Digital Government Strategy

- Vision and Objectives
- Digital Government Platform Architecture
- Ownership and Governance
- Implementation Roadmap

Vision and Objectives

Smart Rwanda Master Plan Context

In October 2015, The Government of Rwanda issued the “SMART Rwanda Master Plan” (SRMP), which provides the elements needed to achieve the vision of “a Knowledge Based Society”. SRMP identified a set of core objectives, including the following:

- Objective #8: Build a secured, shared robust and resilient infrastructure to underpin service delivery and support national ICT initiatives
- Objective #9: Enhance the National ICT Governance Structure for effectiveness
- implementation of ICT programs
- Objective #10: Transform digital Government through E-Government and effective service delivery

SRMP also identified three main enablers for Rwanda’s digital transformation: Effective ICT Governance and Management, ICT Capacity and Capability, and Secured and Shared Infrastructure.

The following diagram summarizes the expected outcomes from the SRMP in relation the with objectives listed above:



The objectives and outcomes above are to be executed under the SMRP identified policy principles:

- Access:

    - Cloud First
    - Mobile by Default
    - Infrastructure Sharing
    - Bring Your Own Device
    - ICT Affordability
- Security by design
- Service Data and Innovation
    - Open by Default
    - Efficient Business Processes
    - Privacy Data Protection
    - Innovation and PPP
- ICT Skills and Capacity Building
- Governance

SRMP recognizes the fact that building digital government services requires the establishment of a government ICT enterprise architecture and e-government framework that provides shared services needed for service delivery. However, this set of shared services, while critical for digital service delivery, has not yet been fully identified or documented. The objective of this document, and the corresponding Rwanda Digital Government Platform, is to define the framework for these services.

The One-Stop-Shop Vision

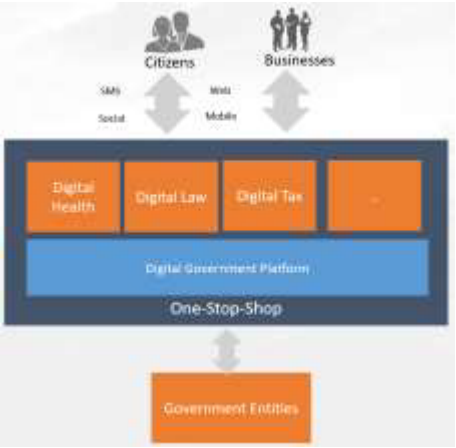
The Government of Rwanda is actively engaged in a program of evolution into a smart, Digital Government. The objective is to deliver and manage services electronically and efficiently—both internally and to businesses and citizens.

Better, broader, and more efficient access to the wide diversity of public services is a key driver for these changes. Equally key is the development of more efficient and streamlined internal business processes. Rwanda would like to capitalize on the development of digital channels such as mobile services and interactive citizen services – to encourage citizens to participate more actively with government. Businesses too can see the benefits: reducing the complexity and bureaucracy of their interactions with the government through the smart application of technology.

The vision is best summarized through the concept of a one-stop-shop, where all government services are presented in an integrated, seamless way that simplifies access to citizens and businesses.



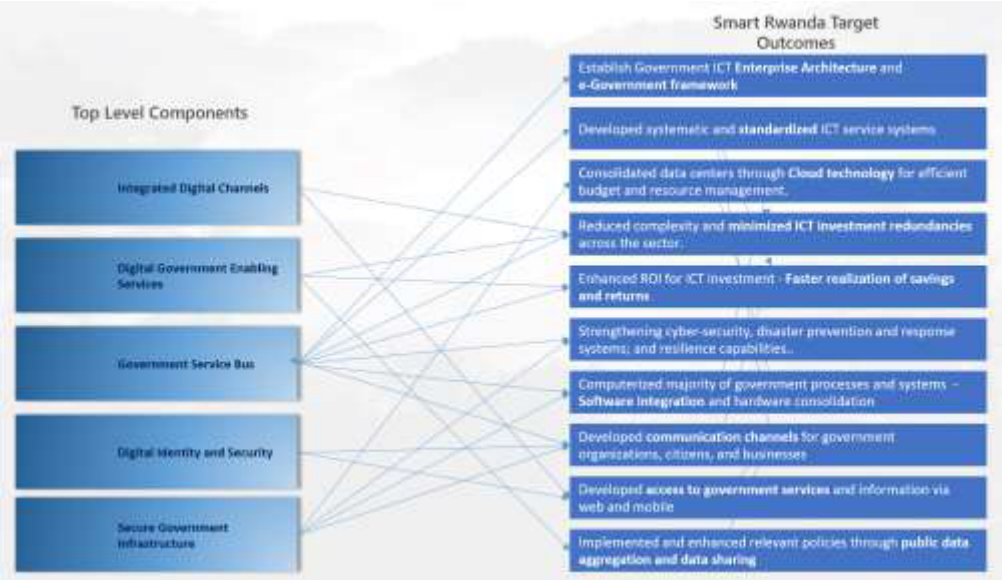
To enable the One-Stop-Shop concept, a set of critical information technology services need to be made available to the entire ecosystem. We refer to these services as the **Digital Government Platform**. On top of this platform, and within the One-Stop-Shop concept, vertical solutions can be built up, including enabling digital health, law, and others.



IMPORTANT: The Digital Government Platform depends on having automation within the government entities. It does not provide the automation of government entity processes but helps in integrating existing automated processes and using them to provide digital services to citizens.

The Digital Government Platform will enable the adherence to the policy principles highlighted in the SMRP as well as the facilitation of the objective outcomes.

