Can Government to Person Payments and Services be made easier using Digital Public Goods?

An Assessment Report of DPGs in the G2P Connect Initiative

The better the question. The better the answer.
The better the world works.

CO-DEVELOP

Building a better working world

Table of Contents

Foreword

The digitization of Government-to-Person (G2P) services and payments is about more than mere comfort and convenience. It represents a paradigm shift in how governments can directly impact its people's lives through efficient, seamless, and timely service or benefit delivery, realizing multiple benefits across all stakeholders of the G2P ecosystem – be they governments at all levels, businesses, service providers of all kinds, and the people themselves.

G2P payments have long been an integral element of the financial ecosystems of nations worldwide, serving as a pivotal channel through which governments can directly support individuals and households. The shift towards digitalization of these payments brings along a transformative power that promises not only enhanced efficiency and transparency but also an unprecedented reach and inclusivity, and the power to transform people's livelihoods.

We stand today at the cusp of a significant revolution, as digital technologies reshape the way governments interact with their citizens, particularly in terms of financial transactions. The ongoing transition from cash to digital payments has opened a window of opportunity to improve the effectiveness, efficiency, and inclusion of every financial service -across lending, insurance, pensions, and investing.

The G2P Connect Initiative represents a commitment to re-envision the way public services are delivered. It aims at catalyzing the potential of digital technology to not only ensure that support reaches the intended beneficiaries without dilution, but also as a catalyst for financial inclusion, particularly for those segments of the population that have traditionally been underserved by formal financial systems.

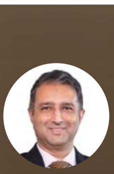
By breaking down a hitherto monolithic approach for G2P services and benefit delivery into more tractable building blocks, each of which may be implemented independently, and in any order, G2P Connect aims to build a robust digital infrastructure, to enable government-to-person digital payments built through interoperable standards and design blueprints. The G2P Connect solution blueprint, comprised of these building blocks that work with each other through open standards, help accelerate implementations. Developed as open-source software, these building blocks are available as Digital Public Goods (DPGs), that are accessible at low-cost, and around which an ecosystem of implementers is growing.

To provide insights to policy makers, implementation institutions and agencies, and other relevant stakeholders, we feature the assessment report of Digital Public Goods (DPGs) as part of the G2P Connect Initiative. Specifically with respect to G2P payments, governments can implement these open-source building blocks quickly, independently of each other, and in standard ways. The intent of this report is to facilitate wider acceptance, appropriate investment, and effective adoption of these DPGs, positioning them as key enablers in the G2P payments ecosystem. The report also encourages the DPGs to learn from good practices, from each other, and from what we believe governments will value.

In this report,

we explore the potential of seven digital public goods assessing the inclusivity, relevance, efficacy, and efficiency of these solutions in digitizing Government to person payments. It provides a summary of the DPGs' self-assessments across the various parameters, from a functional and technical perspective, from the context of its fitment into the G2P payments Infrastructure.

CV Madhukar
CEO
Co-Develop



Prakash Jayaram
Partner
Ernst & Young LLP India

1. Part-I: Brief overview and recall of G2P Connect

1.1. Introduction to DPI for higher and inclusive infrastructure

Digital transformation has changed the way the world communicates, conducts businesses, pays for goods and services, and more. The common enabler for digital transformation across countries is the digital public infrastructure (DPI) - population scale systems operating digital services, enabling various functions and services across the society. DPIs have the potential to transform how people and businesses access services through improved service delivery and fostering inclusion by removing physical and cost barriers enabling everyone to participate equally in the digital economy with confidence and trust.

Supported by robust regulatory frameworks, governance, and funds as part of an enabling environment and the required capacity across technical, human resource and infrastructure, DPI provides a digital foundation for sector-specific applications, allowing organizations to build innovative user applications to cater to specific use cases democratized through application programming interfaces (APIs).

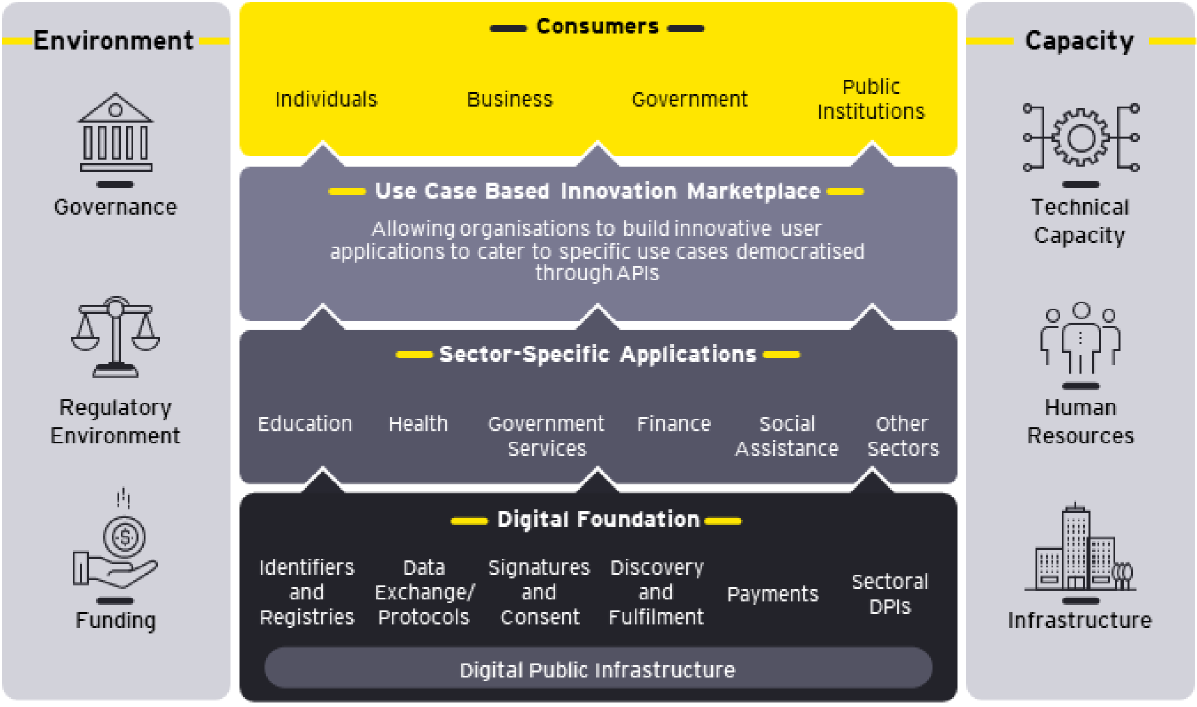
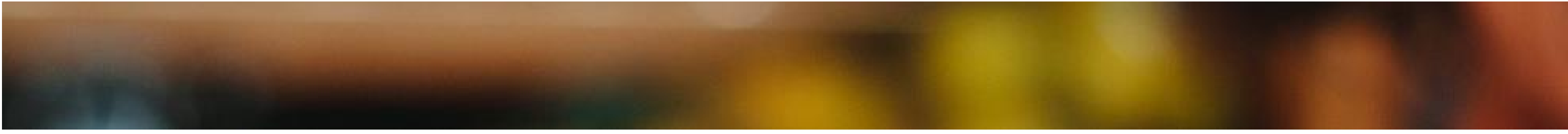


Figure 1: DPI Architecture

The DPI approach entails using shared infrastructure or interoperable digital building blocks rather than a siloed approach for implementing digital solutions at a national scale. To unleash the digital capabilities of a nation and stimulate its digital economy, it is crucial to establish a reliable method for verifying individuals' identities and access their profiles, enabling creation of verifiable digital credentials and secure sharing of data or credentials across various systems with consent, facilitating access to services through open protocols, and ensuring seamless and cost-effective financial transactions. These functionalities act as building blocks to create digital ecosystems across multiple sectors, allowing local players to create innovative solutions on top of these blocks, creating new businesses and services for people. One such solution built on these building blocks is the Government to Person (G2P) payments infrastructure to provide cash assistance to people, simplifying service delivery for both government programs and the beneficiaries.



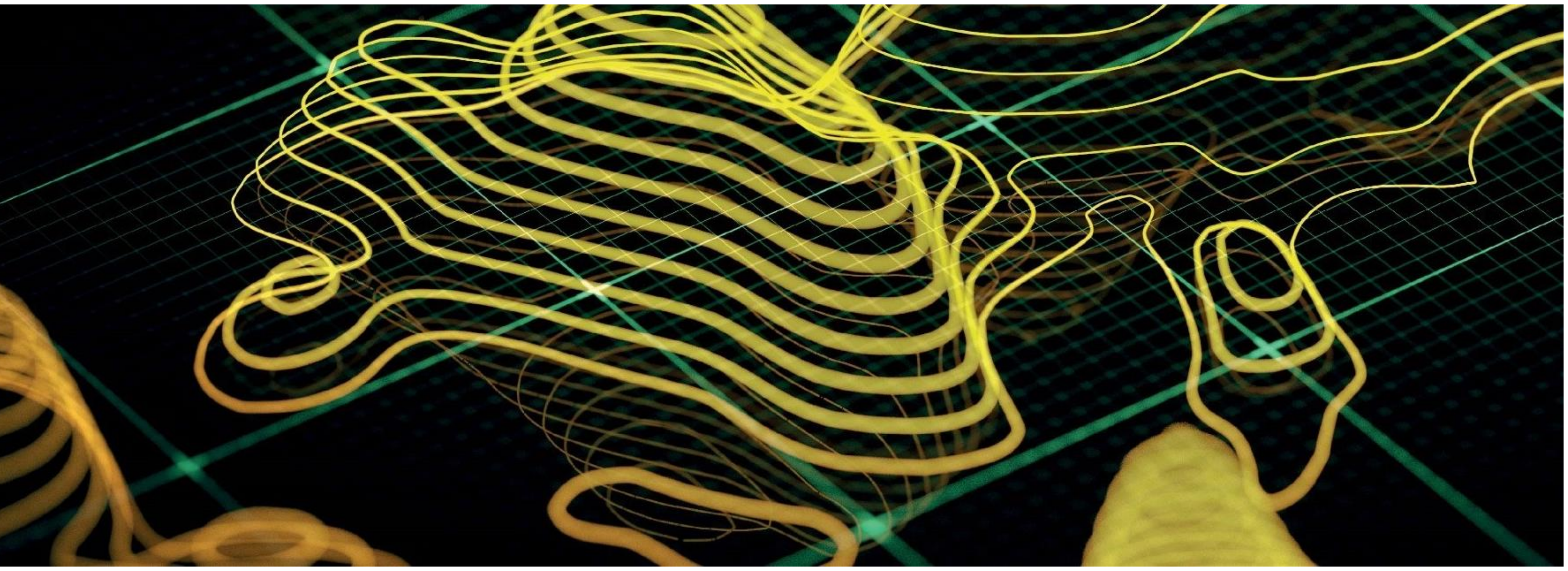
1.2. G2P Infrastructure - an important DPI helping governments build integrated and sustainable solutions

The G2P payments involves processes aimed at targeting, assessing eligibility and registration of individuals, providing benefits, and monitoring the program performance. To ensure efficiency and effectiveness of these processes, governments across the world are shifting from manual paper-based processes to digital online interactions and moving from in person cash payments to digital payments. The easiest way for digitalizing the G2P processes is to build a solution using the common building blocks that the administrative institutions/agencies can then customize as per their requirements. The G2P infrastructure constitutes the following building blocks:

- Scheme management to support eligibility assessment and registration of beneficiaries, benefit calculation, compilation of payroll lists, payment initiation, and monitoring the performance of the schemes.
- Digital identification system for verification and authentication of beneficiaries during registration and benefit distribution to eliminate duplicates and ghost beneficiaries.
- Civil and federated registries to support outreach, targeting and determination of potential eligibility.
- Trusted data sharing and digital credentialing infrastructure to facilitate secure data sharing through consent.
- ID-account mapper to map beneficiary unique identifiers to their account information to enable direct benefit transfers.
- Payment and settlement switch to transfer G2P payments to beneficiary accounts across various payment service providers.
- Bank/wallet system to provide a choice to the beneficiary to select the mode of payment i.e., bank accounts, wallets etc.
- Last mile cash-in/ cash-out systems to help those with little to no digital literacy access the same benefits using their biometric data to drive financial inclusion from the ground up.

G2P Connect initiative solves the problem of building a secure and decentralized architecture providing common building blocks, that individual departments can then customize on top. It is an open-source effort to enable G2P digital payments built through interoperable standards and design blueprints. It serves as a unifying blueprint that facilitates the establishment of a collaborative infrastructure within a country. This infrastructure is designed to cater to various government agencies, enabling them to seamlessly execute digital end-to-end processes for G2P payments.

The diagram below illustrates the G2P Connect solution blueprint building a G2P Infrastructure leveraging the common building blocks.



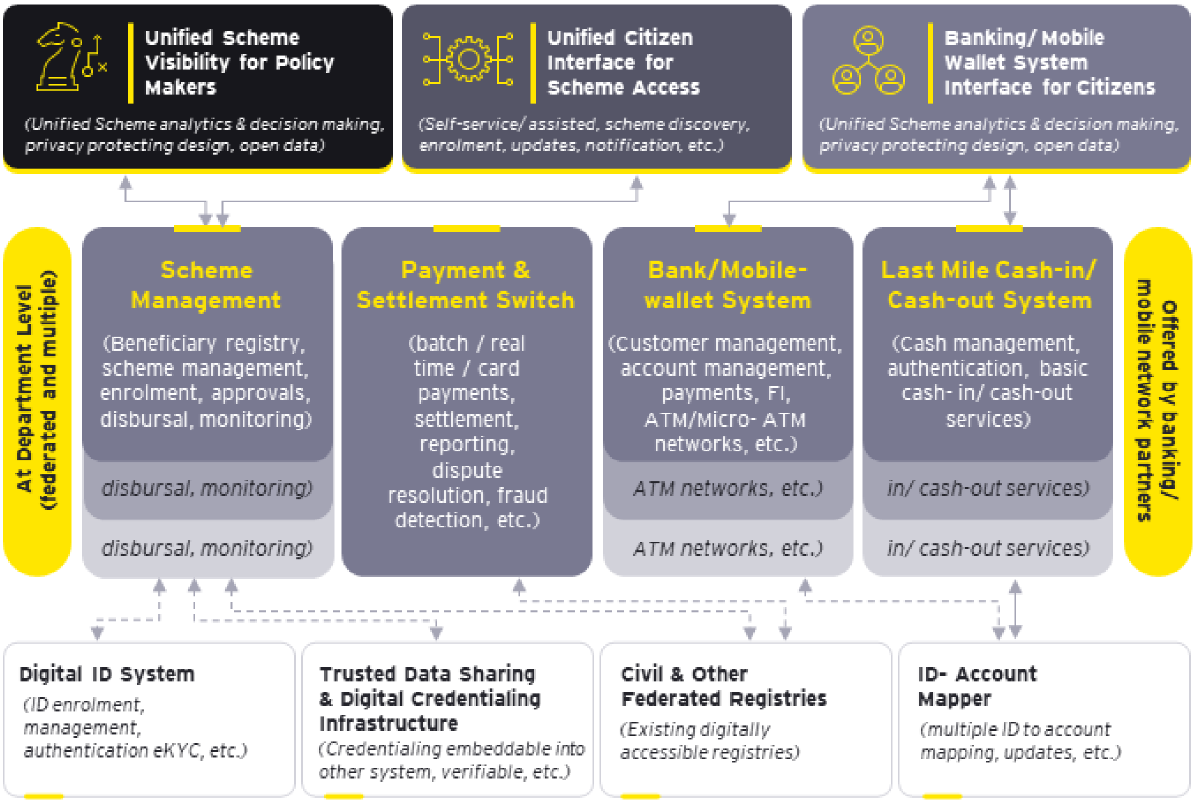

Unified Scheme Visibility for Policy Makers
(Unified Scheme analytics & decision making, privacy protecting design, open data)
Unified Citizen Interface for Scheme Access
(Self-service/ assisted, scheme discovery, enrolment, updates, notification, etc.)
Banking/ Mobile Wallet System Interface for Citizens
(Unified Scheme analytics & decision making, privacy protecting design, open data)
At Department Level (federated and multiple)
Scheme Management
(Beneficiary registry, scheme management, enrolment, approvals, disbursal, monitoring)
disbursal, monitoring)
disbursal, monitoring)
Payment & Settlement Switch
(batch / real time / card payments, settlement, reporting, dispute resolution, fraud detection, etc.)
Bank/Mobile-wallet System
(Customer management, account management, payments, FI, ATM/Micro- ATM networks, etc.)
ATM networks, etc.)
ATM networks, etc.)
Last Mile Cash-in/ Cash-out System
(Cash management, authentication, basic cash- in/ cash-out services)
in/ cash-out services)
in/ cash-out services)
Offered by banking/ mobile network partners
Digital ID System
(ID enrolment, management, authentication eKYC, etc.)
Trusted Data Sharing & Digital Credentialing Infrastructure
(Credentialing embeddable into other system, verifiable, etc.)
Civil & Other Federated Registries
(Existing digitally accessible registries)
ID- Account Mapper
(multiple ID to account mapping, updates, etc.)

Figure 2: G2P Connect Solution Blueprint[1]

G2P Connect offers an integrated solution that streamlines and coordinates the entire lifecycle of government payments, providing a standardized and efficient framework for diverse agencies to leverage. This results in a more cohesive and digitally driven approach to G2P transactions, enhancing the overall effectiveness and accessibility of government payment systems.

1.2.1 Building blocks of G2P infrastructure

This section provides an overview of the different building blocks of the G2P infrastructure and the components that constitute these building blocks.

1.2.1.1 Scheme management

Scheme management systems have gained immense traction on an international stage with developing countries building successful integrated systems to achieve universal coverage. These systems help provide a wide range of benefits and services that reduce poverty and inequality and help ensure preventions from shocks or any other calamity. The effectiveness of a scheme management system depends on the ability to accurately find the people in need, register them, provide relevant benefits and services, and cater to their evolving needs. The program owners or benefit providers also need to track and monitor the program impacts to evaluate the evolving needs and efficiency of program delivery as well as adequately plan expenditures.

Scheme management has the following components, the functionality of which have been described below:

[1] The building blocks mentioned above have functionalities beyond the functionalities enabling a G2P payment process. However, the report focusses on the functionalities of these building blocks from the context of building a G2P payment infrastructure.

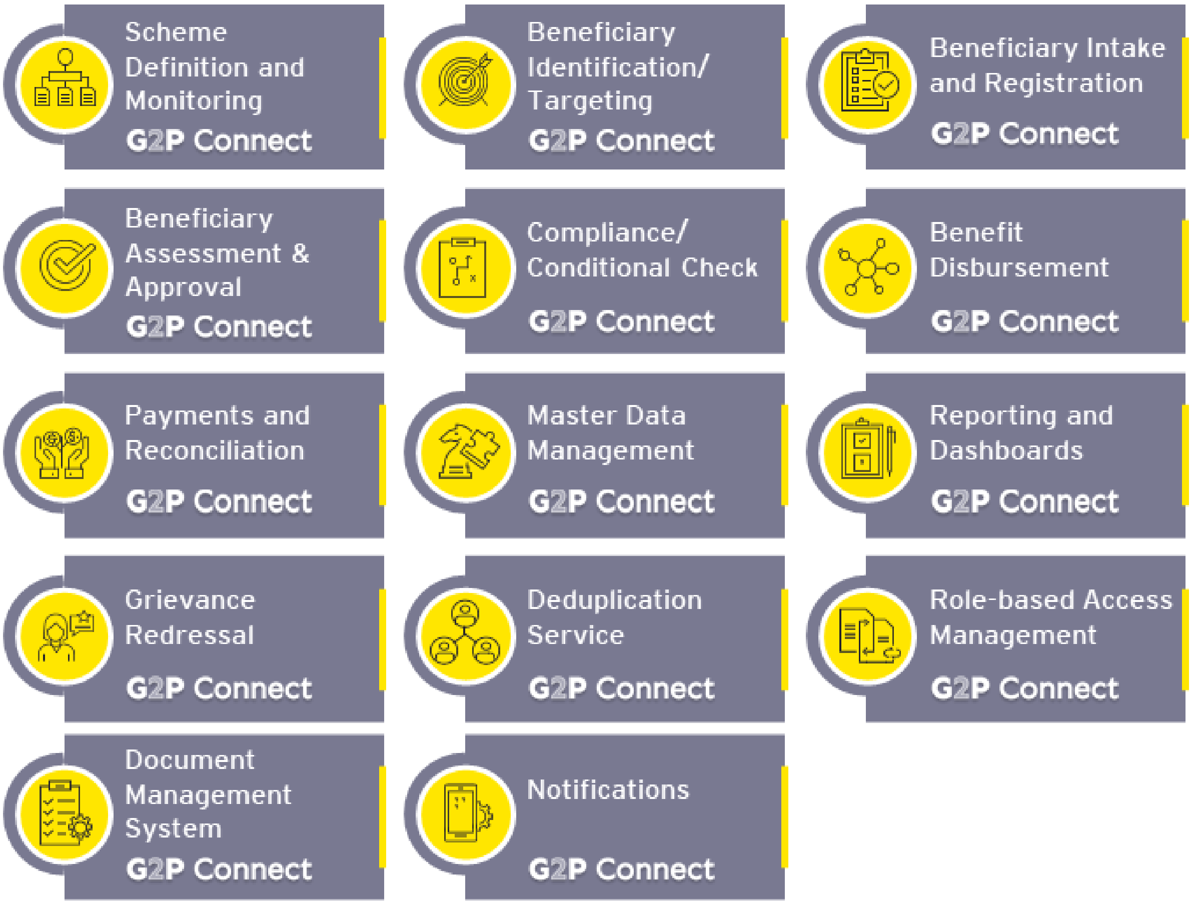


Figure 3: Components of Scheme Management Building Block

- Scheme definition and monitoring: This component enables using shared infrastructure to execute multiple programs in a country. It allows configuration of schemes to assess the eligibility of beneficiaries, calculate the benefit amount, and define disbursement channels and frequency. It also allows monitoring the scheme performance to analyses the impact of the scheme on the beneficiary lives.
- Beneficiary identification/targeting: This component enables proactive identification or targeting of eligible beneficiaries, based on scheme eligibility criteria. It allows for automatic registration of eligible beneficiaries to receive benefits without them having to visit program centers for registration, improving coverage and inclusion of the vulnerable/ remote population. It also allows data to be fetched from other civil and federated registries to validate the eligibility of the beneficiary for schemes or emergency relief programs.
- Beneficiary intake and registration: This component enables beneficiary intake for programs either through self or assisted registrations. It allows for data or documents to be fetched from other registries for eligibility checks and to eliminate redundancy and same data being collected multiple times.
- Beneficiary assessment and approval: This component enables workflow management for scheme implementers to define the levels of approvals required for applications. It allows scheme implementers to validate the information provided through verification of documents or verification/ authentication of information with source registries. It provides capabilities to send back applications in case of discrepancies or incomplete information
- Compliance/Conditional check: This component is crucial for programs which provide benefits to beneficiaries on fulfilment of a conditionality such as cash transfers for pregnant women

post regular check-ups or transfers in case of scholarship programs. It allows implementers to configure the conditions and trigger payments once the requirements or the conditions are met.

- Benefit disbursement: This component is essential to automate the benefit disbursement lifecycle for a program. It allows scheme implementers to calculate benefits to be disbursed based on the type of the scheme, split the benefits in case multiple entities or stakeholders are involved, configure periodicity of the disbursement cycles in case of periodic schemes and approve the disbursement requests.
- Payments and reconciliation: They enable automation of payment lifecycle, allowing implementers to select the relevant payment channels, integrate with payment gateways or ID Mappers, create payment files and trigger payments to beneficiaries. It allows implementers to receive payment receipts and the reconciliation activities.
- Master data management: This component is crucial for storage of reference data such as latitude and longitude, zip codes and area codes, occupations, states and regions, educational institutions, and health centers, which are essential for configuration of eligibility requirements or scheme delivery.
- Reporting dashboard: This component provides reporting and analytical tools to support ongoing program monitoring efforts by various stakeholders. This allows implementers to conduct fair and transparent evaluations of an individual scheme's impact, as well as assist them in planning and budget allocation purposes, through data-driven decision making. It allows to define measurable and traceable indicators for each program/scheme and monitoring on a regular basis.
- Grievance redressal: This component provides all functions required to automate the grievance/complaint management lifecycle.
- Deduplication service: This component allows configuration of algorithms to identify duplicates based on unique ID, biometrics, or demographic data to eliminate double dipping or ghost beneficiaries.
- Role-based access management: This component is crucial to ensure security and privacy of the beneficiary data allowing administrators to provide role-based authorizations to view or use the beneficiary data.
- Document management system: This component allows the storage and management of the documents uploaded by the beneficiaries.
- Notifications: This component ensures multichannel communication between the stakeholders including beneficiaries, scheme implementers and administrators.

While all components of the scheme management building block may not be required for the execution of programs, countries can pick and choose the required components for their end-to-end service delivery. The building blocks provide reusable components, over which the countries can customize or add new functionalities as per the scheme requirements, eliminating the need to build from scratch and minimizing the implementation time.

The assessment framework and the subsequent analysis in the later part of the report is based on the components of scheme management relevant to the G2P payments infrastructure. The report provides an analysis of OpenG2P and OpenSPP- digital public goods (DPGs) that offer scheme management capabilities from the context of its fitment into the G2P payments infrastructure.

1.2.1.2 Payment and settlement switch

Payment and settlement switch serves as the backbone of a financial infrastructure, facilitating seamless and secure electronic transactions. It connects various banks and financial institutions, enabling the smooth exchange of funds, clearing, and settlement processes.

A payment and settlement switch has the following components, the functionality of which have been described below:

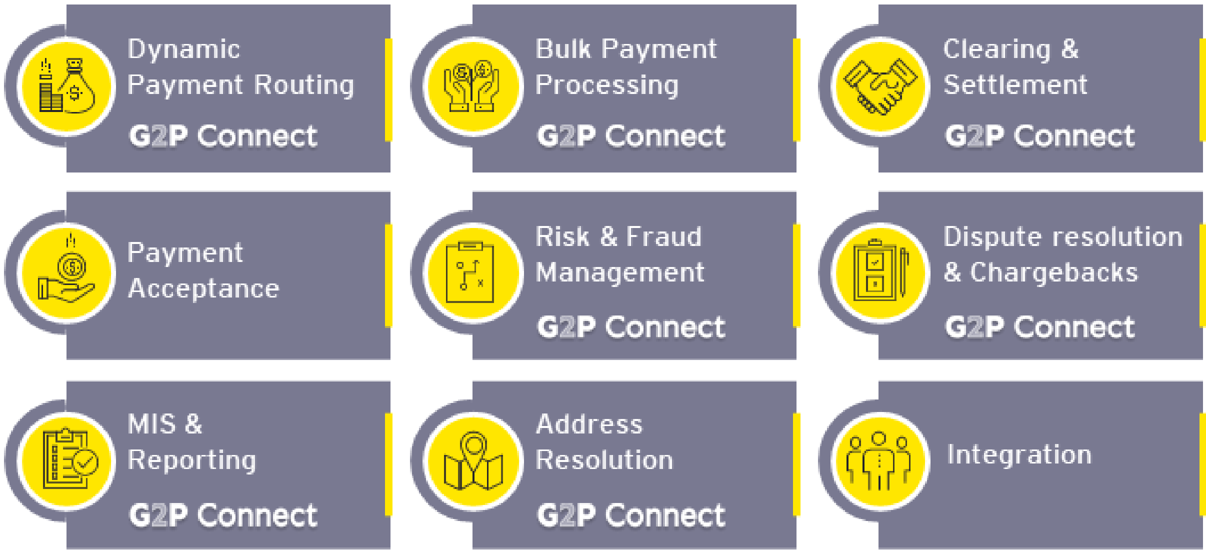
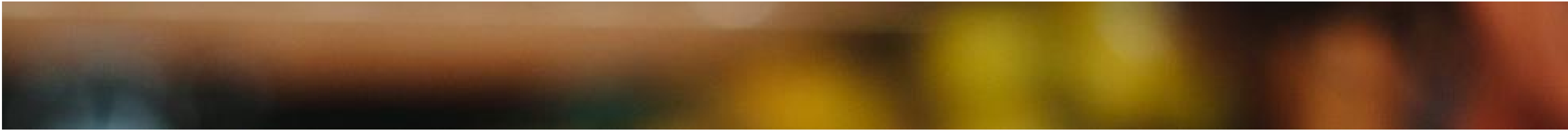


Figure 4: Components of Payment and Settlement Switch

- Dynamic payment routing: This component enables the payment and settlement switch to dynamically select the right payment service provider (PSP) for the transaction based on bank identification number (BIN), transaction amount, time of the day, and detection of downtimes, scheduled maintenance, and excessive load on the payment gateway.
- Bulk payment processing: This component empowers the payment and settlement switch to initiate and process bulk payments through a single file upload, comprising payment details such as unique ID, account number, amount, and payment mode, with no limit on the number of destination accounts where the funds are required to be settled.
- Clearing and settlement: This component is the core to any payment and settlement switch and enables it to perform real-time or batch processing of transactions, automatically crediting the amount collected through the online PG to the designated destination account within the agreed time frame.
- Payment acceptance: This component empowers the payment and settlement switch to accept validated payment requests from multiple payment gateways after performing field-level validations, including syntactic and semantic validations, on all payment details.
- Risk and fraud management: This component ensures that the payment and settlement switch have real-time risk and fraud monitoring capabilities, including transaction monitoring, velocity checks, blacklisting, holding suspicious payments, and a 24x7 alert backend management team.
- Dispute resolution and chargebacks: This component ensures that the payment and settlement switch have capabilities to handle disputes and chargebacks arising due to card network exceptions, issues raised by the user, etc. It can accept or contest a dispute and take the required actions.
- MIS and reporting: This component empower the payment and settlement switch to generate daily, weekly, monthly, or any chosen duration reports for payments, refunds, settlements, disputes, chargebacks, etc.



- Address resolution: This component enables the payment and settlement switch to link the financial addresses (e.g., beneficiary account number) with the unique ID number through integration with open APIs, allowing payments to be processed via a unique ID.
- Integration: This component enables the payment and settlement switch to integrate with merchant portals via API, irrespective of form factor (mobile, website).

The assessment framework and the subsequent analysis in the later part of the report is based on the components of the payment and settlement switch relevant to the G2P payments infrastructure. The report provides an analysis of Mojaloop and Mifos- DPGs that offer payment and settlement switch capabilities from the context of its fitment into the G2P payments infrastructure.

1.2.1.3 Bank/mobile-wallet system

A bank/mobile-wallet system is a digital financial platform that empowers users to manage their finances conveniently. It provides services like account management, fund transfers, payment processing, and loan management through a user-friendly interface. This technology enhances financial accessibility, offering a seamless and secure way for individuals to conduct transactions, monitor accounts, and access various financial services on-the-go.

A bank/mobile-wallet system has the following components, the functionality of which have been described below:

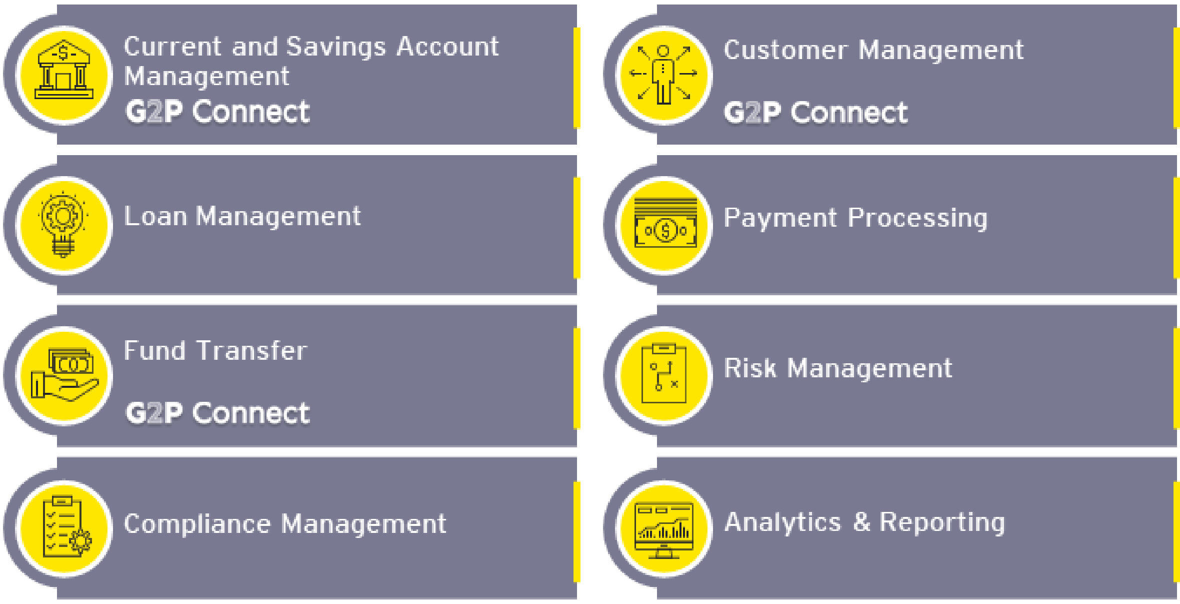
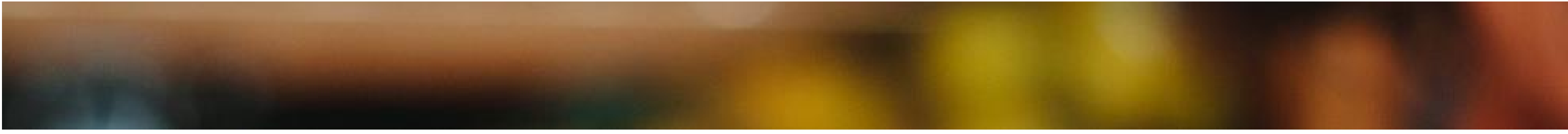


Figure 5: Components of Bank/Mobile-Wallet System

- Current and savings account management: This component enables bank/mobile-wallet system to efficiently oversee and manage transactions, balances, and activities related to current and savings accounts within the bank/mobile-wallet system.
- Customer management: This component ensures that the bank/mobile-wallet system offers personalized services and streamlined communication by effectively handling customer data, profiles, and interactions within the bank/mobile-wallet system.
- Loan management: This component empowers the bank/mobile-wallet system to seamlessly navigate the lifecycle of loans, from origination and disbursement to repayments, while tracking associated financial activities within the bank/mobile-wallet system.
- Payment processing: This component enables bank/mobile-wallet system to facilitate accurate and secure execution and settlement of financial transactions, ensuring a smooth payment experience within the bank/mobile-wallet system.



