solutions relevant to digital public infrastructure. All readers are encouraged to look at the highlighted solutions and the assessments provided when considering potential solutions for funding, development, or deployment.

For implementation, we see this report as a starting point. We encourage further assessment to ensure each DPG meets specific localised implementation needs. This report does not assess or review specific implementations of the highlighted solutions.

For further information and assessment of these tools, please note the considerations section under each highlighted solution.

Methodology

The technical assessment covers the following seven DPGs that were identified by the Financial Inclusion CoP: Apache Fineract, Mifos, Mojaloop, MOSIP, OpenCRVS, X-Road and OpenG2P, all of which can be found within the DPG Registry.

The assessment employed the following approach:

- Identification of primary and secondary data sources including:
    - Research articles
    - Consultation with key personnel
- DPG nomination submission forms in addition to relevant resources including:
    - DPGA: Accelerating financial inclusion during COVID-19 and beyond
    - Global Goods Maturity Index
    - ID4D Principles
    - UN Sustainable Development Goals
    - DPG Standard GitHub
- Research and desk review of publicly available Information from the official websites and blogs of the seven DPGs including:
    - GitHub repositories
    - Accessing the servers and demo sites (where available)
    - Identifying and accessing security audit reports
    - Running vulnerability (Snyk - https://snyk.io/) and fuzz tests (https://owasp.org/www-community/Fuzzing)
      *Please note, because Synk and Fuzz capture only a moment in time, results were shared directly with the digital solutions but are not included in this report.
- Documentation review including technical documentation, installation guides, user manuals, and official publishings
- Consultations with the DPGA technical team and other experts
- Consultation and engagement with the DPG product owners

Community of Practice

The DPGA convenes expert CoPs to support the discovery, assessment and advancement of digital public goods (DPGs) with high potential for addressing critical development needs in low- and middle-income countries. CoPs are convened around areas such as climate change adaptation, education, financial inclusion, and digital health. Within these broad topics, each CoP scopes and defines a particular focus area by considering relevance and potential impact of DPGs. CoPs then source a large number of potentially relevant DPGs. Members convene and discuss the merits and needs of particular considerations and identify additional assessment criteria and processes that should be part of an assessment process in this area.

Based on the input and feedback from the CoP members, the DPGA releases a list of highlighted digital solutions that meet the DPG Standard, and links to additional assessment criteria.
We are grateful for the participation of the following members of the Financial Inclusion Community of Practice (2020/2021) as well as for the contributions of a number of other stakeholders who provided thoughtful input to this report:

- Andrew McCormack, BIS
- Camilo Tellez-Merchan, Better than cash Alliance
- Christina Lomazzo, UNICEF
- CV Madhukar, Omidyar Network
- Daniel Radcliffe, Bill & Melinda Gates Foundation
- Edward Duffus, New Legacy Digital
- Greg Chen, CGAP
- Kanwal Singh, Bill & Melinda Gates Foundation
- Kashmera Self, Interac Corp.
- Kevin O'Neil, Rockefeller Foundation
- Laura Bingham, Open Society Foundation
- Laura Goodwin, Namati
- Linda Bonyo, Africa Law Tech
- Matt Homer, New York Department of Financial Services
- Ory Okolloh, Independent Advisor
- Pamela Eser, UNCDF
- Ryan Beech, WFP
- Sanjay Jain, iSPIRT/MOSIP
- Scott Moore, Gitcoin
- Sudhanshu Shekhar, iSPIRT
- Tanuj Bhojwani, iSPIRT
- Vyjayanti Desai, World Bank

This final report represents the opinions of the DPGA, and does not represent an endorsement by the individuals and organizations who contributed to this report.

Assessment

Digital Public Infrastructure for Financial Inclusion

Unlike DPGs there is no authoritative definition of digital public infrastructures (DPIs). As described in this paper, for the purpose of this community of practice DPI's can be considered: technologies that are "horizontals", solving problems impacting state (taxation, government aid, etc.), market (startups, enterprises), and consumers, and are the rails that other solutions "run on top of". Their implementation typically enables many other solutions & business models to flourish. It is furthermore meaningful to divide DPIs into foundational and functional categories. Foundational technologies refer to the most horizontally and cross-sectorally enabling platforms. For example Digital ID Systems like MOSIP (open source) or Aadhaar (proprietary) enable public service delivery across multiple sectors including health and finance.

How it is applied in this report:

The ultimate goal of the DPGA's Financial Inclusion CoP is to drive financial inclusion at scale. To do this, the CoP sought technologies that had the most potential for impact, and therefore were horizontally enabling, and sat at the intersection of DPGs and foundational DPIs. In addition to a review against the DPG Standard, the CoP used two questions to determine which technologies would fit these criteria:

1. Does it facilitate inclusive financial workflows across state, market, and consumers?
2. Does it enable other solutions (i.e. are other things built on top of it)?

For this report, the DPGA team collected information related to the five dimensions described in the table below for each product. Product owners reviewed and provided additional details and references.

These questions were translated into 5 dimensions in this table, and used to describe a product's relevance as financial inclusion DPIs.

Indicators	Dimensions	Details
DPI Relevance	Enables Financial Workflows	What specific financial services does this product provide or enable?
	Accessibility	Does it have functionality that makes it a usable, accessible provider of services? Is there low-bandwidth and/or offline capability?
	Interoperability	Does it have APIs and follow open standards to facilitate interoperability with existing technologies?
	Security Features: Authentication, Encryption, Updates	Does it have features for authentication/access control? Information encryption? Is it continuously updated?
	Enables other solutions	Does it have functionality that enables other solutions to be built on top of it?
	Scale	What are the planned and current implementations of this product? In which countries has it been implemented?

Since the aim is to highlight foundational DPIs that can be sustainably implemented in multiple countries, they are also verified against the DPG Standard.

The DPG Standard

The Digital Public Goods Standard is a set of specifications and guidelines designed to maximise consensus about whether the design of an open solution conforms to the definition of digital public goods (DPGs) set by the UN Secretary-General in the 2020 Roadmap for Digital Cooperation: "open source software, open data, open AI models, open standards and open content that adhere to privacy and other applicable best practices, does no harm and are of high relevance for attainment of the UN's 2030 Sustainable Development Goals (SDGs)."

The DPG Standard establishes a baseline that must be met in order to earn recognition as a digital public good by the Digital Public Goods Alliance and the broader community. The DPG Standard is itself an open project, open to contribution and developed in collaboration with organisations and experts. It is designed to identify DPGs across multiple sectors and the DPGA maintains an ongoing process of screening nominated projects through the DPG Registry. It is currently in version 1.1.4.