The following diagram shows the mapping between the Digital Government Platform's top-level components and the relevant SMRP outcomes:



Expected Benefits of the Digital Government Platform

Providing a common infrastructure shared by multiple digital government services can produce benefits in several categories:

Constituency (Citizen, Organization, Intermediary)

The benefits for the "clients" of digital government services include:

- Reductions in cost and time to enable online transactions in a consistent, reliable fashion
- Hidden complexity and multiplicity of back-end systems interactions at the point of delivery, presented as a single online interaction
- Simplified processes for interacting with government across silos, including the potential for “joined-up” services
- Faster access to services
- Single online identity to access multiple government services across multiple channels
- An always-available 24x7 service.

Government

For the Government of Rwanda, the common Digital Government Platform:

- Accelerates the delivery of e-Government services by providing reusable common components needed for online service delivery
- Shares common costs across the Government rather than repeating expenditure multiple times by duplication of identical pieces of core infrastructure for each online service
- Enables innovative, joined-up services
- Provides a common user identity management model for all Government services
- Provides a single, consistent access path for Government services
- Scales to meet the growing demand
- Drives the take-up of Digital Government services

Application Developers and Independent Software Vendors

For application developers and software vendors building Digital Government solutions, the Digital Government Platform:

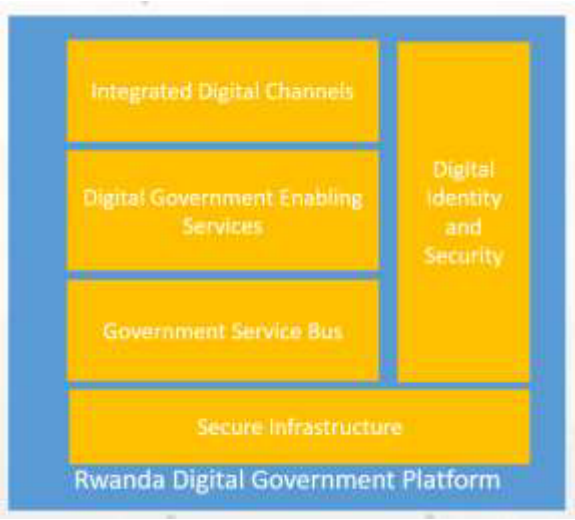
- Provides consistent interoperability—consistent standard interfaces expose the functionality, regardless of the services and departments concerned so applications can be built in a consistent way
- is platform and technology independent
- Complies with open standards

Digital Government Platform Architecture

This section provides an overview of the proposed architecture for the Digital Government Platform.

Architecture Overview

The Digital Government Platform is not one single solution, but rather a set of technology components, architecture artefacts, and guidelines, that work together to facilitate all aspects related to building digital government services. The top-level components are listed below:



Integrated Digital Channels: Allows citizens to have a seamless interaction with the government, leveraging latest devices, social media, and other channels to provide unified citizen experiences.

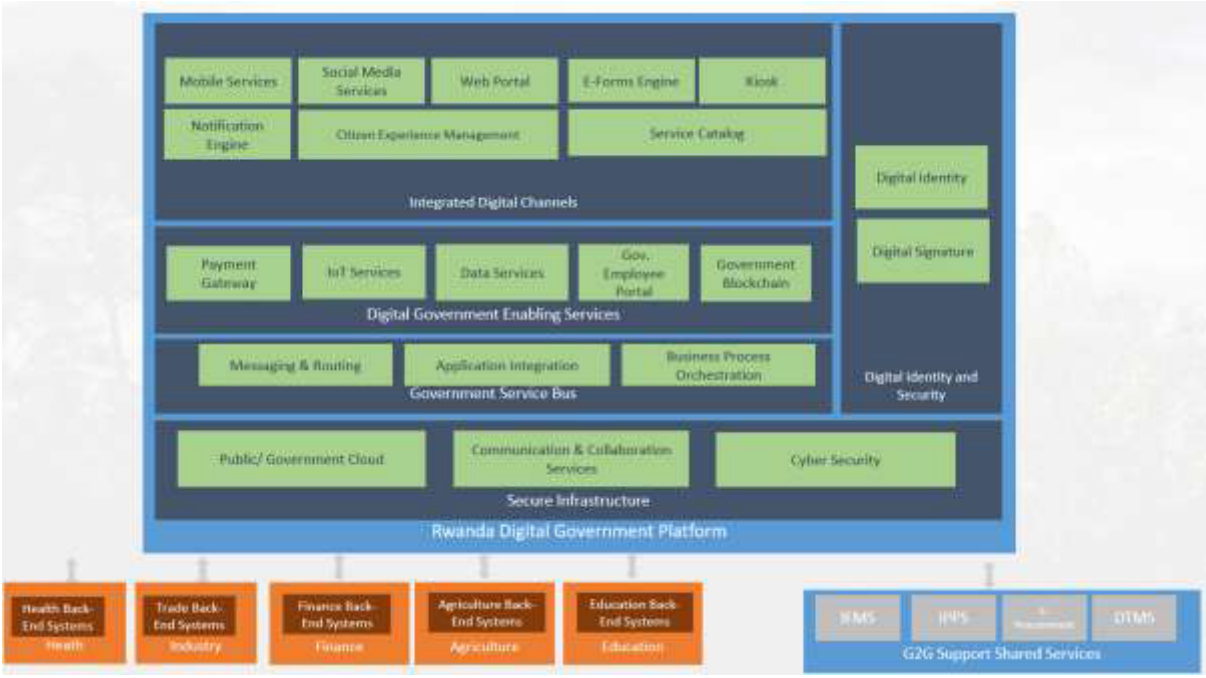
Digital Government Enabling Services: Provide services such as payment, notification, and data management, to facilitate and accelerate the creation of digital services.