- Fund transfer: This component helps bank/mobile-wallet system to enable seamless fund transfers between accounts, both internally and externally, fostering convenience and flexibility within the bank/mobile-wallet system.
- Risk management: This component enables bank/mobile-wallet system to identify, assess, and mitigate potential risks associated with financial operations to uphold system security and protect users within the bank/mobile-wallet system.
- Compliance management: This component ensures that the bank/mobile-wallet system strictly adheres to regulatory standards and legal requirements, maintaining the integrity and legality of the bank/mobile-wallet system.
- Analytics and reporting: This component helps utilize data analytics within the bank/mobile-wallet system to generate valuable insights, trends, and reports, aiding decision-making and enhancing overall system performance.

The assessment framework and the subsequent analysis in the later part of the report is based on the components of Bank/Mobile-Wallet system relevant to the G2P payments infrastructure. The report provides an analysis of Mifos- a DPG that offers bank/mobile-wallet capabilities from the context of its fitment into the G2P payments infrastructure.

1.2.1.4 Last mile cash-in/cash-out system

The last mile cash-in cash-out (CICO) building block is a pivotal component of the G2P Connect framework. This element focuses on the crucial task of facilitating the physical exchange of funds at the grassroots level, ensuring that government disbursements reach beneficiaries in the most remote and underserved areas. In the context of G2P Connect, last mile CICO is designed to bridge the gap between digital disbursements and tangible cash, recognizing that many individuals in marginalized communities may not have access to traditional banking channels.

The last mile CICO building block involves strategically establishing a network of agents or service points in geographically dispersed locations where beneficiaries can seamlessly convert digital funds into physical cash and vice versa. This process is crucial for enhancing financial inclusion, especially in regions where access to formal banking infrastructure is limited. By strategically mapping these service points, G2P Connect aims to optimize the delivery of government payments and subsidies to the last mile, ensuring that beneficiaries can easily access and utilize their funds.

Last mile CICO within the G2P Connect framework prioritizes security, efficiency, and accessibility. The design incorporates elements such as secure authentication, user-friendly interfaces, and compliance with regulatory standards to safeguard financial transactions and protect the interests of beneficiaries. This building block plays a pivotal role in realizing the overarching goal of G2P Connect, which is to streamline and enhance the delivery of government disbursements while ensuring that the benefits of digital financial services reach even the most remote corners of the population.

A last mile CICO system has the following components, the functionality of which have been described below:

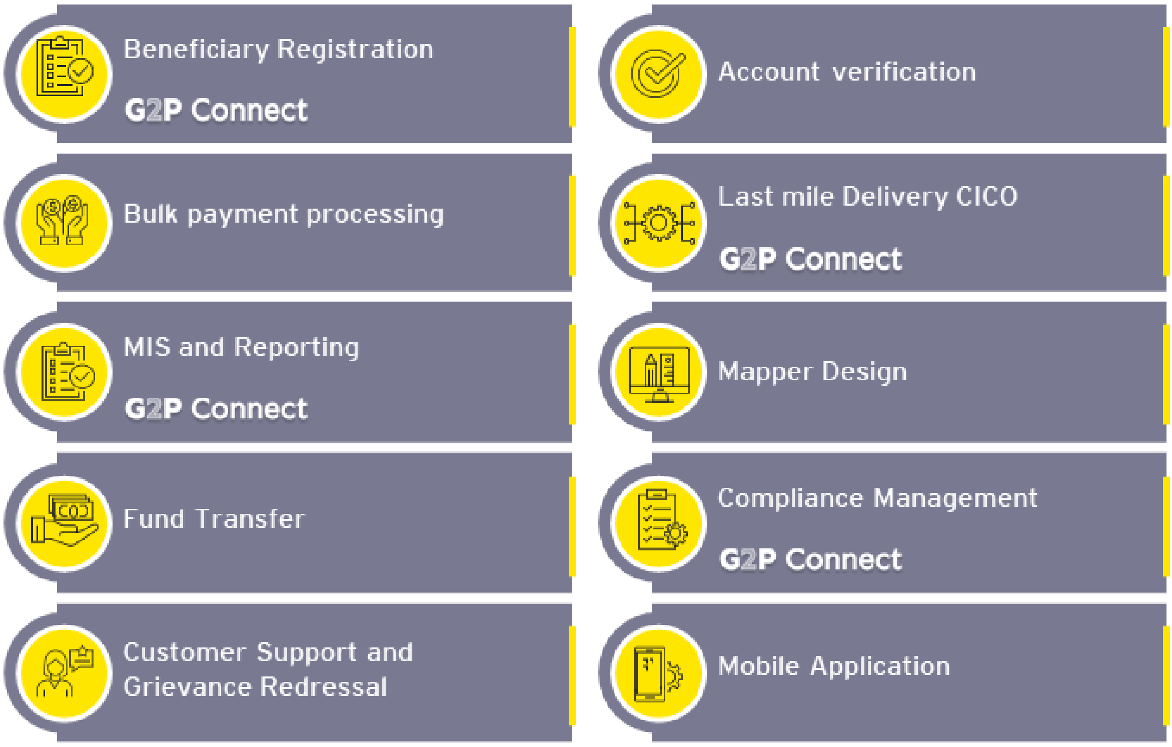
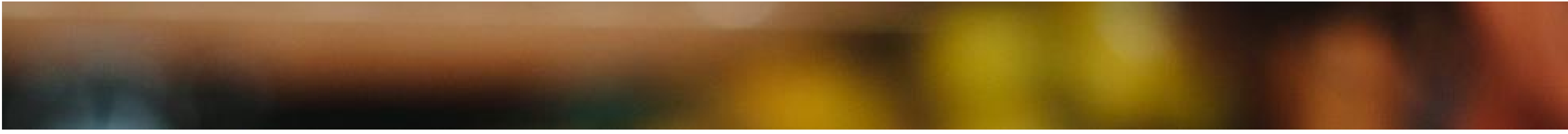


Figure 6: Components of Last mile Cash-in/ cash-out System

A last mile CICO system involves various components to facilitate efficient and secure financial transactions, especially in the context of financial inclusion and remote areas.



- Beneficiary registration: It enables enrolling individuals as beneficiaries for financial transactions, capture and verify beneficiary information, including personal details, biometrics (if applicable), and relevant documentation.
- Management Information System (MIS) and reporting: This component allows monitoring and analyzing transaction data for decision-making. This includes tracking and reporting on transactions, user activity, and system performance.
- Account verification: This component includes use of secure methods such as biometric verification, one-time passwords (OTPs), or multi-factor authentication to ensure the accuracy of beneficiary information for the purpose of verification of identity and account details of beneficiaries.
- Bulk payment processing: This component facilitates large-scale financial transactions efficiently enabling bulk payments to multiple beneficiaries simultaneously, streamlining transactions for disbursements, subsidies, or other financial services.
- Last mile delivery (CICO): This component enables access of funds to users in remote or underserved areas in a very convenient manner. The last mile delivery component is designed to bridge the gap between traditional financial institutions and individuals in areas where banking infrastructure is limited. By establishing a network of agents in these remote locations, last mile delivery enhances the accessibility of financial services, contributing to the overarching goal of providing inclusive and efficient cash transactions for the benefit of underserved communities.
- Mapper design: This component ensures efficient connectivity between beneficiaries, agents, and transaction points. This component involves the creation and implementation of a systematic mapping process that facilitates accessibility and convenience for users in remote or underserved areas.
- Fund transfer: This component enables implementation of a robust fund transfer mechanism that complies with regulatory requirements and ensures the integrity of financial transactions to facilitate the secure transfer of funds between users and accounts.
- Compliance management: This component includes establishment of processes and controls to comply with anti-money laundering (AML) and know your customer (KYC) regulations and regular update of the system to align with changing compliance standards.
- Customer support and grievance redressal: This component includes establishment of a customer support system with helplines, chat support, or other communication channels. It enables implementation of a grievance redressal mechanism to address concerns raised by users.
- Mobile application: This allows development of user-friendly mobile applications and integrate unstructured supplementary service data (USSD) codes for users with feature phones, ensuring accessibility for a wide range of beneficiaries.

The assessment framework and the subsequent analysis in the later part of the report is based on the components of last mile cash-in/cash-out system relevant to the G2P payments infrastructure. The report provides an analysis of Mifos- a DPG that offers last mile cash-in/cash-out capabilities from the context of its fitment into the G2P payments infrastructure.

1.2.1.5 Digital ID system

A digital ID system plays a crucial role by enabling efficient and secure delivery of benefits to eligible individuals. This system helps governments ensure that the programs' benefits are delivered to the intended beneficiaries and that there is no fraud or corruption.

The use of digital ID systems in G2P context brings several benefits, including:

1. Improving the efficiency and effectiveness of welfare programs by ensuring that the benefits are delivered to the right people.
2. Reducing the risk of fraud and corruption by eliminating duplicate or fictitious identities.
3. Enhancing financial inclusion by providing individuals with a formal digital identity that are used to access financial services.
4. Simplifying the process of enrolment and verification for beneficiaries, reducing the burden on government, and improving the overall user experience.

A digital ID System has the following components, the functionality of which have been described below:

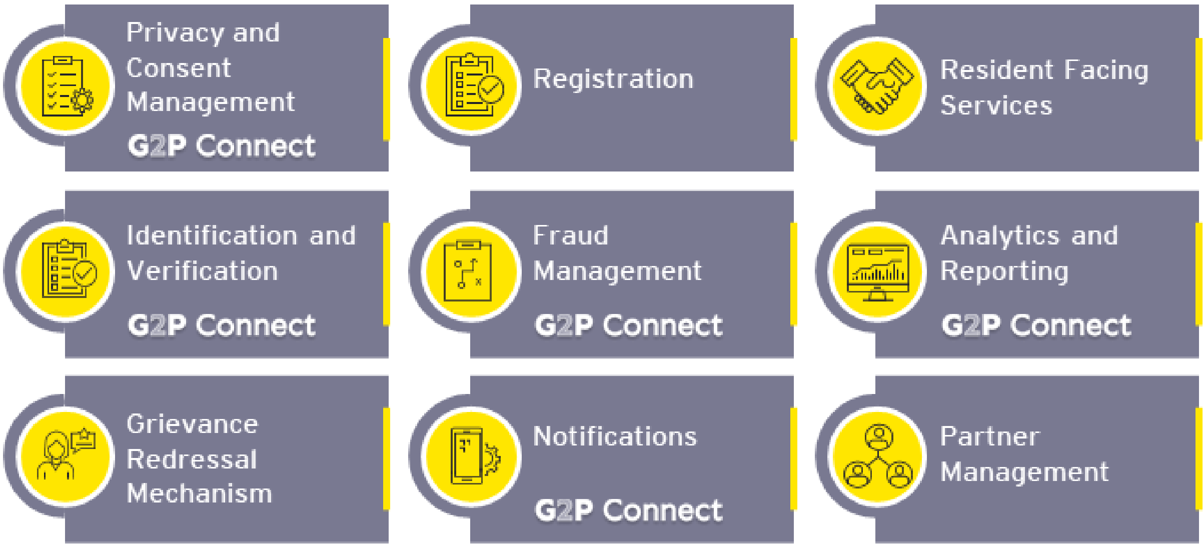
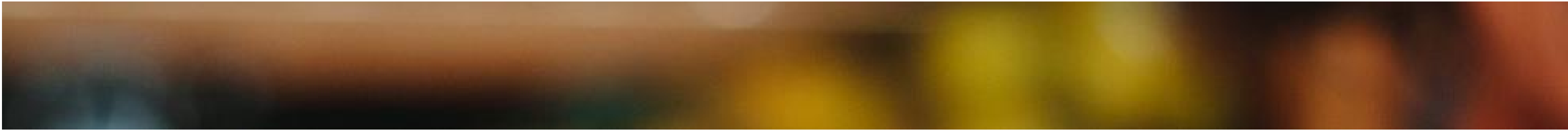


Figure 7: Components of a Digital ID System

- Registration: This component enables easy enrolment of beneficiaries in G2P programs, without the need for lengthy paperwork or in-person visits. It also involves capturing the personal information of an individual and verifying their identity through various authentication mechanisms. The information collected during this process is then used to create a unique digital ID for the individual.
- Resident-facing services: This component offers various resident-facing services aimed at providing individuals with a secure and convenient way to access various services online. Digital ID systems enable individuals to access online services, such as government, banking, healthcare, and other online services. These services are accessed securely using the individual's digital ID. Other services may include personal data management, digital signatures, and mobile access.
- Identification and verification: They provide a reliable and secure way to identify and verify residents, ensuring that only eligible individuals receive the benefits. Digital ID also provides biometric authentication services, such as facial recognition and fingerprint scanning, which offer a high level of security and accuracy in verifying the identity of citizens.



- Partner management: This component enables managing the relationships and interactions with partners, such as government agencies, financial institutions, and other service providers, which rely on the Digital ID system to deliver services to citizens. In the G2P context, partner management plays an important role in ensuring the delivery of benefits and services to eligible citizens in a timely and efficient manner involving onboarding and managing partners, integration with partner systems, monitoring and reporting, collaboration, and coordination.
- Fraud management: The fraud management component enables maintaining the security and accuracy of G2P transfers. In a G2P setting, financial assistance or subsidies are given by the government to needy people or households, and the digital ID system aids in identifying and authenticating the recipients of these benefits.
- Privacy and consent management: It empowers individuals to control how their identity information is shared and used. This includes mechanisms for obtaining informed consent, defining privacy preferences, and ensuring compliance with data protection regulations.
- Analytics and reporting: This component help in providing insights into system performance, user behavior, and security risks. This may involve system monitoring, user behavior analysis, fraud detection, compliance monitoring, system optimization, etc.
- Grievance redressal mechanism: This component of the digital ID system allows addressing concerns, complaints, or disputes raised by individuals regarding their digital identity or the functioning of the system.
- Notifications: This component of a digital ID system allows the users to be informed of the various stages of the identity lifecycle, ensuring security, and maintaining a positive user experience.

The assessment framework and the subsequent analysis in the later part of the report is based on the components of digital ID system relevant to the G2P payments Infrastructure. The report provides an analysis of Modular Open-Source Identity Platform (MOSIP)- a DPG that offers digital ID capabilities from the context of its fitment into the G2P payments infrastructure.

1.2.1.6 Digital credentialing

Digital credentialing systems play a crucial role in the emerging digital ecosystems providing electronic identity documents, certificates, academic achievements, licenses and more. These credentials are digital, securely encrypted versions of both traditional paper documents and digital records, allowing them to be presented as proof across various platforms. Embracing digital credentialing systems have enabled organizations to verify the authenticity of the presented credentials in a secure manner, eliminating time consuming and error-prone manual verification processes. Additionally, individuals benefit by being able to access and present their credentials from any location with an internet connection without having to provide physical documents or personal sensitive data. Overall, digital credentialing systems provide a more secure and flexible way to issue, manage and verify identity information, sector-specific documents or certificates, qualifications, and achievements.

Digital credentialing has the following components, the functionality of which have been described below:

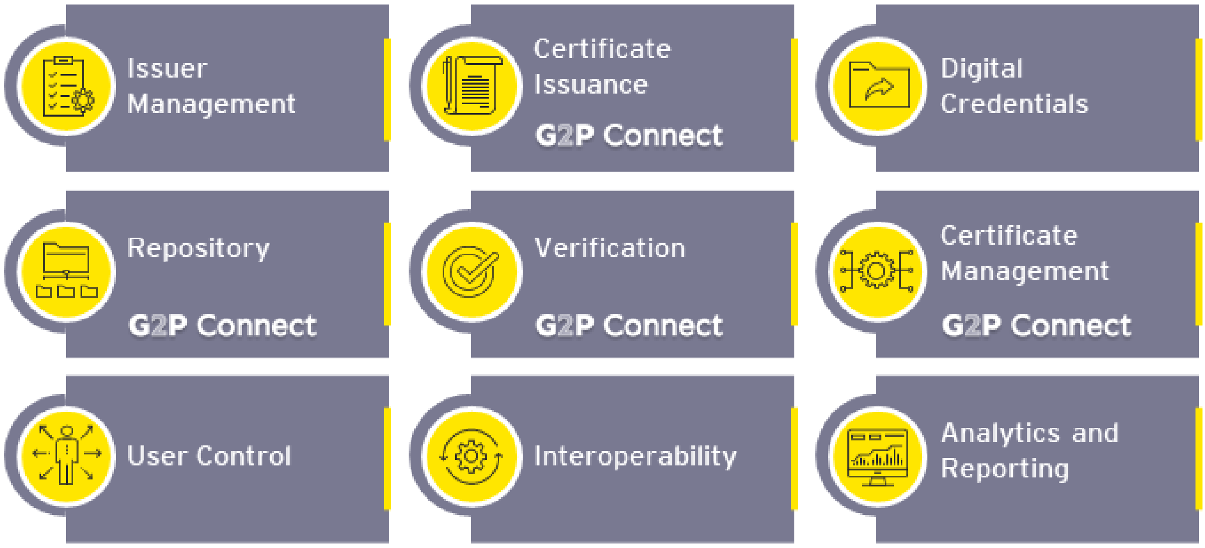


Figure 8: Components of Digital Credentialing Building Block

- Issuer management: This component enables implementation of access control to ensure that only authorized entities can issue digital credentials. It also allows issuers to revoke credentials in case of fraud, expirations, or other reasons.
- Certificate issuance: This component provides an interface for authorized entities to customize, create and issue digital credentials to individuals. It also allows inclusion of relevant data to provide additional context to the credentials.
- Digital credentials: This component supports in creation of credentials in digital, machine-readable formats, typically using standardized data formats. It also allows inclusion of detailed information including evidence of achievement, to enhance the credibility of the credential.
- Repository: This component provides individuals with secure digital wallets to store and manage their digital credentials. It implements mechanisms for users to backup and recover their digital credentials in case of device loss or failure.
- Verification: This component provides a platform for third-parties, service delivery agents or relying parties to confirm the authenticity and validity of the digital credential during service delivery. It majorly supports real-time verification mechanisms to ensure that the information presented is accurate.
- Certificate management: This component provides a user-friendly interface for individuals to provide or share their credentials to third parties in a verifiable manner when needed. It enables individuals to selectively disclose specific information within a credential without revealing the entire document.
- User control: This component empowers individuals with control over when and how they want to share their digital credentials, including the ability to provide selective disclosure promoting trust and privacy. It incorporates mechanisms for individuals to explicitly provide consent before sharing their digital credentials.
- Interoperability: This component provides open APIs encouraging third party applications and services to integrate and interact with the credentialing system. It adheres to industry standards for interoperability, allowing the seamless exchange of digital credentials between different systems and platforms.
- Analytics and reporting: They offer data analytics and reporting features to issuers to track the usage and impact of their digital credentials.

Digital credentialing has multiple use cases across different sectors and domains including identity and civil registration, education, health and vaccination, land ownership, among others. However, the assessment framework and the subsequent analysis in the later part of the report focuses on the components of digital credentialing relevant to G2P Infrastructure. The report provides an analysis of Sunbird RC- a DPG that offers digital credentialing capabilities from the context of its fitment into the G2P infrastructure.

1.2.1.7 Civil and other federated registries

Civil and other federated registries play a crucial role in the context of G2P programs. Civil registries providing a reliable source for verification of identity, information related to birth, death or marital status and other sector information. G2P programs often involve the distribution of benefits or services to individuals and ensuring that the right person receives the intended benefits is essential. Civil and other federated registries help governments target and deliver services more effectively. These registries provide a basis for governments to efficiently allocate resources by identifying areas with higher concentrations of eligible recipients or specific demographic groups in need of assistance. Accurate and up-to-date registries help prevent duplicate payments and reduce the risk of providing benefits to the same individual multiple times. They support evidence-based policy planning and evaluation of G2P programs and help ensure that programs are inclusive and reach all eligible individuals, including marginalized and vulnerable populations. They are foundational to the success of G2P programs, providing the necessary infrastructure for accurate identification, targeted service delivery, and efficient resource management. They enhance the overall effectiveness, transparency, and accountability of government assistance programs.

Civil and other federated registries have the following components, the functionalities of which have been described below:

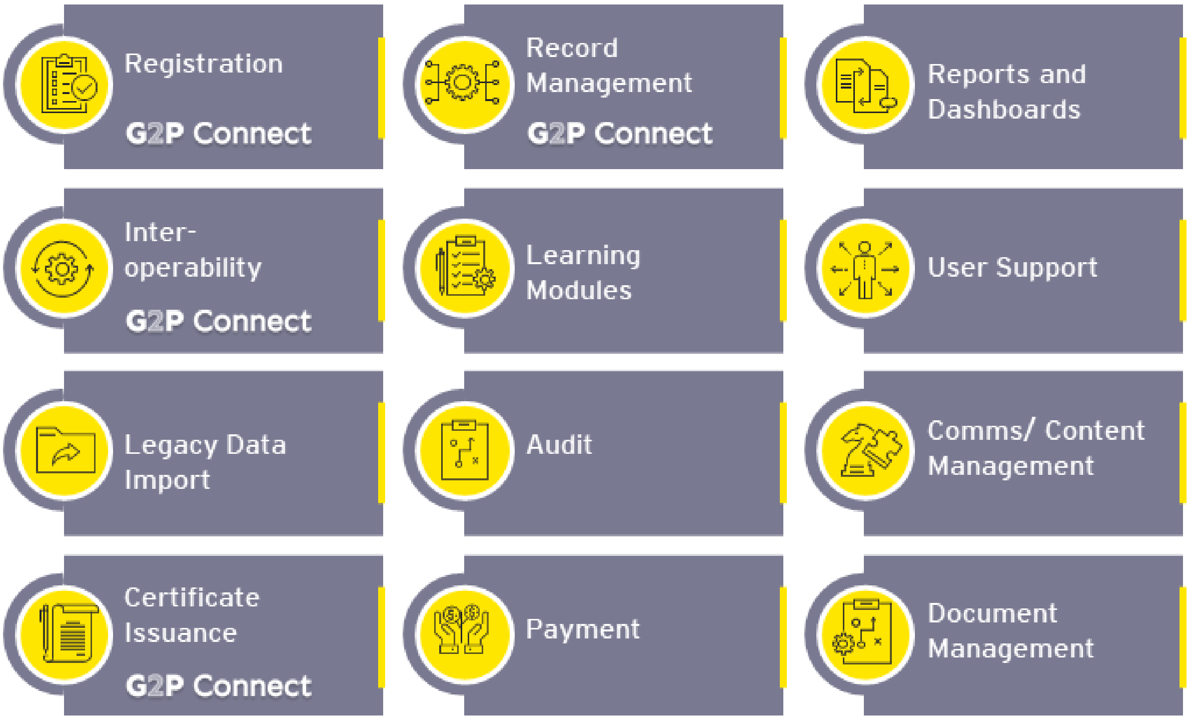


Figure 9: Components of a civil registry

- Registration: This component facilitates the registration of vital events or other sector specific information, ensuring that the information is recorded accurately and in a timely manner. It includes features for verification of information and authentication to ensure the accuracy and integrity of the registered data.
- Record management: This component is crucial for effective data management, including the storage, retrieval, and analysis of the collected data.

- Reports and dashboards: This allows real-time reporting of information, allowing for quicker response to emerging trends and better decision-making.
- Interoperability: This enables interoperability with other systems, allowing for seamless integration with existing government databases and information systems.
- Learning modules: Learning modules are essential for training registration officers and other personnel involved in managing civil and other federated registries. These modules provide structured and standardized training programs to ensure that staff members are well-equipped with the necessary knowledge and skills to perform their roles effectively.
- User management: This component allows managing role-based privileges and permissions for various authorized users of civil registries.
- Legacy data import: This component supports migration of legacy digital records and transformation into formats compatible with the registry.
- Audit: The audit functionality allows tracking of individual records for civil and other federated registries; it allows users to search for and view audit logs for a record thus helping verify the accuracy of the data recorded in civil registries.
- Communication/content management: This component allows managing communications that are sent to both residents and system users.
- Certificate issuance: It allows issuance of a certificate post successfully creating records.
- Payment: This component allows the registry to support different channels for making and receiving payments.
- Document management: This allows storing of documents uploaded by the beneficiaries and various other relevant documents.

The assessment framework and the subsequent analysis in the later part of the report is based on the components of civil and other federated registries relevant to the G2P payments Infrastructure. The report provides an analysis of OpenCRVS- a DPG that offers civil and other federated registries capabilities from the context of its fitment into the G2P payments Infrastructure.

1.2.1.8 ID account mapper

ID account mapper is an innovative approach leveraging a key/value lookup registry that maps an individual's ID with an account address, which is then used to perform transactions using the minimal information. The database entries in the ID account mapper can be added, deleted, updated, resolved to an account address, and verified for status. The individual's ID is a functional or foundational ID while the account address is a bank account number, mobile wallet address, voucher, prepaid card, or digital currency. The account address can also point to the financial institution holding the account.

From a G2P or social protection perspective, the beneficiary ID mapped to a financial account address is used to transfer cash benefits, subsidies, scholarships, and pensions digitally to beneficiaries. The ID account mapper provides a minimalistic component that enables programs to direct payments to beneficiary accounts using just the beneficiary identity numbers from an existing ID system.

An ID account mapper has the following components, the functionality of which have been described below:

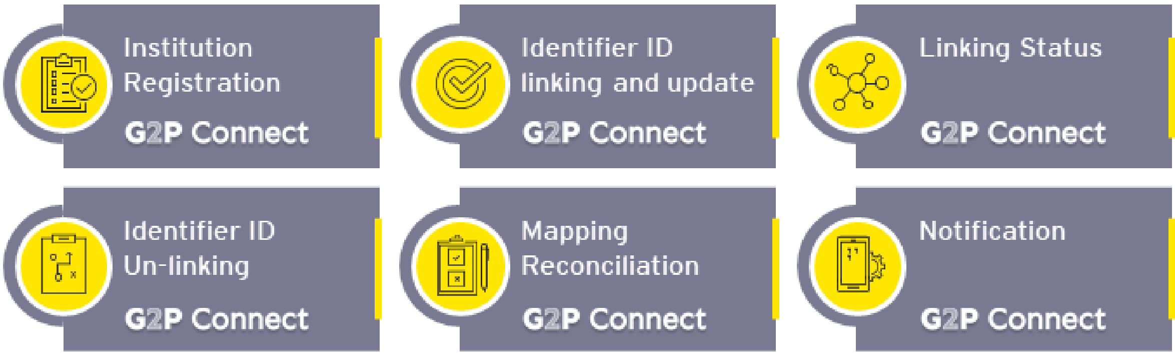


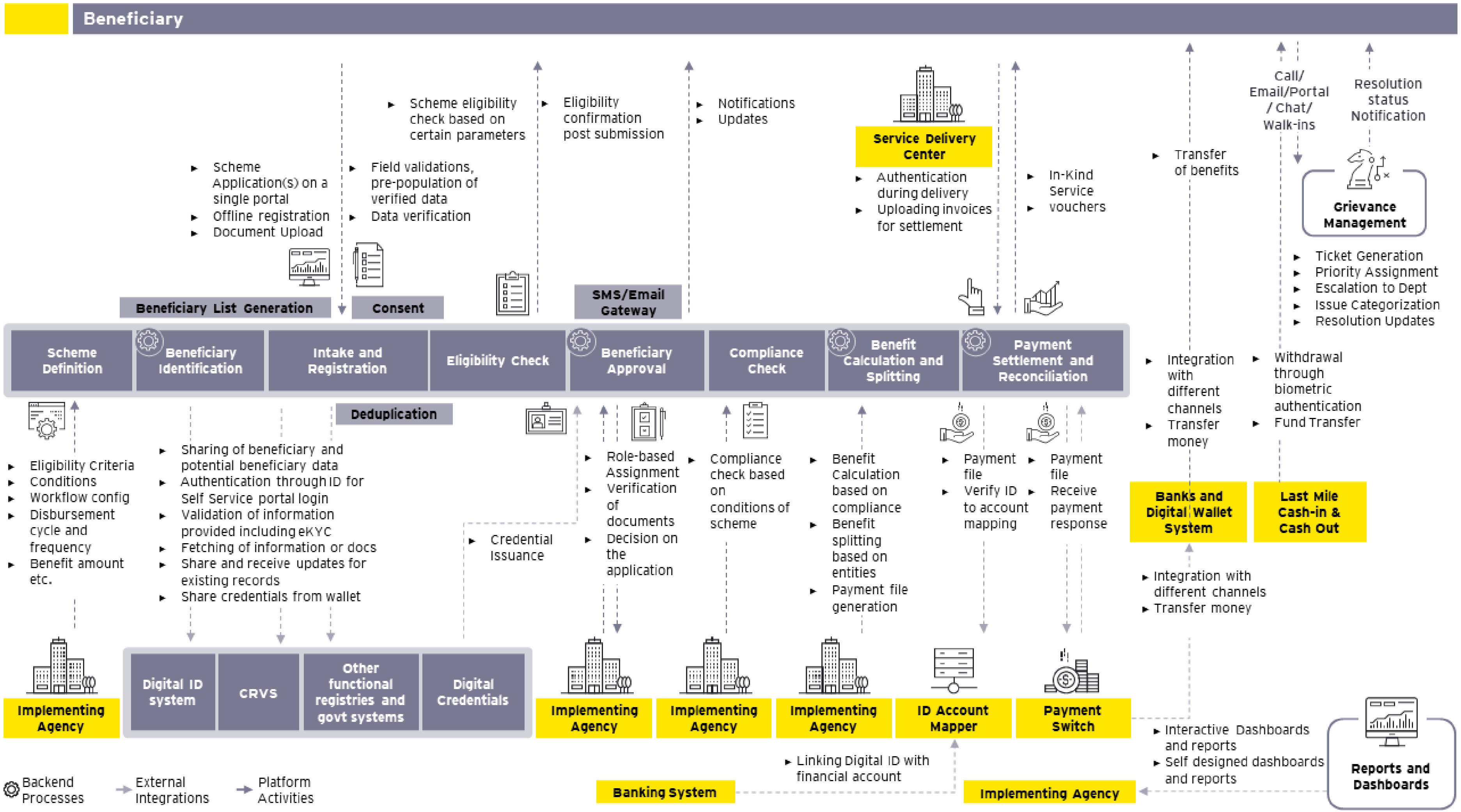
Figure 10: Components of ID Account Mapper

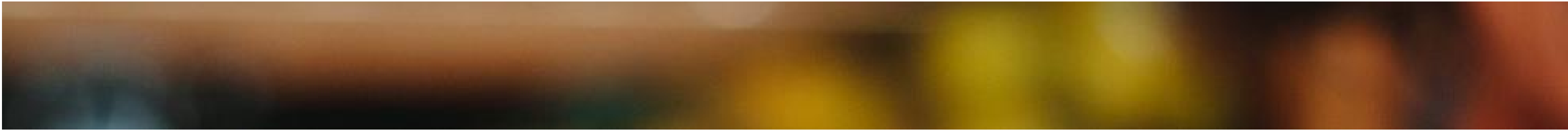
- Institution registration: This component enables the registration of institutions, either source or the destination, and listing in the mapper database, with the requisite details to perform transactions.
- Identifier ID linking and update: This allows the creation of a record/entry in the mapper database, with the linkage of the unique identifier (beneficiary ID) to the respective account address basis the communication through an operating entity in adherence to the defined processes and rules. It also provisions the updating of the financial or other linked information as per individual's choice through the defined process and with the required consent.
- Linking status: This component enables the respective user to check the status of the ID and account address linkage, which is enabled through required system integrations.
- Identifier ID un-linking: This component allows an entry in the mapper database to be deleted, based on the communication through the respective operating entity in adherence to the defined processes and rules. For example, in case of inactive accounts, fraud accounts, etc.
- Mapping reconciliation: This component allows the respective users to perform a reconciliation of linking status between ID account mapper database and core banking system.
- Notification: This component provisions sending of notifications to individuals or entities for the defined events like transaction success/failure, status, linking/update/ unlinking of identifier ID with a financial address in the ID account mapper database, or any form of communication at defined time intervals or frequencies, as per the defined process.