How it is applied in this report:

For this report, individuals with authority to speak on behalf of the solution provided information to the DPGA that was used to assess whether a product meets the minimum requirements to be considered a digital public goods according to the indicators set out in the DPG Standard. For indicators 1-6 in the standard (see below) the DPGA takes steps to verify the information for accuracy by comparing it to publicly accessible information such as the code, documentation and license. For indicators 7-9, this information is *self-reported* and is not verified by the DPGA.

Below is an overview of the DPG Standard, the full standard is visible here.

Digital Public Goods Standard:

Indicators	Requirements
SDG relevance	1) SDG relevance
Open source	2) Use of approved license 3) Clear ownership 4) Platform independence 5) Technical and operational documentation 6) Mechanism for extracting data
Adherence to laws, standards & best practice	7) Adherence to privacy and applicable laws 8) Adherence to standards & best practices
Steps taken to mitigate & avoid harm in product design	9a) Data privacy & security 9b) Inappropriate & illegal content 9c) Protection from harassment

The next section presents a summary of the findings for each of the six DPGs reviewed. The findings are presented based on a review against the DPG Standard and an assessment of their relevance to financial inclusion.

Considerations & Limitations of this Report

An effort was made to consider all of the digital solutions suggested by members. Inevitably, some relevant digital solutions were not captured in our discussions, some digital solutions didn't respond to our request for information, and some opted not to participate because of their own assessment of their licensing and/or maturity. Only solutions that were deemed digital public infrastructure with relevance to financial inclusion were included in this report and this report is not inclusive of all DPGs or DPIs. This is a living document and the DPGA will periodically review and update this report with relevant solutions.

In this report we only evaluated the intention and design of the generic open source digital solution and not specific implementations or deployments. As a result, especially on dimensions such as compliance with laws, adherence to standards, and doing no harm, which are key components of the UNSG's definition of digital public goods, much is dependent on how the digital solution is implemented and adapted to the local context. Acknowledging this as a limitation within the report, we asked digital solution owners to describe the steps they have taken in the design and development of the digital solution to address and ensure good practices in these areas.

Lastly, the nature of open source digital solutions is that they are constantly developing and changing. This report is clearly time-stamped, each of these digital solutions is re-assessed against the DPG Standard on an annual basis, and we are exploring innovative ways to rapidly update digital solution information. It will be important to consider the evolving nature of digital solutions when utilising this report.

To try and mitigate these limitations, all of the information provided by the digital solutions is published transparently, in full, alongside our assessments and we urge those considering implementations, investments, and development to use this as a starting point for additional critical evaluation of these digital solutions.

Assessment

This section presents the assessment summaries for six of the seven DPGs based on the methodology outlined above.

1. Apache Fineract

URL	https://fineract.apache.org/,
Repository	https://github.com/apache/fineract
License	Apache 2.0
Most Current Version	1.5.0 May 21, 2021
OS Environment	OS Agnostic

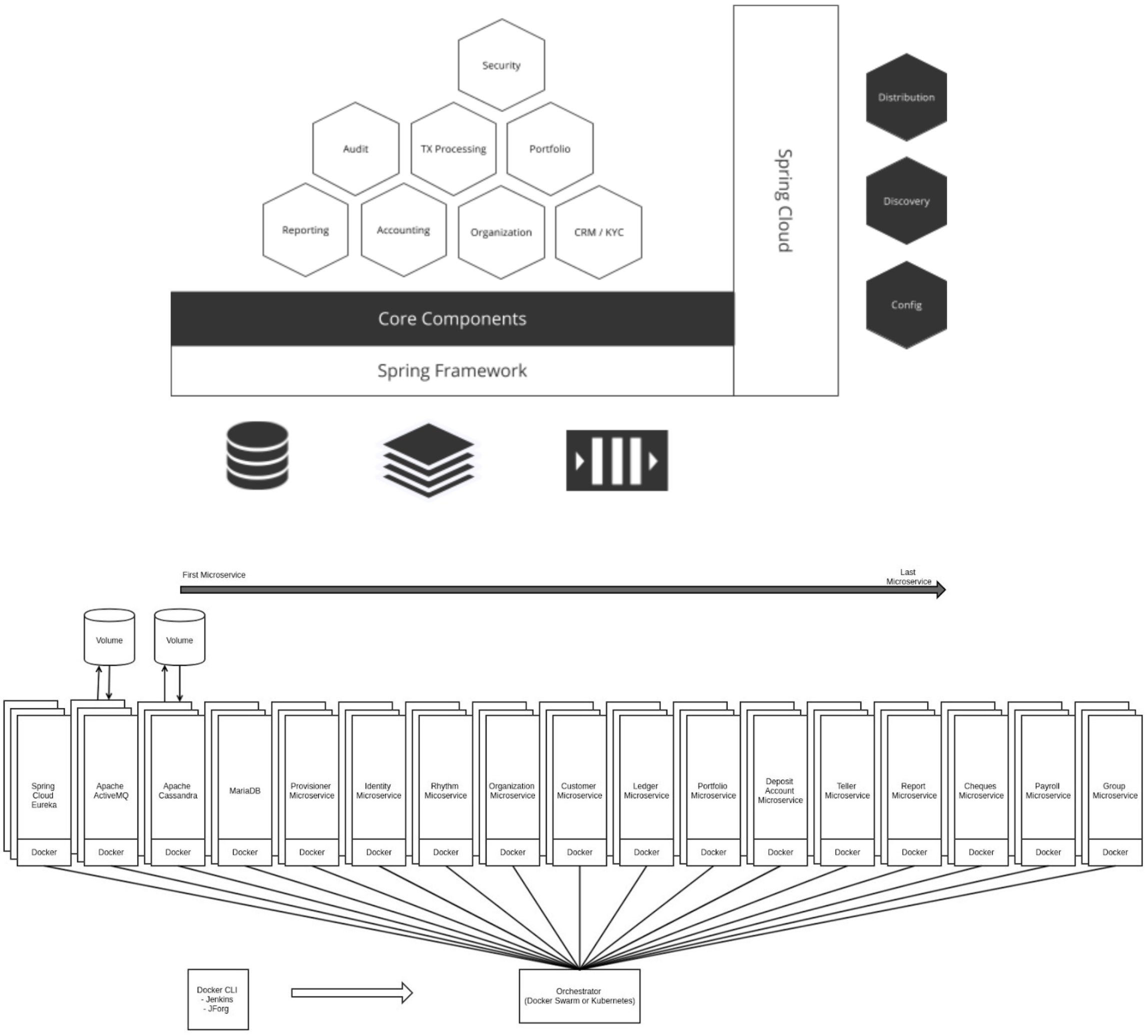
Description:

Fineract is a core banking system that provides a reliable, robust, and affordable solution for entrepreneurs, financial institutions, and service providers to offer financial services to the world's 3 billion underbanked and unbanked. Fineract is aimed at innovative mobile and cloud-based solutions, and enables digital transaction accounts for all. Apache Fineract originated from the underlying Mifos X platform and APIs when it was donated to the Apache Software Foundation by the Mifos Initiative. The Mifos digital public goods are a set of reference staff and customer-facing web and mobile apps as well as payment integration tools on top of Apache Fineract.