Digital Identity and Security: provides technology-based solutions for authenticating citizens and ensuring the security of transactions.

Government Service Bus: Accelerates the creation of new e-services through surfacing government data and processes, simplifying the creation of services that span multiple government entities.

Secure Infrastructure: Provides the backbone of systems, hardware, networking, and security that ensures a reliable, secure, and low-cost operation of government services.

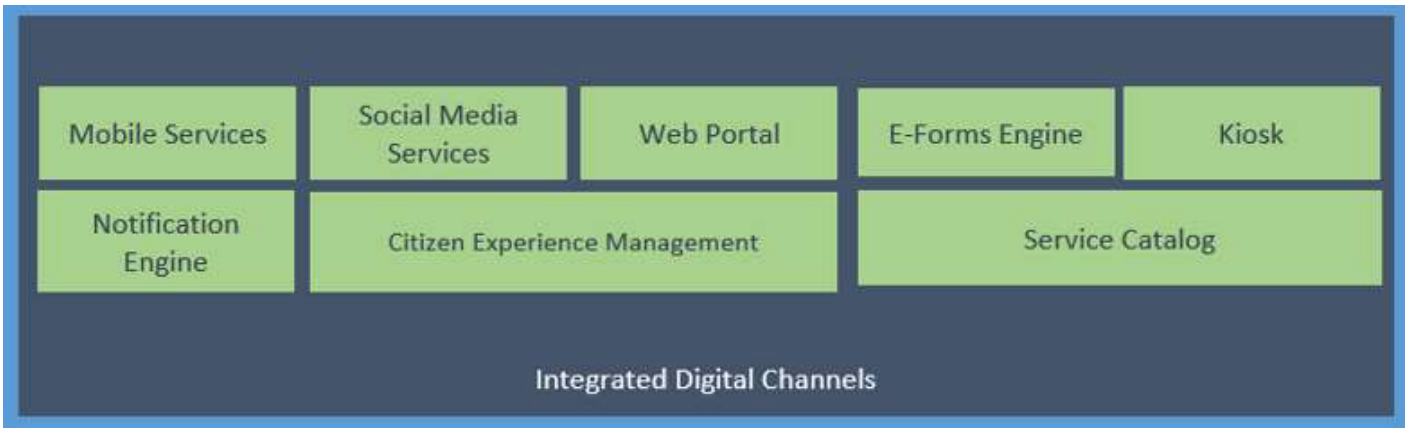
These components are further broken down in the following diagram:



These components are described below.

Integrated Digital Channels

Overview



Integrated Digital Channels provide the possibility for seamless interaction of citizens with the government using multiple channels. Government services will be accessible from any location, through multiple types of devices, using a consistent user experience that is also contextaware.

Government Web Portal

The single point of access to government services on the web is the government web portal. “Irembo” is the current implementation of the Government Web Portal.

Using the portal, citizens and businesses can:

Get information on government and its services

Browse the catalog of services and get redirected to the proper location for accessing services (refer to the catalog services section)

Communicate directly with government entities

Transact with the government services directly using e-services

The web portal would provide some additional features that help in ensuring the best user experience for users:

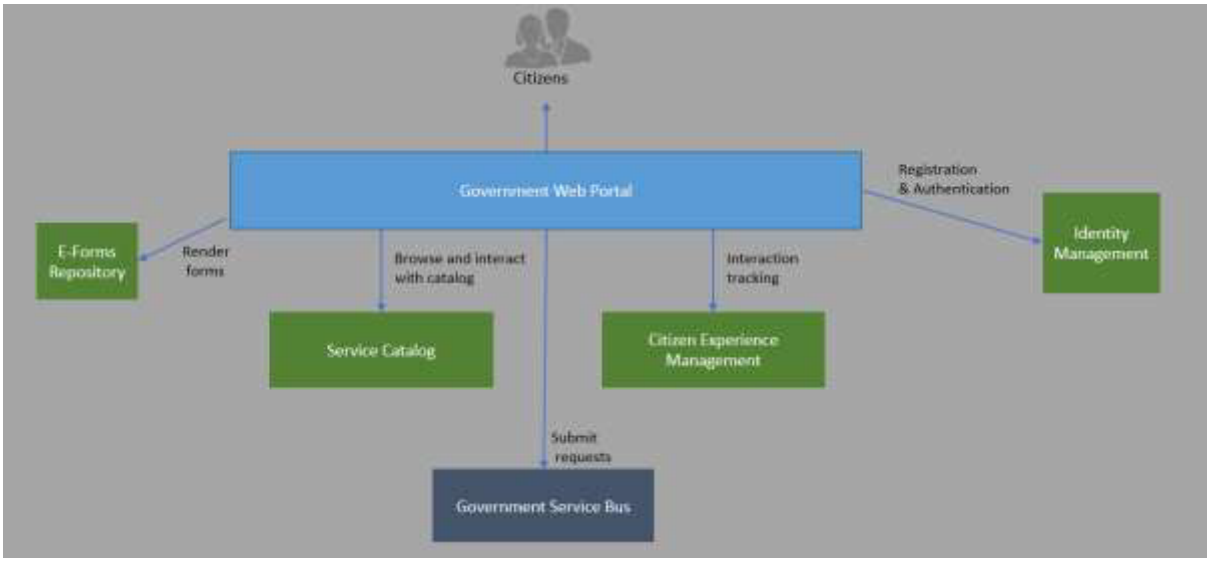
Integrate with Identity management to allow users to log in with chosen credentials and leverage single sign-on to access other services

Transaction History: Provide users with a history of the transactions that they have conducted with the government

Search: ability to search information available on the government portal as well as all government websites from a central place

Chatting/Chatbots: Provide ability to do online chatting with government service representatives, potentially leveraging automated artificial intelligence-enabled chatbots in appropriate scenarios.