The assessment framework and the subsequent analysis in the later part of the report is based on the components of ID Account Mapper relevant to the G2P payments infrastructure. The report provides an analysis of Mifos- a DPG that offers ID account mapper capabilities from the context of its fitment into the G2P payments infrastructure.

1.2.2 Combining the building blocks to build a seamless G2P payments ecosystem

The diagram illustrates the G2P payments ecosystem build through combining the multiple building blocks:

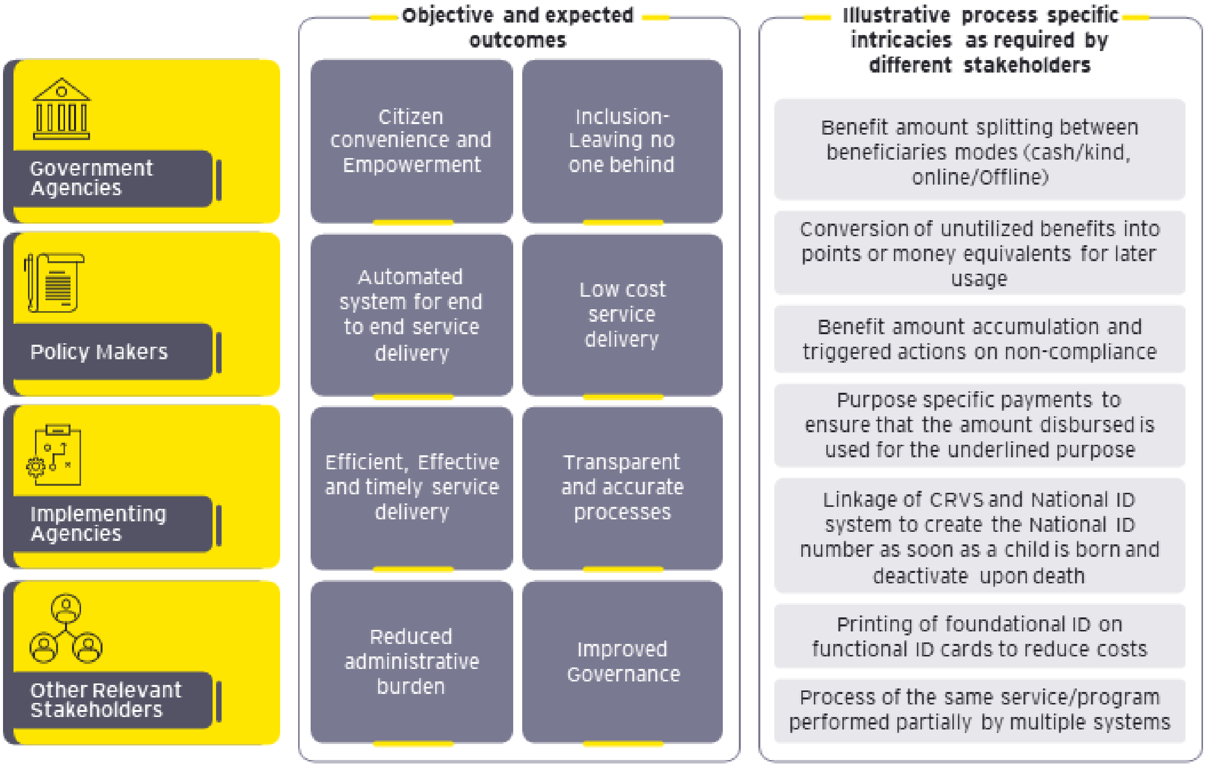

Beneficiary
Scheme Application(s) on a single portal
Offline registration
Document Upload
Field validations, pre-population of verified data
Data verification
Scheme eligibility check based on certain parameters
Eligibility confirmation post submission
Notifications Updates
Service Delivery Center
Authentication during delivery
Uploading invoices for settlement
In-Kind Service vouchers
Transfer of benefits
Call/ Email/Portal / Chat/ Walk-ins
Resolution status Notification
Grievance Management
Ticket Generation
Priority Assignment
Escalation to Dept
Issue Categorization
Resolution Updates
Beneficiary List Generation
Consent
SMS/Email Gateway
Scheme Definition
Beneficiary Identification
Intake and Registration
Eligibility Check
Beneficiary Approval
Compliance Check
Benefit Calculation and Splitting
Payment Settlement and Reconciliation
Deduplication
Eligibility Criteria Conditions
Workflow config
Disbursement cycle and frequency
Benefit amount etc.
Sharing of beneficiary and potential beneficiary data
Authentication through ID for Self Service portal login
Validation of information provided including eKYC
Fetching of information or docs
Share and receive updates for existing records
Share credentials from wallet
Credential Issuance
Role-based Assignment
Verification of documents
Decision on the application
Compliance check based on conditions of scheme
Benefit Calculation based on compliance
Benefit splitting based on entities
Payment file generation
Payment file
Verify ID to account mapping
Payment file
Receive payment response
Integration with different channels
Transfer money
Withdrawal through biometric authentication
Fund Transfer
Banks and Digital Wallet System
Last Mile Cash-in & Cash Out
Integration with different channels
Transfer money
Implementing Agency
Digital ID system
CRVS
Other functional registries and govt systems
Digital Credentials
Implementing Agency
Implementing Agency
Implementing Agency
ID Account Mapper
Payment Switch
Interactive Dashboards and reports
Self designed dashboards and reports
Reports and Dashboards
Linking Digital ID with financial account
Banking System
Implementing Agency
Backend Processes
External Integrations
Platform Activities



1.3. G2P infrastructure: customizable to incorporate country requirements and needs

The customization of G2P infrastructure is essential to ensure its alignment with the unique needs and nuances of each country's socio-economic landscape. A flexible and adaptable G2P infrastructure allows for customization based on factors such as existing financial ecosystems, regulatory frameworks, business processes, policies, and the digital maturity of a specific country ensuring seamless coordination with existing government payment processes and other relevant institutions. This customization can encompass the integration of various systems across the G2P lifecycle. The design should also consider the preferences of the target population, offering user interfaces and communication channels that are culturally sensitive and easily understandable. A customizable G2P infrastructure empowers countries to tailor their systems to unique contextual variables, fostering effective and inclusive government disbursements that meet the diverse needs of their citizens.

The following diagram illustrates the process specific intricacies as required by different countries as per the needs to arrive at the expected outcomes for the relevant stakeholders. The G2P infrastructure and open-source solutions allow customizations to various use cases like cash benefits, subsidies, scholarships, pensions etc., and the G2P infrastructure building blocks are capable to offer the required functionality as per the specific needs of the country.



Government Agencies

Policy Makers

Implementing Agencies

Other Relevant Stakeholders

Objective and expected outcomes

Citizen convenience and Empowerment

Inclusion-Leaving no one behind

Automated system for end to end service delivery

Low cost service delivery

Efficient, Effective and timely service delivery

Transparent and accurate processes

Reduced administrative burden

Improved Governance

Illustrative process specific intricacies as required by different stakeholders

Benefit amount splitting between beneficiaries modes (cash/kind, online/Offline)

Conversion of unutilized benefits into points or money equivalents for later usage

Benefit amount accumulation and triggered actions on non-compliance

Purpose specific payments to ensure that the amount disbursed is used for the underlined purpose

Linkage of CRVS and National ID system to create the National ID number as soon as a child is born and deactivate upon death

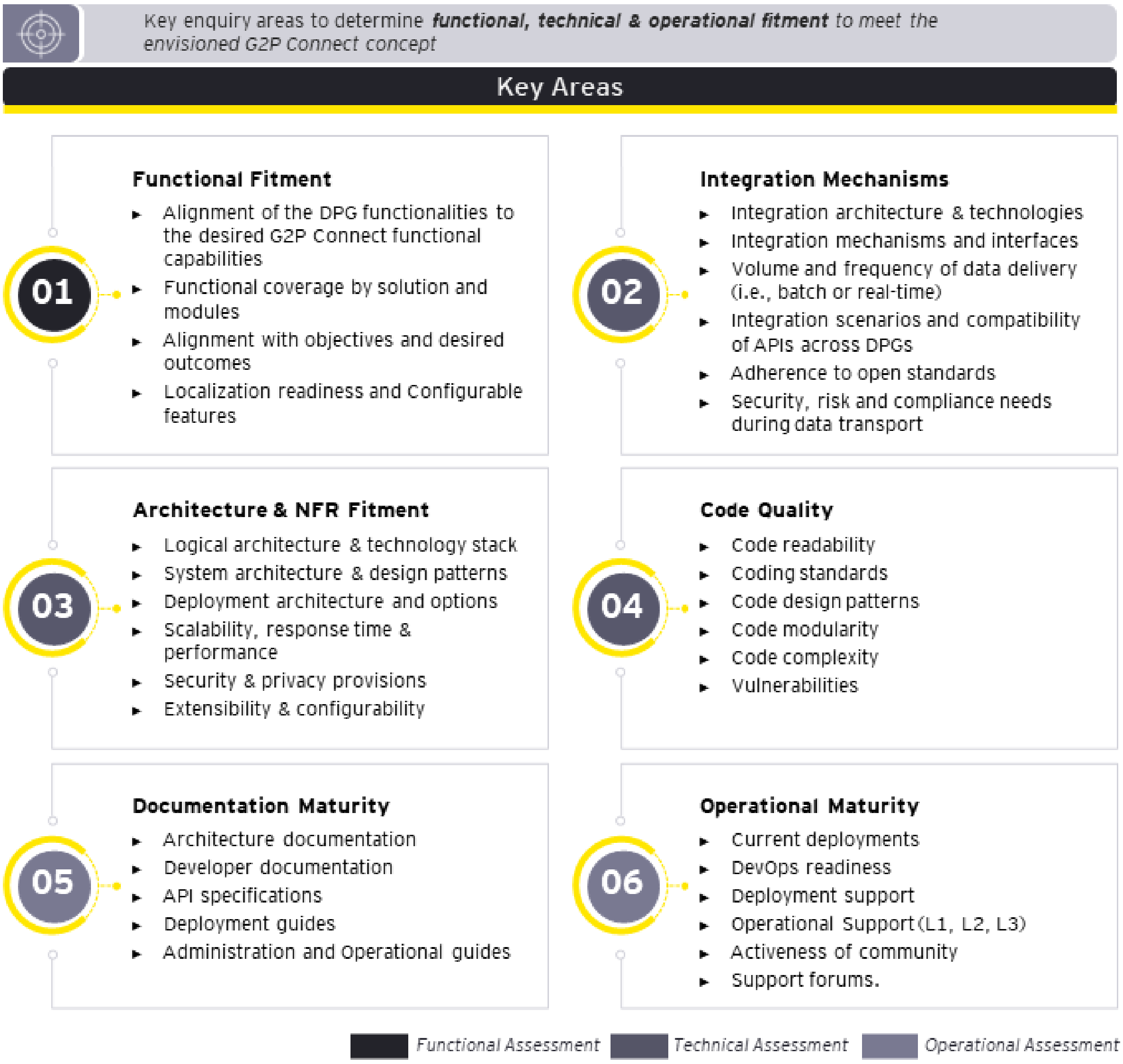
Printing of foundational ID on functional ID cards to reduce costs

Process of the same service/program performed partially by multiple systems

Figure 11: Country-specific customizations to achieve desired outcomes.

2. Part-II: Assessment framework

In the dynamic landscape of digital ecosystems, the seamless integration and effective functioning of various building blocks play a pivotal role in shaping the reliability, security, and adaptability of a system. The DPG Standard, stewarded by the Digital Public Goods Alliance, establishes the baseline requirements that must be met in order to earn recognition as a digital public good. This report's assessment goes further, and endeavors to scrutinize and evaluate the functionalities of key building blocks within the digital framework. The focus lies on comprehensively analyzing each building block's capabilities, functional attributes, and its adaptability to changing requirements. Constructing a meticulous assessment framework for each building block emerges as an indispensable step in guaranteeing the resilience, security, and efficiency of the overarching system.



Key enquiry areas to determine ***functional, technical & operational fitment*** *to meet the envisioned G2P Connect concept*

Key Areas

01

Functional Fitment

- Alignment of the DPG functionalities to the desired G2P Connect functional capabilities
- Functional coverage by solution and modules
- Alignment with objectives and desired outcomes
- Localization readiness and Configurable features

02

Integration Mechanisms

- Integration architecture & technologies
- Integration mechanisms and interfaces
- Volume and frequency of data delivery (i.e., batch or real-time)
- Integration scenarios and compatibility of APIs across DPGs
- Adherence to open standards
- Security, risk and compliance needs during data transport

03

Architecture & NFR Fitment

- Logical architecture & technology stack
- System architecture & design patterns
- Deployment architecture and options
- Scalability, response time & performance
- Security & privacy provisions
- Extensibility & configurability

04

Code Quality

- Code readability
- Coding standards
- Code design patterns
- Code modularity
- Code complexity
- Vulnerabilities

05

Documentation Maturity

- Architecture documentation
- Developer documentation
- API specifications
- Deployment guides
- Administration and Operational guides

06

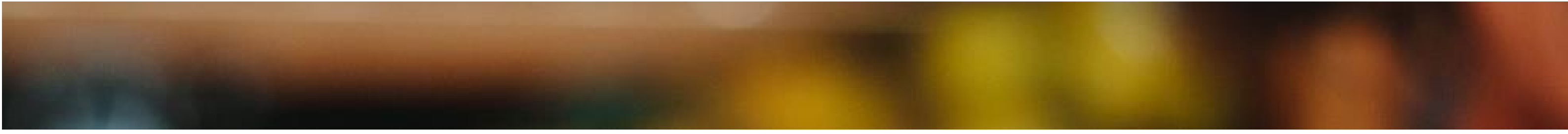
Operational Maturity

- Current deployments
- DevOps readiness
- Deployment support
- Operational Support (L1, L2, L3)
- Activeness of community
- Support forums.

Functional Assessment *Technical Assessment* *Operational Assessment*

Figure 12: Assessment Framework Dimensions

The formulation of this framework was methodically orchestrated, covering a spectrum of key areas and their respective components to bring to fruition the envisioned G2P Connect concept and solution blueprint, aligning seamlessly with the diverse needs of customers and prospects. Within the functional fitment domain, an exhaustive examination of the individual building blocks transpires across various critical parameters. These parameters include the intrinsic capability of each functionality, its overall functional prowess, and the degree to which the functionality can be tailored, configured, and extended to adapt to evolving requirements. This comprehensive analysis



serves as a litmus test for the robustness and maturity of the distinct modules encapsulated within each building block. By scrutinizing the strengths and adaptability of these functionalities, the assessment framework provides valuable insights into the efficacy of the overall system, fostering a foundation conducive to innovation and growth.

The assessment framework extends its purview to the technical fitment aspect, recognizing the critical role it plays in the overall effectiveness of the digital ecosystem. Under the umbrella of technical fitment, a comprehensive evaluation is conducted across multiple criteria to gauge the synergy and compatibility of the building blocks with the broader technological landscape. Integration capabilities stand as a cornerstone, assessing the seamless amalgamation of each building block with existing systems, ensuring a harmonious and interoperable digital environment. The evaluation further delves into the architectural framework and non-functional requirements (NFR), scrutinizing the design robustness, scalability, and performance under varying conditions. A pivotal facet of this assessment is the scrutiny of documentation maturity, aiming to ensure clarity, completeness, and accessibility of technical documentation, thereby facilitating efficient system maintenance and troubleshooting. Additionally, the framework addresses the maturity of code and release management, emphasizing version control, code quality, and the efficiency of release processes. Lastly, the deployment aspect is assessed to identify the effectiveness and reliability of the deployment processes, ensuring seamless transitions and minimal downtime during updates or implementations. The technical fitment evaluation aims to fortify the digital infrastructure by ensuring not only functional prowess but also a resilient and technically sound foundation that can adapt to the evolving technological landscape.

The following sections elaborate on the assessment frameworks for individual building blocks, emphasizing the importance of scalability, security, interoperability, and compliance. By meticulously scrutinizing each aspect, we aim to provide a comprehensive understanding of the functional landscape and lay the groundwork for building resilient and adaptable digital systems. This assessment not only serves as a diagnostic tool but also as a roadmap for enhancing the capabilities of each building block to meet the evolving demands of the digital era.

2.1. Functional assessment framework for DPI

The section provides a snippet of the assessment framework to analyze the functional fitment of the DPG. It captures questions on capabilities that are essential from the G2P context for each building block.

https://github.com/G2P-Connect/common/tree/main/assessments/self_assesments

2.2. Technical assessment framework for DPI

The section provides a snippet of the assessment framework to analyze the technical capabilities of the DPG. It captures questions on capabilities that are essential from the G2P context for each building block.

https://github.com/G2P-Connect/common/tree/main/assessments/self_assesments

3. Part III: Findings from the assessment

3.1. OpenG2P

Integrations present with	MOSIP	OpenSPP	Mifos	Mojaloop	Payment Channels

OpenG2P, an open-source platform, housed in IIIT Bengaluru (Bangalore), a university in India, provides the foundation to countries to build solutions for G2P payments and large-scale social protection transfers. It provides tools to digitalize the scheme management functionalities i.e., enabling governments and humanitarian organizations the ability to deliver critical benefits directly to the beneficiary's bank accounts. Its modular technology reuses and augments existing systems in countries, without discarding what works or starting from scratch.

This section provides a summary of OpenG2P's self-assessment across the assessment parameters, followed by a detailed representation of the functional fitment and the technical fitment which covers architectural coherence, compliance with non-functional requirements, integration potential, the maturity of code and release management processes, operational preparedness, and the quality of documentation.

Legend

Functional Fitment

The functional fitment dimension helps identify if the solution has the capabilities that allows governments, to quickly fulfil their immediate G2P, needs modularly.

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

This dimension block, in the summary provides an analysis on the strength/ maturity of the module with respect to the answers provided. The percentages are calculated based on the number of functionalities present in the module as against the functionalities that should ideally be present

Integration Capabilities

The integration capabilities dimension provides an understanding on how interoperable the solution is with other building block

☑ Present 📈 Planned ☒ Not Available N/A Not Applicable

This dimension block in the summary provides an analysis on the functionalities that are present, planned or not available and not applicable in the solution

Architecture and NFR

The Architecture and NFR dimension provides an analysis if the solution uses modern design paradigms, architectures and technologies

This dimension block in the summary provides the maturity of the dimensions under architecture and NFR. The percentages are calculated based on the number of functionalities present in the module

Documentation Maturity

The documentation maturity provides an analysis, if the solution documentation is easy for a nascent/ fledgling vendor to understand, so that the ecosystem scales up quickly

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

This dimension block provides an analysis on the strength of the capability . The percentages are calculated based on the number of functionalities present in the module

Code and Release Management Maturity

The code and release maturity dimension provides an overview if the solution code is structured and well-managed, modular, well-written - so it can be easily understood and modified, if required

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

The dimension block in the summary provides an analysis on the strength of the capability . The percentages are calculated based on the number of functionalities present in the module

Deployment

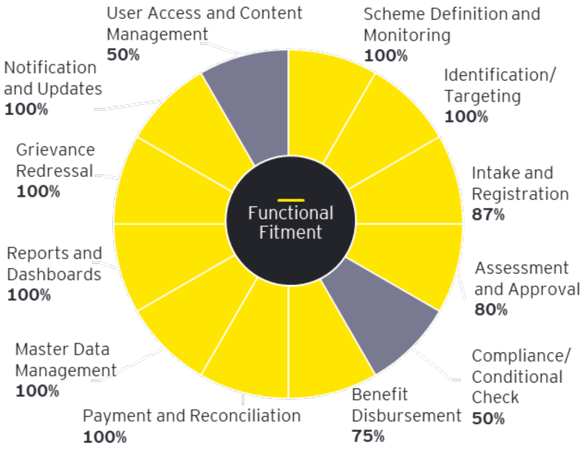
The deployment dimension provides an overview of the pilots conducted by the solution in various countries showcasing its strength, learnings and challenges faced.

📍 Implemented 📍 Interested in Implementing

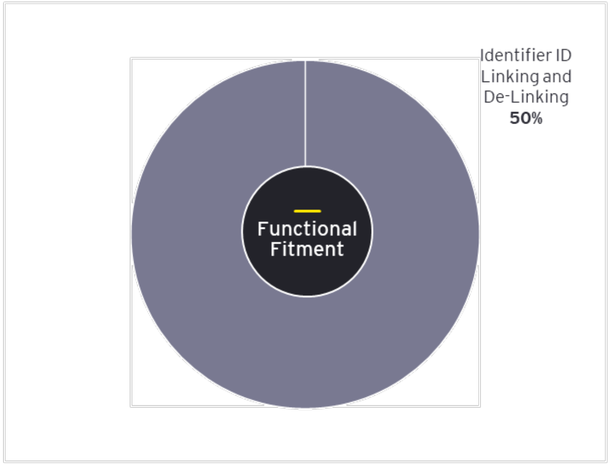
This provides the countries the solution has been implemented, or interested in implementing being show by a country to deploy the solution

Scheme Management for G2P Connect using OpenG2P

Functional Fitment



Scheme Management System



ID Account Mapper

Operational Maturity

Deployment

- Supports automated testing , continuous integration, automated deployment & roll-back
- Supports Blackbox testing and high-test coverage
- Support containers and virtual machines
- Supports centralised logging and monitoring capabilities
- Large scale deployment supported, scalability and distributed deployment in progress
- Planned integration with CI/CD tools

Monitoring

- Kibana considered for BI and visualisation, reporting and analytics, Database model and real time updation
- Supports real-time monitoring of various data sources
- Supports visualization and reporting capabilities
- Planned alerting mechanism to notify administrators
- Planned provision of customizable alert rules and threshold levels

Support

- L3 Support provided for bug fixes and customisation
- SLAs for critical issue resolution in core system is present
- No Financial method. Solution is free for use

Challenges and Learnings

- OpenG2P was provided with a tight turnaround time during the pilot in Philippines, but due to the configurability of the platform the entire scope of the pilot could be delivered
- On-premise challenges such as hardware issues which needed to be improvised and calibrated on the spot. Occasional issues in the network and power infrastructure issues resulted in temporary halting of operations
- Technology adoption challenges were prevalent wherein a few (<5%) of the beneficiaries found it difficult to use a self-sign on portal as they had previously been accustomed to an assisted / in-person method of receiving assistance
- The target during Philippines pilot was to register 35 beneficiaries per day, this target was achieved with an enrolment of 178 beneficiaries

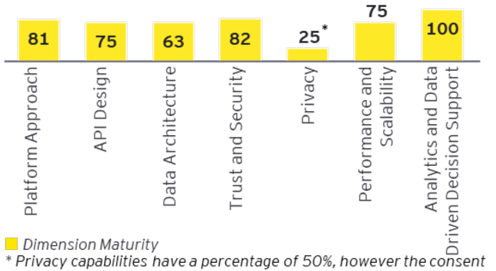
Integration Capabilities

- ☑ Data exchange with external systems in non-proprietary and recognized formats
- ☑ File based integration
- ☑ API-based integration
- ☑ Message-based (Event driven) integration
- ☑ Service orchestration
- ☒ Integration for telemetry dataset for downstream systems
- 📈 Data pipeline architecture

Implementations

Iraq
Philippines
Sierra Leone
Ethiopia

Architecture and NFR



* Privacy capabilities have a percentage of 50%, however the consent management framework is currently being planned in the next version

Code & Release Management Maturity

Code and Repository Mgmt.	Release Mgmt.
Strong	Strong
Configuration Mgmt.	**Documentation Maturity**
Strong	Strong

Impact

Users impacted in Philippines: **178 beneficiaries**

Users impacted in Sierra Leonne: **5074 Schools**

3.1.1 Functional fitment

OpenG2P digitizes various processes such as providing residents integrated access to register for multiple schemes based on eligibility, digitally verify the identity through integration with ID systems and direct benefit transfer to their bank accounts. The platform allows building new functionalities over an existing functionality for specific business operations, customize functionalities or configure through the user interface (UI) of the platform. OpenG2P is collaborating with other DPGs to strengthen the solutions which allows it to reuse modules which already exists in the DPG space reducing the development and implementation time.

The assessment is conducted based on the capabilities of OpenG2P relevant to the G2P payments context. The assessment considered the extent to which these functional capabilities catered to the needs of various stakeholders, including implementing agencies and residents. Additionally, these capabilities were evaluated for its potential towards customization, configuration, or extensibility. A summary of the assessment findings, including what is there or has been planned for implementation in upcoming releases, has been provided below.

Functionality	Maturity	Analysis
Scheme definition and monitoring	100%	▶ OpenG2P allows governments to customize and configure multiple schemes on a single platform defining eligibility criteria, disbursement cycles and other scheme parameters and is extensible to add new functionalities or integrate with other modules. ▶ It enables configuration of scores and thresholds to evaluate beneficiaries based on a Proxy Means Test (PMT). ▶ The Kibana dashboard can be configured and customized based on the requirements of the program for scheme performance and monitoring.
Beneficiary identification/ targeting	100%	▶ OpenG2P enables creation of beneficiary lists based on scheme eligibility criteria and also provides APIs to fetch and upload data from civil or other functional registries. CSV data upload capability present. These functionalities are customizable and can be extended to add additional features as per the scheme requirements. ▶ As the platform is collaborating with different DPGs, Geospatial tagging capabilities already present in OpenSPP, can be leveraged to identify beneficiaries based on regions strengthening the module and helping countries identify households or beneficiaries during disaster relief or emergency support.

Functionality	Maturity	Analysis
Beneficiary intake and registration	87%	▶ OpenG2P provides a self-service portal to enable residents to register for multiple schemes on a single platform providing information and uploading documents in different formats. Post submission of an application the first time, it allows auto-population of data from previously submitted applications during initiation of a new application. It also provides users with options to edit the auto-populated information or continue with the application submission. ▶ The capability to save half-filled applications or a draft feature is planned in the Self-Service Portal 2.0 for which development is currently under progress. ▶ The e-Signet component allows residents to digitally authenticate themselves during registration and a deduplication module based on unique ID, demographic data or rules ensures that a person is registered only once. ▶ The platform provides capabilities to check the eligibility based on certain parameters, eligibility check during submission of application forms or fetch details from other registries. It also enables residents to modify or provide additional details/docs for application returned for modification. ▶ The ODK connector supports offline registrations or registrations in assisted mode for areas with low network or literacy rates. ▶ Vendor registrations or registrations of institutions collaborating for scheme implementation are supported by the platform. For NGOs and other such entities, an account can be created as a User/Institution on their behalf. ▶ Additional functionalities such as fetching information or documents from other registries are currently planned and are included in the product roadmap to strengthen the module.
Beneficiary assessment and approval	80 %	▶ OpenG2P offers capabilities to operators or scheme implementers to search for beneficiaries and their uploaded information and enables them to accept and reject application forms (one by one or bulk) ▶ For the purpose of ranking of households or beneficiaries, it provides capabilities to generate evaluation scores based on the thresholds defined for a particular program. ▶ The capability to return application forms is still being developed. Currently, the OpenG2P self-service portal does not allow the user to apply without complete information. In case of discrepancies, the OpenG2P administrator/ program manager will either request information directly from the user or reject the application allowing the user to resubmit the application with complete information.

Functionality	Maturity	Analysis
		▶ Capabilities to verify uploaded data through integration with other government registries is planned in the upcoming versions.
Beneficiary compliance and conditional check	50%	▶ The platform supports configuration of program/ scheme conditions to ensure payments/service delivery is done only to beneficiaries complying to conditions of the scheme e.g., in case of scholarship programs or conditional cash transfers. ▶ The capability to monitor the conditionality checks for beneficiaries before generating the entitlement or payment files is planned in the next version.
Benefit disbursement	75 %	▶ OpenG2P enables scheme implementers to configure the disbursement cycles along with aspects such as type of benefit, frequency and also compute the amount to be transferred to beneficiaries based on scheme requirement. Additional features required for the operations can be extended to the existing functionality. ▶ OpenG2P provides capabilities to track various stages from the point of entitlement to receiving of benefit, including various stages of payment/transfer. ▶ Capabilities to split the benefit amount across multiple entities e.g., schemes such as scholarships where benefit is divided between university and student is planned in the upcoming versions.
Payments and reconciliation	100%	▶ OpenG2P allows generation of payment files as per the scheme specifications which is readable by a payment gateway. ▶ Payments are triggered by an interoperability layer which allows for integration. It handles payments to different channels. ▶ It provides capabilities to generate vouchers to enable benefit disbursement to the unbanked population or for purpose specific scheme e.g., food assistance, medicine etc. ▶ The system ensures duplicate payment records are not created and has a deduplication engine to detect duplicates in payments. ▶ The platform provides capabilities to a Public Financial Management System (PFMS) and ID Mapper to verify ID to account mapping and also integrates with Mojaloop for account mapping. In addition, OpenG2P is building an in-house solution for ID Mapping. A capability demonstration for PFMS was done as part of the pilot in Philippines.

Functionality	Maturity	Analysis
		▸ Capabilities to support bulk transfer and reconciliation activities such as receive payment response from payment gateways/PFMS/ID Mapper, manage invoices and receipts uploaded by service delivery are offered by the platform. ▸ To ensure that the intended beneficiary is provided the service or assistance during offline payments, OpenG2P offers capabilities to verify digital credentials of the beneficiary during payments.
Master data management	100 %	▸ OpenG2P provides master data management capabilities to store reference data e.g., latitude and longitude, zip codes and area codes, occupations, states and regions, educational institutions, health centers, etc.
Reports and dashboards	100 %	▸ OpenG2P provides capabilities to scheme implementers to create dynamic real-time interactive self-designed dashboards to view the impact of the programs for faster and easier decision making. These features are customizable, configurable and can be extended to add new features as per the requirements of the decision maker. ▸ It also provides capabilities to export these reports in desired formats.
Grievance redressal	100 %	▸ The OpenG2P platform collaborates with other DPGs to reuse models that are available in the DPG space. As OpenSPP has built a GRM module, it can be used in OpenG2P implementation. The OpenSPP GRM module integrates well with OpenG2P since it is built on the same platform.
Notification and updates	100 %	▸ OpenG2P provides APIs to support notifications through multiple channels allowing communications with stakeholders during events and changes such as change in application status, disbursement approval and payments.

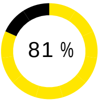
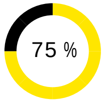
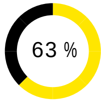
Functionality	Maturity	Analysis
Use access and consent management	50 %	▶ To ensure data security and prevent unauthorized access, OpenG2P supports implementation of role-based access to individuals. ▶ Capabilities to manage privileges of beneficiaries such as permissions to view profile, share profile with another user are planned in the upcoming versions.
ID Account Mapper		
Identifier ID linking and de-linking	50 %	▶ OpenG2P through its self-service portal allows beneficiaries to update their account/ bank information with their unique IDs for direct benefit transfers. It provides the capabilities to link beneficiary IDs/ unique IDs with a single financial address (no dual mappings) in the account mapper database and verification of the details provided. It also allows the beneficiaries to check the status of linking post submission. ▶ Additional capabilities to un-link inactive accounts in the ID account mapper, generate reports for periodic reconciliation and notifications for linking/ unlinking/ updates are planned in the upcoming versions.

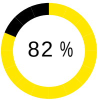
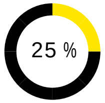
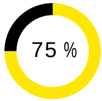
Implementation record

OpenG2P has successfully completed a social welfare digital payments pilot in the Philippines for the Assistance to Individuals in Crisis Situations program under the Department for Social Welfare and Development (DSWD). The platform helped digitize the existing benefit delivery system and highlight its integration with PhilSys ID KYC data extraction. A total of 158 beneficiaries seeking aid under the AICS program were enrolled and benefitted from the OpenG2P platform during the pilot test using the physical or digital copies of their Philsys ID. These beneficiaries were registered on the OpenG2P platform through streamlined and faster processes. The second phase of the pilot would include the incorporation of digital payments.

In Ethiopia, three departments have adopted OpenG2P at National rollout scale across various Safety Net Emergency Relief and agriculture programs. Sierra Leone has adopted OpenG2P for providing social benefits to various schools across the country

3.1.2 Technical fitment

Functionality	Maturity	Analysis
Architecture and NFR		
Platform approach		▶ OpenG2P supports microservice based architecture. It is deployment agnostic such as on-premises data centers, hybrid, private/public cloud, PaaS etc. ▶ OpenG2P allows for integration with other building blocks such as identity systems, payment channels from within the ecosystem. It supports integration with MOSIP, e-Signet, and Mifos. ▶ It has the ability to handle updates and versioning for different release is available through add on. A part of the delivery chain (like registration) can be done offline using ODK module to handle low network and other related constrains. ▶ The platform supports configurability and extensibility on existing modules to meet future needs and uses Elasticsearch as COTS product. ▶ It is currently being used in Sierra Leone and Iraq (National rollout) and in Philippines (Pilot phase).
API-first design		▶ OpenG2P is designed to expose key functionalities as APIs following Open API Specifications. Entry modules of OpenG2P are API based and follows the Open API Specs. ▶ The solution offers well documented APIs. As the API is based on Python (Fast API) and Odoo, they are highly extensible to add new functionalities. These APIs are designed to be secure, follow data privacy principles and are built to be used upon authentication. ▶ The solution supports synchronous /asynchronous/webhook/WebSocket API communications (wherever applicable). ▶ OpenG2P provides sandbox support to perform API testing. It has solutions ready to setup Sandbox in the developer environment. ▶ The APIs are designed as headless APIs. ▶ Additional functionalities supporting API governance, APIs versioning management for backward compatibility and forward innovation are planned in the upcoming versions.
Data architecture		▶ OpenG2P follows data anonymization principle for confidential information. It employs logical data architecture for layers of separation across transactional, workflow, operational, audit, analytical and MDM data. ▶ Data security is ensured through encryption, data integrity and provides security for data-in-motion. It uses different technology for functionalities such as indexing, searching, and analytical processing.