Relevance as a DPI for Financial Inclusion:

Dimension	Response	Specific Details	Reference
Enables financial workflows	Y	● Client data management ● Loan and savings portfolio management ● Integrated real time accounting ● Social and financial reporting	https://fineract.apache.org/
Accessibility	Y	Designed to accommodate those with low literacy through the use of tab-based browser navigation. An API provides for USSD and SMS based access.	Apache Fineract Design Principles
Interoperability	Y	The system is fully API controlled and all functionality available is mapped to an API. Data exchange is through REST and JSON.	API Layer

Security (authentication)	Y	All authentication is done on the username and password provided. This also can be used to generate a token when using OAuth2 that can be used to authenticate requests. An option is provided for using HTTP Basic Auth or OAuth2 that provides multifactor authentication such as OTP.	Apache Fineract Design Principles
Security (information encryption)	Y	The platform has been configured to reject plain HTTP requests by default and to expect all API requests to be made over HTTPS. All requests must be authenticated. HTTPS encrypts all communication by default.	Security Report
Security (continuous updates)	Y	The platform is updated frequently by Apache Software Foundation with reported software bugs and vulnerabilities updated through Apache Security Team.	Apache Security Publication
Enables other solutions	Y	The API REST framework empowers developers to build apps on top of the Apache Fineract Platform.	Apache finaract API
Scale	Y	Numerous enterprise banks in India, Mexico, Indonesia, and Germany have deployed Apache Fineract serving millions respectively. More than 20 million individual clients are reached by 400+ institutions across 40 countries using systems powered by Mifos and/or Fineract APIs. The underlying APIs of both generations of Apache Fineract (Fineract 1.x and Fineract CN) have been deployed across a number of use cases in more than 40 countries. Adoption has scaled horizontally across traditional brick and mortar institutions from Savings Groups to MFIs to SACCOs to Banks as well as digital-first neobanks, fintechs, digital credit, and wallet/payment providers. *Note: Since the Mifos X back-end platform became Apache Fineract it's difficult to separate out Mifos vs. Fineract implementations. See Mifos entry for additional details.	Powered By Mifos



Fineract CN Architecture

Assessment summarized in the table below is extracted from the DPG Registry:

Indicators	Requirement	Response	Details, Reference
SDGs relevance	Relevant to at least one SDG	Yes	SDGs 1, 16, 17
Open source	Use of approved license	Yes	Open Software, Apache 2.0 License
	Clear ownership	Yes	ASF Source Header and Copyright Notice Policy
	Platform independence	Yes	
	Technical and operational documentation	Yes	Introduction - Fineract Wiki
	Mechanism for extracting non-PII data	N/A	Does not collect or use non-personally identifiable information
	Adherence to applicable laws	Yes	GDPR, PSD2, OFAC, AML, CFT

Adherence to

laws, standards & best practice	Adherence to applicable standards	Yes	W3C, Open Banking Standards, Java Coding Standards Best Practices: Principles of Digital Development
Steps taken to mitigate & avoid harm in product design	Data privacy and security	Yes	Data collected but not shared include: As a financial services core banking platform, customers that use the software collect data on their individual clients like name, date of birth, address, ID/SSN, etc.
	Inappropriate and illegal content	N/A	Does not collect, store or distribute content
	Protection from harassment	Yes	We have a code of conduct and a PMC to oversee community interactions. When we participate in programs like Google Code-In, we follow Google norms for restricting access to PII of high-school contributors only having them share their avatar, etc. fineract/CODE_OF_CONDUCT

2. Mifos

URL	https://mifosforge.jira.com
Repository	https://github.com/openMF/
License	Mozilla Public License 2.0
Most Current Version	Mifos X - June 2021 | Payment Hub EE - November 2020
OS Environment	OS Agnostic

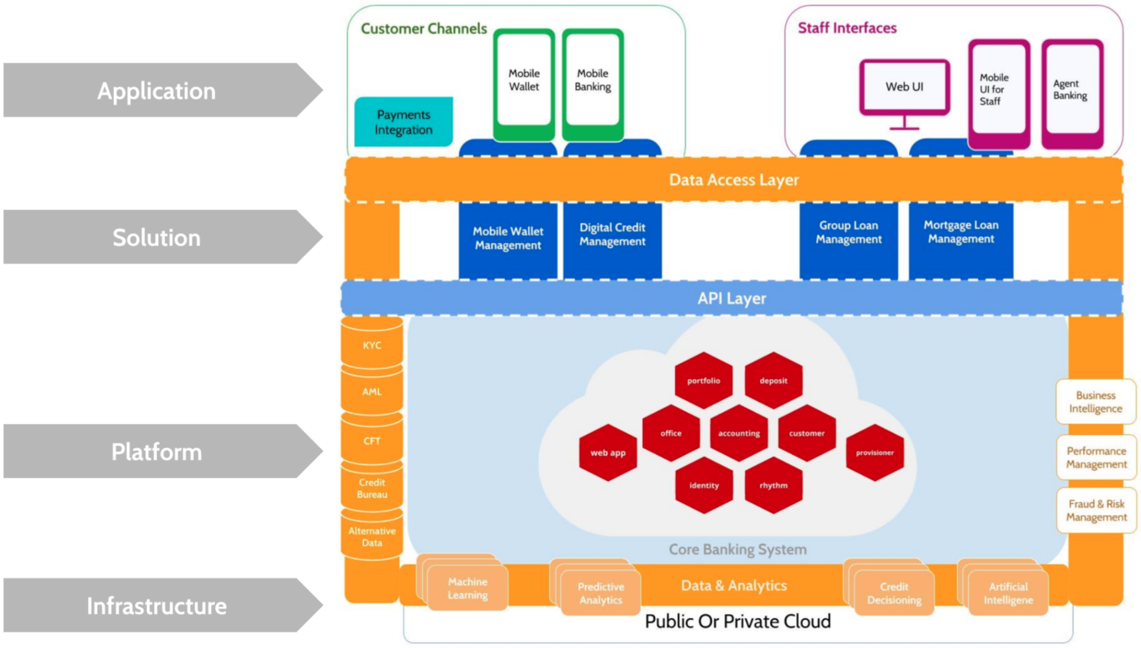
Description:

Mifos X is an extended platform for delivering the complete range of financial services needed for an effective financial inclusion solution. Built on Fineract, and integrated with Mojaloop, Mifos provides an end to end open source architecture for digital financial services with open APIs for integration to the payment rails, account management and core banking, and third party app innovation. It provides a ready-to-deploy end to end core banking product on top of Apache Fineract including the reference web and Android UI for staff, web and mobile self-service apps for customers, a payment integration layer and orchestration engine, reporting, and other decisioning tools like credit scoring, credit bureau and chatbot modules. The code repositories include: staff web UI (community and web-app), staff mobile UI (android-client and fineract-cn-mobile), payments integration (payment hub-ee), mobile banking app (mifos-mobile), mobile wallet app (mifos pay), online banking apps (online-banking-app), and more.

Relevance to DPI for Financial Inclusion:

Dimension	Response	Specific Details	Reference
Enables financial workflows	Y	● Client management ● Financial services product management ● Mobile delivery and transaction management ● Business management ● Payment processing & orchestration	Mifos Initiative: Homepage
Accessibility	Y	The original design of the Mifos web user interface was designed by Stanford usability experts with tab-based browser navigation for those with low technical literacy. Ongoing updates were led by a UX expert from VMware and continuing to follow the Material design guidelines. Our mobile applications are designed according to Material design standards and adhere to responsible design principles. As a single-page application, Mifos X is designed to perform well in low-bandwidth environments with limited connectivity. Browser-based offline access is in progress using Service Workers APIs. Offline data synchronization is part of native Android field operations app for tablets/smartphones.	Mobile Version
Interoperability	Y	The API Layer is built entirely as a RESTful Webservice, using JSON to transmit data, and utilizes standard HTTP Methods for interactions.	API Layer
Security (authentication)	Y	The Service Layer provides module specific business logic and rules, and role based access control. Transaction awareness and data validity is encapsulated, and extension points are available to enhance built-in workflows. All authentication is done on the username and password provided. This also can be used to generate a token when using OAuth2 that can be used to authenticate requests Option provided for using HTTP Basic Auth or OAuth2 that provide multifactor authentication such as OTP.	Service Layer
Security (information encryption)	Y	The platform has been configured to reject plain HTTP requests by default and to expect all API requests to be made over HTTPS. All requests must be authenticated. HTTPS encrypts all communication. By default encryption is enabled for all requests.	Mifos API authentication
Security (continuous updates)	Y	The platform is updated frequently by Apache Software Foundation with reported software bugs and vulnerabilities updated through http://www.apache.org/security/.	Apache Security publication
Enables other solutions	Y	By providing reference UIs on top of Apache Fineract, Mifos enables DFS solutions at an infrastructure as well as application level. Nationwide efforts can be built out on top of Mifos through the OpenG2P framework, small, medium and large brick and mortar institutions are digitized at scale through cloud banking via their multi-tenancy and a wide variety of digital-first fintechs use Mifos for payment, lending, and savings-led use cases. Mifos provides a direct integration to Mojaloop via the Payment Hub EE orchestration engine as well as an Open Banking API layer for third party innovation.	Mifos Initiative: Homepage
Scale	Y	More than 20 million individual clients are reached by 400+ institutions across 40 countries using systems powered by Mifos and/or Fineract APIs.	Powered By Mifos and

		Mifos X and the corresponding web and mobile apps for staff and customers provide an out of the box solution on top of Apache Fineract. More than five dozen partners worldwide provide hosting, customization, implementation and support of Mifos X as is. *Note: Since the Mifos X back-end platform became Apache Fineract it's difficult to separate out Mifos vs. Fineract implementations. See the Apache Fineract entry for additional details.	Partner Directory



Generation 3 Mifos I/0 (Fineract CN) Architecture

Assessment summarized in the table below is extracted from the DPG Registry:

Indicators	Requirement	Response	Details, Reference
SDGs relevance	Relevant to at least one SDG	Yes	SDG 1, 8
Open source	Use of approved license	Yes	Open Software, Mozilla Public License 2.0
	Clear ownership	Yes	Financial and Legal Information
	Platform independence	Yes	
	Technical and operational documentation	Yes	Mifos X Overview - Mifos User GuideTHe
	Mechanism for extracting non PII data	N/A	Does not collect or use non-personally identifiable information
Adherence to laws,	Adherence to applicable laws	Yes	GDPR, OFAC

standards & best practice	Adherence to applicable standards	Yes	W3C Project Wiki; Best Practices: Principles of Digital Development
Steps taken to mitigate & avoid harm in product design	Data privacy and security	Yes	Personal data not collected
	Inappropriate and illegal content	N/A	Does not collect, store or distribute content
	Protection from harassment	Yes	During programs like GCI, students full names aren't referenced - just their online ID or avatar; a code of conduct is maintained and aims to mediate and resolve issues that arise amongst community members.