The following diagrams show the interaction of the portal with other components:



While Irembo already provides a good entry point to a number of government services, some enhancements are recommended to be put in the roadmap for it to act as a gateway:

Integration with other government websites and services, including catalogs, yellow pages, search and sign-on capability across all government websites and other digital channels

Omni-Channel Access: The ability to start a transaction on one channel and continue it on another, such as beginning a birth certificate request on a phone app and then completing it and submitting it through Irembo.

Control of government entities over web form creation and maintenance, enabling the government entity owning the business to be able to manage the updates to the data and validation it requires from users. Refer to the e-Forms Engine section for details.

Mobile Services

More than 90% of Rwandans[1] access the Internet on their mobile devices. Therefore, it is natural that the interaction with the government should use mobile as the priority channel. Some government services are currently enabled on mobile using USSD. Irembo provides a responsive-design interface for rendering forms on small-screen devices, which helps significantly in making the e-services available on smartphones.

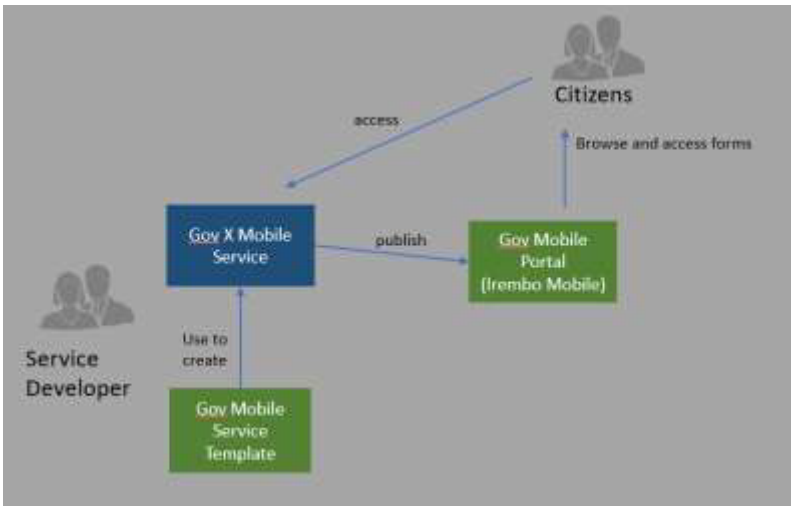
In addition to USSD apps and responsive web design, it is beneficial to create smartphone apps that provide a fluid and responsive mobile service to citizens. Creating one mobile app for government services would be desirable but is not feasible in practice, as it would provide significant challenges in terms of providing useful functionality that is easily accessible to citizens. Therefore, it is expected that multiple mobile apps would be created by the respective owners of services based on the needs.

In that context, centralized government mobile services would have the following objectives:

Enable standardized mobile-based access to services. Standardization would cover security, communication, branding, and look-and-feel, among others.

Ensure integration with other Digital Government Platform components, most notably, Identity Management and Single Sign-On on mobile devices, so that citizens can access mobile services using their assigned credentials.

Provide a central place (portal) for discovering and accessing mobile apps for government. The portal would be accessible through Irembo and as a mobile app used for launching other government apps.



Provide guidance, standards, and templates to government entities and third-party developers for building cross-platform mobile services. These would help ensure consistency even if the

development of mobile app is created by multiple developers or vendors, as it is expected.

Social Media Services

Social media (Facebook, Twitter, etc.) is increasingly playing a critical role in the digital lives of citizens. They provide a direct, live, and transparent way of reaching out to citizens and encouraging inclusion. The Government of Rwanda needs to leverage this channel to harness the power of social networks to help build relationships and communities with citizens. This will be done in a proactive way with the following objectives:

Communicate frequently and announce on events and news:Social networks provide an opportunity to raise awareness about what's happening with citizens

Openly listen and respond to citizen queries and feedback: Social networks contain a trove of information about citizens and government services. Addressing comments quickly can turn a good or bad citizen experience into long-term satisfaction. It also helps identify the things citizens care about. Social communities can also be a great source of highly detailed feedback and discussion from the people who use government services the most.

Analyze general sentiment and context-specific sentiment: Analyzing social streams allows the government to gather information, intelligence, and insights—leveraging connections with citizens and other organizations at local, national, and international levels.

Within the Digital Government Platform, Social Media Services provide the policies, procedures, and tools for a government agency to achieve the above objectives. It also integrates social media with other components, including the web portal, mobile services, and citizen experience management.

E-forms Engine

Automating government paper forms is a common requirement in accelerating the digitization of government business. At the moment, the Irembo team creates online forms for e-services, which requires an extensive programming effort, with the government entities having no control over form fields and validations. It is desirable to have a way to accelerate the form
creation and make it easy to publish and update government forms.