Functionality	Maturity	Analysis
Trust and Security		▶ OpenG2P design follows zero trust architecture principle. It is designed for user authentication and supports pluggable multiple authentication systems. ▶ OpenG2P clearly articulates scope and role capabilities for each functionality. It offers configurability to monitor user behavior, devices, and services. It ensures strongly typed, sanitized, and parameterized input/queries and supports sanitization and encoding of all outputs including error messages to prevent unintended disclosure of confidential or internal information. ▶ The solution provides session management controls using well vetted algorithms to ensure random session identifiers along with generating new session identifier on re-authentication and termination of session identifier post logout. It ensures non-repudiation using digital signature. ▶ OpenG2P uses cryptographic algorithms for encryption/hashing during transit or at rest. The solution supports whitelist file format and limit file size for uploading documents and ensures coverage of all the assets while logging for all levels without storing any confidential data. ▶ The upcoming releases of OpenG2P are planned with features such as encryption keys generation, protection, and storage and vulnerability assessment and penetration testing (VAPT) of application, API & infrastructure. It will also support secure configuration review of network & security devices.
Privacy		▶ OpenG2P supports privacy of personal information protected through encryption, anonymization, or other methods. It has an encryption module to encrypt PII information. The solution follows the principle of data minimization. ▶ Consent management framework has been planned in the upcoming versions of the platform. ▶ The upcoming releases of OpenG2P will support federation and horizontal scalability, use consent management for each functionality. The platform will support reusability, customizations for various functions like timeframe, apply, revoke, auto-expiration etc. It will support governments or implementing agencies to conduct privacy risk assessments regularly to identify and mitigate potential privacy risks and support the right to be forgotten.
Performance and scalability		▶ OpenG2P supports different test strategies at ecosystem scale like automation, deployment etc. The platform's capabilities are tested and validated in real-world scenarios. ▶ The upcoming releases of OpenG2P are planned to incorporate different performance KPIs.

Functionality	Maturity	Analysis
Analytics and data-driven decision Support (Unified scheme view)	100 %	▶ OpenG2P is built to capture telemetry data and designed to follow data anonymizations and aggregation for specific usability of analytical functionalities. ▶ The solution provides configurability features for data warehousing which is achieved by configuring dashboards and analytical KPIs. ▶ OpenG2P provides dynamic reporting capabilities web-based querying, dashboards, Open Data capabilities and data visualization.
Integration capabilities		
Interoperability	71 %	▶ OpenG2P can easily exchange data with other systems in a format that is widely recognized and non-proprietary. It supports File-based integration, API-based integration, Message-based (Event driven) integration and service orchestration. ▶ Data pipeline architecture is planned in the upcoming releases.
Code and release management maturity		
Code repository management	100 %	▶ OpenG2P is present under public GitHub with contributor profiles. ▶ Standard guidelines are present and have been followed to ensure code quality and code coverage best practices. ▶ The solution provides different reports such as static code analysis, code review and security. It allows branch management and merging of code changes along with metrics and analytics for tracking code repository activity and usage.
Release management	75 %	▶ OpenG2P offers planning and scheduling of releases, product backlogs, innovation functions for future releases. It provides mechanism for managing the risk of releases, such as rollback plans and supports integration with other development tools such as code repository management, CI/CD, and issue tracking systems.

Functionality	Maturity	Analysis
Configuration management	75 %	▶ OpenG2P provides automation of configuration management tasks, such as server provisioning and configuration updates. It supports integration with other development tools such as code repository management and issue tracking systems. ▶ The solution allows for the management of multiple configuration profiles for different projects and environments. ▶ OpenG2P has planned to integrate with popular configuration management tools such as Puppet, Chef, and Ansible in their future releases.
Operational maturity		
Deployment	83 %	▶ OpenG2P has capabilities for automated testing and continuous integration, including automated deployment and rollback. It supports Blackbox testing and test coverage, various deployment models such as containers, virtual machines and serverless environments. ▶ The solution provides centralized logging and monitoring capabilities to support rapid identification and resolution of issues and also able to manage large-scale, distributed deployments with ease, and support the needs of growing organizations. ▶ The platform plans to integrate with popular CI/CD tools like Jenkins, Travis CI, and CircleCI in its upcoming releases.
Monitoring	60 %	▶ The design considerations followed by OpenG2P for monitoring, telemetry and auditing include Kibana for BI and visualization, reporting, and analytics, database-based model, real-time update. ▶ The solution supports real-time monitoring of various data sources like logs, metrics, events. It provides detailed visualization and reporting capabilities to understand the monitored data and identify trends and patterns. ▶ The upcoming releases of OpenG2P are planned to have an alerting mechanism to notify administrators in case of anomalies or threshold breaches and customization for alert rules and threshold levels to fit specific needs.
Support	33 %	▶ OpenG2P provides Bug fixes, customization for resolution of critical vulnerabilities. ▶ The solution is free to use, and the support system does not have any subscriptions associated with it. ▶ The solution is planned to have SLA associated for critical issue resolution in core system.
Documentation maturity		

Functionality	Maturity	Analysis
Enterprise documentation	100 %	▶ OpenG2P provides documentation to ensure the solution is easily adapted by various governments and implementing agencies. These include- general overview documentation, architecture and infrastructure documentation and installation documents for various environments and solutions. ▶ It uses GitHub repository to manage state and version of documentation update and are easily accessible for public/developer/other stakeholders. The documentations include examples or screenshots to help illustrate the solution and offers clear instructions for usage of the solution and troubleshooting. ▶ The solution also provides administrator guides, functional use cases, design docs and a knowledge repository.

3.2. OpenSPP

Integrations present with	MOSIP	OpenCRVS	OpenG2P	Mifos	Payment Channels	OpenFn

Scheme management systems have gained immense traction on an international stage with developing countries building successful integrated systems to achieve universal coverage. Open-Source Social Protection Platform (OpenSPP), an open-source solution providing countries and government with a digital integrated system to manage social protection programs. It is a modular system providing all the required blocks to implement end to end scheme or benefit delivery services. The solution is scalable for small as well as large scale projects and can be implemented as a complete solution or in conjunction with other systems.

This section provides a summary of OpenSPP’s self-assessment across the assessment parameters, followed by a detailed representation of the functional fitment and the technical fitment which covers architectural coherence, compliance with non-functional requirements, integration potential, the maturity of code and release management processes, operational preparedness, and the quality of documentation.

Legend

Functional Fitment

The functional fitment dimension helps identify if the solution has the capabilities that allows governments, to quickly fulfil their immediate G2P, needs modularly.

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

This dimension block, in the summary provides an analysis on the strength/ maturity of the module with respect to the answers provided. The percentages are calculated based on the number of functionalities present in the module as against the functionalities that should ideally be present

Integration Capabilities

The integration capabilities dimension provides an understanding on how interoperable the solution is with other building block

☑ Present ▨ Planned ☒ Not Available N/A Not Applicable

This dimension block in the summary provides an analysis on the functionalities that are present, planned or not available and not applicable in the solution

Architecture and NFR

The Architecture and NFR dimension provides an analysis if the solution uses modern design paradigms, architectures and technologies

This dimension block in the summary provides the maturity of the dimensions under architecture and NFR. The percentages are calculated based on the number of functionalities present in the module

Documentation Maturity

The documentation maturity provides an analysis, if the solution documentation is easy for a nascent/ fledgling vendor to understand, so that the ecosystem scales up quickly

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

This dimension block provides an analysis on the strength of the capability . The percentages are calculated based on the number of functionalities present in the module

Code and Release Management Maturity

The code and release maturity dimension provides an overview if the solution code is structured and well-managed, modular, well-written - so it can be easily understood and modified, if required

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

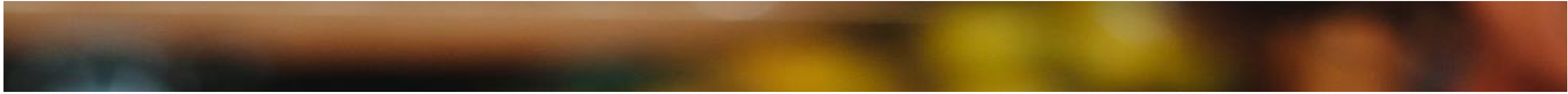
The dimension block in the summary provides an analysis on the strength of the capability . The percentages are calculated based on the number of functionalities present in the module

Deployment

The deployment dimension provides an overview of the pilots conducted by the solution in various countries showcasing its strength, learnings and challenges faced.

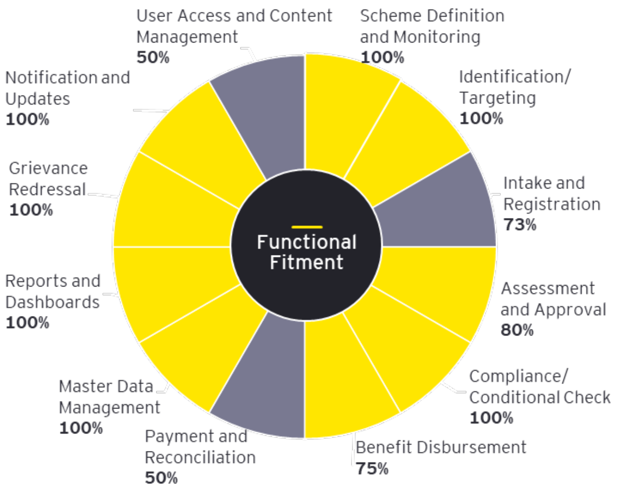
📍 Implemented 📍 Interested in Implementing

This provides the countries the solution has been implemented, or interested in implementing being show by a country to deploy the solution

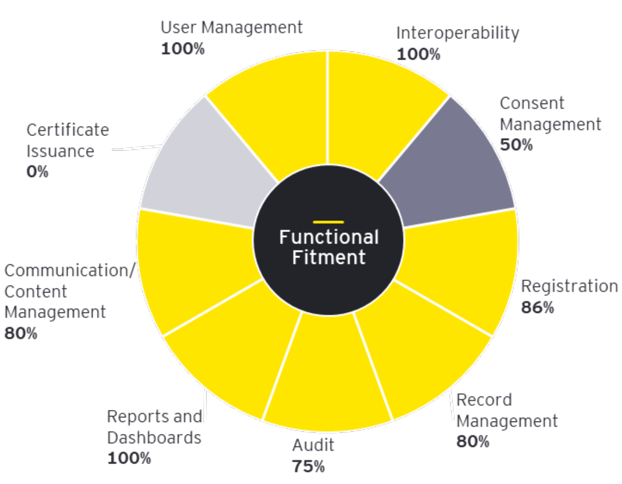


Scheme Management for G2P Connect using OpenSPP

Functional Fitment



Scheme Management System



Registry

Operational Maturity

Deployment

- Supports automated testing and continuous integration but no automated roll-back
- Supports Blackbox testing and high-test coverage
- Support containers and virtual machines
- Large scale and distributed deployments with ease, supporting growing organisations
- Supports integrations with CI/CD via GitHub actions
- No centralized logging solution

Monitoring

- Built on principles following scalability, minimizing latency, security and privacy, flexibility, automation, accessibility, optimization, and standardization
- Supports real-time monitoring of various data sources
- Provision of alerting mechanism to notify administrators
- Provision of customizable capabilities for alert rules and threshold levels
- Supports visualization and reporting capabilities

Support

- L3 Support provided by partner Newlogic
- Financial method inclusion
- SLA support provided by Newlogic

Challenges and Learnings

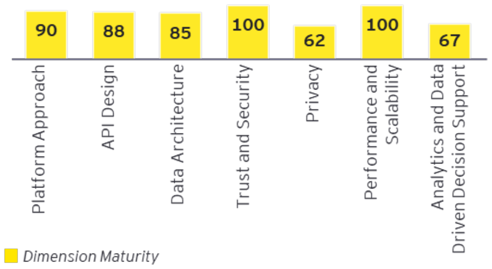
- OpenSPP can handle a large number of beneficiaries even on limited hardware, such as three servers.
- While customizing registry indicators, it's crucial for developers to consider scalability to avoid system slowdowns.
- Proper database configuration and index optimization can greatly improve performance

Integration Capabilities

- ✓ Data exchange with external systems in non-proprietary and recognized formats
- N/A File based integration
- ✓ API-based integration
- 📈 Message-based (Event driven) integration
- N/A Service orchestration
- 📈 Integration for telemetry dataset for downstream systems
- N/A Data pipeline architecture

Implementations

Architecture and NFR



Code & Release Management Maturity

Code and Repository Mgmt.	Release Mgmt.
Strong	Strong
Configuration Mgmt.	**Documentation Maturity**
Moderate	Moderate

Impact

People registered on OpenSPP = **Over 20 million beneficiaries**

3.2.1 Functional fitment

OpenSPP is based on World Bank’s sourcebook model and allows governments or scheme implementing agencies to customize, configure or extend the capabilities for seamless and efficient operations of schemes and programs across countries. The platform supports building new functionalities over an existing functionality for specific business operations, to customize functionalities or configure them through its user interface (UI).

The assessment focused on OpenSPP’ s capabilities within the context of G2P payments. It considered the extent to which these functional capabilities catered to the needs of various stakeholders, including implementing agencies and residents. Additionally, these capabilities were evaluated for their potential towards customization, configuration, or extensibility. A summary of the assessment findings, including what is there or is planned for implementation in upcoming releases is provided below:

Functionality	Maturity	Analysis
Scheme definition and monitoring	100 %	▶ OpenSPP allows governments or scheme implementing agencies to customize and configure multiple schemes on a single platform, defining eligibility criteria, disbursement cycles and other scheme parameters. It is extensible to add new functionalities. ▶ It allows to define scores and thresholds to evaluate beneficiaries based on proxy means test. This can be done through building modules to define the formula or it can be configured through the UI. ▶ It allows monitoring the scheme performance e.g., beneficiary inclusion, benefit pay-outs, grievances, and service delivery parameters like time, savings, accuracy, etc. However, indicators need to be defined, added and are not available as default
Beneficiary identification/ targeting	100%	▶ OpenSPP supports the configuration of eligibility criteria as per the scheme requirements to proactively identify beneficiaries. It also supports the implementation of an eligibility manager to fetch data from other civil and federated registries. ▶ It supports checks after initial identification, to update the status of the existing beneficiaries in the event of a change in circumstance. ▶ The platform supports the integration with a GIS module to identify beneficiaries from different areas, which is essential for disaster relief initiatives. It has default in-built capabilities to attach beneficiaries to an area tree, which defines the different administrative areas. ▶ Once identified, it supports the creation of the beneficiary list in different formats through the UI:CSV, Excel, or an API: JSON.

Functionality	Maturity	Analysis
Beneficiary intake and registration	73 %	▶ OpenSPP provides APIs to enable self-registration of beneficiaries through the National ID or functional ID authentication. It also supports offline mode for low network areas and submission of applications in assisted mode. An interface is also planned to enable residents to create a beneficiary profile and register for multiple schemes on a single platform supporting auto-population of existing data. ▶ The platform captures beneficiary information for identification and eligibility assessment and account information for payment disbursement. The platform supports hardware integrations that allows automated scanning and uploading of documents directly into the OpenSPP platform, such as beneficiary identification documents or other proof documents. ▶ It also has the capability to fetch documents from source registries to verify the eligibility of the individual for a particular scheme. ▶ Post submission of application, OpenSPP provides capabilities to modify or provide additional details. ▶ The platform supports a deduplication engine to identify the uniqueness of the record and ensure a beneficiary is registered only once for a program. ▶ Additional features such as capabilities to save application form as drafts, customization of pre-defined questions based on scheme requirement, provision of digitally verifiable credentials post successful registration are planned in the upcoming versions.
Beneficiary assessment and approval	80 %	▶ OpenSPP offers capabilities to operators or scheme implementers to search for beneficiaries and their uploaded information and it enables them to accept and reject application forms (one by one or bulk). ▶ The platform supports the verification of uploaded data through integration of other government registries as per the scheme requirement. ▶ For the purpose of ranking households or beneficiaries, it provides capabilities to generate evaluation scores based on the thresholds defined for a particular program. ▶ Capabilities for implementers to send back application forms to beneficiaries in case of discrepancies or incomplete data are planned in the upcoming versions.
Beneficiary compliance and conditional check	100 %	▶ The platform supports the configuration of program/ scheme conditions to ensure payments/service delivery is done only to beneficiaries complying with the conditions of the scheme e.g., in case of scholarship programs or conditional cash transfers. ▶ It supports the monitoring/ conditionality check for beneficiaries before generating the entitlement or payment files.

Functionality	Maturity	Analysis
Benefit disbursement	75 %	▶ OpenSPP enables scheme implementers to configure the disbursement cycles along with aspects such as the type of benefit and frequency, and to compute the amount to be transferred to beneficiaries based on scheme requirement. Additional features required for the operations can be extended to the existing functionality. ▶ It also enables beneficiaries to track their benefits at various stages of disbursement. ▶ Capabilities to split the benefit amount across multiple entities is possible for the implementation of two programs and is planned in the upcoming versions.
Payments and reconciliation	50 %	▶ OpenSPP allows generation of payment files as per the scheme specifications and share the files to a payment gateway, Public Financial Management System (PFMS) or an ID mapper. ▶ It supports different channels for payments- banks, mobile money, prepaid cards for benefit disbursement. ▶ The platform supports generation of vouchers to enable benefit disbursement to the unbanked population or for the purpose of a specific scheme e.g., food assistance, medicine etc. ▶ The system ensures duplicate payment records are not created; however, a deduplication engine is not present during the payment file creation. ▶ Capabilities to support bulk transfer and reconciliation activities such as to receive payment response from payment gateways/PFMS/ID Mapper, manage invoices and receipts uploaded by service delivery are planned to be incorporated to the platform. ▶ To ensure that the intended beneficiary is provided with the service or assistance during offline payments, upcoming versions will incorporate capabilities to verify digital credentials of the beneficiary
Master data management	100 %	▶ OpenSPP provides master data management capabilities to store reference data such as latitude and longitude, zip codes and area codes, occupations, states and regions, educational institutions, and health centers.
Reports and dashboards	100 %	▶ OpenSPP provides capabilities that enable scheme implementers to create dynamic and interactive dashboards in real time. These self-designed dashboards facilitate the visualization of the program impact, enabling faster and easier decision-making. These features are customizable, configurable and can be extended to add new features as per the requirements of the decision-maker. ▶ It also provides capabilities to export these reports in desired formats.

Functionality	Maturity	Analysis
Grievance redressal	100 %	▶ OpenSPP offers a grievance redressal mechanism for residents to raise complaints or issues with respect to the programs. It provides multi-channel support for ticket creation, tracking of status, capability to escalate tickets and to provide feedback. ▶ It also provides an interface for operators to assign tickets and updates on resolution.
Notification and updates	100 %	▶ OpenSPP allows APIs to support notifications through multiple channels, allowing communications with stakeholders during events and changes such as amendment in application status, disbursement approval and payments.
Use access and consent management	50 %	▶ To ensure data security and prevent unauthorized access, OpenSPP supports role-based access to control user rights. The user access management component of the OpenSPP enables scheme implementers to control and manage user access to the platform's features and data. It defines various levels of access for individual users or groups, ensuring that only authorized users have access to specific data and features. ▶ Capabilities to manage the privileges of beneficiaries such as permissions to view profile and share profile with another user are planned in the upcoming versions.

The registry component of OpenSPP provides a 360-degree view of the beneficiaries. The information is stored in one place and can be accessed by key stakeholders while providing advanced access management, auditability, and accountability.

Functionality	Maturity	Analysis
Interoperability	100 %	▶ OpenSPP provides capabilities to integrate with external systems, send or receive triggered notifications in case of updates to the records stored in the registry. This enables governments and implementers to develop an interoperable ecosystem ensuring consistent and accurate data of beneficiaries are stored in the database. ▶ The platform provides capabilities to integrate with external systems to share the requested information from other databases such as eligible beneficiary lists to programs for service delivery. It also offers yes/no authentication services and certificates in case data is queried by external databases.

Functionality	Maturity	Analysis
		▶ The platform has capabilities to integrate with other existing government databases and fetch information from sector specific databases for verification, or to update existing records such as validating education, health, tax, and asset information of the beneficiary from the relevant databases.
Consent management	50 %	▶ OpenSPP provides a built-in consent management system that allows scheme implementers to record, store and manage consent of beneficiaries for data processing and sharing. ▶ The platform offers capabilities to individuals to provide their consent for the collection, use, storage, and sharing of their personal data. By giving beneficiaries control over how their data is used and shared, OpenSPP' s consent management helps to build trust and confidence in social protection programs. ▶ The capability to revoke consent at any time can be done through API. Its audit log cannot be revoked. ▶ Additional functionalities such as seeking individual consent to utilize information at every instance are planned in the upcoming versions.
Registration	86 %	▶ The registry provides capabilities to create records by accepting inputs for data fields, create and submit declaration forms remotely through client portals, and upload documents in multiple formats. It has set field validations to ensure data is entered in the correct formats and junk values are not stored in the registry. ▶ It offers capabilities to verify individual information through data exchange with external databases such as verification of sector specific information- education, health, land records, tax, etc. ▶ Once the data is validated and submitted, the OpenSPP registry has the capability to auto-generate and assign random-alphanumeric unique IDs based on the program requirements. ▶ The deduplication capabilities to ensure uniqueness of the record is available at the program level and not at the registry level.
Record management	80 %	▶ OpenSPP' s change request management system allows individuals to request changes to their registration or program participation such as updates to personal information or changes in eligibility. The system also enables scheme implementers to manage and track change requests in a structured and efficient manner, ensuring that requested changes are validated and processed in a timely manner. ▶ The registry provides capabilities to search records based on defined fields, such as ID number, name etc. ▶ The registry provides capabilities for archival, or disposal of old records or records exited from a program due to completion of tenure, failure to meet conditions etc. ▶ Additional features to store records with classifying attributes as public, private or consent based are planned in the upcoming versions.

Functionality	Maturity	Analysis
Audit	75 %	▶ OpenSPP provides an audit log feature to record information of all activities- who accessed the system, what actions they performed and time the actions took place. It currently does not capture the location of the user, but that can be incorporated as an add-on. This would enable governments and scheme implementers to monitor user activity, detect potential security breaches, and investigate issues arising within the system. ▶ It provides capabilities to administrators to search and view audit logs for certain records, and archive it based on the time period configured in the system. ▶ Capabilities to restrict users or system administrators to change audit logs are planned in the upcoming versions. ▶ The audit log can be configured and enabled by the administrators and can be customized based on the needs of the program.
Reports and dashboards	100%	▶ OpenSPP allows scheme implementers to generate customized reports and dashboards that track key performance indicators and provide real-time data on program performance. ▶ It provides capabilities to configure parameters as per the requirements and export the reports and dashboards to an excel or pdf file. ▶ The reports and dashboard features are available with Metabase, Apache superset or directly in OpenSPP.
Communication/ content management	80 %	▶ OpenSPP provides capabilities to manage communications and updates that are sent to residents and system users. This is done through SMS, grievance redressal management or activity stream of the user. ▶ It provides capabilities to manage product content, including making content available in local languages. ▶ Capabilities to send alerts to users in case of duplicate records and options for merging or removal of user records are planned in the upcoming versions.
Certification issuance	0 %	▶ Capabilities to create certificates, integrate with wallets/ digital lockers for digital credentials, authenticate certificates via digital signatures and secured QR codes are planned in the future iterations.

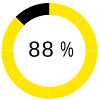
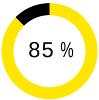
Functionality	Maturity	Analysis
User management	100 %	▶ The user access management component of the OpenSPP enables scheme implementers to control and manage user access to the platform's features and data. It defines various levels of access for individual users or groups, ensuring that only authorized users have access to specific data and features. ▶ It enables system users to authenticate and login by role before gaining access to the system. ▶ It also provides capabilities to revoke system permissions of a particular user.

Implementation record

OpenSPP was implemented in Iraq to reform the Public Distribution System (PDS) of the country. The solution currently stores 20 million records in the country and is planned to scale up to 40 million records. OpenSPP has also signed a contract with global countries to automate the cash aid programs. Based on the inputs from the implementations and the specific country requirements, the solution is being enhanced to incorporate additional features to resolve the changes faced by the countries during the scheme delivery.

3.2.2 Technical fitment

Functionality	Maturity	Analysis
Architecture and NFR		
Platform approach	90 %	▶ OpenSPP employs microservices for high-load services and a monolithic approach for other components. The solution is based on a service-oriented architecture with API integration. It can be deployed on bare-metal servers on-premises without relying on the cloud. ▶ OpenSPP allows schema and table-level multitenancy, enabling data separation for different departments. While the solution is modular, but it cannot be scaled in silo. ▶ It uses semantic versioning with Odoo version numbers for product releases, and updates to components can be made without affecting the entire solution. ▶ The solution supports configurability and extensibility without altering the existing code, utilizing open-source applications like Odoo, Apache Superset, Metabase, PostgreSQL, and Docker. ▶ Additional features to design the system to manage low network areas and other constraints are planned in the upcoming versions. Some of the features can be run on a slow network but are not recommended as it will not allow optimal operations of functions. Further offline operations are not available.

Functionality	Maturity	Analysis
API-first design		▶ OpenSPP provides well documented APIs, and the APIs are designed as headless APIs. These APIs are designed to be secure and follow data privacy principles. The solution APIs are secure, but work is needed to handle data privacy better and reduce the amount of data shared depending on the context. ▶ The platform supports synchronous/asynchronous/webhook/WebSocket API communications, wherever applicable as per need. ▶ OpenSPP supports API versioning management for backward compatibility and forward innovation. These are handled manually, but a product such as an API Manager will be deployed in the future. ▶ The platform provides sandbox support to perform API testing. An invitation-only access is provided via demo.openspp.org for prospective integrations. ▶ OpenSPP plans to incorporate the features to expose key functionalities as APIs following Open API specifications. The solution does not directly implement Open API Specifications, but it complies with G2P Connect, which implements Open API Specifications and provides integration specifications to ensure interoperability across the systems supporting G2P delivery. ▶ Support for API governance is planned in the future. Currently, the API governance is handled manually through a process rigorously, but a product (API Manager) will be deployed later.
Data architecture		▶ OpenSPP partially implements data anonymization principles by minimizing identifiability, protecting sensitive data, securing data, and monitoring data. However, a full-blown implementation of data anonymization principles with masking data and randomizing data is yet to be implemented. ▶ The logical data architecture supports layers of separation across transactional, workflow, operational, audit, analytical and MDM data. The data are separated across multiple tables as per the business requirements. ▶ The solution supports encryption for data at rest and in motion. Data integrity is ensured through strong authentication and access control measures, data encryption, data backup, and recovery plans, and regular monitoring and auditing of data, but data integrity checks such as checksums, hashes, and digital signatures are yet to be implemented. ▶ TLS encryption, authentication, and access control are supported, and intrusion detection and network segmentation can be added based on deployment requirements. ▶ The solution supports both Apache Superset and Metabase for specific functionalities (indexing, searching, analytical etc.). ▶ OpenSPP is designed to manage low latency - high volume and vice versa. These functionalities are supported based on use cases and business implementation requirements. ▶ The solution has documented a certain level of detail, including the name, type, data format, description, and other relevant information. It also includes any restrictions, constraints, or validations that apply to the attribute. ▶ Features of data architecture to provide data layer scalability to Massively Parallel Processing (MSP) are not applicable for the functions of OpenSPP

Functionality	Maturity	Analysis
Trust and security	100 %	▶ OpenSPP follows the principles of zero-trust architecture and supports user authentication, including integration with external ID systems such as MOSIP. ▶ The platform clearly articulates scope/ role capabilities for each functionality and how it is decoupled from the main business logic. ▶ It enables log analysis, event monitoring, input validation during data collection, and output validation to prevent unintentional disclosure of confidential information. ▶ Session management algorithms ensuring random session identifiers, generation of new session identifiers on reauthentication and support on termination of session identifier post logout are supported by OpenSPP via Odoo. It also supports cryptographic algorithms used for encryption/ hashing during transit as well as rest. ▶ Cryptographic management which entails generation, protection and storage of encryption keys can be implemented through HSM based on the country's requirements during implementation. An alternate approach includes the implementation of SoftHSM as per the requirements. ▶ OpenSPP via Odoo supports file management features such as whitelisting file formats and limiting file size while uploading documents. ▶ In alignment with data privacy principles, the solution ensures that it does not store any confidential data while logging. All the assets are covered while logging. The log level can be selected/ enabled as part of the configurations. ▶ The solution ensures usage of non-executable stacks and address space randomization for operation. ▶ Security assessments such as vulnerability and penetration testing (VAPT) of the application, API and infrastructure, secure configuration review of the network & security devices is conducted during both the development and deployment stages. During development stage, the assessment is conducted via tools. Once deployment is done for a country, another round of security assessments is conducted.
Privacy	62 %	▶ The OpenSPP includes a built-in consent management via a framework. The consent management framework is customizable for various functions which include timeframe and auto expiration. ▶ It supports authentication mechanisms like OAuth and OpenID Connect to enable federation between different systems. ▶ The solution is designed to collect the minimum required data for specific tasks, and data can be deleted or anonymized as needed. ▶ Additional functionalities such as using consent management for each functionality and protection of personal information through encryption, anonymization or other methods are planned in the upcoming versions. ▶ Conducting regular privacy risk assessments to identify and mitigate potential privacy risks are planned. However, it is encouraged to carry out security assessments during the implementation.

Functionality	Maturity	Analysis
Performance and scalability	100 %	▶ Different performance KPIs are defined for the solution which include: ▶ Beneficiary reach: Initially supports twenty million beneficiaries; scalable to 40 million without operational delays. ▶ Database performance: All queries are executed within three hundred minutes. ▶ System performance: Standard operations complete within two seconds. Performance may vary with deployment configurations and active modules. ▶ OpenSPP incorporates different test strategies at ecosystem scale. It utilizes CI/CD for deployment, followed by manual testing and analysis. ▶ The platform functionality available to produce sample data with quality akin to production. The volume is adjustable based on testing requirements. ▶ OpenSPP is tested and deployed in one of the Middle Eastern countries. Currently, it manages twenty million beneficiaries and five million households in a production environment. In this setup, OpenSPP serves as a registry, a program/targeting system, and an entitlement issuance and reconciliation system.
Analytics and data-driven decision support (Unified scheme view)	67 %	▶ OpenSPP is built to capture telemetry data. The platform provides configurability for data warehousing and can be connected to reporting platforms such as Apache Superset, Tablo. ▶ The solution provides dynamic reporting capabilities through Apache Superset or Metabase. ▶ The solution approaches data visualization through Apache superset or Metabase after anonymization of the data. ▶ Additional functionalities such as data anonymizations and aggregation for specific usability for analytical functionalities and OpenData capabilities are planned in the upcoming versions.
Integration capabilities		
Interoperability	50%	▶ OpenSPP allows easy exchange of data with other systems in a format that is widely recognized and non-proprietary. The platform supports XML-RPC and REST APIs to integrate with external systems. ▶ Additional features such as message-based integration and integration for telemetry dataset for downstream systems are planned for future implementation.
Code and release management maturity		

Functionality	Maturity	Analysis
Code repository management	100 %	▶ OpenSPP is hosted on GitHub and follows a meritocracy governance model for securing and managing community contributions in code repositories. Code commits undergo scanning with SonarCube for code quality, and peer reviews are conducted to ensure high-quality code. ▶ SonarCube is implemented for code analysis/code review/security reports. ▶ The Solution allows for branch management and merging of code changes and provides metrics and analytics for tracking code repository activity and usage via GitHub.
Release management	100 %	▶ OpenSPP is developed using the Scrum methodology with two-week sprints, followed by releases. ▶ Internal releases occur every two weeks, while public releases are scheduled every three months. ▶ Risk management for releases includes rollback plans and automated deployment pipelines, continuous integration, and automated testing. ▶ Users can roll back to previous code versions in case of deployment failures/other issue. ▶ The solution integrates with GitHub for code repository management, GitHub Actions for CI/CD, and Jira for issue tracking.
Configuration management	50%	▶ OpenSPP allows integration with code repository management systems like GitHub and issue tracking systems like Jira. ▶ It also supports configuration profiles that enable storing and managing different settings and parameters for various projects and environments. ▶ The solution provides support for automation of configuration management tasks, such as server provisioning and configuration updates and integration with popular configuration management tools (Ansible) is under development.
Operational maturity		
Deployment	83 %	▶ The OpenSPP includes CI/CD as part of its engineering process but lacks automatic rollback. ▶ It supports black box testing with high test coverage. It can be deployed using both containers and virtual machines. ▶ While the platform does not have a centralized logging solution, logs are kept for auditability. ▶ The solution is designed to scale easily and accommodate changes in country requirements, deployable across various platforms, and manageable from a single interface. It also offers performance monitoring and management tools. ▶ CI/CD is supported through GitHub Actions.