3. Mojaloop

URL	https://mojaloop.io/
Repository	https://github.com/mojaloop/mojaloop
License	Apache 2.0
Most Current Version	12.0.0 February 26, 2021
OS Environment	Linux, Mac, Windows

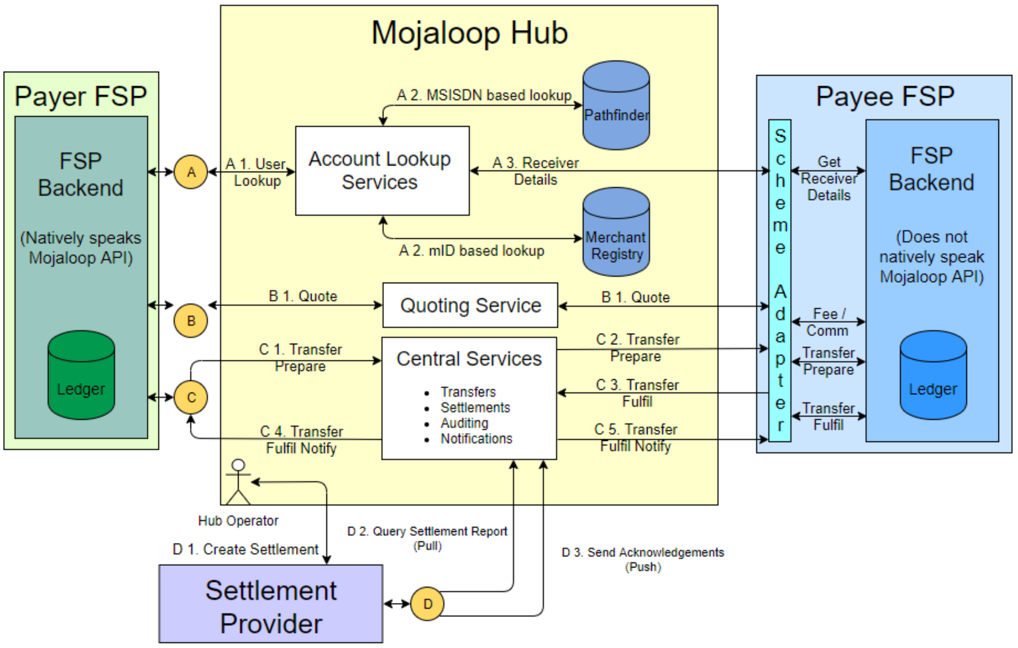
Description:

Mojaloop is an open source software empowering organizations to create interoperable digital payment systems to increase financial inclusion.

Relevance to DPI for Financial Inclusion:

Dimension	Response	Specific Details	Reference
Enables financial workflows	Y	• A reference model for payment interoperability for digital financial services	Mojaloop Foundation
Accessibility	Y	Mojaloop provides APIs to enable the use of the Mojaloop platform by service providers that create the appropriate UIs to target consumers. The flexible design allows service providers to tailor their offerings to unbanked and underserved populations without requiring smart phones and high bandwidth.	Core Scenarios
Interoperability	Y	Interoperability is realized through the interoperability layer. Mojaloop uses open APIs for Financial Service Providers	Mojaloop API architecture

		(FSP) as well as open data standards and open data formats to achieve interoperability.	
Security (authentication)	Y	Mojaloop implements user access control through requiring authentication for any operation on the system. User roles are also used to provide different sets of users with different privileges. Multifactor authentication is provided API request signing, HTTPS Authentication and OAuth.	Mojaloop API signatures
Security (information encryption)	Y	When an API client sends an HTTP request (such as an API request or callback message) to a counterparty, the API client can determine whether there are sensitive fields in the API message to be protected according to the regulation or local schema. If there is a field to be protected, then the API client uses JWE to encrypt the value of that field. Subsequently, the cipher text of that field will be transmitted to the counterparty.	Mojaloop Communication encryption protocols
Security (continuous updates)	Y	The platform is updated frequently by the Mojaloop community of developers who are actively developing the system.	Mojaloop Vulnerability Reporting Procedure -
Enables other solutions	Y	By connecting multiple digital Financial services Providers (DFSPs) into an interoperable network.	https://mojaloop.io/
Scale	Y	Several financial institutions are in the process of deploying Mojaloop-based systems. Mowali, a joint venture between MTN and Orange, has released services in Cote d'Ivoire and Egypt.	Mowali | Slogan



Mojaloop Architecture

Assessment summarized in the table below is extracted from the DPG Registry:

Indicators	Requirement	Response	Details, Reference
SDGs relevance	Relevant to at least one SDG	Yes	SDGs 1, 9,10,16,17
Open source	Use of approved license	Yes	Open Software, Apache License 2.0
	Clear ownership	Yes	Mojaloop Background · GitBook Terms of Use
	Platform independence	Yes	
	Technical and operational documentation	Yes	Mojaloop Overview - GitBook
	Mechanism for extracting non PII data	N/A	Non PII data not collected
Adherence to laws, standards & best practice	Adherence to applicable laws	Yes	EEA Data Subject Terms of Use Mojaloop Foundation Privacy Policy Github documentation
	Adherence to applicable standards	Yes	PCI, DSS, GDPR documentation artefacts
Steps taken to mitigate &	Data privacy and security	N/A	Personal data not collected

avoid harm in product design	Inappropriate and illegal content	N/A	mojaloop Code of Conduct
	Protection from harassment	Yes	License Agreement

4. MOSIP

URL	https://www.mosip.io/
Repository	https://github.com/mosip
License	Mozilla Public License 2.0
Most Current Version	1.1.5 April 20. 2021
OS Environment	OS Agnostic

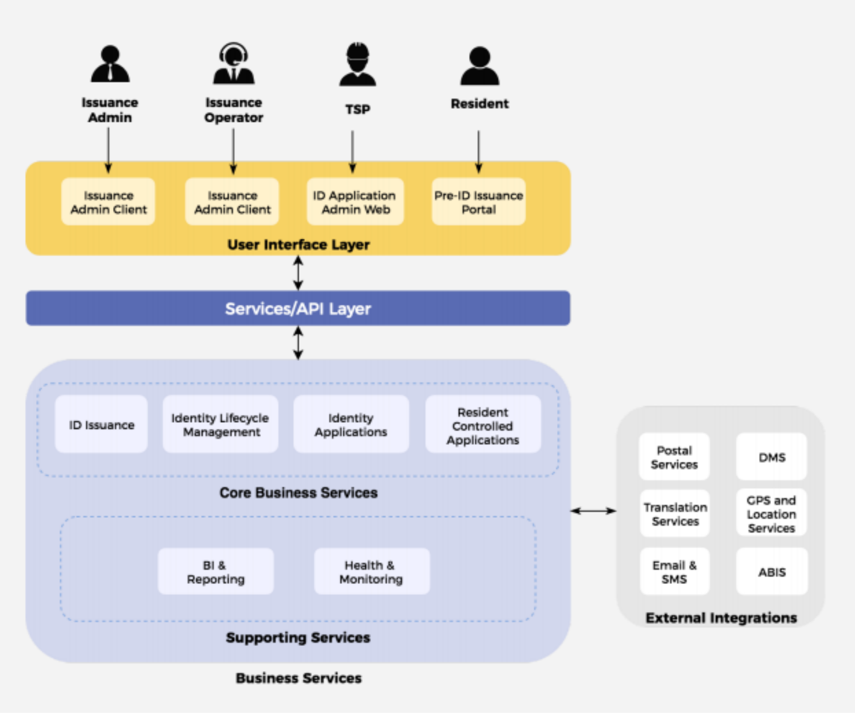
Description:

Mosip is a modular and open source/open standard identity platform that helps governments and other user organisations implement a digital, foundational ID in a cost effective way.