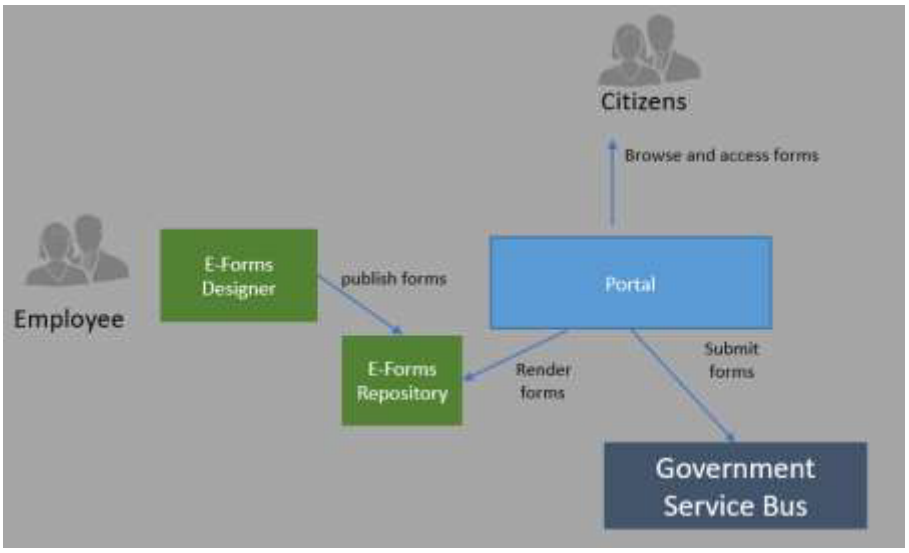
The e-Forms Engine complements the government web portal by providing a system for hosting e-form templates, a designer for templates creation and functionality that allows rendering e-forms in web browsers. The features from the e-Forms engine would be:

Simplify the creation of online forms following a standardized visual design

Simplify the submission of forms to web services for processing

Allow rendering of forms on multiple devices

Provide a centralized repository of forms



Two main components are there:

The e-forms Designer: supports easy creation of e-Form

It should be possible to create a form which will look like the paper version of the form

No deep technical knowledge or programming required

Should support multiple languages

Allow entry validation

Allow complex logic and calculation

Ability to call web services during e-Form filling

The e-forms repository provides central repository of published e-Forms templates. Through web services it allows communication with e-Forms Designer and with the portal that is responsible for hosting e-Form Renderer and which is responsible for showing the list of templates.

Service Catalog

Hosted within the government web portal and mobile services, the Service Catalog provides a central place for citizens to learn about and navigate government services. It facilitates three main ways to browse services:

E-Services catalog: the catalog lists all services available to citizens, whether on the central government site or other government sites or channels. For each e-service, the catalog lists the service name, target users, benefits, fees, access mechanisms, government owner. The catalog also allows users to browse the services through different hierarchical categories.

Government Yellow Pages: hosted on the government web site, the government yellow pages allow citizens to navigate the structure of the government, including all departments and local

offices, showing information about their web presence, contact information (phone, e-mail, etc.), and the services provided by these government entities.

Life Events: citizens and organizations interact with the government and access different services based on the lifecycle. After birth, citizens require birth registration, birth certificates, vaccination, and others. As he/she progresses in age, he/she will require education services, and others. Similarly, organizations pass through multiple
stages throughout their lifecycle. The Life Events feature allows citizens and organizations to access services organized per their lifecycle stages.

Moreover, by integrating with the Citizen Experience Management component, this module allows the government to be able to propose services to citizens proactively based on their own stage in the lifecycle, through integrating with notification services.

Kiosks

For citizens who are not able to access Internet-connected devices whether permanently or temporarily, the self-service Kiosk channel provides the opportunity for digital engagement with the government. Typically positioned in crowded public places, commonly accessed government offices, or in remote areas, the kiosks would be equipped with:

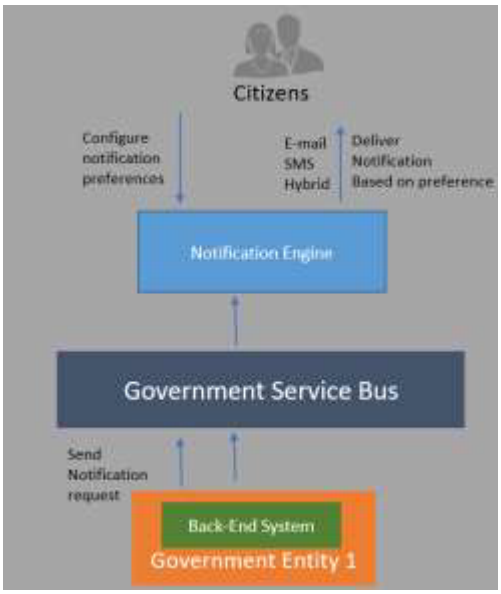
- Secure computer
- Touch-enabled screen
- A Web Camera
- Bio-metric authentication device
- Printer for receipts and others
- Connects the services with other channels
- Leverages touch screens for seamless experience

Kiosks should enable the customer experience to flow in an omni-channel way with the other channels such as web and mobile, in a way that allows starting one transaction in one of these channels and continuing on the kiosk, such as to print out a receipt.

Notification Engine

While delivering with services to citizens, the government sends multiple kinds of notifications in the lifecycle of service delivery, including e-mails, mobile text Messages, standard mail notifications, and others. It is important to standardize as well as consolidate and streamline messages sent to citizens, to ensure that messages are sent to citizens are consistent and result
in actionable outcome.

Currently the Irembo site delivers SMS and E-mail notification to users of its services, while other government entities have their own separate agreements with service providers to deliver SMS Messages.