Functionality	Maturity	Analysis
Monitoring	100 %	▶ The design considerations are scalability, minimizing latency, security and privacy, flexibility, automation, accessibility, optimization, and standardization. ▶ The solution supports real-time monitoring of various data sources through tools such as Zabbix, sentry. ▶ It provides an alerting mechanism to notify administrators in case of anomalies or threshold breaches and provides customization for alert rules and threshold levels to fit specific needs via Zabbix. ▶ OpenSPP provides detailed visualization and reporting capabilities to understand the monitored data and identify trends and patterns via Zabbix and Grafana.
Support	100 %	▶ Currently, L3 support is provided by the commercial partner -Newlogic.
Documentation maturity		
Enterprise documentation	64 % `	▶ OpenSPP provides documentation on general overview, architecture, and infrastructure, which are available at docs.openspp.org. The administrator guide is available for certain features, but currently is work in progress stage. ▶ The documents are easily accessible by public/developer/other stakeholders and are detailed with examples and screenshots to illustrate the solution. The documentation also provides clear instructions on how to use the solution and troubleshoot any issues that may arise. ▶ The solution manages the state and version of documentation update. The document is versioned in a git repository and is currently versioned as 1.0. ▶ Documentation on installation for various environments and solutions, functional use cases and a knowledge repository are planned to be created. The design documents are also planned to be created; however, the high-level design details are available on the website.

3.3. Mojaloop

Integrations present with	MOSIP	OpenG2P

Mojaloop is an open-source software platform designed to facilitate digital financial transactions and promote interoperability among diverse financial service providers, especially in developing regions. The primary mission of Mojaloop is to enhance financial inclusion by empowering organizations to create interoperable payment systems that enable digital financial services for all. Serving as an instant payment clearing and settlement system, Mojaloop features a highly flexible settlement engine.

Mojaloop' s significance lies in its commitment to breaking down barriers and fostering collaboration between financial institutions, thus paving the way for more accessible and inclusive financial systems. By providing a standardized and open framework, Mojaloop allows different players in the financial ecosystem to seamlessly connect, facilitating peer-to-peer transactions, merchant payments, and other essential financial activities. This not only streamlines processes but also contributes to the broader goal of ensuring that digital financial services are available to a wider population, promoting financial well-being on a global scale.

This section provides a summary of Mojaloop' s self-assessment across the assessment parameters, followed by a detailed representation of the functional fitment and the technical fitment which covers architectural coherence, compliance with non-functional requirements, integration potential, the maturity of code and release management processes, operational preparedness, and the quality of documentation.

Legend

Functional Fitment

The functional fitment dimension helps identify if the solution has the capabilities that allows governments, to quickly fulfil their immediate G2P, needs modularly.

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

This dimension block, in the summary provides an analysis on the strength/ maturity of the module with respect to the answers provided. The percentages are calculated based on the number of functionalities present in the module as against the functionalities that should ideally be present

Integration Capabilities

The integration capabilities dimension provides an understanding on how interoperable the solution is with other building block

☑ Present 📈 Planned ☒ Not Available N/A Not Applicable

This dimension block in the summary provides an analysis on the functionalities that are present, planned or not available and not applicable in the solution

Architecture and NFR

The Architecture and NFR dimension provides an analysis if the solution uses modern design paradigms, architectures and technologies

This dimension block in the summary provides the maturity of the dimensions under architecture and NFR. The percentages are calculated based on the number of functionalities present in the module

Documentation Maturity

The documentation maturity provides an analysis, if the solution documentation is easy for a nascent/ fledgling vendor to understand, so that the ecosystem scales up quickly

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

This dimension block provides an analysis on the strength of the capability . The percentages are calculated based on the number of functionalities present in the module

Code and Release Management Maturity

The code and release maturity dimension provides an overview if the solution code is structured and well-managed, modular, well-written - so it can be easily understood and modified, if required

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

The dimension block in the summary provides an analysis on the strength of the capability . The percentages are calculated based on the number of functionalities present in the module

Deployment

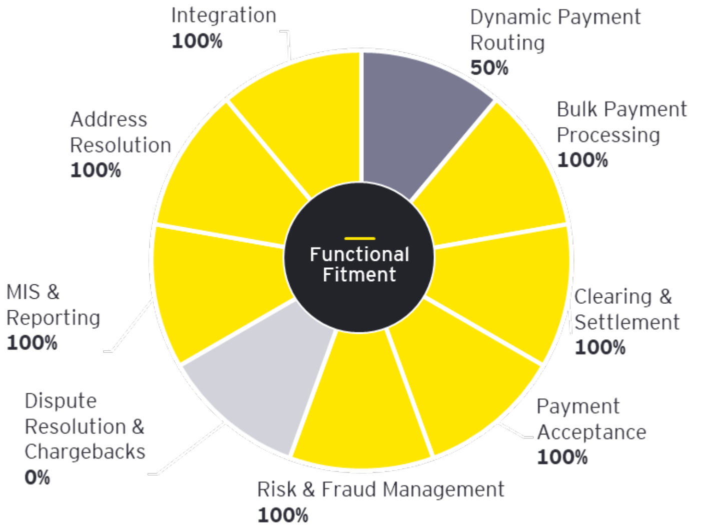
The deployment dimension provides an overview of the pilots conducted by the solution in various countries showcasing its strength, learnings and challenges faced.

📍 Implemented 📍 Interested in Implementing

This provides the countries the solution has been implemented, or interested in implementing being show by a country to deploy the solution

Payment & Settlement Switch for G2P Connect using Mojaloop

Functional Fitment



Operational Maturity

Deployment

- Automated testing and partially completed automated deployment
- Blackbox testing and high test coverage
- Mojaloop has been designed to be deployed in Docker containers, with Kubernetes orchestration.
- Centralized logging and monitoring capabilities
- Large scale and distributed deployments with ease
- CircleCI is used for continuous build and deployment

Monitoring

- Design considerations for monitoring, auditing, telemetry, analytics-three different aspects (non-technical operations, technical operations, and logging & auditing)
- Real-time monitoring of various data sources
- Alerting mechanism to notify administrators
- Customizable alert rules and threshold levels

Support

- Solution Support (L3) -Critical vulnerabilities are raised with the Mojaloop Community by the service operator using Mojaloop
- Financial method inclusion
- SLAs may be agreed between a payments system operator - a deployer of Mojaloop - and an SI, but it is not part of the Mojaloop DPG

Challenges and Learnings

- Most government or development bank procurement processes heavily favor proprietary vendors.
- Many countries do not provide adequate market signals for local firms to bid and implement.
- Multiple government and related agencies are directly involved in payment system decision-making
- Importance of clear project management roles and responsibilities
- Regular stakeholder meetings which include all participants in the project - FSPs, central bank, technology teams.
- Use a proof of concept phase to identify decision gaps prior to contracting or selecting a final technology

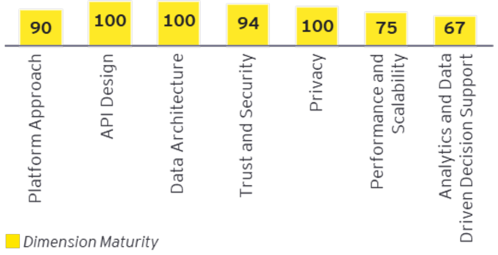
Integration Capabilities

- ✓ Data exchange with external systems in non-proprietary and recognized formats
- ✓ File based integration
- ✓ API-based integration
- 📈 Message-based (Event driven) integration
- ✓ Service orchestration
- ✓ Integration for telemetry dataset for downstream systems
- ✓ Data pipeline architecture

Implementations

Guinea
South Sudan
Rwanda
Tanzania
Myanmar

Architecture and NFR



Code & Release Management Maturity

Code and Repository Mgmt.	Release Mgmt.
Strong	Strong
Configuration Mgmt.	**Documentation Maturity**
Strong	Moderate

Impact

Users impacted in Philippines: **178 beneficiaries**

3.3.1 Functional Fitment

Mojaloop is an open-source software that implements a payment and settlement switch, dynamically routing payments based on Bank Identification Numbers (BIN). Mojaloop excels in bulk payment processing, efficiently handling large lists of beneficiaries. The platform operates in real-time, offering a flexible settlement engine and integrates with various Payment Gateways. Mojaloop supports dispute resolution, provides robust reporting capabilities, enables address resolution through Open APIs, and supports API-based integrations with merchant portals and end-user applications for seamless connectivity. The principal software and system elements of Mojaloop consist of:

- Mojaloop Hub: Mojaloop Hub serves as the central component of the Mojaloop ecosystem, working in concert to provide all the functionalities of the payment and settlement switch.
- Interconnection “means of interconnecting financial institutions (FI) to the Hub”: Interconnection can be achieved through various mechanisms, including:
  - Utilizing the Mojaloop-defined open-source Financial Services Provider Interoperability Protocol (FSPIOP), an asynchronous protocol that supports all the functionalities of the Mojaloop payment switch.
  - Employing a Mojaloop connector, an open-source component that implements FSPIOP and establishes a direct connection to an FI's core banking system.
  - Leveraging the open-source payment manager, which offers self-onboarding capabilities for FIs and manages both the connection with the Hub and the transactions routed through it.
- Oracles “directories for routing payments”: In Mojaloop, payments are addressed using aliases, such as an email address, a mobile phone number, or any other unique identifier. Oracles serve as directories for routing payments by resolving these aliases to identify the participants in a transaction. For example, a mobile phone number oracle can be utilized by the Mojaloop Hub to identify the financial institution hosting the account for the beneficiary of a transaction. Integration with at least one oracle is necessary for a Mojaloop deployment.
- Fraud management services: The Mojaloop Hub allows external fraud/AML monitoring services to access the stream of transactions processed by the hub for analysis.
- Settlement services: The Mojaloop hub does not directly transmit money. Instead, it transmits all the details of a transaction to all participants involved. The actual transfer of funds occurs behind the scenes during the settlement process. In this phase, funds to cover transactions that occurred since the last settlement are transferred from debtors to creditors.

Moreover, the assessment considered the extent to which these functional capabilities catered to the needs of various stakeholders, including implementing agencies and residents. Additionally, these capabilities were evaluated for its potential towards customization, configuration, or extensibility. A summary of the assessment findings, including what is there or has been planned for implementation in upcoming releases, has been provided below.

Functionality	Maturity	Analysis
Dynamic payment processing	50 %	▶ Mojaloop has the capability to enable payment routing by BIN. Mojaloop can dynamically identify the acquirer and the issuing bank through the BIN for selecting the right Payment Service Provider (PSP) for the transaction. As a standard, Mojaloop' s Account Lookup Service (ALS) is able to use a broad range of account identification methods, including BIN, Mobile Station International Subscriber Directory Number (MSISDN) and general aliases. ▶ Mojaloop can enable and establish communication between the acquirer and the issuing bank. Mojaloop' s ALS service enables the identification of the participant PSPs to a transaction, based on the account alias data provided, and resolved through ALS. This includes communication with both parties to establish the accuracy of the routing information. ▶ Mojaloop can be integrated with multiple payment service providers to provide multiple options for transaction processing. ▶ As of now, Mojaloop does not have the capability to route transactions on basis of amount, time of the day, and detection of downtimes, scheduled maintenance, and excessive load on payment gateway.
Bulk payment processing	100 %	▶ Mojaloop can initiate bulk payments (payments to multiple payees) from connected financial institutions. It efficiently processes the payment list, considering the capabilities of these institutions. In the optimal scenario, Mojaloop divides the list into separate lists, one for each connected financial institution, and delivers each sub-list to the respective institution. This approach allows Mojaloop to handle bulk payment lists containing millions of entries. ▶ The connection between the financial institution (FI) and Mojaloop follows the standard API, designed to optimize the processing of bulk payment lists, enabling the handling of lists containing tens of millions of beneficiaries. ▶ Mojaloop has the capability to process bulk payments without any restrictions on the number of destination accounts where funds needs be settled.
Clearing and settlement	100 %	▶ Mojaloop is a real time and instant payment clearing system with a highly flexible settlement engine. ▶ Mojaloop has the capability to automatically credit the amount collected through the online payment gateway to the designated destination account within the agreed time limit.
Payment acceptance	100 %	▶ Mojaloop being a real time payments hub has a core functionality to accept validated payment requests from multiple payment gateways. ▶ Mojaloop conducts comprehensive field-level validation on incoming inputs at all platform boundaries, comparing them against well-documented and publicly available open API schemas. This validation encompasses both syntactic and semantic checks, guaranteeing that only valid payment requests are forwarded to the system core for processing. The validation occurs at multiple layers, including the API gateway and each microservice boundary.

Functionality	Maturity	Analysis
Risk and fraud management	100 %	▶ Mojaloop integrates with the open source FRMS anti-fraud, AML and CTF platform. FRMS reaches deep into Mojaloop to monitor transactions and apply rules defined by the scheme owner, building on the base set of rules defined by the FRMS team.
Dispute resolution and chargebacks	0 %	▶ Mojaloop supports integration with dispute management services for resolving disputes involving customers of connected financial institutions. ▶ As an instant push payment clearing and settlement platform, Mojaloop does not maintain direct connectivity with card associations, even for purposes of dispute resolution and chargebacks.
MIS & reporting	100 %	▶ Mojaloop' s business operations framework serves as an API-based solution for generating reports, dashboards, and management portals designed for use with the Mojaloop Hub. ▶ The real-time analytics dashboard offers a summary of transactions, providing management of the connection to Mojaloop through a series of dashboards and robust search tools for tracking the detailed status of individual transactions. ▶ It offers reports on successful settlements, failed settlements, and settlements on hold. These reports include information on settlement amounts, fee and tax breakdowns, and explanations for failures or holds.
Address resolution	100 %	▶ Mojaloop has capability to provide financial addresses (e.g., beneficiary account number) resolution through integration with Open APIs, allowing payments to be processed via a unique ID. ▶ Core functionality for Mojaloop' s ALS service.

Functionality	Maturity	Analysis
Integration	100 %	▶ Mojaloop Schemes can setup API based integrations with merchant portals and other end-user facing applications. ▶ Integration with merchant technology is via connected service providers e.g., banks, mobile network operators and not direct to the switch. The switch provides comprehensive, customizable, configurable, and extensible APIs for service providers.

Implementation record

Mojaloop successfully implemented its open-source platform in multiple African countries through the Mowali (Mobile Wallet Interoperability) project. This collaboration helped seamless interoperability among mobile money providers, significantly broadening financial access for millions. Individuals can now transact effortlessly across various mobile money platforms, fostering a more inclusive and interconnected financial ecosystem in the region.

3.3.2 Technical fitment

Functionality	Maturity	Analysis
Architecture and NFR		
Platform approach	90 %	▶ Mojaloop employs a microservices-based architecture and utilizes the Kubernetes orchestration platform. Each Mojaloop microservice can be individually scaled to handle load hotspots within the system. It exposes comprehensive, open, and secure APIs. The system uses the HELM toolchain for managing updates, follows a semantic versioning scheme, and undergoes a formal release process involving rigorous testing and quality gates. The solution supports the upgradation of individual components or the entire system via mechanisms exposed by the HELM toolchain. Mojaloop API protocols are designed from the ground up to address connectivity issues between scheme participants, incorporating failure and retry protocol mechanisms to maintain financial integrity. The system supports configuration mechanisms for customization without the need for code changes. Currently, it is implemented in the Tanzania Instant Payments System and WynePay, Myanmar.

Functionality	Maturity	Analysis
API-first design	100 %	▶ Mojaloop' s administrative APIs facilitate the customization of the solution, allowing for the configuration of role-based access control, permissions models, account registration, and lookup, among other features. The system implements several layers of security, including mutually authenticated transport layer security (mTLS) using X.509 PKI certificates, OAuth 2.0/OIDC authentication, JSON web signatures (JWS), and IP filtering. ▶ Mojaloop' s APIs support best-practice API governance models and encompass both asynchronous call-back-oriented and synchronous models. They facilitate versioning and provide version negotiation mechanisms, enabling both clients and servers to manage upgrades independently. Mojaloop offers various environments, such as development, test, staging, customer sandbox, and production. Additionally, it can operate in a completely headless mode.
Data architecture	100 %	▶ Mojaloop adheres to data anonymization principles, supporting master data management (MDM) with opaque identifiers. It utilizes relational data stores employing third normal form data modelling to ensure integrity. The storage layer technologies native to Mojaloop facilitate encryption both at rest and in transit. The solution employs Mutually Authenticated Transport Layer Security (mTLS) to ensure robust encryption, authentication, and authorization between system processes. ▶ Mojaloop' s storage layer technology supports flexible partitioning and sharing, aligning data store technology with application data characteristics. Additionally, it provides a horizontally scalable microservices architecture.
Trust and security	94 %	▶ Mojaloop follows a zero-trust model and employs mTLS to ensure robust encryption, authentication, and authorization between system processes. It adheres to OAuth 2.0 and OIDC protocol standards, offering flexible role-based access control that enables operators to define relationships between permissions, roles, and users. ▶ The solution supports logging facilities for auditing user behavior, API requests (including origin addresses and security parameters), strong type checking, and input validation against published OpenAPI specifications. Mojaloop utilizes standards-compliant "off-the-shelf" identity and access control platforms, implementing best practices in session identifier management. It employs JSON Web Signatures (JWS) to provide non-repudiation between payment scheme participants and continuously scans for known security vulnerabilities. ▶ For key management, Mojaloop uses PKI, with each entity in a Mojaloop scheme responsible for generating key pairs on their own infrastructure. Hub private keys are securely stored in vaults, such as HashiCorp Vault or hardware security modules (HSM). The solution leverages the log management facilities of the Kubernetes container orchestration platform and supports address space randomization (Linux). Additionally, the Mojaloop Foundation sponsors penetration testing and security audits for all Mojaloop source code.

Functionality	Maturity	Analysis
Privacy	100 %	▶ Mojaloop provides a consent management framework for selected cases. In PISP transfers, it establishes a trust relationship between DFSPs (or FIs), PISPs (FinTech's/3PPIs), and the User. During this process, credentials are registered for future consent validation by users. Consents are stored per account, per user, allowing for manageable and limited access to the type of consent used, providing granularity for various functions. ▶ Mojaloop' s consent and credential management adhere to the FIDO standard and follow cryptography standards for encryption, ensuring the security of user-specific data without storing it. The system conducts regular scans and security assessments, either at the PI level or half-yearly, to identify and address risks. ▶ In compliance with regulations and scheme rules, Mojaloop only relays user information as allowed and stores mappings between identifiers and financial institutions.
Performance and scalability	75 %	▶ Mojaloop employs various key performance indicators (KPIs) to measure its performance, including Financial Transactions per Second (FTPS), latency (average time taken for each transfer), time taken for 99% of transactions, number of transfers taking greater than 1 second in a given time period, sustaining a certain number of FTPS for a specified duration, and graceful degradation of service. Additionally, there are KPIs related to resilience, measuring the time taken to restore normal functionality after a failure, and upgradability. ▶ For testing purposes, Mojaloop utilizes the Mojaloop Testing Toolkit (TTK) for end-to-end testing of a Mojaloop deployment. The testing strategy includes unit tests at a basic level, integration tests as part of the Continuous Integration/Continuous Deployment (CI/CD) process, and automated checks for licensing, scans, audits, and other quality criteria.
Analytics and data-driven decision support (Unified scheme view)	67 %	▶ Mojaloop utilizes an event framework to capture data and supports the Elastic Search, Fluentd, Kibana, Loki stack with Prometheus & Grafana for monitoring primarily, along with APM for traceability. It primarily uses transactional data for processing, enabling monitoring and tracing for debugging, monitoring, and other operational aspects. The solution supports portals for querying and dashboards. ▶ The Finance Portal V3 provides the necessary portals for backend office functionality and is coupled with technical operations supporting tools like Loki, EFK, Promfana for technical operations.
Integration capabilities		
Interoperability	86 %	▶ Mojaloop adheres to Mojaloop messaging standards and supports integration with ISO 20022 and ISO 8583 standards. It facilitates API communication with other systems based on FSP Interoperability API, PISP API, etc. Mojaloop schemes can support the financial institutions (FIs) / financial service providers (FSPs) by providing file-based integrations to their end-users for uploading payment instructions. ▶ The solution uses Kubernetes for microservice orchestration of dockerized containers, providing benefits such as abstract deployment infrastructure, self-healing, and the use of operators. It also employs the ElasticSearch, Fluentd,

Functionality	Maturity	Analysis
		and Kibana stack (EFK) for log collection and supporting monitoring capabilities. Mojaloop provides the necessary tools for data pipeline architecture, transforming stored data for presentation and reporting purposes.
Code and release management maturity		
Code repository management	100 %	▶ Mojaloop has a Design Authority governance group that is elected yearly. Code owners manage critical, priority repositories, while DevOps teams and Mojaloop Foundation staff handle general DevOps and GitHub maintenance. Additionally, several technical and community-related governance groups are supported by advisory groups and Mojaloop Foundation Staff. ▶ For release-level repositories, code coverage should be >90% at each file and branch level. GitHub best practices and tools, such as Dependabot alerts, Snyk, CodeQL, GitHub secret scanner, License scanning, and dependency scanning, are incorporated into CI/CD processes. Code quality and reviews are conducted periodically and during every change/commit to GitHub repositories. ▶ Main/primary branches are protected with merges and require reviews from code owners, along with completion of all CI steps, including unit and integration tests, along with auditing and licensing checks. Code metrics are tracked and reported to the Technical Governance Board (TGB) periodically.
Release management	100 %	▶ Mojaloop follows the Scaled Agile Framework (SAFe) to manage workstreams in Agile delivery. GitHub, via the Zenhub plugin, is utilized for managing issues, backlogs, and release management. Releases occur every three months; however, Mojaloop adapts release cycles based on changes involved, adhering to the semantic versioning standard. Additionally, there may be patch releases for bug fixes and minor version increments. ▶ Patch releases are generated for fixes or rollbacks when issues are identified in the releases. Mojaloop' s code is integrated with CircleCI, providing CI/CD, and 10-20 CI steps run during pull requests and commits to Mojaloop repositories. GitHub releases can automatically publish packages to the npm repository and images to DockerHub using relevant CI/CD mechanisms.
Configuration management	100 %	▶ Mojaloop employs infrastructure as code for deployment, utilizing various tools for provisioning, setup, validation, and general maintenance of Mojaloop deployments. Mechanisms based on Mojaloop' s score, helm charts can be implemented, with customizations and configurations added on top of that. Kubernetes is used for container orchestration, and operators in Kubernetes manage configuration and other updates. Ansible is utilized alongside Terraform. ▶ GitHub, via the Zen hub plugin, is used to manage issues and code repository, while Jira and GitLab are also employed for deployment management. Configuration and scheme rules can be customized based on specific needs, regulations, and scheme rules.
Operational maturity		

Functionality	Maturity	Analysis
Deployment	83 %	▶ In Mojaloop, a suite of automated blackbox tests is run against each component at least every 24 hours, and the results are reported on the Mojaloop slack. The development of every component of Mojaloop follows a process where the requirements for the module, acceptance criteria, and tests must pass before acceptance are defined. Development teams use this process to validate the completion of the module and contribute to overall black box testing. ▶ Mojaloop has been designed to be deployed in Docker containers, with Kubernetes orchestration independent of the environment. Kibana/ElasticSearch is used to provide centralized logging and monitoring capabilities, supporting rapid identification and resolution of issues. Mojaloop adopts a "scale-out" approach instead of "scale up." Rather than relying on a few high-cost servers, real or virtual, Mojaloop relies on a larger number of low-cost, less reliable machines. Kafka messaging is used to route the next stage of transaction processing to the next available instance of a process. CircleCI is used for continuous build and continuous deployment.
Monitoring	80 %	▶ Mojaloop provides a monitoring/auditing feature with three aspects: Operational, where the non-technical operations team manages the operations of the Mojaloop Hub; Logging and auditing, for the purpose of regulatory compliance and operational security; and technical operations, where telemetry, monitoring, and analytics are used in troubleshooting problems and diagnosing bugs. ▶ The Hub operator has access to portals allowing them to view the load on the hub in terms of transaction volumes, and the technical operations teams have access to Kibana to analyze logs, metrics, and explore individual events. Mojaloop uses Kibana to alert the technical operations team in case of anomalies or threshold breaches, supporting customization.
Support	67 %	▶ Mojaloop provides support for raising critical vulnerabilities by the service operator initially using Mojaloop with system integrators (SI) support/partner organizations. Subsequently, either directly or through the SI, the concerns are communicated to the Community via the Community portal. These issues are then escalated through the Design Authority for investigation and solution identification. A deployer of Mojaloop, typically the operator of a payments scheme, will often subscribe to a support contract with an SI.
Documentation maturity		
Enterprise documentation	70 %	▶ Mojaloop provides documentation covering a general overview, architecture and infrastructure, design, and deployment in AWS and Azure environments. The documentation is managed on GitHub and is easily accessible via the Mojaloop website. Core use cases P2P, RTP, PISP, loan disbursement, and repayment are currently available, and a merchant payments extension (supporting USSD and QR) is coming soon.

3.4. Mifos

Integrations present with	Mojaloop	MOSIP	OpenG2P	OpenSPP	Open IMIS	Fineract

Mifos is an open-source platform that provides financial management and microfinance services to microfinance institutions, banks, and other financial service providers. The platform was developed to provide financial services to underserved communities, including those in developing countries. The key features of Mifos include:

- Loan management: Mifos provides a comprehensive loan management system, including loan origination, approval, disbursement, repayment, and delinquency management.
- Savings management: Mifos provides savings management, including savings account creation, deposit and withdrawal, and interest calculation.
- Wallet and transactional account management: Mifos provides wallet and transactional account management including processing of transaction as per defined workflow, fund transfers, transaction history, transaction authorizations among other functionalities.
- Client management: Mifos provides a comprehensive client management system, including client onboarding, identity verification, and demographic information tracking.
- Reporting and analytics: Mifos provides advanced reporting and analytics capabilities, including financial statements, portfolio performance, and risk management.
- Integration: Mifos is designed to integrate with other systems, including payment gateways, mobile banking, and SMS.
- Customization: Mifos is designed to be customized to meet the specific needs of financial service providers, including custom workflows, business rules, and product configurations.

Mifos is used by financial institutions around the world to provide financial services to underserved communities. Its open-source nature and customizable design make it an attractive option for financial service providers looking to expand their services to new markets. Core banking system offered by Mifos facilitates financial inclusion and microfinance. It is a comprehensive solution designed not only for traditional financial inclusion and microfinance needs but also adaptable to the evolving landscape of digital financial services. Mifos serves a diverse range of entities, including fintech companies, wallet providers, neo-banks, and similar organizations.

This section provides a summary of Mifos' self-assessment across the assessment parameters, followed by a detailed representation of the functional fitment and the technical fitment which covers architectural coherence, compliance with non-functional requirements, integration potential, the maturity of code and release management processes, operational preparedness, and the quality of documentation.

Legend

Functional Fitment

The functional fitment dimension helps identify if the solution has the capabilities that allows governments, to quickly fulfil their immediate G2P, needs modularly.

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

This dimension block, in the summary provides an analysis on the strength/ maturity of the module with respect to the answers provided. The percentages are calculated based on the number of functionalities present in the module as against the functionalities that should ideally be present

Integration Capabilities

The integration capabilities dimension provides an understanding on how interoperable the solution is with other building block

☑ Present 📈 Planned ☒ Not Available N/A Not Applicable

This dimension block in the summary provides an analysis on the functionalities that are present, planned or not available and not applicable in the solution

Architecture and NFR

The Architecture and NFR dimension provides an analysis if the solution uses modern design paradigms, architectures and technologies

This dimension block in the summary provides the maturity of the dimensions under architecture and NFR. The percentages are calculated based on the number of functionalities present in the module

Documentation Maturity

The documentation maturity provides an analysis, if the solution documentation is easy for a nascent/ fledgling vendor to understand, so that the ecosystem scales up quickly

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

This dimension block provides an analysis on the strength of the capability . The percentages are calculated based on the number of functionalities present in the module

Code and Release Management Maturity

The code and release maturity dimension provides an overview if the solution code is structured and well-managed, modular, well-written - so it can be easily understood and modified, if required

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

The dimension block in the summary provides an analysis on the strength of the capability . The percentages are calculated based on the number of functionalities present in the module

Deployment

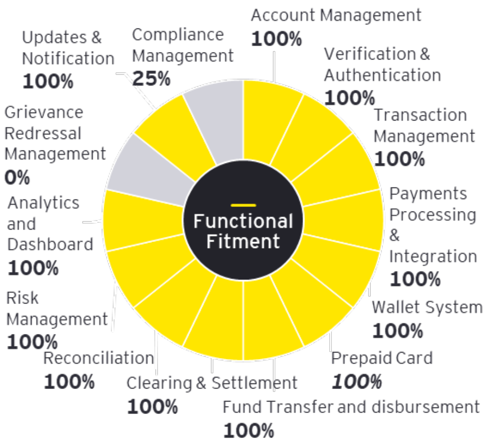
The deployment dimension provides an overview of the pilots conducted by the solution in various countries showcasing its strength, learnings and challenges faced.

📍 Implemented 📍 Interested in Implementing

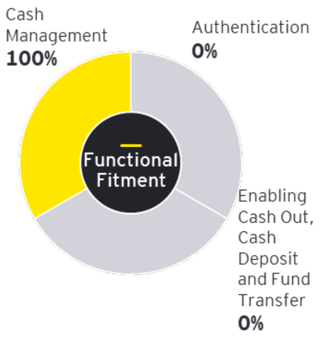
This provides the countries the solution has been implemented, or interested in implementing being show by a country to deploy the solution

Bank & Mobile Wallet System, Payment & Settlement Switch, Last Mile Cash-in & Cash-out, ID Account Mapper for G2P Connect using Mifos

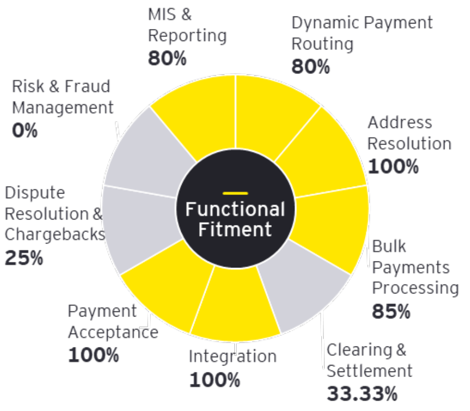
Functional Fitment



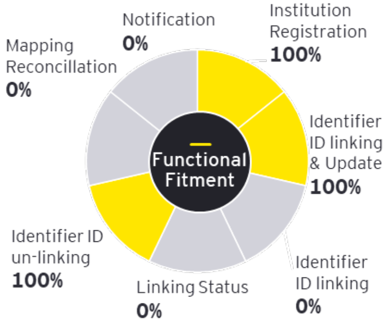
Bank & Mobile Wallet System



Last Mile Cash-in & Cash-out



Payment & Settlement Switch



ID Account Mapper

Challenges and Learnings

- Extended procurement/sales cycles necessitate the presence of a substantial single vendor capable of instilling confidence, assuming liability, and mitigating risks.
- Countries have apprehensions regarding cloud security and data sovereignty constraints which adds complexity to cloud-based deployment and testing.
- Importance of People, Process, and Technology for the successful implementation of Mifos in any country.
- Efficient business process optimization is crucial. Frequently, processes and policies exhibit inefficiencies and require thorough mapping and optimization to align with the new systems.
- ROI measurements are essential for showcasing the influence of adopting DPG/DPI.

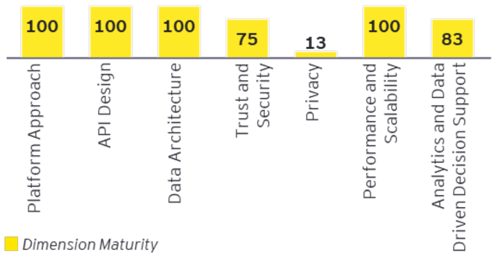
Implementations

- Mifos Fineract is currently in use by financial institutions in 65 countries.
- Payment Hub EE Deployments are currently active in 4 countries, with deployments underway in 4 additional countries. There are plans for deployment in 5 more countries.
- Please refer to the Annexures for a detailed list of these countries.