Relevance to DPI for Financial Inclusion:

Dimension	Response	Specific Details	Reference
Enables financial workflows	Y	• Unique identifier used for identity assertion and verification as foundational IDs that can be used to access variety of government and private services	MOSIP: Open Source Platform - National Foundational Id
Accessibility	Y	MOSIP supports offline and online capabilities at key points in the process flow, where data is either collected or a service is delivered. This is done through offline capable thick clients for data capture for ID issuance, and through a standards compliant authentication and credential service, which can be used to perform authentication in several ways - QR Codes, OTP, biometric authentication. MOSIP also supports and encourages assisted models to cater to those with low digital proficiency.	Registration Mosip documentation ID Authentication
Interoperability	Y	Mozilla Public Licence 2.0 that is distributed with the platform provides grants of copyright licence and right to redistribute. This provides an option for the software to be integrated and used	Mozilla Public Licence v2.0

		together with any other platform. System is fully API controlled and all functionality is mapped to an API.	
Security (authentication)	Y	MOSIP depends on LDAP implementation to manage users, organizational hierarchy and roles for users in the hierarchy. MOSIP will use an open source LDAP server as the LDAP implementation. Administrators can create hierarchy and users using Apache Directory Studio. In addition, the system uses OAuth2 token based authentication. Client uses a given username and password to generate a token that will be used to access resources.	Privacy and Security User Guide
Security (information encryption)	Y	The platform has been configured to reject plain HTTP requests by default and to expect all API requests to be made over HTTPS. All requests must be authenticated. HTTPS encrypts all communication, all requests are encrypted by default.	Privacy & Security
Security (continuous updates)	Y	Mosip, through github, has an active bounty program for security researchers to be able to stress test the system and report any vulnerabilities on the platform.	Mosip issue reporting guidelines -
Enables other solutions	Y	Foundational IDs can be used to issue purpose-specific or functional specific IDs to identify individuals entitled to particular services such as healthcare, insurance and subsidized goods.	MOSIP: Open Source Platform - National Foundational Id
Scale	Y	National scale Implementations in Philippines, Morocco; pilots in Guinea, Ethiopia, Sri Lanka.	Morocco Bangalore and PSA, Republic of the Philippines MOSIP 'Stories from the field Ethiopia



Mosip Architecture

Assessment summarized in the table below is extracted from the DPG Registry:

Indicators	Requirement	Response	Details, Reference
SDGs relevance	Relevant to at least one SDG	Yes	SDGs 1, 2, 3, 4, 5,8,9,10,16,17
Open source	Use of approved license	Yes	Open Software/Open Standard Mozilla Public License 2.0
	Clear ownership	Yes	Resources detail
	Platform Independence	Yes	For every closed source software/hardware component interacted with , standard interfaces for interaction through open standards or defining new standard interfaces
	Technical and operational documentation	Yes	MOSIP Docs: Introduction
	Mechanism for extracting non PII data	Yes	The project allows each deployment to define what data they collect. Some of these could be non-PII data
Adherence to laws, standards & best practice	Adherence to applicable laws	Yes	GDPR,MOSIP enables the compliance of privacy laws through its security and feature implementations. However, the owners of specific implementations are responsible for complying with legislation in their jurisdictions.
	Adherence to applicable standards	Yes	OpenID Connect, JWT, ISO/IEC 19794-4:2011 ISO/IEC 19794-5:2011,ISO/IEC 19794-6:2011 ISO 8601,ISO/IEC 19785-3,OASIS patron format ISO/IEC JTC 1 SC 37,digital signatures, PKI and cryptography Best Practices: ID4D

Steps taken to mitigate & avoid harm in product design	Data privacy and security	Yes	PII collected include legal name,- age, address and additional fields are collected as needed Biometric information is collected for the purpose of ascertaining uniqueness and for authentication, based on countries' policy, - fingerprint, face, iris data is captured one time during the enrollment process. Data is shared for KYC credentials for service within a governance framework mandated by the project owner in addition to the policies as expressed here Privacy & Security
	Inappropriate and illegal content	N/A	Does not collect, store or distribute content
	Protection from harassment	N/A	No interactions between users, for protection of udergage users there is code of conduct here Code of Conduct

5. OpenCRVS

URL	https://www.opencrvs.org/
Repository	https://github.com/opencrvs
License	Mozilla Public License 2.0
Most Current Version	Alpha 3.0 December 21, 2020 (https://github.com/opencrvs/opencrvs-core/releases)
OS supported	Ubuntu

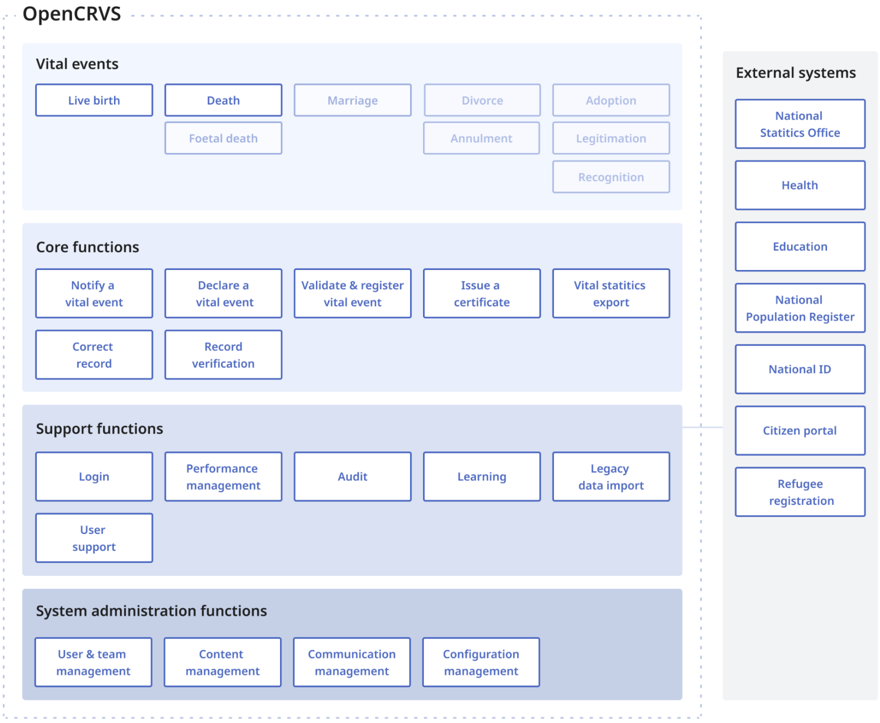
Description:

OpenCRVS is a digital public good to help achieve universal civil registration and evidence-based decision making in all country contexts.