The Notification Engine is a centralized component for streamlining citizen communication in relation with government services by:

Standardizing the format of messages

Customizing the delivery mechanism

Personalization of notification delivery

Centralization of messaging – such as citizens view all notifications in a single place

The Notification Engine will work as follows:

Citizens can configure, globally, their preferred notification mechanism (whether by SMS messages, e-mail, or others) and the corresponding contact addresses. They can also customize the type of notification based on service type and urgency. If the citizen changes his address or phone number or any contact mechanism, they only change it
from one place (through the government portal), and the new address is used for further notification.

When a government service wants to deliver a message to a citizen, it sends the message to the Notification Engine, specifying the target citizen, the Notification Engine will then deliver the message that is appropriate to the citizen's preferences.

In the back-end, the entity responsible for Notification Engine will ensure the right contractual and technical mechanisms are put in place with vendors (such as SMS vendors) to leverage economies of scale for message transmission. The notification engine will also provide the feature of a Hybrid Inbox. This is an advanced notification mechanism that provides:

Centralized inbox containing all notifications for a citizen, accessed through web, mobile or other channels.

Digital signing of notifications to ensure authenticity and non-repudiation, through integration with the Digital Signature (PKI) infrastructure.

Certified proof of delivery, which can be leveraged for legally binding notifications.

Citizen Experience Management

As citizens get leverage multiple government services, on various channel, it is important toensure that all these interactions are managed in a coordinated way. The component ‘CitizenExperience Management’ acts as the unifying place for managing all citizen interactions andproviding a 360 degree view of the citizen. Borrowing from the concepts of “Customer Relationship Management”, effectively treating citizens as customers, this component delivers the following:

Records all citizen interactions across all channels, whether they are web or mobile service requests, social media comments, or calls to the call center, and enables them to be viewed per citizen.

It provides an update to date record on the status of all transactions that can be viewed by the citizen directly on the available channels

Provides consolidate information, a single version of the truth, about citizens to government employees, enabling them to provide exceptional service

Connect with data services, feeding information about citizen interactions and getting insights around best actions for servicing the citizen.

Digital Government Enabling Services

Overview

This component provides services to facilitate and accelerate the creation of government digital services. They are used by the digital channels as well as by back-end systems to compete the back-end processing.



Payment Gateway

Most government transactions require some form of payment. In the digital government, payment for government services is expected to be made as simple and friction-free as possible. While the current government web site, Irembo, already has support for credit card payment through Visa

and MasterCard, payment options need to be expanded further and made usable across channels. The government payment gateway will have the following objectives:

Payment Gateway should support pluggable payment providers, allowing for flexible payment options that will change over time. These options would include:

Credit/debit/prepaid card payment

Mobile Payment

Payment with NFC

Payment through bank transfer

Payment through bank direct debit

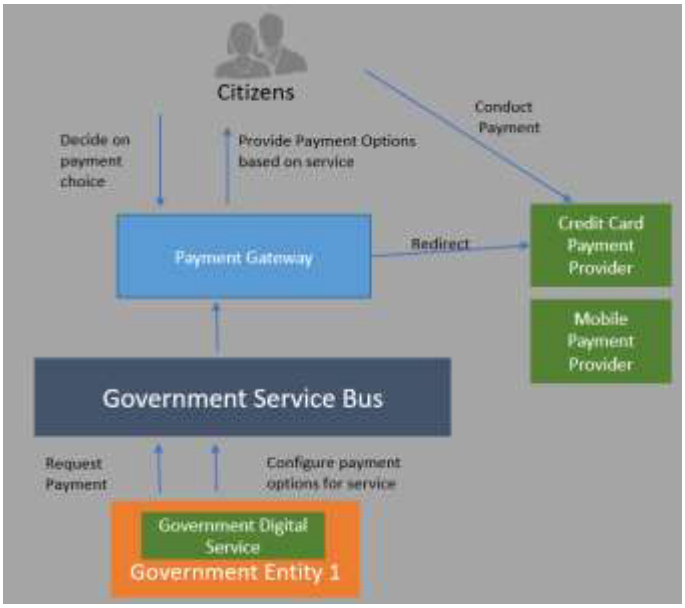
Payment through third party payment providers that operate in Rwanda (such as PayPal)

That payment gateway should publish standardized API-based integration to alloweasy onboarding of government service providers that require using online payment, as well as the integration of new payment providers.

In case the Government Gateway forms global agreements with payment providers onbehalf of the government, the Payment Gateway will provide settlement, dispute resolution and reconciliation services on behalf of the respective government entities that utilize the payment services.

That Payment Gateway would leverage the government PKI to ensure integrity and non-repudiation of transactions

The following diagram describes how the Payment Gateway is used in delivery of an online service:



Data Services

It is important for the government to make sense of available data in all aspects of delivery of information and services — from reducing operational costs to enhancing mission efficiency and delivering new and innovative citizen services — all the while preventing fraud/waste and abuses.

Data Services enables the government to leverage the vast amount of data it owns and collects to deliver the highest quality citizen services, leveraging data for insights and decisions. This has 3 components: Master Data Services, Big Data and Analytics, and Open Data Services, described below.

Master Data Services: Master Data is data that represents core business entities that enables consistent use across systems, of the most accurate, timely, and relevant version of truth. Examples are data about citizens, businesses, land registrations, etc. Related to Master Data are Reference Data, which are standardized terms, code values and other unique identifiers, business definitions for each value, business relationships within and across domain value lists. Examples are region codes, city codes, list of government hospitals, schools, etc. Master and Reference Data is used throughout government services, and the objectives of this component include:

Standardize codes used for all reference data

Ensure consolidation of duplicate records within and across data sources to build and maintain global IDs to enable information integration.

Reconciliation across data sources and providing the —golden record or the best version of the truth.