Code & Release Management Maturity

Code and Repository Mgmt.	Release Mgmt.
Moderate	Strong
Configuration Mgmt.	**Documentation Maturity**
Strong	Strong

Architecture and NFR



Operational Maturity

Deployment

- Automated testing and continuous integration but there is significant gap in rollout capabilities
- Blackbox testing and high-test coverage
- Support containers and virtual machines
- Provide centralized logging and monitoring capabilities through elastic search and Kibana
- CI/CD via Jenkins and circle CI
- Helm charts are maintained for large/small scale deployment

Monitoring

- Using Prometheus, Grafana, Kibana for operational maturity
- Real-time monitoring of various data sources
- Alerting mechanism to notify administrators
- Customizable alert rules and threshold levels
- Visualization and reporting capabilities

Support

- L3 support provided through number of system integrators and partners
- Financial method inclusion
- No SLA associated for critical issue resolution in core system

Integration Capabilities

- ☑ Data exchange with external systems in non-proprietary and recognized formats
- ☑ File based integration
- ☑ API-based integration
- ☑ Message-based (Event driven) integration
- ☑ Service orchestration
- ☒ Integration for telemetry dataset for downstream systems
- ☑ Data pipeline architecture

Impact

No of financial institution using Mifos = **402**
Clients registered on Mifos = 20,000,000

3.4.1 Functional fitment

Mifos has been employed by a diverse range of financial institutions and non-profit organizations globally to extend financial services to underserved communities, enhance financial education, and foster economic empowerment. The platform remains dynamic and flexible, continuously adjusting to address the evolving requirements of the financial inclusion sector. Mifos has below mentioned products, services, policies, and processes to effectively deliver financial inclusion:

Loans Products:- Individual Lending, Group Lending, SME Lending, Business Loans, Agricultural Loans, JLGL (Joint Liability Group Lending), Incremental Disbursement Loans, Open End Lending, Variable Instalment Loans, and Custom Loan Program

Guarantor Management:- Collateral, Loan Guarantors, and Automatic Loan Payment Transfers

Loan Tools:- Collection Sheets, Bulk Loan Reassignment, Delinquency Control, Reassign Loans Between Branches, Payment Types, Loan Frequency Rescheduling, Loan Cycle Tracking, Floating Interest Rates, Amortization, Automated Loan Payment, Manage Holidays, Loan Loss Provisioning, Loan Rescheduling/Refinancing, and Manage Non-Performing Assets

Saving Products:- Basic Savings Accounts, Passbook Savings, Mandatory Savings, Interest Bearing Savings, Term Deposits, Recurring Deposit Term Accounts, Share Accounts, and Custom Savings Programs

Saving Tools:- Recurring Deposit, Standing Instructions, Interest Calculation, Dividend Calculation, Receipt Printing, Dormant Account Management, and Amount-Interest Rate Charts

Wallet & Transactional Account Management:- Current/Checking Accounts, Overdraft Automatic Transfer, Wallet Account, Transaction history, Account creation

Client Management:- Client Identification (KYC), Online Photographs and Signatures, Document Attachment (Photos, Applications, IDs), Data Tables, Client Relationship Management, Client Risk Analysis, Credit Scoring, Document Templates, Product Mix, and Social Performance Management

Business Management:- Multi-Functional Institution Support, Unlimited Individual Patrons (Members), Unlimited Hierarchy, and Branch Management

Reporting:- Reporting, Customizable Fields, Manage Reports, and Statement Generation

Accounting:- Accrual & Cash Based Accounting, General Ledger Integration, Journal Voucher Support, Chart of Accounts Management, Flexible Accounting Classifications, and Account Number Preferences

Business Rules and Workflows:- User Permissions, and Workflows (Entity Data Table Checks)

Cash Management:- Cash Management, Funds Transfer, and Funds Management

Central Product Configuration:- Loan Configurator, Savings Products Configurator, and Account Number Preferences

Fees and Charges:- Membership Fee, Late Fees & Automatic Penalties, Recurring Fees, One-Time Fees, Flexible Accounting Classifications, Define Charges, and VAT Tax Withholding

Internationalization:- Multi-Currency and Multi Language

Security:- Access, Authorization, and Audit

Client Messaging & Self-Service Operations:- Event-Based SMS Messaging, SMS Campaigns, and Self-Service APIs

Mobile Field Tools & Processes:- Android Field Operations App, Mobile Field Operations Via Tablet, On-line / Off-line (Store & Forward Capability), and Mobile Money Integration

System Migration & Configuration Tools:- Entity to Entity Mapping, Manage Hooks, Account Number Preferences, Global Configurations, Scheduler Jobs, Manage Data Tables, and Manage Codes

An assessment was conducted to assess the functionalities of Mifos, with a special focus on their applicability in the context of G2P payments. The specific functionalities under assessment included account management, verification & authentication, transaction management, payments processing & integration, wallet system, prepaid card, fund transfer and disbursement, clearing & settlement, reconciliation, risk management, analytics & dashboard, grievance redressal management, updates & notifications, compliance management, dynamic payment routing, address resolution, bulk payment processing, clearing & settlement, integration, payment acceptance, authentication, authorization, dispute resolution & chargebacks, risk & fraud management, MIS & reporting, enabling cash out, cash deposit, and fund transfer, cash management, institution registration, identifier ID linking & update, identifier ID linking, linking status, identifier ID un-linking, identifier ID un-linking, mapping reconciliation and notification. The assessment considered the extent to which these functional capabilities catered to the needs of various stakeholders, including implementing agencies and residents. Additionally, these capabilities were evaluated for its potential towards customization, configuration, or extensibility. A summary of the assessment findings, including what is there or has been planned for implementation in upcoming releases, has been provided below.

Bank and mobile wallet system:

Functionality	Maturity	Analysis
Account Management	100%	▶ Account management functionality enables integration with the payment hub to store financial details and other information like a composite of registration and scheme associated with the functional ID. The platform has APIs for integration with other systems and platform-level API consumers can update/add new functional ID mapping and new financial addresses to map with the account. The platform does not support validations on the format of IBAN, BIC, and routing number and the platform supports real-time updates. The platform ensures the accuracy and validity of the linked registry and scheme IDs via source/registry building blocks.
Verification and authentication	100%	▶ The platform supports both basic types of authentications and key cloak authentication. The key cloak is integrated with the payment hub. The platform provides authentication using basic and OAuth. Key cloak OpenID Connect (OIDC)-based authentication is planned for upcoming releases. ▶ Partial authorization is available using platform-level authentication which can be used by authorized parties. Sensitive data is masked in audit logs and encrypted using SSL authentication during the transmission of data to protect the privacy and security of IDs during transmission and storage. ▶ Key cloak OIDC-based authentication is integrated with the payment hub to verify identity with external ID systems.
Transaction management	100%	▶ The platform assigns unique transaction IDs to all transactions and has APIs to capture external transaction IDs, receipt numbers, routing numbers, etc. It also allows tracking of transaction IDs and status of transactions and supports multiple ID linkages with transaction IDs. ▶ The payment hub of the platform has the capability to process transactions as per defined workflow and can be customized as per the requirement. It can also be integrated with order and accounting software. ▶ The platform can handle the load of multiple transactions. The account management system and payment schema errors are standardized to capture payment hub errors to notify the error messages to user and developer. ▶ The platform supports authorization of transactions as per the delegated authority. Authorization is managed using roles and permission using Command Query Responsibility Separation (CQRS). ▶ The platform does not support multiple levels of authorization to be defined for transactions such as dual control or multi-level approval. Additionally, it does not support the configuration of transaction authorization rules based on transaction amount, merchant, or any other criteria.

Functionality	Maturity	Analysis
Payments Processing & Integration	100%	▶ The platform supports the processing of payment to beneficiary account, wallets, and prepaid cards through multiple channels like bank transfers, mobile wallets, PoS, USSD, and SMS gateway. It provides unified APIs for integration with multiple payment channels and separate APIs for each channel. ▶ Mifos supports multi-currency, exchange rate preview and the booking exchange rate feature. It does not support recurring payments and subscriptions through APIs and does not detect the preferred payment channel of the customer and the corresponding payment option at checkout. ▶ The platform supports open standard protocols like ISO 20022, ISO 27001, GSMA MM v1.1, GSMA pathfinder, and Mojaloop v14/ Interledger protocol. ▶ It does not support decentralized exchanges, and provides Auth-n, wallet lifecycle APIs, transactional APIs, and SDK APIs for integration with other systems and services. The wallet system provided by the platform supports backup and recovery mechanisms in case of any data loss. ▶ Integration with the MOSIP biometric auth-n (eSignet) is in the planned phase.
Wallet system	100 %	▶ Mifos supports the integration of the beneficiary account with various types of wallet systems through saving account API. It offers back-office capabilities to manage the store of value within the wallet account. ▶ The wallet system supports partial processing of online transactions, and offline transactions can be pushed to the platform through bulk import. ▶ Transport layer security is used for end-to-end encryption of sensitive information and transactions. ▶ The platform is designed to support a large volume of microtransactions and enhanced performance and real-time updates and notifications of the transactions. It supports integration with multiple devices such as smartphones, desktops, and tablets through APIs.
Prepaid card	100%	▶ The platform supports the integration of payment accounts with prepaid card solutions through saving account APIs. ▶ The platform does not support virtual and physical prepared card options. ▶ It supports loading and reloading of funds in the prepaid card using APIs. The platform supports real-time balance tracking of prepaid cards using AMS system workflows. ▶ The platform neither supports disputes/chargebacks for prepaid card transactions nor handles the redemption of rewards or loyalty points for prepaid cardholders. ▶ Wallet's system management is used to handle the activation and deactivation of prepaid cards.
Fund transfer and disbursement	100%	▶ The platform supports a wide range of last-mile payment processing through various channels like banking correspondents, merchant vouchers, prepaid cards, etc., through APIs. ▶ Mifos supports processing of government to agent/ merchant/ BC payments in batch format as well as voucher redemption flow. Furthermore, the community has developed connectors to integrate with various payment rails, including Mpesa and other mobile money networks in Africa, CODI in Mexico, Mojaloop, PIX in Brazil, SEPA in Europe, and UPI in India.

Functionality	Maturity	Analysis
		▶ The platform supports wallets in multiple currencies and international remittances. It supports country-specific payment methods which are limited to Africa and India. ▶ The platform supports webhooks that provide notifications related to hold/ release/ debit/ credit and fees transactions. It supports splitting, throttling, rate limiting, and batch size limits for the processing of high volumes transactions.
Clearing and settlement	100 %	▶ Mifos supports real-time/ batch processing of transactions through extensive APIs in a timely manner. It triggers notifications in the event of payment failures or errors using implementation workflows. ▶ The platform supports integration with payment platforms for the settlement of transactions between different financial service providers through APIs. However, this capability is not customizable, configurable, and extensible. ▶ The platform provides configurations to manage information using Fineract report APIs and PHEE get transfer APIs, but the platform does not support trail balance report APIs, list report APIs, and retrieve report APIs. It does not use any external APIs for fetching payment information with a minimum number of fields. ▶ The platform does not provide APIs/ Scripts for automating the batch process
Reconciliation	100 %	▶ The platform supports the generation of periodic reconciliation reports of all transactions which are customizable and configurable via Kibana dashboard and transfer API. It supports integration of transfer/ batch details API and customizations of trail balance, ledger, and agent reports with other systems and the configuration of published data periodically through APIs. ▶ The platform enables and supports a comprehensive reconciliation system to handle, interchange, settlement, chargebacks, etc. by providing several report interfaces for reconciliation. It does not have the capability to generate periodic reconciliation of linking status between the ID account mapper database and the core banking system. ▶ The platform enables and supports an auto-reconciliation mechanism to reconcile all transactions with other financial service providers through extensive APIs like GET transfers API, GET batch details API, and GET report API. It supports the export of transaction data in CSV format. ▶ The platform supports the real-time update of transaction data and real-time notification of transaction change status but does not support bulk real-time notifications. It provides tools for reporting, reconciliation reports and dashboards. ▶ Additionally, the platform also supports multiple currencies and payment methods.
Risk management	100 %	▶ Mifos offers capabilities to manage and mitigate risks in a financial institution such as credit risk, market risk, operational risk, enterprise risk, and other types of risks using credit bureau integration. It supports APIs such as transfer API, transactional API, etc. for integration with other systems. ▶ The platform does not provide real-time fraud detection and prevention capabilities. However, it provides configurations to implement custom fraud rules. ▶ The platform does not have the ability to perform velocity checks, IP address filtering, and device fingerprinting. It does not provide risk scoring based on multiple factors such as amount, address, and past transaction history.

Functionality	Maturity	Analysis
		▶ The platform is integrated with external fraud prevention services or databases. However, it does not have any dispute management process dashboard or reporting tool for monitoring and managing fraud incidents.
Analytics and dashboard	100 %	▶ Mifos supports real-time analytics dashboard for accounts, loans, payments, refunds, settlements, disputes & chargebacks etc. and generation of periodic reports. It supports various types of analytical dashboards based on workflow implementations. Visualization and dashboards can be customized. ▶ The platform does have APIs available for integration with other systems. It can push data in real-time to the analytical system from Fineract via customizable hooks and in-payment hub data. ▶ The platform has the capability to create unique dashboards based on role-based access of the individuals at the report level, dashboard level, graph level, etc., through Kibana. It provides a UI interface of Kibana to create and publish a dashboard. ▶ Multiple integration plugins are available but compatibility with open-source platforms is minimal. Moreover, Mifos and Fineract provide support for Pentaho open-source business intelligence, along with built-in HTML reports. Recently, dashboard support through Apache Superset has been incorporated, and integration with BIRT reporting is planned in the upcoming versions.
Grievance redressal management	0 %	▶ The current platform lacks the capability to integrate with diverse channels for grievance resolution, including helpdesk, calls, chatbots, and mobile apps. It does not possess the functionality to track grievance status and facilitate escalation. However, the future roadmap for Mifos includes plans to integrate a CRM with helpdesk functionality for effective ticketing and support resolution. ▶ Mifos's mobile banking application seamlessly incorporates Rocket Chat or messaging, and the Mifos community has developed chatbots to enable users to interact with their data in Fineract.
Updates and notification	100 %	▶ Mifos has the capability to send real-time notifications of activities in the account including debit/ credit transactions, debit card charges, transaction status, loan transactions, online payment, etc. via multiple channels- SMS/email using APIs. This capability can be customized to send notification on different transaction actions. ▶ The platform supports the creation of multiple webhooks for events and actions, which are used to send daily reminders. However, it does not have customizable settings for downtime and failure notifications. ▶ The platform includes a retry configuration feature within payment hub workflows. KYC checks in the platform can be configured through workflow and AML needs to be integrated with the platform.

Functionality	Maturity	Analysis
Compliance management	25 %	▶ The current version of Mifos lacks the capability to comply with various regulations such as anti-money laundering (AML) laws and know-your-customer (KYC) regulations. However, Mifos has plans to incorporate this capability in future releases. ▶ Presently, Mifos supports the attachment of any KYC document, and has plans to integrate with additional KYC automation frameworks like Ballerina. ▶ The solution is capable of seamlessly integrating with various watchlists and screening tools. While Mifos is planning to directly build this capability into the system, it can currently be supported through workflow runs, ensuring appropriate screening of customers.

Payment and settlement switch:

Functionality	Maturity	Analysis
Dynamic payment routing	80 %	▶ Mifos has the capability to enable and establish communication between the acquirer and the issuing bank through asynchronous APIs and notifications. It supports real-time notification for all relevant transactions via multiple channels. Notifications sent by the platform can be customized to match the specific needs of the acquirer or issuing bank. It provides mechanisms for reliable delivery and retry of notifications in case of any network or any other failure. ▶ The platform has the capability to integrate with multiple payment service providers supporting multiple options for transaction processing through the implementation of specific connectors. ▶ It enables connections to various external payment rails and provides the flexibility to define executable BPMN diagrams that orchestrate these flows across multiple systems. ▶ Capabilities to route transactions based on the time of the day and employ intelligent routing mechanisms to detect downtimes, scheduled maintenance, and excessive load on payment gateway (PG) are to be planned in the upcoming versions. ▶ The current version of Mifos does not include the capability to enable payment routing through Bank Identification Number (BIN), where the switch dynamically identifies the acquirer and issuing bank through the BIN to select the appropriate PSP for the transaction. Additionally, the capability to route transactions by the amount to select the right PSP for the transaction is also not present in the current version of Mifos, and there are no plans to include these features in future releases as of now.

Functionality	Maturity	Analysis
Address resolution	100 %	▶ The platform has the capability to provide financial address (e.g., beneficiary account number) resolution through integration with Open APIs, allowing payments to be processed via a unique ID. ▶ It has well-documented APIs, and it is easy to add new functionality through the API.
Bulk payments processing	85 %	▶ Mifos has the capability to initiate bulk payments (payments to multiple payees) through single file upload consisting of payment details such as unique ID, account number, amount, payment mode, etc. It supports splitting large files into sub-batches and the files are processed in smaller chunks. Details related to the reporting of batches are available for fetching transaction details. ▶ The platform has the capability to process bulk payments with no limit on the number of destination accounts, where the funds are required to be settled. In such cases, large payment files can be broken into smaller files as required. This capability is available as part of the G2P use case where the destination accounts can be different and large in number. ▶ The capability to provide customizable file upload formats are planned to be included in the upcoming versions.
Clearing and settlement	33 %	▶ The platform supports real-time and batch processing of transactions through API integration. ▶ Capabilities to support real-time or batch settlement of the transactions, automatically credit the amount collected through the online PG to the designated destination account within the agreed time limit, is not present and currently, Mifos has not planned to include it in future version releases.
Integration	100 %	▶ Mifos supports API-based integration with merchant portals which can be customized and configured as per the requirements. It has well-documented APIs and the security of payment transactions made through API is ensured by additional system user auth-n steps, non-repudiation, and TLS. ▶ The platform can handle high transaction volumes and ensure fast processing times when integrated with merchant portals via API. However, it does not support recurring payments and subscription integration with merchant portals.

Functionality	Maturity	Analysis
Payment acceptance	100 %	▶ Mifos has the capability to accept validated payment requests from multiple payment gateways which can be integrated through APIs. It provides real-time processing and updates and supports multiple payment methods. Additionally, the platform can handle invalid or missing fields during requests. ▶ The platform has the capability to perform field-level validations (including syntactic and semantic validations) on all the payment details. It has a set rule for validating the format of data entered for each payment field and supports encryption of sensitive field data. It does not have specific formatting requirements for sensitive fields. ▶ The platform has the capability to read the pre-defined merchant rules and accordingly process transactions (transaction amount limit, etc.). It allows SMEs and corporates to set their own rules and requirements for processing payments. ▶ The merchants can set various types of payment processing rules, based on which Mifos can reject transactions that violate the merchant’s payment processing rules. The platform allows the merchant to update/change their payment processing rules as per their requirement.
Dispute resolution and chargebacks	25 %	▶ Mifos supports the handling of disputes and chargebacks arising due to card network exceptions, issues raised by the user, etc. ▶ Mifos currently lacks direct connectivity with various card associations (VISA, MasterCard, Discover, Amex, etc.). However, it has plans to introduce this functionality in future release versions, intending to establish connections to VISA Direct and Mastercard Send as destination endpoints for G2P payments. While partners have implemented this capability, it is not currently available in community versions. ▶ The platform does not adhere to the rules and regulations of the respective card associations or does not accept or contest a dispute and processes required actions. These features are currently not planned in the future version releases.
Risk & fraud management	0 %	▶ Mifos currently does not support real-time risk and fraud monitoring capabilities such as real-time transaction monitoring, velocity checks, blacklisting, holding suspicious payments, 24x7 alert backend management team, etc. This feature is planned to be included in the upcoming version releases. ▶ The platform does not have the capability to detect frauds like address verification service (AVS), card verification value (CVV), device identification, payer authentication (3-D Secure), block list support, etc. Mifos is not planning to include this functionality in future version releases.
MIS & reporting	80 %	▶ The platform has the capability to generate a daily, weekly, or monthly report or any chosen duration for payments, refunds, settlements, disputes, chargebacks, etc. using the Kibana dashboard. It has customizable reporting and dashboard options available for different types of transactions through API and uses configuration to publish data periodically / scheduled through APIs.

Functionality	Maturity	Analysis
		▶ The platform has the capability to generate a real-time analytics dashboard for transaction summary (transaction status, payment method, time, etc.), payments, refunds, settlements, disputes, chargebacks, etc. using ES, Kibana, Grafina, and Prometheus. It has customizable reporting and dashboard options. ▶ The platform does not have APIs for integration with other systems. ▶ The platform has the capability to perform searches on payment details through various filters. The platform offers a search function for transactions within the MIS reports and allows the configuration of search criteria as per the requirement. The platform allows advanced filtering options for search results and allows the search results to be exported in a usable format (e.g., CSV, Excel). ▶ The platform has the capability to create and enable unique access and views for different team members based on their roles. It provides a user interface to create and publish dashboards through Kibana and Grafana. It provides the capability to apply for role-based access at the report level, dashboard level, graph level, etc. through Kibana and in the Fineract web app. The platform provides in-built/third-party integration to generate dashboards using drag/drop. ▶ The platform does not have the capability to provide reports for successful settlements, failed settlements, and settlements on hold, detailing the settlement amount, fee and tax breakdown, and reasons for failure or hold. These functionalities are not planned to be included in the future version releases.

Last mile cash-in and cash-out:

Functionality	Maturity	Analysis
Authentication	0 %	▶ Capabilities to support 'Know Your Customer' (KYC) utilities, authentication of the beneficiary against his/her bank account, validate a beneficiary by giving a thumb impression or electronic signature to receive the money, are not present in the Mifos and is not being planned in the future version releases.

Functionality	Maturity	Analysis
Enabling cash out, cash deposit, and fund transfer	0 %	▶ Capabilities to allow a beneficiary to withdraw money by giving a thumb impression or electronic signature, online transactions at Micro ATM/Kiosk/mobile devices through the authorized Business Correspondent (BC) of any banks, transfer funds from one account to another account (own or other) are not present in Mifos and is not being planned in the future version releases.
Cash management	100 %	▶ The platform has the capability to provide the operational and banking processes for the collection, aggregation, holding, and disbursement of cash and the capability for reconciliation for detailed visibility into cash availability, accurate reporting, etc. It can simultaneously process cash and card payments. ▶ The platform has a module for handling cash reconciliation and reporting. It does not support offline transactions and batch processing. ▶ The platform can provide real-time reporting and tracking of cash collections. It can generate invoices and receipts for customers and has the ability to track inventory levels and update them post transactions.

ID Account Mapper:

Functionality	Maturity	Analysis
Institution registration	100 %	▶ Mifos supports issuing of a unique Institution Identification Number (IIN) to the institution upon successful registration in the ID account mapper database ▶ The platform has a registering institution ID field that helps in identifying the institution that has registered a particular record in the account mapper service. This functionality is customizable, but not configurable and extensible. ▶ There are APIs available to populate the Account Mapper with beneficiary data. However, it does not have APIs to populate and get IIN from the AM Service. Currently, the setup of IIN is back-end configurable. ▶ In order to prevent unauthorized access, JSON Web token (JWT) authentication is being used.

Functionality	Maturity	Analysis
Identifier ID linking and update	100 %	▶ Mifos is capable of accepting consent (physical/digital form) for linking identifier ID with a single financial address (no dual mappings) in the account mapper database and verification of resident identity using various authentication methods like OTP, Yes/No, e-KYC, etc. The ID Account Mapper has interfaces to populate and update records. These records can be updated as Active or Inactive and cannot deleted from the mapper. ▶ Currently, the platform does not store data for linking with other systems, but this can be extended easily.
Identifier ID linking	0 %	▶ The ID account mapper service is not built to validate financial addresses on their type. As an assumption, it assumes the information passed in the financial address is both valid as well as authentic. The authenticity is not ensured by the ID Mapper itself.
Linking status	0 %	▶ The ID Account Mapper does not provide any interfaces to query information from any external source.
Identifier ID un-linking	100 %	▶ Mifos has the capability of unlinking the inactive accounts in the ID account mapper database and records can be updated as Active or Inactive. The records cannot be deleted and has no automatic de-linking capabilities. At the business level, there are no functional reports planned for monitoring purposes, however, logs are available. This functionality is customizable but not configurable and extensible.
Mapping reconciliation	0 %	▶ This is not applicable to Mifos. The vision of the account mapper is not of one where information is shared between a financial core banking and the account mapper. In fact, the account mapper only identifies individual users through a token that is never shared with FSPs.

Functionality	Maturity	Analysis
Notification	0 %	▶ The capability to send notifications such as linking/ update/unlinking of identifier ID with a financial address in the ID account mapper database etc. is not applicable for Mifos. It does not perform any task other than its core function. If notifications of updates to information have to be provided, they have to be handled elsewhere as a result of API responses, which the account mapper may provide to the seeding or orchestrating service.

Implementation record

Over 20 million individuals have registered on Mifos through more than 500 institutions spanning across 63+ countries. The Mifos & Fineract core banking and account management platform, catering to use cases in microfinance, financial inclusion, loan management, and wallet management, has been successfully deployed in 65 countries across various regions, including Latin America & Caribbean, Sub-Saharan Africa, SE Asia, South Asia, MENA, Europe, North America, and Oceania. Additionally, Payment Hub EE, designed for use cases like integration with RTP systems like Mojaloop, mobile money integration, and bulk G2P payment processing, is actively operational in four countries: Brazil, India, Kenya, and Mexico. Presently, Mifos is interconnected with several DPGs such as Fineract, Mojaloop, MOSIP, OpenG2P, OpenSPP, and Open IMIS, with forthcoming integration plans involving two additional DPGs, namely Core MIS and X-Road.

3.4.2 Technical fitment

Functionality	Maturity	Analysis
Architecture and NFR		
Platform approach	100 %	▶ Mifos payment system is designed with a ‘microservices first’ strategy. The solution uses microservices that distribute the system into loosely coupled and highly cohesive modules. ▶ The solution is platform agnostic. Fineract has built-in support to run on-premises and with cloud data centers. The solution supports multitenancy with data isolation at the database level. This is a core feature of both Fineract and Payment hub. ▶ The system uses semantic versioning for releases and uses GitHub releases to manage each release tag. System upgrade in terms of database happens automatically with the help of migration scripts as the new version is deployed. The system supports configurability in multiple levels like deployment level configurability using HELM charts, system level configurability to setup system-level, etc.

Functionality	Maturity	Analysis
API-first design	100 %	▶ The solution has key functionality exposed by APIs and follows Open API specs. The Solution has well-documented APIs which are updated automatically using Swagger, APIs are designed to be secure using SSL and also support API Governance through the API GW Kong. The solution supports synchronous APIs, asynchronous APIs with call-backs and polling, and Webhooks, etc. are also available. API versioning is also present. Mifos has a sandbox environment for Fineract. The platform exposes all its functionality via a RESTful API, which communicates using JSON.
Data architecture	100 %	▶ The Mifos has followed the data anonymization principle by using a masking filter which is configurable. The data architecture separates different layers by orchestration engine/RaftDB for transactional and workflow data. RDBMSs and ES for operational and audit data. ES for analytical data. MDM is managed through Helm. The solution provides data security by encrypting the fields and providing security for data in motion by TLS, non-repudiation/JWS, and idempotency. The solution uses ES for indexing, searching, and analytical purposes. The solution is a completely asynchronous architecture with support for GRPC supports low latency and Kafka, ES, RaftDB, and Redis supports high volume.
Trust and security	75 %	▶ The Mifos has Keycloak and Kong Plugins to support different OIDC providers and also supports pluggable multiple authentication systems by using spring security-based plugins. The solution has an audit, maker/checker, eventing and observability framework, and other features that support monitoring user behavior & services, but the device monitoring is limited. The solution has cryptographic algorithms such as JWS, RSA, SHA256, and Blowfish for encryption/hashing during transit. A masking feature is present to prevent sensitive data storage. The solution has different logging levels such as ERROR, WARN, INFO, DEBUG, and TRACE. Memory management is used in the majority of places.
Privacy	13%	▶ Mifos has used cryptographic algorithms to keep the privacy of personal information protected. ▶ Capabilities like consent management framework, support for federation and horizontal scalability, use of consent management for each functionality and supporting reusability, customization of consent framework for various functions (timeframe, apply, revoke, auto-expiration, etc.), support for the right to be forgotten are not available and not planned for future release. The solution does not conduct privacy risk assessments regularly and does not follow principles of data minimization.
Performance and scalability	100 %	▶ Mifos performance KPIs encompass portfolio quality, loan portfolio, and client outreach metrics, including portfolio at risk, loan disbursement rate, and active clients. These indicators help evaluate operational efficiency, financial sustainability, and social impact while ensuring regulatory compliance. The solution utilizes deployment strategies like continuous integration and monitoring tools to maintain scalability and performance.

Functionality	Maturity	Analysis
Analytics and data-driven decision support (Unified scheme view)	83 %	▶ The Mifos solution captures the telemetry data using an elastic search database, Prometheus, and Grafana. The solution uses Kibana for visualizations. The sensitive data is masked in analytical databases to provide maximum visibility to processes without violating data security. The solution approaches different dashboards for data visualization.
Integration capabilities		
Interoperability	70%	▶ The solution supports file-based integration by bulk API with CSV upload and has swagger implemented. The solution supports message-based integration by Hooks. The solution has Zeebe to support service orchestration and has data pipeline architecture.
Code and release management maturity		
Code repository management	67 %	▶ The Mifos solution has source code under public GitHub with contributor profiles. The solution has some rules and checklists to ensure code quality and code coverage, along with code review and analysis check style rules. The solution provides metrics and analytics for tracking code repository activity and usage.
Release management	75 %	▶ The solution uses JIRA for planning and scheduling of releases. In the solution, minor version releases are given after every sprint (in two-week intervals). The solution has a code repository (GitHub) and issue tracking system (JIRA) which are integrated to provide easy tracking, and the issue is updated with the links to the code change. For CI and GitHub checks, CircleCI is used to build and test the code changes before they are added to the code base.

Functionality	Maturity	Analysis
Configuration management	100 %	▶ The Mifos solution supports the automation of configuration management tasks, such as server provisioning and configuration updates by having integration with Helm, Kubernetes, and AWS. The solution is integrated with JIRA, and CircleCI for code repository management and issue tracking systems and also allows for the management of multiple configuration profiles for different projects and environments.
Operational maturity		
Deployment	100 %	▶ The solution uses CircleCI integrated with Git to support automated testing and deployment. The solution also supports various ways of deployment and in the payment hub K8s is preferred. The solution provides centralized logging and monitoring capabilities through Elasticsearch and Kibana. The solution has integration with Jenkins and CircleCI for CI/CD. For large/small scale deployments the solution has helm charts that are maintained and parameterized.
Monitoring	100 %	▶ The solution uses Prometheus, Grafana, and Kibana for operational monitoring. To support real-time monitoring of various data sources solution uses an ELK/EFK stack. AWS CloudWatch and Graphana dashboards are integrated with a solution to have an alerting mechanism to notify administrators in case of anomalies or threshold breaches. The solution also provides customization for threshold levels using an API gateway. The solution also provides detailed visualization and reporting capabilities to understand the monitored data and identify trends and patterns.
Support	33 %	▶ Mifos provides L3 support for critical vulnerability resolution through partners and system integrators. The solution has planned financial method inclusion in the system.
Documentation maturity		

Functionality	Maturity	Analysis
Enterprise documentation	90 %	▶ The solution provides general overview documentation on a public site. It has easily available architecture and infrastructure documentation, and installation documentation for various environments and solutions for public/developer/ other stakeholders. There are examples of screenshots included in the documentation to help illustrate the solution and clear instructions are provided on how to use the solution and troubleshoot any issues that may arise. The solution has made administrator guides, functional use cases, and design docs available. It also provides a knowledge repository.

3.5. MOSIP

Integrations present with | OpenG2P | OpenCRVS

MOSIP, which stands for Modular Open-Source Identity Platform, provides the foundation for countries to develop a robust, scalable, and inclusive digital identity solution providing unique digital ID for all residents. MOSIP is built on an open-source framework, making its source code freely available to the public. This open approach fosters collaboration and innovation, allowing governments and organizations to customize and adapt the platform to their specific needs. With a modular architecture, MOSIP can be easily customized and extended to meet the unique requirements of different identity ecosystems. This flexibility allows for the integration of various identity components and services seamlessly. Security and privacy are paramount in identity management, hence focus on privacy and security is essential for building trust in identity systems. MOSIP incorporates robust security features and follows best practices to protect individuals' personal information and ensure data integrity. MOSIP also enables interoperability allowing secure data sharing and seamless integration between different identity platforms, enabling governments and organizations to create a unified and efficient identity ecosystem. Being an open-source DPG, MOSIP significantly reduces the cost of developing and implementing identity management systems. Governments and organizations can leverage MOSIP to save resources while ensuring robust and secure identity services. Localization of MOSIP modules through customization to cater to specific cultural, legal, and operational requirements makes it a valuable tool for governments to implement identity solutions tailored to their unique circumstances. These features make it a versatile and cost-effective solution for governments and organizations aiming to provide secure and inclusive identity services to their populations while adhering to international standards and principles of privacy and security.

This section provides a summary of MOSIP’s self-assessment across the assessment parameters, followed by a detailed representation of the functional fitment and the technical fitment which covers architectural coherence, compliance with non-functional requirements, integration potential, the maturity of code and release management processes, operational preparedness, and the quality of documentation.

Legend

Functional Fitment

The functional fitment dimension helps identify if the solution has the capabilities that allows governments, to quickly fulfil their immediate G2P, needs modularly.