Relevance to DPI for Financial Inclusion:

Dimension	Response	Specific Details	Reference
Enables financial workflows	Y	Digital Civil Registration and Vital Statistics Records for every individual for legal identity for access to basic rights	OpenCRVS
Accessibility	Y	OpenCRVS utilises award winning design patterns proven to be user friendly and assist high-quality data entry. Users are presented with one question per page and guides them through the form, which is available in multiple language options in online and offline modes.	Key features Offline and low connectivity working Usability of forms Multi-language options

Interoperability	Y	OpenCRVS makes use of the HL7 FHIR interoperability standard to support data exchange with other systems. Standards-based APIs connect to health systems and National ID systems for real time validation of national IDs of parents and retrieval of personal details. Open architectural style and data formats supported.	Interoperability
Security (authentication)	Y	OpenCRVS mobile applications and microservices are secure, protected by 2-Factor Authentication utilising OAuth JWT best practices. A PIN must be entered each time the user accesses the application. Once a week an additional 2-factor authentication is required, including a code being sent via SMS to the field agent.	OpenCRVS technology specification - OpenCRVS System Key Features
Security (information encryption)	Y	The platform has been configured to reject plain HTTP requests by default and to expect all API requests to be made over HTTPS. All requests must be authenticated and HTTPS encrypts all communications. Automatic LetsEncrypt SSL configuration and microservice cloud router using Traefik is used to secure transmissions.	OpenCRVS Security
Security (continuous updates)	Y	Independent contractors are responsible for ensuring security of the system. Reported issues are also escalated through Github Issues where a maintainer gets assigned high priority security tickets to resolve. OpenCRVS uses Github Issues for reporting and resolving security vulnerabilities.	OpenCRVS Security Core issues
Enables other solutions	Y	Like foundational IDs, service delivery functions are built on top of population registers that CRVS enables.	OpenCRVS Overview
Scale	Y	Implemented in Bangladesh (pilot completed and scoping scaleup), Gambia (birth registration using OpenCRVS during COVID vaccination drives), Niue (reference implementation for the Pacific Islands).	OpenCRVS goes live in Bangladesh



OpenCRVS Functional Architecture

Assessment summarized in the table below is extracted from the DPG Registry:

Indicators	Requirement	Response	Details, Reference
SDGs relevance	Relevant to at least one SDG	Yes	SDGs 16, 17
Open source	Use of approved license	Yes	Open Software, Mozilla Public License 2.0
	Clear ownership	Yes	OpenCRVS Readme
	Platform independence	Yes	
	Technical and operational documentation	Yes	Functional: Introduction Technical: Introduction
	Mechanism for extracting non PII data	Yes	Non personally identifiable information can be extracted from OpenCRVS through a non-proprietary export of performance management reports (in csv format)
Adherence to laws, standards & best practice	Adherence to applicable laws	Yes	Bangladesh: Birth and Death Registration Act, 2004 Bangladesh: Birth and Death Registration Rule, 2006. Configurable to conform to international and domestic laws

	Adherence to applicable standards	Yes	WCAG2.1, W3C, HL7/FHIR, CREST Best Practices: Principles of Digital Development, principles of sustainable development, Handbook on CRVS systems, management, operation and maintenance.
Steps taken to mitigate & avoid harm in product design	Data privacy and security	Yes	Collects PII data such as full name, home address,- personal identification number, telephone number, DoB,gender and is shared with other government systems (as a foundational registry) as per laws and regulations of the jurisdiction subject to the following privacy policy.
	Inappropriate and illegal content	N/A	Does not collect or distribute content
	Protection from harassment	N/A	Does not facilitate interaction between users

6. X-Road

URL	https://x-road.global/
Repository	https://github.com/nordic-institute/X-Road
License	MIT License
Most Current Version	6.26.0 March 26, 2021
OS supported	All components: Ubuntu; Some components: Red Hat Enterprise Linux, Docker

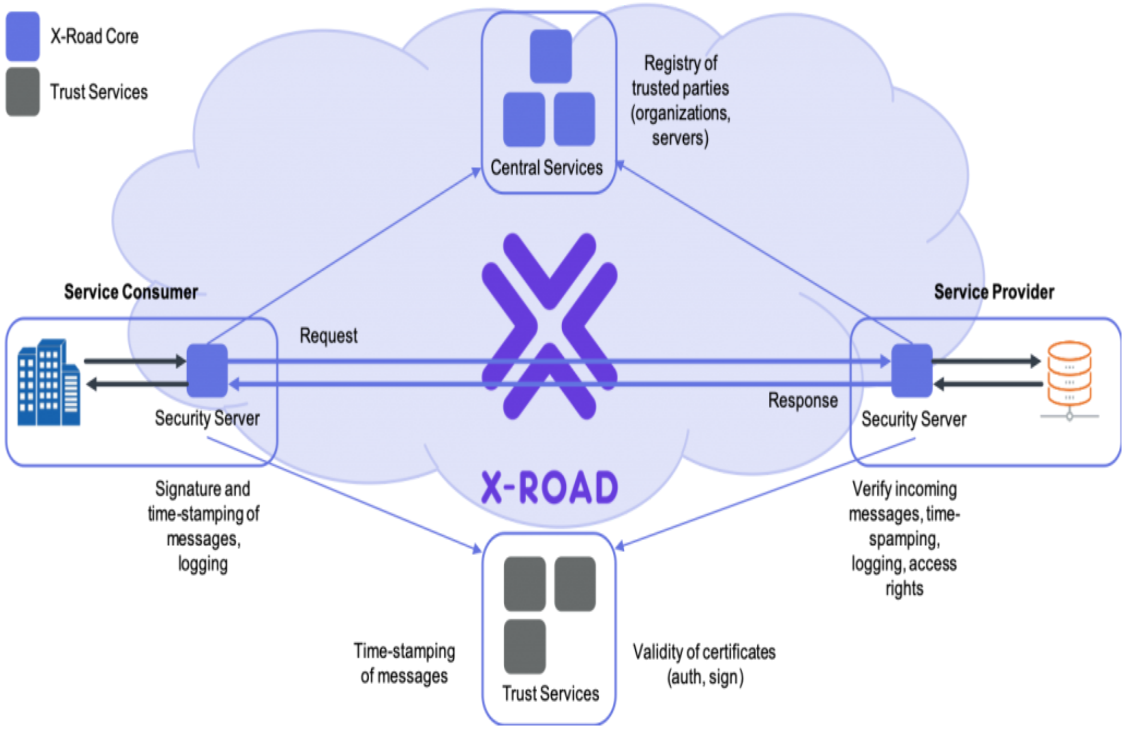
Description:

X-Road is open source software and ecosystem solution that provides unified and secure data exchange between organizations.