Provision of access to the golden data across government applications, either through direct reads (web services through the Government Service Bus), or by replication feeds to databases

Big Data and Analytics: this component provides the tools and processes for storing, processing, and analyzing large amount of structured and un-structured data within the government. This allows monitoring and spotting trends that can help control costs, reduce waste, drive new efficiencies, and streamline overall operations. The objectives for Big Data would be:

Enable faster decision speed through greater access to insights

Manage government performance by linking collected data to government goals and Key Performance Indicators

Improve resource management by identifying areas of inefficiencies

Apply predictive analytics to uncover “unintended consequences”, unexpected patterns and associations and evaluate trends.

Open Data: Open Data for the government is a set of policies, process and tools that promotes transparency, accountability, and value creation by making government data available to all. This data can be used to attract nongovernmental sector and community, in general, for participation aiming at strong civic engagement.

The government produces large quantities of data and information, by making this data available, the private, social and government sectors are equipped with strong effective planning tool to institute new, value added, and innovative services for citizens, communities, and the society at large.

This component will provide the elements needed for exposing various types of data, weather structured or unstructured, allowing the ability to define the relevant sets of data catalogues, formats, and enables the rules for managing data publishers, subscribers, and data caching and delivery.

Government Employee Portal

The Government Employee Portal is used as a central place for employees to facilitate services to citizens, in addition to being an Intranet for information common to government workers.

The Government Employee Portal also includes the Task Management Service that allows employees to participate in long running government processes where no back-end system is present. It would work as follows:

As part of executing a Government Digital service, a service requires a task to be conducted by a government employee of an entity that has not automated its operations

The service would send a message to the Task Management Service to log a task for the employee, with the details of the task

The employee will log on to the Task Management service on the Employee Portal and views all his/her pending tasks

The employee will complete his task offline, and once done he/she will complete he will mark the task as complete in the portal

The service will be notified through a message that is sent over the Government Service Bus, and it will resume processing the service request.

Government Blockchain

Blockchain is a revolutionary technology that has started to gain grounds in government services after it has initially been used mainly in financial services. Blockchain provides a distributed ledger, that is secure, shared and immutable. In the government context, Blockchain technology promises greater integrity and transparency through fighting fraud and corruption, reduced cost of operations, and reduced costs of protecting citizens' data while creating the possibility to share data between different entities. While the technology is still in its infancy, and as such presents

risks associated with any new technology, it is beneficial to start experimenting with its applications.

Within the Digital Government Blueprint, the approach to blockchain is as follows:

Ensure that knowledge and expertise about the technology starts to develop within the government

Explore scenarios where the blockchain can be used to solve existing challenges. For example, the blockchain has been used in other African countries to facilitate distributed secure land registries. This could be one of the high priority scenarios for Rwanda as well.

Conduct Proof-of-Concepts to apply the usability of the technologies to the above scenarios. Again, the land registry scenario might be the one to start with.

Use the learnings from the Proof-of-Concepts to do detailed planning for rolling out the technology in production based on its feasibility assessment.

Digital Identity and Security

Overview

Providing Digital Identity that is secure and ubiquitous is one of the foundations of Digital Government. As described by the World Bank Digital Identity Toolkit:

“Digital Identity (eID) provides technology-based solutions for identification in order to uniquely establish a person’s identity and to credential it, so that the identity can be securely and unambiguously asserted and verified through electronic means for delivery of services across sectors, including healthcare, safety nets, financial services, and transport.”

The following definitions are important in addressing this section:

User: the individual to be identified, authenticated, and authorized to use certain services. It can be one of the following:

Individual: a citizen or non-citizen that will use the Gateway.

Employee of an Organization: a defined user that is linked to an organization for the purpose of using the e services

Agent Employee: a defined user that is linked to an Agency (defined below) for the purpose of using the e-services on behalf of other users

Identity: represents and identifies a user.

A user can choose to maintain several separate identities

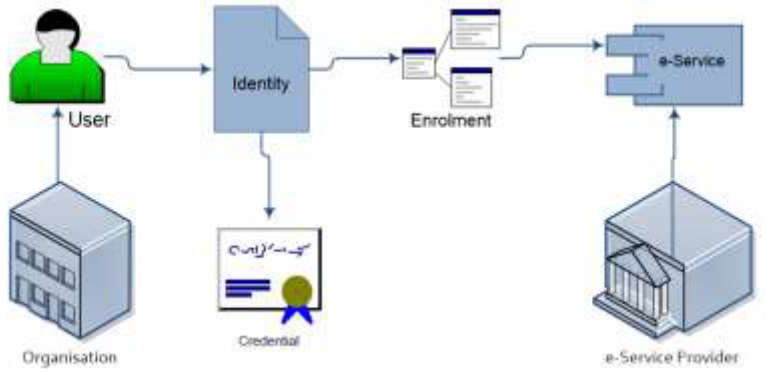
Credential: information or other items that is verifiable to assert an identity. Multiple credentials may be associated with the same identity.

e-Service (or Service, or Digital Service): a logical grouping of business functionality offered by a service provider, with consistent rules governing authorization and access for users.

e-Service Provider: A Government Organization that provides online e-Services.

Enrolment: The linkage of an identity to a particular e-Service.

Agency: An organization that us authorized to use the e-Services on behalf of other users or organizations.