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

This dimension block, in the summary provides an analysis on the strength/ maturity of the module with respect to the answers provided. The percentages are calculated based on the number of functionalities present in the module as against the functionalities that should ideally be present

Integration Capabilities

The integration capabilities dimension provides an understanding on how interoperable the solution is with other building block

✓ Present 📈 Planned ☒ Not Available N/A Not Applicable

This dimension block in the summary provides an analysis on the functionalities that are present, planned or not available and not applicable in the solution

Architecture and NFR

The Architecture and NFR dimension provides an analysis if the solution uses modern design paradigms, architectures and technologies

This dimension block in the summary provides the maturity of the dimensions under architecture and NFR. The percentages are calculated based on the number of functionalities present in the module

Documentation Maturity

The documentation maturity provides an analysis, if the solution documentation is easy for a nascent/ fledgling vendor to understand, so that the ecosystem scales up quickly

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

This dimension block provides an analysis on the strength of the capability . The percentages are calculated based on the number of functionalities present in the module

Code and Release Management Maturity

The code and release maturity dimension provides an overview if the solution code is structured and well-managed, modular, well-written - so it can be easily understood and modified, if required

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

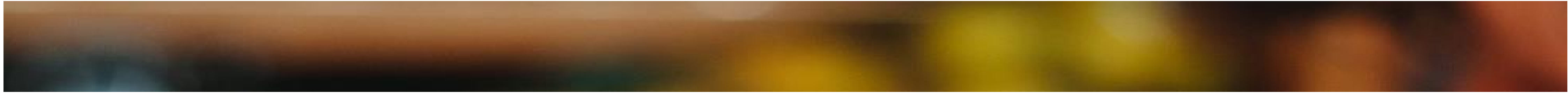
The dimension block in the summary provides an analysis on the strength of the capability . The percentages are calculated based on the number of functionalities present in the module

Deployment

The deployment dimension provides an overview of the pilots conducted by the solution in various countries showcasing its strength, learnings and challenges faced.

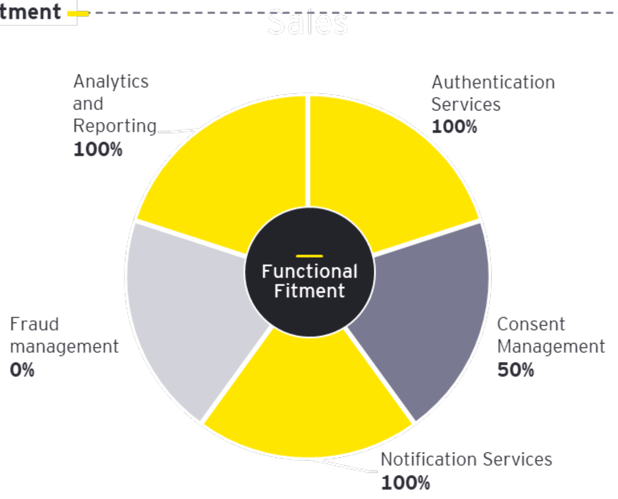
📍 Implemented 📍 Interested in Implementing

This provides the countries the solution has been implemented, or interested in implementing being show by a country to deploy the solution



Digital Identity Management for G2P Connect using MOSIP

Functional Fitment



Operational Maturity

Deployment

- Automated testing and continuous integration including automated deployment and roll-back
- Blackbox testing and high-test coverage
- Support containers and VMs
- Support Centralised logging and monitoring capabilities
- Large scale distributed deployments with ease, supporting growing organisations
- CI/CD via GitHub actions

Monitoring

- Built on principles following scalability, minimizing latency, security and privacy, flexibility, automation, accessibility, optimization, and standardization
- Real-time monitoring of various data sources
- Alerting mechanism to notify administrators in case of anomalies
- Customizable alert rules and threshold levels
- Visualization and reporting capabilities

Support

- L3 Support for critical vulnerabilities resolution based on MOU
- Financial method inclusion not applicable
- SLA associated for critical issue resolution in core system not applicable

Challenges and Learnings

- Multiple issues in hardware in terms of slowness of disk speed, network issues, old hardware and old software etc
- Delay in rolling out registration clients in multiple centers. Issues in registration client crashes
- IRISs of residents in various cases were summarily rejected by ABIS due to template extraction issue citing poor quality biometrics.
- Successfully implemented new features like USSD feature, QR Code scanning of Pre-reg from reg client, Pre-registration Migration Utility, Tools for analysing corner cases and monitoring, Multi-language feature, Anonymous profile feature, etc.

Integration Capabilities

☑ Data exchange with external systems in non-proprietary and recognized formats

☒ File based integration

☑ API-based integration

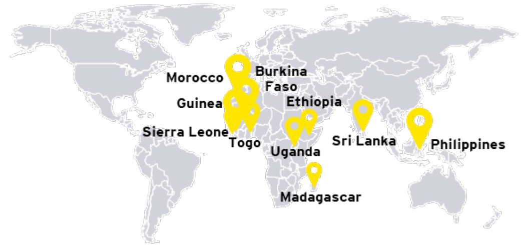
☑ Message-based (Event driven) integration

☑ Service orchestration

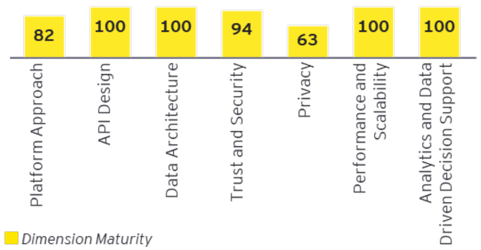
☑ Integration for telemetry dataset for downstream systems

☑ Data pipeline architecture

Implementations



Architecture and NFR



Code & Release Management Maturity

Code and Repository Mgmt.	Release Mgmt.
Strong	Strong
Configuration Mgmt.	**Documentation Maturity**
Strong	Strong

Impact

People registered on MOSIP = **100+ million**

3.5.1 Functional fitment

MOSIP is based on several foundational principles and technologies. MOSIP’s modular architecture enables independent development, deployment, and updates of different components and modules. It is designed to handle a wide range of identity-related functions, from registration and authentication to data management and verification. Its scalability ensures that it can cater to identity ecosystem implementations catering to both small and large populations, with the required customizations as per the needs.

MOSIP 1.2.0 includes various modules such as:

Administration - Exclusively accessible to a select group of authorized administrative staff through Management of resources via CRUD operations and Registration administration

Automation Testing - MOSIP provides automation test repositories for all UI components, Registration Client, Functional Tests, End to End Automation Tests

Artifactory - The artifactory stores various libraries that modules can dynamically download during runtime.

Commons – This encompasses all the shared services, sometimes referred to as the "kernel," that are utilized by various other modules within MOSIP.

Datashare - The Datashare service facilitates the sharing of data with trusted services and partners, and this data sharing process is governed by the Datashare policy.

ID Authentication Services - Constructed as a standalone service capable of being populated with authentication data by MOSIP encompasses the following services like Authentication Services, OTP Service, Internal Services

ID repository - The ID Repository houses an individual's identity records and offers an API-based mechanism for other MOSIP modules to store, retrieve, and modify identity information.

Inji - The MOSIP Resident app, a mobile application, serves as a digital wallet that that enables storage and offline sharing of various forms of identification and verifiable credentials.

KeyCloak - This is an opensource identity and access management (IAM) application which is integrated with MOSIP. KeyCloak provides strong authentication methods, including multi-factor authentication (MFA) and single sign-on (SSO).

Key Manager - The Key Manager Service can connect with an HSM and offer a secure repository for storing, provisioning, and management of secret keys.

Packet Manager - Packet Manager can connect to any object store and performs the functions like Manages the reading and writing of registration packets to and from the Object Store, Conducts in-memory encryption and decryption of packets, Enforces security checks, checksum verifications, and Furnishes packet-related information to other services through APIs.

Partner Management - Partner Management Services (PMS) module through services like Partner Management Service and Policy Management Service

Config Server - MOSIP uses Spring Cloud Config Server that shares module-specific properties with all MOSIP modules.

Pre-Registration - Pre-registration module enables a resident to provide demographic information and upload relevant supporting documents, schedule appointments for single or multiple users, selecting a suitable registration center and a convenient time slot, receive notifications regarding scheduled appointments, adjust or cancel appointments as needed.

Reference Implementations - Reference implementations of modules or components are prototypes that are not intended for production use but serve as demonstrations of a reference design or architecture.

Registration Client - The Registration Client is a robust Java-based application used for collecting a resident's demographic and biometric information, along with the necessary supporting documents, whether in online or offline mode.

Registration Processor - The Registration Processor (Regproc) serves as a backend processing engine designed to facilitate ID Lifecycle management.

Reporting - MOSIP offers a reporting framework that enables the real-time streaming of data and its visualization.

Resident Portal - The Resident Portal is a web-based user interface application that offers residents within a country a range of services associated with their Unique Identification Number (UIN).

Persistence –

- Postgres DB - MOSIP uses Postgres DB for all relational data storage.
- Object Store – It functions as an abstracted storage layer utilized by various parts of the system.

WebSub - WebSub offers a universal means of communication between content publishers of all types and their subscribers, utilizing HTTP web hooks as the foundation.

An assessment was conducted to examine MOSIP's functionalities, focusing on their relevance in a G2P payments context. The specific functionalities under assessment included ID authentication services module and other supporting modules such as consent management, notifications, fraud management, analytics, and reporting. The assessment also considered the extent to which these functional capabilities catered to the needs of various stakeholders, including implementing agencies and residents. Additionally, these capabilities were evaluated for their potential towards customization, configuration, or extensibility. A summary of the assessment findings, including what is present or has been planned for implementation in upcoming releases is provided below.

Functionality	Maturity	Analysis
Authentication services	100 %	▶ MOSIP provides identity verification services that empower individuals to utilize their identity across diverse scenarios. Following the successful issuance of an ID, these identity verification services become accessible to the resident. ▶ Online authentication - Capability to support authentication (Yes/No) – MOSIP allows online authentication using APIs, and supports OpenAPI capabilities to support authentication using security schemes. Single factor and multi-factor authentication are configurable in SSO, and recovery mechanism is available to reset multi-factor authentication. This functionality can be customized and is configurable. ▶ Online authentication - Capability to support e-KYC - MOSIP allows online authentication to support e-KYC using API. This functionality can be customized and is configurable to accommodate for the appropriate laws and regulations. ▶ Offline Authentication - Capability to support QR-based authentication – MOSIP allows offline QR based authentication. This capability supports the generation of a QR code which can be used as plug and play component, and can be easily integrated into other systems and processes. This functionality can be customized and is configurable. ▶ Capability to support authentication through Virtual IDs – MOSIP has the capability to support authentication through Virtual IDs using APIs. These APIs follow OpenAPI standards and provide configurability to measure authenticity of virtual IDs. MOSIP also supports managing scenarios where a virtual ID is lost, stolen, or compromised. This functionality can be customized and is configurable. ▶ Capability to uniquely identify a resident using token IDs – MOSIP offers the functionality to share a unique token ID with the resident and the associated relying party post authentication. However, this functionality is configurable but is not customizable. ▶ Validation of biometric devices used for biometric authentication – MOSIP has defined a standard called the secure biometric interface (SBI) which is used to integrate with various biometric devices to support authentication with different biometric modalities. However, this functionality is configurable but is not customizable.
Consent management	50%	▶ MOSIP offers the capability for individuals to provide their consent for the collection, use, storage, and sharing of their personal data. This is a customizable functionality with options available for users to manage their consent preferences. The solution provides configurability to ensure that user consent is honored, and personal data is used only in accordance with user preferences. This functionality is customizable can be modified, adjusted, or tailored to meet specific requirements, preferences, or needs. ▶ The capability to manage consent submitted by the residents - record, revoke, etc. is not present currently. However it is planned for the future.

Functionality	Maturity	Analysis
Notifications	100 %	▶ MOSIP offers the ability to provide notifications to the residents about the various events in the ID lifecycle including authentication status, etc. Engine support channels such as SMS, Email and WebSub are used for delivering notifications however depending on the system integrator, the notification delivery failures are handled differently. For example, WebSub handles delivery failures by retrying. It also supports personalized notifications and dynamic content through data share and velocity templates, and failover in WebSub is auto handled. ▶ These functionalities are customizable and can be modified, adjusted, or tailored to meet specific requirements, preferences, or needs.
Fraud management	0 %	Capabilities used to detect, monitor, and reduce fraud in the registration and authentication processes, and capabilities used to identify and flag outliers as suspicious activity (e.g., anomalous, synthetic, gummy, or non-live biometrics) for further investigation are currently not present and are planned for the future. While MOSIP does not explicitly have any fraud system implemented, implementing fraud management strategies are considered highly critical as it helps organizations to detect and prevent fraud, as well as form an understanding of which areas are more susceptible to fraudulent attacks. MOSIP provides hot list APIs which can be used to hot list relying parties, UINs, VIDs, and devices (using serial numbers) and block them from performing authentication. These APIs can be integrated with any fraud or anomaly detection system to prevent fraud. ▶ MOSIP has numerous validations at various stages that help in taking preventive actions against frauds. e.g., operator validation (biometrics based) during registration of an individual using registration client, supervisor’s approval for registrations that have biometrics exceptions, supervisor’s review & approval prior to uploading each packet, server-side checks to validate operator & supervisor details as part of the operator validator stage and supervisor validator stage, and so on. ▶ Additionally, MOSIP has a workflow mechanism that enables tagging of records as well as creating anonymous profiles, which can be used by policymakers to take corrective measures as and when required. MOSIP also provides the capability to plug in various external systems like fraud management systems. ▶ Tags and anonymous profile data can be analyzed to identify fraud using various pluggable mechanisms. Once a fraud is identified, which could be a registration centre/registration officer/registration machine/biometric device/authentication partner (relying party), the entity can be hot listed or deactivated in MOSIP. The registration or authentication by/for that entity would be withheld. ▶ As part of the authentication service, MOSIP has the feasibility to share data with respect to failure responses with external fraud detection systems via webhooks, to identify frauds. Countries can plug-in fraud management systems to handle such frauds. ▶ Frauds can also be reported by citizens using the grievance management system, as implemented by a Country.

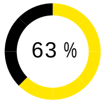
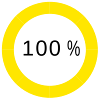
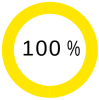
Functionality	Maturity	Analysis
		Data extracted through these mechanisms of external systems can be fused back into MOSIP for preventive action such as hot listing the UIN/VID/partner/auth device, etc., thus, accommodating fraud detection.
Analytics and reporting	100 %	MOSIP's analytics and reporting capabilities are essential components of the platform that allow governments and organizations to derive valuable insights from their identity data. MOSIP offers the following capabilities which are customizable, configurable and can be extended. ▶ Capability to create reports and dashboards to highlights the performance and operations of the pre-registration, registration, profiles of residents in the registration phase and unique ID issued and authentication phases through charts & numbers. ▶ Capability to create combined dashboards- highlights the comparison of pre-registration, registration, unique ID issued, and authentications transactions. ▶ Capability to enable exporting reports and dashboards to excel files.

Implementation record

The total number of residents registered on MOSIP has reached 100+ million. MOSIP has been successfully adopted by 10 countries, each at different stages of deployment. These countries include Burkina Faso, Ethiopia, Guinea, Madagascar, Morocco, Philippines, Sierra Leone, Sri Lanka, Togo, and Uganda. Learnings from these implementations have been integrated into their respective systems. Several of these countries have expressed interest in integrating their ID systems with social protection programs and civil registries. The countries are actively pursuing integrating MOSIP with various DPGs related to Civil Registration and Vital Statistics (CRVS), social benefits registry, etc.

3.5.2 Technical fitment

Functionality	Maturity	Analysis
Architecture and NFR		
Platform approach	82 %	▶ MOSIP is designed to support microservices based architecture and support agnostic for deployment like on-premises data centers, hybrid, private/public cloud, PaaS etc. ▶ It is designed to support modularity and scalability of modules in silos. The solution handles updates and versioning for different releases and it is tailored for system/component upgrade. ▶ It is designed to support operations in low network areas and other related constraints. It supports configurability and extensibility to meet future needs without altering the existing code. ▶ MOSIP is in the pilot phase in seven countries, and is live in three.
API-first design	100 %	▶ MOSIP is designed to expose key functionalities as APIs following Open API specifications and offer well-documented API where new functionalities can be added easily through the API. ▶ The solution follows data privacy principles to ensure implementation of secure APIs. ▶ It supports API governance, synchronous/asynchronous/webhook/WebSocket API communications, API versioning management for backward compatibility and forward innovation, sandbox support to perform API testing. ▶ The APIs are designed as headless API.
Data architecture	100 %	▶ MOSIP follows data anonymization principle for confidential information. The logical data architecture allows for layers of separation across transactional, workflow, operational, audit, analytical and master data management (MDM) data. ▶ Solution provides data security using encryption and data integrity, security for data-in-motion. ▶ It provides data layer scalability to support MPP and uses different technologies for functionalities such as indexing, searching, analytical etc. ▶ MOSIP is designed to manage low latency – high volume and vice versa with specific software technologies and provide detailed document granularity with respect to each attribute defined.
Trust and security	94 %	▶ MOSIP application is internally controlled using OpenID and OAuth 2.0. Apart from that all the dockers are signed which ensure zero trust architecture principle. ▶ It is designed for user authentication and support different pluggable authentication systems. ▶ The solution clearly articulates scope / role capabilities for each functionality which is decoupled from main business logic. The solution offers configurability to monitor user behavior, devices, and services. ▶ It ensures strongly typed, sanitized, and parameterized input/queries, and provides sanitization and encoding of all outputs, including error messages, to prevent unintended disclosure of confidential or internal information.

Functionality	Maturity	Analysis
		▶ MOSIP provides session management controls which ensure random session identifiers using JWT and sessions are managed using KeyCloak or any equivalent to ensure new session identifier on re-authentication and ensure termination of session identifier post logout. ▶ It provides non-repudiation using digital signatures. ▶ The solution uses cryptographic algorithms for encryption/hashing during transit or at rest. ▶ MOSIP has an inbuilt plugin for antivirus to whitelist file format and limit file size for uploading documents. It ensures coverage of all the assets while logging for different levels like info, debug, and error errors without storing any confidential data. ▶ MOSIP conduct vulnerability assessment and penetration testing (VAPT) of application, API & infrastructure, and secure configuration review of your network & security devices. Third party and research academicians regularly review the MOSIP code and publish reports.
Privacy		▶ MOSIP provides a consent management framework which is designed to be used for each functionality and supports reusability. It protects personal information through encryption, and follows principles of data minimization. Institutes like Alan Turing, CMU, IIITB and third-party organizations conduct privacy risk assessments regularly to identify and mitigate potential privacy risks.
Performance and scalability		▶ MOSIP provides various performance KPIs, and numerous test strategies at ecosystem scale which include automation and deployment. The capability of the platform was tested and validated in real-world scenario (Philippine)
Analytics and data-driven decision support (Unified scheme view)		▶ MOSIP captures telemetry data. It follows data anonymization and aggregation for specific usability for analytical functionalities. It provides configurability for JSON based open data capabilities, data warehousing, and supports business intelligence and dynamic reporting capabilities like web-based querying, and dashboards. It is integrated with Kibana for data visualization.
Integration capabilities		

Functionality	Maturity	Analysis
Interoperability	86 %	▶ MOSIP allows exchange of data with other systems in a format that is widely recognized and non-proprietary. It supports API-based integration, message-based (event driven) integration, and service orchestration. It provides integration for telemetry datasets for downstream systems and data pipeline architecture.
Code and release management		
Code repository management	100 %	▶ MOSIP source is under public git with contributor profiles. All code contributions go through an approval process which is enforced through GitHub settings. Also, automated code reviews are enabled which are part of the release gate process. The solution adheres to code quality and code coverage best practices along with static code analysis, code review, and security reports. It allows for branch management and merging of code changes, and provides metrics and analytics for tracking code repository activity and usage.
Release management	100 %	▶ MOSIP support planning and scheduling of releases like product backlogs, and innovation functions for future release using Jira. It provides a Docker and helm-based mechanisms for managing the risk of releases, such as rollback plans. It supports integration with other development tools such as code repository management, CI/CD, and issue tracking systems through Jira and GitHub actions.
Configuration management	100 %	▶ MOSIP support automation of configuration management tasks, such as server provisioning and configuration updates. It also supports integration with popular configuration management tools such as Puppet, Chef, and Ansible, and allows integration with other development tools such as code repository management and issue tracking systems. It allows for the management of multiple configuration profiles for different projects and environments.
Operational maturity		

Functionality	Maturity	Analysis
Deployment	100 %	▶ MOSIP provides automated testing and continuous integration, including automated deployment and rollback capabilities, Blackbox testing and test coverage. It supports various deployment models like containers, virtual machines, serverless. The solution provides centralized logging and monitoring capabilities to support rapid identification and resolution of issues. It uses Helm to manage large-scale, distributed deployments with ease, and support the needs of growing organizations and integrate with popular CI/CD tools like Jenkins, Travis CI, and CircleCI through GitHub actions.
Monitoring	100 %	▶ MOSIP provides real-time monitoring of various data sources like logs, metrics, events. It has an alerting mechanism to notify administrators in case of anomalies or threshold breaches and provides customization for alert rules and threshold levels to meet specific needs. The solution ensures detailed visualization and reporting capabilities to understand the monitored data and identify trends and patterns.
Support	100 %	▶ MOSIP provides L3 support which is done based on MOU.
Documentation maturity		
Enterprise documentation	100 %	▶ MOSIP provides general overview documentation, architecture and infrastructure documentation, and environments, and solutions documentation. It uses GitHub repository state and version of documentation updates. The documents are easily accessible for the public/developer/other stakeholders. For example, screenshots and instructions are included in the documentation to help illustrate the solution and troubleshoot any issues that may arise. It provides administrator guides, functional use cases, design docs. It also provides knowledge repository using Jira.

3.6. Sunbird RC

Integrations present with	ABHA	Aadhaar	DigiLocker	Academic Bank of Credit	National Academic Depositary (NAD)

Sunbird RC, open sourced under the MIT license, is a versatile and adaptable software solution designed for the swift creation and deployment of cutting-edge electronic registries and verifiable digital credentials, encompassing both attestation and verification workflows.

Sunbird RC is a “low code” framework, empowering organizations to expedite the development of next-generation electronic registries. Leveraging a collection of configurations, this platform allows for the rapid construction of registries, automating the generation of CRUD (create/read/update/delete) APIs without the need for manual coding. Furthermore, it facilitates registry searches and access through open APIs, offers tools for issuing and managing verifiable credentials, provides the means to manage user consent processes if necessary, and enables the oversight of attestation and verification workflows. Sunbird RC offers out-of-the-box capabilities for issuance, management, and verification of digital verifiable credentials.

Sunbird RC is recognized globally as a digital public good (DPG) and is listed within the Digital Public Good Alliance (DPGA) registry. It adheres to the DPG standard, ensuring privacy and compliance with relevant best practices, while also being designed with a commitment to do no harm. The platform holds great significance in advancing the United Nations 2030 Sustainable Development Goals (SDGs).

Sunbird RC serves as the foundational engine within DIVOC, a globally acclaimed DPG used for vaccination and health credentialing. Moreover, it plays a pivotal role in India's extensively adopted DIKSHA school education platform, which runs at a population-wide scale.

Under the MIT license, Sunbird RC is openly available for use by individuals and organizations alike, free of charge. We strongly encourage active participation in the community and invite contributions to further enhance and refine this remarkable project.

This section provides a summary of Sunbird RC’s self-assessment across the assessment parameters, followed by a detailed representation of the functional fitment and the technical fitment which covers architectural coherence, compliance with non-functional requirements, integration potential, the maturity of code and release management processes, operational preparedness, and the quality of documentation.

Legend

Functional Fitment

The functional fitment dimension helps identify if the solution has the capabilities that allows governments, to quickly fulfil their immediate G2P, needs modularly.

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

This dimension block, in the summary provides an analysis on the strength/ maturity of the module with respect to the answers provided. The percentages are calculated based on the number of functionalities present in the module as against the functionalities that should ideally be present

Integration Capabilities

The integration capabilities dimension provides an understanding on how interoperable the solution is with other building block

✓ Present   📈 Planned   ☒ Not Available   N/A Not Applicable

This dimension block in the summary provides an analysis on the functionalities that are present, planned or not available and not applicable in the solution

Architecture and NFR

The Architecture and NFR dimension provides an analysis if the solution uses modern design paradigms, architectures and technologies

This dimension block in the summary provides the maturity of the dimensions under architecture and NFR. The percentages are calculated based on the number of functionalities present in the module

Documentation Maturity

The documentation maturity provides an analysis, if the solution documentation is easy for a nascent/ fledgling vendor to understand, so that the ecosystem scales up quickly

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

This dimension block provides an analysis on the strength of the capability . The percentages are calculated based on the number of functionalities present in the module

Code and Release Management Maturity

The code and release maturity dimension provides an overview if the solution code is structured and well-managed, modular, well-written - so it can be easily understood and modified, if required

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

The dimension block in the summary provides an analysis on the strength of the capability . The percentages are calculated based on the number of functionalities present in the module

Deployment

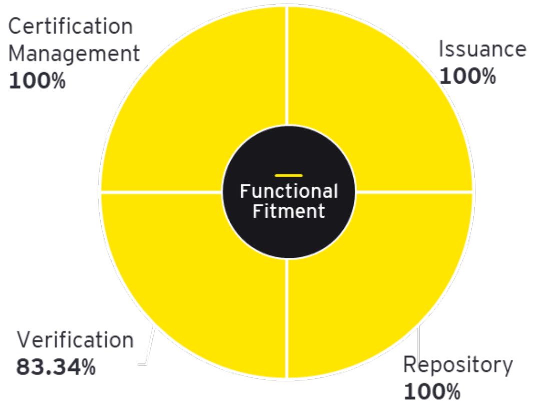
The deployment dimension provides an overview of the pilots conducted by the solution in various countries showcasing its strength, learnings and challenges faced.

📍 Implemented   📍 Interested in Implementing

This provides the countries the solution has been implemented, or interested in implementing being show by a country to deploy the solution

Digital Credentialing for G2P Connect using Sunbird RC

Functional Fitment



Operational Maturity

Deployment

- Does not support automated testing , continuous integration, automated deployment & roll-back
- Supports Blackbox testing and high-test coverage
- Support containers and virtual machines deployment
- Supports large scale deployment supported, scalability and distributed deployment
- Supports integration with CI/CD tools

Monitoring

- Does not support design considerations for monitoring, auditing, telemetry and analytics
- Supports real-time monitoring of various data sources
- Does not provide customization for alert rules and threshold levels for specific needs
- Does not have alerting mechanism for notifying administrators in case of anomalies
- Does not have virtualization and reporting capabilities

Support

- Does not provide L3 support for bug fixes and customisation
- No SLAs for critical issue resolution in core system
- No Financial method. Solution is free for use

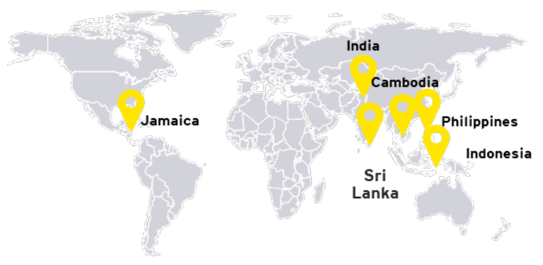
Challenges and Learnings

- Multi-tenancy support: Currently, Sunbird-RC allows multiple issuers to issue credentials within a single installation. However, it does not permit multiple issuers to issue credentials based on the same schema.
- Key Rotation/Storage: Sunbird-RC does not offer the capability to store private keys in secure vaults; instead, they are stored within configuration files. This setup lacks the ability to perform key rotation in cases of key loss.
- Localization: Sunbird-RC currently facilitates registry and credentialing exclusively in English, lacking support for localization in multiple languages.

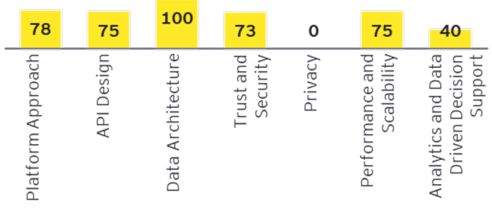
Integration Capabilities

- ✓ Data exchange with external systems in non-proprietary and recognized formats
- ✓ File based integration
- ✓ API-based integration
- ✓ Message-based (Event driven) integration
- N/A Service orchestration
- ✓ Integration for telemetry dataset for downstream systems
- N/A Data pipeline architecture

Implementations



Architecture and NFR



🟨 *Dimension Maturity*

* *Privacy capabilities have a percentage of 50%, however the consent management framework is currently being planned in the next version*

Code & Release Management Maturity

Code and Repository Mgmt.	Release Mgmt.
Strong	Moderate
Configuration Mgmt.	**Documentation Maturity**
Needs Improvement	Strong

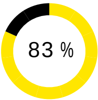
Impact

No of Users/ beneficiaries impacted across six countries: **1 Bn +**

3.6.1 Functional fitment

An assessment was conducted to assess the functionalities of Sunbird RC, with a special focus on their applicability in the context of G2P payments. The specific functionalities under assessment included issuance, repository, verification, and certificate management. Moreover, the assessment considered the extent to which these functional capabilities catered to the needs of various stakeholders, including implementing agencies and residents. Additionally, these capabilities were evaluated for their potential towards customization, configuration, or extensibility. A summary of the assessment findings, including what is currently present or has been planned for implementation in upcoming releases is provided below.

Functionality	Maturity	Analysis
Issuance	100 %	▶ Sunbird RC implements and extends various global standards for verifiable credentials such as W3C VC. ▶ Sunbird RC has the capability to authenticate the requestor's identity. The system has a mechanism for generating token IDs for the requestors, using secure random number generators and unique identifier algorithms, such as UUID or GUID. The platform provides a mechanism for validating the token IDs using validation algorithms and libraries. The system has a mechanism to revoke token IDs in case of any theft, loss, or unauthorized access. ▶ Sunbird RC has the capability to encrypt data using public key infrastructure (PKI) for sharing data and the system allows revocation of certificates. ▶ Sunbird RC has the capability to issue/reissue a digitally signed or machine-readable credential/certificate with a timestamp. The platform offers a mechanism for generating and digitally signing the certificate using certificate generation and digital signature algorithms. It also provides a mechanism to generate a timestamp for each certificate. ▶ It has a secure mechanism in place for the certificates, using databases such as MySQL or PostgreSQL, or cloud-based solutions, such as AWS or Google Cloud. The system has a mechanism for retrieving the certificates using certificate retrieval algorithms and APIs, such as REST or GraphQL. It allows validation of the certificates, using certificate validation algorithms and libraries. ▶ Sunbird RC does not have the capability to raise a request for a digital credential/ certificate or receive a digital credential/certificate from different agencies. It does not plan to include this functionality in the platform in the future.
Repository	100 %	▶ Sunbird RC has the capability to save and store the credential/certificate using wallets or other platforms. The platform does not have secure storage for the credentials/ certificates. It has backup and recovery mechanisms for lost or damaged credentials/ certificates and allows storage of credentials/ certificates as per data privacy regulations such as GDPR or HIPAA. ▶ Sunbird RC has the capability to share the credential/certificate with approved authorities for a certain period using Keycloak authentication, but this feature is not configurable. It provides mechanisms to authenticate the requestor and the recipient of the credential/ certificate to ensure that the right information is shared with the correct authority using API. It has secure sharing mechanisms such as secure file transfer protocols (SFTP), secure socket layer (SSL) encryption, or secure hypertext transfer protocol (HTTPS).

Functionality	Maturity	Analysis
		▶ Sunbird RC has the capability to share credential/certificate in different contexts (public and private) with the required information and this feature can be defined using APIs. Public data attributes are accessible without requiring permission or authorization by default, and all fields are public by default in the platform. Private attributes can be accessed by the owner by default, and with the owner's consent, third parties can access these data fields. However, internal fields, which are used for internal system functions, are never accessible to any actors in the platform. It provides mechanisms to authenticate the requestor and the recipient of the credential/ certificate to ensure correct information is shared with the correct authority using API. The platform provides secure sharing mechanisms such as SFTP, SSL encryption, or secure HTTPS.
Verification		▶ Sunbird RC can read or scan digital certificates for verification, supporting the issuance of verifiable credentials with QR codes. These QR codes can be easily scanned using a verification module or a third-party verifier app, facilitating seamless verification and access to credential information. The platform's NPM module is specifically designed for scanning QR codes within Angular applications. Sunbird RC offers the capability to scan certificates through QR or barcode scanners and can integrate with third-party scanners for enhanced flexibility. Its decryption mechanisms support QR-based authentication, and it provides hooks/events for extending or enhancing the authentication process. ▶ Sunbird RC has the capability to use PKI to verify the digital signature of credentials and certificates. It uses cryptographic keys generated via PKI technology, such as RSA or ECDSA algorithms, to digitally sign the credentials. Verifiers can then use the corresponding public key to verify the authenticity and integrity of the signed credentials. ▶ Sunbird RC has the capability to have QR-based authentication. It has the capability to read or scan credentials. ▶ Sunbird RC has the capability to verify the authority of the Issuing Authority to issue the credential/certificate. This feature can be defined using APIs. It has the mechanism to authenticate the requestor and the recipient of the credential/ certificate to ensure correct information is shared with the correct authority using API. The system has secure sharing mechanisms such as SFTP, SSL encryption, or secure HTTPS. ▶ Sunbird RC has the capability to verify the validity of the credential/certificate. When a credential is issued, it is signed via the issuer's private key. This can then be verified by an issuer's public key which is made available to whoever is trying to verify the credentials. This is taken care of by the certificate-signer service. Certificate signer service provides an API that takes signed credentials as input. From the issuer name, it fetches the public key of the issuer. Using this public key, the verifier verifies the authenticity of the credential. The system has a mechanism for validating the certificates, using certificate validation algorithms and libraries such as X.509 or JWT. ▶ Sunbird RC has the capability to verify the digital signature of the issuer.