Relevance to DPI for Financial Inclusion:

Dimension	Response	Specific Details	Reference
Enables financial workflows	Y	• Address management • message routing • access rights management • organizational level authentication • machine-level authentication • transport-level encryption • time-stamping • digital signature of messages • logging, error handling	X-Road® Data Exchange Layer
Accessibility	Y	X-Road doesn't provide an UI for end users and/or citizens. X-Road UIs are for a limited number of technical users only. APIs can be used for programmatic access.	X-Road® Architecture — X-Road® Data Exchange Layer

		X-Road's architecture is extremely flexible and it supports various kinds of setups. It enables different approaches when it comes to the speed and scale of the implementation.	
Interoperability	Y	X-Road is decentralized – the data exchange happens directly between organizations. There are no intermediaries. If the two organizations have established a secure connection, the continuous data exchange depends only on availability of the organizations and the network between them. All communication is implemented as [SOAP] or REST service calls. SOAP services are described using the [WSDL] language and REST services are described using the [OPENAPI] Specification v3.	X-Road Cross Border Data Exchange
Security (authentication)	Y	X-Road implements an authorization framework that is used to manage access rights to services. Access rights management is based on the organization and service level identifiers. The key idea of X-Road is that each service provider owns its data and is responsible for managing access rights of its services. Access rights are granted on the information system level – a service provider grants a specific information system access to a service. Network connections between data exchange parties are authenticated using mutual TLS authentication. Only certificates issued by approved certification authorities are accepted. Also, the certificates must be registered to the system during the onboarding process and they're linked to a specific node.	Technology-overview
Security (information encryption)	Y	Messages transmitted over the public Internet are secured using digital signatures and transport-level encryption. Encryption is enabled for all requests by default.	X-Road Security Server architecture
Security (continuous updates)	Y	System bugs and attack types are captured from the available bug bounty program and updated with an average timeline of 4 days.	X-Road Vulnerability Report
Enables other solutions	Y	Uses core digital infrastructure that enables access to other services	X-Road® Data Exchange Layer
Scale	Y	Implemented in Germany, Azerbaijan, Palestine, Kyrgyzstan,Djibouti, Cambodia, Vietnam, Finland, Estonia, Barbados, Columbia, Iceland, Brazil, Argentina , Cayman Islands, El Salvador, Mexico, Japan, Faroe Islands	X-Road® World Map


X-Road Core
Trust Services
Central Services
Registry of trusted parties (organizations, servers)
Service Consumer
Service Provider
Request
Response
Security Server
Security Server
X-ROAD
Signature and time-stamping of messages, logging
Verify incoming messages, time-spamping, logging, access rights
Time-stamping of messages
Trust Services
Validity of certificates (auth, sign)

X-Road Architecture

Assessment summarized in the table below is extracted from the DPG Registry:

Indicators	Requirement	Response	Details, Reference
SDGs relevance	Relevant to at least one SDG	Yes	SDGs 1, 3,7,8,9,11, 13, 16
Open source	Use of approved license	Yes	Open software , MIT License
	Clear ownership	Yes	nordic-institute/X-Road-development
	Platform independence	Yes	
	Technical and operational documentation	Yes	X-Road® Developer Resources
	Mechanism for extracting non PII data	N/A	Non-PII data not collected
Adherence to laws, standards & best practice	Adherence to applicable laws	Yes	GDPR, all relevant Estoian domestic laws
	Adherence to applicable standards	Yes	RFC6960, RFC3161,ETSITS 102 98 Best Practice: principle of Digital Development
Steps taken to mitigate & avoid harm in product design	Data privacy and security	N/A	PII data not collected
	Inappropriate and illegal content	No	Only technical documentation and materials related to knowledge sharing collected
	Protection from harassment	Yes	Interaction between users does not involve underage users

Overarching Considerations

i. Apache Fineract, Mifos, Mojaloop, Mosip, OpenCRVS, X-Road

We urge those considering implementations, investments, and development to use this report as a starting point, we hope the following considerations support additional evaluation of these solutions:

1. Operating System: Most of these DPGs are supporting all common operating systems with only two currently offering Ubuntu only (OpenCRVS & X-Road).
2. Sustainability & Revenue: All six DPGs are exploring additional sustainability and revenue models to complement support from donors and philanthropists.
3. Security: As part of benchmarking, additional vulnerability and audit tests can be done on the source code using third party tools. Most of the DPGs already have such reports available upon request from the product owners.
4. Roadmap: The DPGs make frequent updates to the source code and the accompanying documentation. Some even show the features update roadmap. All these are easily accessible from Github repositories where new releases can be obtained.
5. Multilingual Documentation: There is growing consideration to offer multilingual documentation by the DPGs. This will greatly improve adoptability and should be part of any product consideration.
6. Community: X-Road and Mojaloop have active communities working to support new innovative features and to improve the systems. It can be helpful to understand the community maturity and governance structures of these DPGs.

ii. OpenG2P

A pre-assessment of OpenG2P revealed that it is still undergoing development and enhancement, and therefore a detailed assessment will be carried out once the development, testing and pilot deployment on a site has been completed.

Conclusion

Based on the assessment above, the DPGA found the current releases of the six DPGs: Apache Fineract, Mifos, Mojaloop, MOSIP, OpenCRVS and X-Road to be DPIs and DPGs with high potential to drive financial inclusion at scale. We are therefore highlighting these solutions as DPGs/DPIs that address a critical development need. Readers of this report are encouraged to look at the highlighted solutions and the assessments provided when considering potential solutions for funding, development, or deployment.

Digital Public Goods Alliance

www.digitalpublicgoods.net