Functionality	Maturity	Analysis
Certificate management	100 %	▶ Sunbird RC has the capability to store, retrieve, and manage certificates. It has the capability to implement secure storage for the credentials/certificates, using encryption algorithms, such as AES or RSA. It provides the capability to implement a secure storage mechanism for the certificates, using databases, such as MySQL or PostgreSQL, or cloud-based solutions, such as AWS or Google Cloud. The platform has a mechanism for retrieving the certificates, using certificate retrieval algorithms and APIs, such as REST or GraphQL. ▶ Sunbird RC has the capability to revoke the certificates. Revoke API revokes a verifiable credential by updating the signature data attached to it. This is done by updating the _osSignedData field in the corresponding entity table to an empty string. and storing the signed Data in the revoked credential register. The platform has a mechanism for revoking token IDs in case of loss, theft, or unauthorized access, using revocation lists or certificate revocation services, such as CRL or OCSP. It has a mechanism for renewing token IDs after a certain period of time, to ensure the security and privacy of the requestor's identity. ▶ Sunbird RC has the capability to provide an interoperable credentialing ecosystem. Certificate revocation is handled through the certificate revocation list (CRL). Digital certificates are compatible with W3C's standards. It currently uses digital certificates and/or PKI for authentication and encryption.

Implementation record

More than one billion individuals have successfully registered on Sunbird RC across more than five countries. Currently, Sunbird RC is either operational or in the pilot stage in six countries: India, Sri Lanka, Philippines, Indonesia, Cambodia, and Jamaica for various use-cases ranging from social protection, healthcare, agriculture, education, etc. Sunbird RC incorporates an audit log and infrastructure monitoring mechanism designed to prevent significant and critical fraudulent activities. At present, Sunbird RC is seamlessly interconnected with various digital public infrastructures, including ABHA (Ayushman Bharat Health Account), Aadhaar, DigiLocker, Academic Bank of Credit (ABC), and National Academic Depository (NAD). There are also upcoming integration plans that involve multiple DPGs, such as DIVOC, Sunbird ED, Sunbird Lern, Sunbird Serve, MOSIP, Inji, DIGIT, OpenG2P, etc.

3.6.2 Technical fitment

Functionality	Maturity	Analysis
Architecture and NFR		
Platform approach	78 %	▶ Sunbird RC is a microservices-based architecture with all the services and third-party services built using open-source solutions and can be deployed on many types of infrastructures. All services are modular and scaled independently. All microservices expose Open APIs, which enables developers to build services around them. Sunbird RC services are backward compatible, which handles updates and versioning. It supports custom modules as microservices that wrap around Sunbird RC to provide configurability and extensibility to meet future needs. Sunbird RC also plans to provide solutions tailored for system/component upgrades.
API-first design	75 %	▶ Sunbird RC exposes key functionalities as APIs following Open API Specifications and the APIs are well documented. The APIs are secured by JWT token-based authentication. It supports synchronous/asynchronous/webhook/WebSocket API communications. Sunbird RC itself is versioned, but the APIs versioning is not provided. It provides sandbox support to perform API testing. The API services are headless, and they can be directly used from the UI.
Data architecture	100 %	▶ Sunbird RC follows the data anonymization principle with data mask, hashing, or encryption and is built to support data security (encryption) and data integrity. Data in motion can be secured by HTTPS over TLS/SSL. It uses different technologies for specific functionalities (indexing, searching, analytical, etc.) and is designed to manage low latency - high volume and vice versa with specific software technologies. The solution provides detailed document granularity with respect to each attribute defined.
Trust and security	73 %	▶ Sunbird RC follows the zero-trust architecture principle and uses Keycloak for user authentication; it also supports custom adapters for other OAuth2 and OIDC authentication providers. The solution clearly articulates the scope/role capabilities for each functionality. It leverages the functionalities of Java SpringBoot and Swagger Code Gen to build out services that automatically take care of validations, and sanitizations and also support sanitization and encoding of all outputs including error messages to prevent unintended disclosure of confidential or internal information. The user session is managed with JWT Tokens which ensure random session identifiers, generating new session identifiers on re-authentication and termination of session identifiers post logout. The solution supports AES/RSA algorithms for encryption, does not log any PII data, and all standard logging levels like DEBUG, WARN, INFO, and ERROR. The solution ensures the usage of non-executable stacks and addresses space randomization for operation. It is planned to provide encryption key generation, protection, and storage using HashiCorp Vault in future releases.

Functionality	Maturity	Analysis
Privacy	0%	▸ Sunbird RC does not provide a consent management framework, support for federation and horizontal scalability, use of consent management for each functionality and supports reusability, personal information protected through encryption, anonymization, regular risk assessments, and support for the right to be forgotten. There is no consent management in the platform.
Performance & scalability	75 %	▸ Sunbird RC provides automation and integration test strategies at the ecosystem scale. Sunbird-RC serves as the backend for generating virtual certificates through CoWIN. At its peak, it issued twenty-five million certificates in a day. Its capabilities are tested and validated in real-world scenarios.
Analytics and data-driven decision support (Unified scheme view)	40 %	▸ Sunbird RC uses sunbird telemetry to capture telemetry data. It follows data anonymization for specific usability for analytical functionalities. Capabilities like configurability for data warehousing and how it supports business intelligence, dynamic reporting, OpenData, and data visualization are not present.
Integration capabilities		
Interoperability	100%	▸ Sunbird RC can exchange data using REST APIs with other systems. It provides a microservice called bulk issuance which can ingest a CSV file, API base integration, and consume and produce to Kafka for message-based integration. The solution provides integration for telemetry datasets for downstream systems.
Code and release maturity management		

Functionality	Maturity	Analysis
Code repository management	100 %	▶ Sunbird RC source is present under public git with contributor profiles. Every PR passes through a static code quality and coverage check as part of the GitHub actions workflow. Static code analysis/code review/security reports are available as part of GitHub actions workflows. It uses a GitHub branching strategy for branch management and merging of code changes. Metrics and analytics for tracking code repository activity and usage are implemented using GitHub.
Release management	67 %	▶ Sunbird RC supports the planning and scheduling of releases (product backlogs, innovation functions for future releases) through GitHub projects. Integration with other development tools such as code repository management, CI/CD, and issue tracking systems is currently implemented through GitHub actions and GitHub issues.
Configuration management	33 %	▶ Sunbird RC supports integration with other development tools such as code repository management and issue tracking systems. Deployment files are present for capabilities (like automation of configuration management tasks such as server provisioning and configuration updates, integration with popular configuration management tools such as Puppet, Chef, and Ansible, and management of multiple configuration profiles for different projects and environments) but hardware provisioning to be done by the implementor.
Operational maturity		
Deployment	100 %	▶ Sunbird RC supports black box testing and has unit tests and integration tests as part of its code base. It supports containers and VMs various deployment models. Sunbird RC leverages Kubernetes and Docker Swarm for horizontal and vertical scaling to manage large-scale distributed deployments with ease and support the needs of growing organizations. It is integrated with GitHub actions.

Functionality	Maturity	Analysis
Monitoring	20 %	▶ Sunbird RC supports real-time monitoring of various data sources (e.g., logs, metrics, events). Capabilities like monitoring, auditing, telemetry, analytics, alerting mechanisms to notify administrators in case of anomalies or threshold breaches, customization for alert rules and threshold levels, and detailed visualization and reporting capabilities are not planned for future versions but those can be achieved through tools like Grafana.
Support	0 %	▶ Sunbird RC does not provide support for critical vulnerabilities resolution, financial method inclusion, SLA association for critical issue resolution in the core system.
Documentation maturity		
Enterprise documentation	82 %	▶ Sunbird RC provides documentation for general overview, architecture and infrastructure, installation for various environments and solutions, design, and knowledge repository. It also provides instructions to use the solution and troubleshoot any issues that may arise, functional use cases. Examples or screenshots are included in the documentations. It is planned to manage state and version of documentation updates in future releases. These documentations are available on Sunbird RC microsite.

3.7. OpenCRVS

Standards based Integrations available with	Digital ID	Scheme Management	Health systems

Integrations present with	MOSIP	OpenSPP	IN Groupe	Secure Identity Alliance	DCI	Intellisoft

OpenCRVS is a digital public good designed to digitize civil registration and vital statistics of a country and enable evidence-based decision making. In a civil registration and vital statistics (CRVS) system, civil registration refers to the process of recording the details of all vital life events of an individual, such as births, deaths, marriage, divorce, and adoption while vital statistics refers to the compilation, analysis, and dissemination of data on these events. Civil registration provides the sole continuous source of population data in a country and provides the foundation for human rights, government service delivery, and the measurement of development goals. OpenCRVS is an open-source software platform that provides a digital solution for building civil registries and it is specifically designed for low resource settings. It provides the core features of such a system and allows for the capturing and storing of digital CRVS records for every individual to establish a legal identity for access to basic rights. It allows for the collection, management and analysis of vital events data and generation of data visualization dashboards and analytics. The software is available free of cost and can be adapted by any country wanting to strengthen their CRVS system.

This section provides a summary of OpenCRVS's self-assessment across the assessment parameters, followed by a detailed representation of the functional fitment and the technical fitment which covers architectural coherence, compliance with non-functional requirements, integration potential, the maturity of code and release management processes, operational preparedness, and the quality of documentation.

Legend

Functional Fitment

The functional fitment dimension helps identify if the solution has the capabilities that allows governments, to quickly fulfil their immediate G2P, needs modularly.

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

This dimension block, in the summary provides an analysis on the strength/ maturity of the module with respect to the answers provided. The percentages are calculated based on the number of functionalities present in the module as against the functionalities that should ideally be present

Integration Capabilities

The integration capabilities dimension provides an understanding on how interoperable the solution is with other building block

☑ Present 📈 Planned ☒ Not Available N/A Not Applicable

This dimension block in the summary provides an analysis on the functionalities that are present, planned or not available and not applicable in the solution

Architecture and NFR

The Architecture and NFR dimension provides an analysis if the solution uses modern design paradigms, architectures and technologies

This dimension block in the summary provides the maturity of the dimensions under architecture and NFR. The percentages are calculated based on the number of functionalities present in the module

Documentation Maturity

The documentation maturity provides an analysis, if the solution documentation is easy for a nascent/ fledgling vendor to understand, so that the ecosystem scales up quickly

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

This dimension block provides an analysis on the strength of the capability . The percentages are calculated based on the number of functionalities present in the module

Code and Release Management Maturity

The code and release maturity dimension provides an overview if the solution code is structured and well-managed, modular, well-written - so it can be easily understood and modified, if required

75-100%	50-74%	0-49%
Strong	Moderate	Needs Improvement

The dimension block in the summary provides an analysis on the strength of the capability . The percentages are calculated based on the number of functionalities present in the module

Deployment

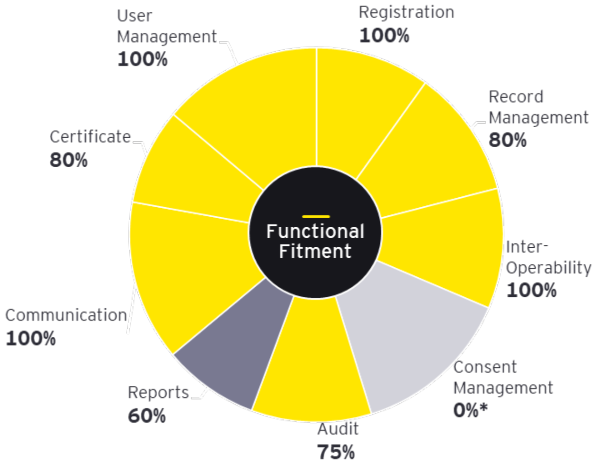
The deployment dimension provides an overview of the pilots conducted by the solution in various countries showcasing its strength, learnings and challenges faced.

📍 Implemented 📍 Interested in Implementing

This provides the countries the solution has been implemented, or interested in implementing being show by a country to deploy the solution

Civil and other federated registries for G2P Connect using OpenCRVS

Functional Fitment



* Capability does not form part of the solution presently, as the initial system was designed for core use of civil registration which is a government mandated action for users, consent by design is an inherent property of traditional CRVS systems

Operational Maturity

Deployment

- Automated testing and continuous integration but no automated roll-back
- Blackbox testing and high-test coverage
- Support containers
- Centralized logging & monitoring - supports rapid identification & resolution of issues
- Large scale and distributed deployments with ease, supporting growing organisations
- CI/CD via GitHub actions

Monitoring

- Built on principles following scalability, minimizing latency, security and privacy, flexibility, automation, accessibility, optimization, and standardization
- Real-time monitoring of various data sources
- Alerting mechanism to notify administrators
- Customizable alert rules and threshold levels
- Visualization and reporting capabilities

Support

- Hotfix released out within a single sprint for any critical issue discovered
- Financial method inclusion is planned
- SLA for critical issue resolution is planned

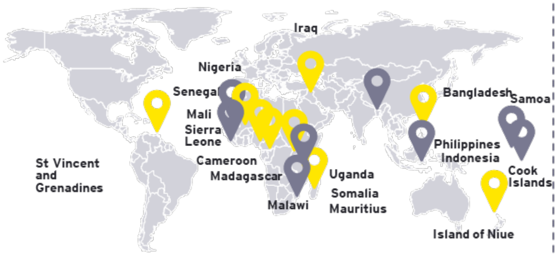
Challenges and Learnings

- Countries want to digitise based on their existing laws, which are often constraints to achieving universal registration and are not written for a digital world
- Countries often propose very aggressive timelines for all functionalities to be implemented, rather than a more phased approach, where progressively elaboration of requirements would be possible (and advisable)

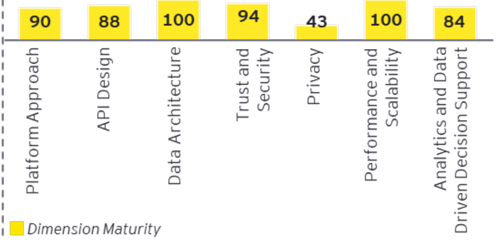
Integration Capabilities

- ☑ Data exchange with external systems in non-proprietary and recognized formats
- ☒ File based integration
- ☑ API-based integration
- 📈 Message-based (Event driven) integration
- ☑ Service orchestration
- 📈 Integration for telemetry dataset for downstream systems
- ☒ Data pipeline architecture

Implementations



Architecture and NFR



* Privacy capabilities have a percentage of 50%, however the consent management framework is currently being planned in the next version

Code & Release Management Maturity

Code and Repository Mgmt.	Release Mgmt.
Strong	Strong
Configuration Mgmt.	**Documentation Maturity**
Strong	Strong

Impact

People registered on OpenCRVS: **multiple registrants across the globe**

3.7.1 Functional fitment

OpenCRVS is available as a digital public good (DPG) and has been designed specifically for low-resource settings. It utilizes an interface that is easy to use for all user-personas and assists them with data entry and data management. Users are presented with an easily navigable form which is available in multiple languages in both online and offline modes. The form contains a set of logical questions per page. OpenCRVS supports 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, for example, open architectural style and data formats are supported. In terms of security, OpenCRVS mobile applications and microservices are secure. Role-based access is provided and a PIN must be entered each time the user accesses the application. Once a week, an additional two-factor authentication is required, including a code being sent via SMS or email to the field agent. Some of the key functionalities associated with OpenCRVS have been mentioned below:

Registration of Vital Events: OpenCRVS allows for the registration of various vital events, including births, deaths and marriages. This includes capturing essential information about the individuals involved and the event itself

Data Entry and Verification: The system provides tools for data entry, often designed to be user-friendly and efficient. It also includes features for data verification to ensure accuracy.

Record Storage and Management: OpenCRVS stores vital records securely in a central database. It enables easy retrieval and management of these records for authorized users.

Security and Access Control: Robust security features are crucial for CRVS systems to protect sensitive personal data. OpenCRVS includes user access controls, 2-factor authentication and encryption to safeguard data.

Reporting and Statistics: The platform generates performance reports, statistical data visualizations related to vital events. This data is valuable for government planning, public health, and policy development.

Auditing and Logging: OpenCRVS includes auditing and logging capabilities to track all changes and access to vital records. This helps maintain data integrity and security.

Integration: It supports integration with other government systems, such as healthcare, identity management, social protection and population databases, to ensure data consistency and accuracy

User Management: User administration features provided are essential to manage the roles and permissions of individuals who interact with the system.

Data Quality Improvement: The platform includes features to improve data quality, such as data validation checks, identification of duplicate entries and error correction mechanisms.

Data Export: OpenCRVS allows for the export of fully anonymized vital statistics data for reporting, analysis, and sharing with other government agencies and organizations.

Mobile and Offline Capabilities: In regions with limited connectivity, OpenCRVS supports mobile data collection and offline data entry, which can later be synchronized with the central database

Localization and Multilingual Support: To accommodate diverse regions and languages, OpenCRVS supports localization and multilingual user interfaces.

Scalability and Customization: OpenCRVS is scalable and able to handle varying volumes of vital event registrations. Customization options are available to meet specific regional or country requirements.

Training and Support: OpenCRVS comes with training and support services to help government agencies implement and maintain the system effectively.

An assessment was conducted to examine OpenCRVS's functionalities, focusing on their relevance in a G2P payments context. This assessment was carried out against the functionalities of generic registries as per the G2P Connect architecture which include registration, consent management, audit mechanisms, reports and dashboards, interoperability, communication and content management, certificate issuance, user management and the ability of all these features to support various personas such as the implementing agency and residents. Moreover, the assessment considered the extent to which these functional capabilities catered to the needs of various stakeholders, including implementing agencies and residents. Additionally, these capabilities were evaluated for its potential towards customization, configuration, or extensibility. A summary of the assessment findings, including what is there or has been planned for implementation in upcoming releases is provided below.

Functionality	Maturity	Analysis
Interoperability	100 %	▶ OpenCRVS is a scalable and cost-effective civil registration system which utilizes a modular microservice architecture, with each microservice written in Node.js and deployed as a Docker container. OpenCRVS follows the OpenHIE architectural standard and supports interoperability using HL7/FHIR. It is also compatible with the G2P-Connect interoperability framework standards and the DCI CRVS Alpha 1.0 standard payloads. The system follows a versioning approach with automated migration scripts. The platform is highly configurable and fully open source and has been piloted or considered for implementation in several countries.

Functionality	Maturity	Analysis
Consent management	0 %	▶ Not available in the OpenCRVS UI but can be customized by exposing the OpenHIM FHIR API. ▶ Not planned as a feature going forward, owing to the legal mandates in countries for residents to share information related to vital events, and for governments to capture the same ensuring consent by default.
Registration	100 %	▶ Capability to create records, upload documents, de-duplication, data field validations, multiple levels of record validation and generating unique IDs against records. ▶ OpenCRVS enables integration with MOSIP which allows the authentication of the informant and the pre-population of the declaration form.
Record management	80 %	▶ Capability to store, correct, search, archive and dispose records. ▶ Capability to make updates to existing records following triggers/requests is planned soon. ▶ Records can only be stored with classifying attributes such as public and private currently, they cannot be stored as consent- based records, but the system can be customized to accommodate the same.
Audit	75 %	▶ Searching and viewing logs for records and data exchange, keeping log of all activities-additions, changes, amendments, searches performed by user, place, and time and to not allow users even system administrators) to change audit logs. ▶ Capability to keep the log of all changes for a certain configurable period of time, and then archiving it is not currently present
Reports and dashboards	60 %	▶ Capabilities available for generating reports of individuals registered, having configurable parameters entered by user (period of time, etc.) for reports and exporting reports or dashboards to a pdf or an excel file. ▶ Capabilities to design and create dashboards to track/analyze key metrics and key data points, etc. and to view a suite of performance and operational level data in a dashboard. ▶ Generation of data quality, timeliness, error reports and to perform trend analysis are planned.

Functionality	Maturity	Analysis
Communication	100 %	▶ Capabilities available for managing product content, language translation, sending updates to informants via SMS or email notifications, managing communications that are sent to external systems and sending alerts to users in case of duplicate records and provide options for archiving of records.
Certificate issuance	80 %	▶ Capabilities for requesting, creating, printing, and re-printing certificates are available. ▶ Capabilities for QR codes to be used as a form of verifiable credential to support authenticity verifying capabilities are available ▶ It currently lacks integration capabilities with wallets/digital lockers to issue certificate as a digital credential.
User access Management	100 %	▶ Capabilities are available for managing role-based privileges and permissions for various authorized users of the portal, authenticating each user by role before providing access to the system and revoking system permissions for user(s)

Implementation record

OpenCRVS has been deployed and is live in Cameroon, Niue, and Madagascar. It is in the implementation phase in Somalia, Uganda, and the Philippines. It has been successfully tested as a pilot in Nigeria and Bangladesh.

3.7.2 Technical fitment

Functionality	Maturity	Analysis
Architecture and NFR		
Platform approach	90 %	▶ OpenCRVS is a scalable and cost-effective civil registration system which utilizes a modular microservice architecture, with each microservice written in Node.js and deployed as a Docker container. OpenCRVS follows the OpenHIE architectural standard and supports interoperability using HL7/FHIR. The system follows a versioning approach with automated migration scripts. The platform is highly configurable and fully open source. It has been piloted or considered for implementation in several countries.
API-first design	88 %	▶ OpenCRVS follows the OpenHIE architectural standard and provides FHIR APIs through the OpenHIM middleware component. The platform exposes specific APIs, including FHIR event notification, FHIR location, and a WebSub webhooks API. OpenCRVS is also compatible with the G2P-Connect interoperability framework standards and the DCI CRVS Alpha 1.0 standard payloads. A GraphQL record search API is also available for custom integration needs. ▶ Data privacy has full visibility and traceability of external client interactions, audited within the OpenCRVS UI. ▶ Technical governance meetings are held bi-annually, involving technical architects from system implementers and interoperating systems.
Data architecture	100 %	▶ OpenCRVS utilizes a layered approach. The presentation layer is a ReactJS progressive web application, while the application layer includes the GraphQL API gateway and OpenHIM for interoperability. ▶ The business layer consists of microservices like workflow and user management, and the persistence layer uses the FHIR-standardized database server called Hearth. OpenCRVS ensures data security through encryption both in transit and at rest using SSL certificates and sha-secret encryption. ▶ The database layer is based on NoSQL MongoDB, providing horizontal scalability and replication. OpenCRVS integrates open-source technologies like ElasticSearch, InfluxData, and Minio for search functionality.
Trust and security	94 %	▶ OpenCRVS prioritizes security and trust by implementing measures such as SSL certificates, JWT-based authentication, and two-factor authentication for user and device validation. User actions and system interactions are audited and tracked, providing visibility and accountability. The use of certificate-based public/private PKI factors and encrypted Docker secrets enhances the security of OpenCRVS. Regular penetration testing is conducted by a certified third-party to identify and address any potential vulnerabilities in the system.

Functionality	Maturity	Analysis
Privacy and consent management	43 %	▶ Access to OpenCRVS records is restricted to civil registration staff, ensuring that only authorized personnel can view or edit records. Personally identifiable information is not downloaded without an audit record tracking the access to the record by the client, ensuring accountability. The platform removes personally identifiable information from performance analytics and statistics exports, prioritizing data privacy. OpenCRVS thus ensures 100% data privacy as per assessment parameters. ▶ Consent management capability does not form part of the solution presently, as the initial system was designed for core use of civil registration, which is a government mandated action for users, consent by design is an inherent property of traditional CRVS systems. However, this capability has been planned for the future as it will enable sharing of key foundational data based on consent.
Performance and scalability	100 %	▶ OpenCRVS has undergone performance testing to ensure its scalability and stability. The tests focused on the resource-intensive operation of birth declaration submission. Multiple target request rates were tested, ranging from 40 to 200 birth declarations per minute. The tests were conducted on a scaled production cluster with three server nodes, utilizing Docker Swarm for effective load balancing.
Analytics and data-driven decision support (Unified scheme view)	84 %	▶ OpenCRVS utilizes InfluxData and Metabase to power real-time performance dashboards. Anonymized performance analytics are captured to display registration rates, completeness rates, and business intelligence metrics. OpenCRVS utilizes InfluxData and Metabase to power real-time performance dashboards. OpenCRVS follows the FHIR standard for the administrative hierarchy, aiding system integration. OpenCRVS leverages the D3 graphing library to provide custom data visualizations, offering flexibility, and enabling users to configure new visualizations using the Metabase embedded analytics tool.
Integration capabilities		
Interoperability	50 %	▶ OpenCRVS is designed to be interoperable by using the fast healthcare interoperability resources (FHIR) healthcare data standard. FHIR uses a modern web-based suite of API technology, including a HTTP-based RESTful protocol, and in OpenCRVS JSON is used for data representation. OpenCRVS utilizes the OpenHIE interoperability reference middleware OpenHIM, a FHIR standard enterprise service bus that exposes the FHIR API and provides additional APIs for data exchange, including event notification, national ID system integration, record search, and OpenCRVS webhooks. ▶ OpenCRVS is compatible with the G2P Connect interoperability framework standards and the DCI CRVS Alpha 1.0 standard payloads. ▶ OpenCRVS microservice orchestration in the architecture is achieved by Docker Swarm and the Traefik ingress controller. OpenCRVS internally uses event driven microservices but are not yet publicly consumable.

Functionality	Maturity	Analysis
Code and release management		
Code repository management	100 %	▶ Branch protection rules ensure that no contribution can be submitted without a pull request. A pull request cannot be initiated without a fully documented user story or issue containing acceptance criteria that satisfies a business need. Each completed pull request code is reviewed by a minimum of two core technical leads and the technical architect. A number of quality gates must also pass automated unit and end-to-end testing. OpenCRVS includes linters that run on every commit using pre-commit hooks to ensure strict typing, style, and enforcement of standards. OpenCRVS also uses the Codecov tool to broadcast unit testing code-coverage. OpenCRVS strictly follows the “Gitflow” branching model.
Release management	100 %	▶ OpenCRVS follows an agile scrum methodology with an evolving backlog. The roadmap for each release is broadcasted after public webinars, prioritizing community feature requests from country implementations, technical debt improvements, and integrations with other DPGs. The release calendar is publicly available, with three releases per year, following semantic versioning. OpenCRVS undergoes quality assurance processes at each stage of feature development, beta release, and stable release, including automated and manual testing. The code repository is on GitHub, compatible with other tools like Gitlab, and utilizes GitHub actions for CI/CD pipelines. OpenCRVS also offers options for issue tracking, application monitoring, and threshold breach detection.
Configuration Management	100 %	▶ OpenCRVS offers an ansible script for automated server provisioning, allowing for single or clustered server setups. The ansible scripts can be re-run multiple times to incorporate configuration updates for new releases. Provisioning profiles are available for development, quality assurance, and production environments. The default script installs OpenCRVS on ubuntu servers with root user SSH access. Customized ansible scripts are provided as examples for deploying OpenCRVS on private cloud infrastructure in-country data centers or on AWS cloud. OpenCRVS integrated with ansible for configuration management and support integration with other development tools such as code repository management and issue tracking systems via GitHub and Sentry.
Operational maturity		
Deployment	84 %	▶ OpenCRVS employs GitHub actions for continuous integration, running automated unit tests, linting, and Cypress end-to-end tests. Pull requests require passing the continuous integration suite before merging. A GitHub action compiles microservices, builds Docker containers, and pushes them to Docker hub. Automated deployment scripts are provided for continuous deployment pipelines, utilizing GitHub secrets for sensitive keys. The suite includes Jest and ViTest unit tests with code coverage above 90% and deploys OpenCRVS to a staging server for black box testing using Cypress. Logging is done through the Elasticsearch, Logstash, Kibana (ELK) stack, with real-time log monitoring available in Kibana, and optional Sentry issue tracking. OpenCRVS utilizes Docker Swarm for container replication and distribution, providing load balancing and redundancy. Performance tests were conducted on a 3-server cluster simulating concurrent traffic for a country with a

Functionality	Maturity	Analysis
		population of 200 million. The CI/CD scripts in OpenCRVS can be easily adapted for other tools such as Jenkins, Travis, CircleCI, or Azure Pipelines.
Monitoring	100 %	▶ OpenCRVS ensures data layer integrity by routing ‘create’ or ‘update’ operations through the OpenHIM message bus, enabling audit trails through transaction logs and error tracking. User interactions with personally identifiable information are audited in the user interface. The ELK stack is used for real-time logging and monitoring, including error logs and configurable data logs for troubleshooting. Anonymized business intelligence metrics are available in the InfluxData time series database. Kibana can be configured to send email notifications via SMTP in case of anomalies, and #787890#787890OpenCRVS can integrate with third-party notification systems like Pingdom and Paper trail. Customization of alerts and monitoring can be done through Kibana and Ansible. The ELK stack provides comprehensive visualization and reporting capabilities through user-friendly graphs and dashboards.
Support	100 %	▶ OpenCRVS follows a release schedule of three minor/major releases per year, with the possibility of interim hotfixes for critical issues. Although there is no officially documented SLA, the team aims to release hotfixes within a single sprint when critical issues arise. OpenCRVS provides ongoing hotfixes to respond to issues identified as part of live country implementations, as per the OpenCRVS release management approach. Support and maintenance services are typically negotiated with implementing countries, with an internal maintenance team being trained during product configuration and installation. Subscription based services are available, depending on funding. An official SLA will be provided.
Documentation maturity		
Enterprise documentation	100 %	▶ The OpenCRVS website provides a high-level overview documentation of the OpenCRVS solution for other stakeholders. OpenCRVS provides comprehensive architecture and infrastructure documentation, including links to external open-source dependencies for architectural review. The installation section explains the steps to set up and run OpenCRVS in both local and hosted environments, while the detailed continuous deployment scripts demonstrate integration flexibility. The documentation, powered by Gitbook, offers versioning and easy navigation through previous releases, along with detailed release and migration notes. Signposting and links to documentation are prominently displayed on the website and GitHub repository. Screenshots and occasional video content aid users in the installation and configuration process. The monitoring section guides system administrators on accessing logs, setting up automatic alerts in Kibana, and troubleshooting individual microservices. The user experience is designed to be intuitive, resulting in minimal UI troubleshooting issues. Users are encouraged to seek assistance through the community or GitHub discussions for specific questions.

Conclusion

As this self-assessment wraps up, the report provides significant findings on the maturity and suitability of DPGs in the framework of the anticipated G2P Connect solution blueprint. Drawing insights from the assessment, it is evident the profound role DPGs can play in shaping a better functioning world. Specifically, within the Government-to-Person (G2P) Connect Initiative, DPGs hold the potential to significantly enhance operational processes and inclusivity.

This report paints a picture of a better working world, showing how well-handled integration of DPGs into systems like the G2P Connect Initiative could have a profound impact. The right moves in this field can lead to significant progress in financial inclusion, interrupt systemic inequities, bolster crucial social protections, and ensure that the *Right Benefit Reaches the Right Person at the Right Time* through the right and preferred channels. However, achieving this vision will need strategic implementation, informed policymaking, and synergistic collaboration among stakeholders.

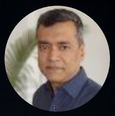
In the broader perspective, the adoption of DPGs is a fundamental aspect of the digital transformation journey. It is in the digital realm where advances in social inclusivity, transparency, accuracy, and efficiency will be realized enabling cheaper, faster, easier, and better service delivery. This is the big picture that has emerged out of this assessment – DPGs are not just a disruptive force, but a transformative one.

As we chart the course for a more inclusive and transformative future, this report serves as a compass, providing the analysis and insights necessary for supporting and harnessing the power of digital public goods.

We urge stakeholders to leverage these findings to position themselves for the future, thus opening a new era of digital empowerment and inclusion.

Acknowledgement

Pramod Varma
Co-Chair
Center for Digital Public Infrastructure (CDPI)

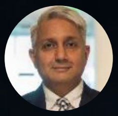


CV Madhukar
CEO
Co-Develop

Anita Mittal
Senior Advisor- Social Protection
GIZ

Christine Kim
Principal Investments
Co-Develop

Vijay Vujjini
CTO
Center for Digital Public Infrastructure (CDPI)



Rahul Rishi
Partner
Ernst & Young LLP India

Rakesh Kaul
Partner
Ernst & Young LLP India

Prakash Jayaram
Partner
Ernst & Young LLP India

Debopam Raha
Partner
Ernst & Young LLP India

Sushmit Mukerji
Senior Manager
Ernst & Young LLP India

The report has been authored by EY, with contributions and self-assessments from Co-Develop and DPG Owners, respectively. The authors from EY are:

Sushmit Mukerji
Anuradha Kamath
Utkarsh Tiwari
Sagar Roperia
Nishkarsh Agrawal
Sneha Arolkar
Snehal Nimbalkar
Biswajit Das
Vinay Yadav
Krishnakant Newale

Ernst & Young LLP

EY | Building a better working world.

About EY

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform, and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data, and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EYG member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian clients serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/en_in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at Ground Floor, Plot No. 67, Institutional Area, Sector - 44, Gurugram - 122 003, Haryana, India.

ED None

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

ey.com/en_in

X @EY_India in EY YouTube EY India f EY Careers India @ey_indiacareers