Digital Identity

This component provides technology-based solutions for identification in order to uniquely establish a person's identity and to credential it. The identity has to be:

- Secure : allowing secure and authenticated access to services
- Multi-purpose: supporting multiple ways of authentication for multiple types of services and different security levels
- Mobile – ready : usable for accessing services through mobile channels The current status for Digital Identity in Rwanda can be summarized as follows:
- The National Population Registry maintained by NIDA forms the authoritative database for citizen identification
- The system also supports storing biometric information
- The citizen records can be tied to mobile phone numbers through collaborating with telco providers
- The government web site, Irembo, currently performs user registration by integrating with NIDA and the Telco providers
- Only user name / password is allowed as credential type in Irembo online services The Digital Identity component supports the following important features:

- Registration:

A user must register to access e-Services. The registration component ensures that a user's credentials (e.g., user name and password, certificate) can be unquestionably tied to a real world identity.

Registration must be efficient, secure and require minimum human interaction

Registration for specific e-service should be allowed: once a user is registered for the Digital Government Platform, the e-service can specify that the user needs to extend his registration to access the e-service, which could include adding additional service-specific information

• Multiple Credentials

Multiple credential types should be supported, including:

Username/Password authentication

Digital Certificates (stored on Smart cards, Tokens, or other secure media)

Biometrics (fingerprints, iris scanning, facial recognition, or others)

Mobile ID (utilizing mobile SIM cards)

One Time Passwords (through SMS, Phone call verification, or others)

Other potential credential types in the future

Multiple security settings are associated with different e-services and as such corresponding credentials for each e-service should be based on its level of security. For example, a land registration transaction requires a higher level of security than filing a traffic complaint. In this example, the Service Provider for land registration would potentially require Digital Certificates, whereas complaint filing would accept username/password credentials.

A user can have multiple credentials and can choose to apply set of credentials based on:

Availability: whether it is possible to use the set of credential (e.g if he is carrying his smart card with him).

Channel: some credential types are not possible with mobile channels for example.

The security level for the service itself: different services might require different level of security assurance, as explained above.

Support for organizations identities and delegation

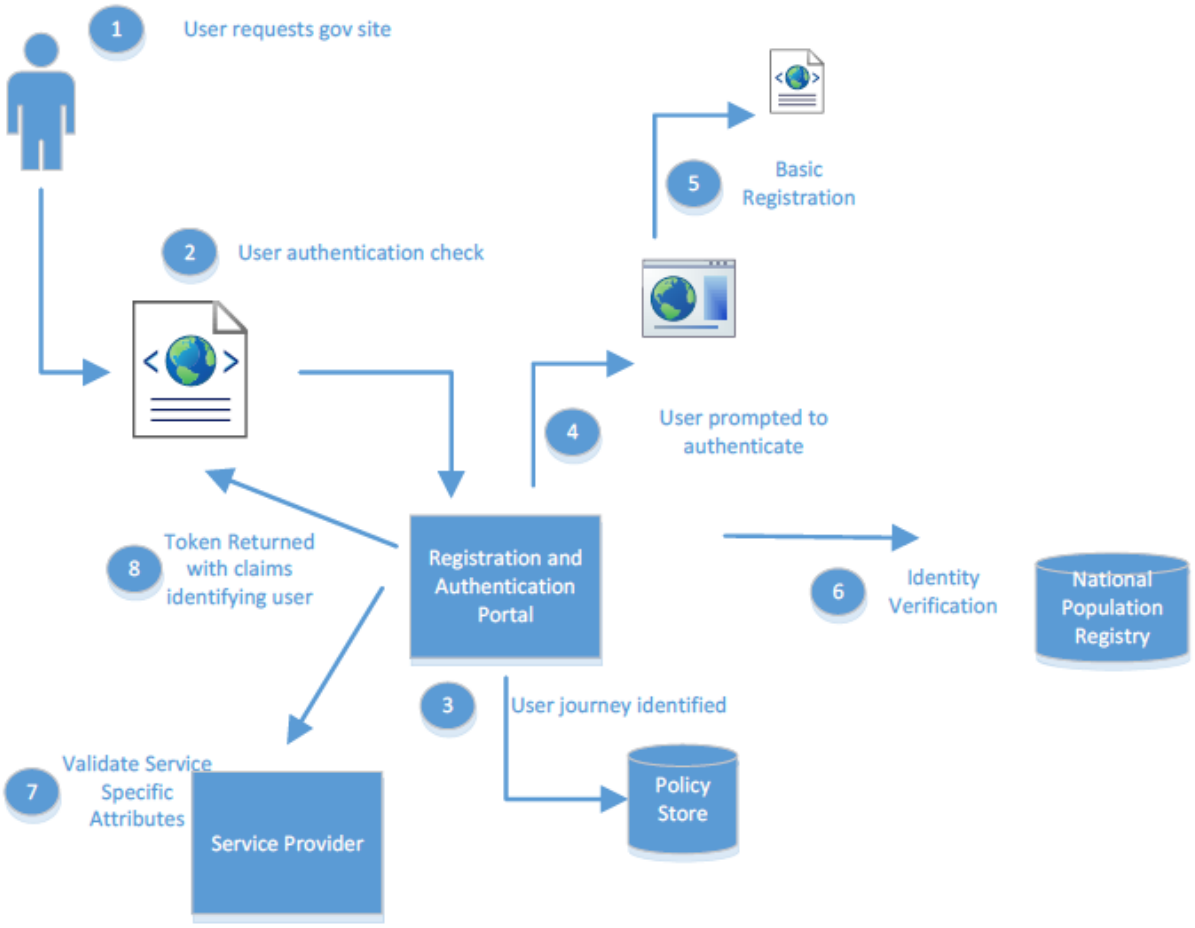
The service should allow identifying and registering organizations and their employees

Registration for businesses need to integrate with the central business registry

The procedure for adding employees shall be simple, in order to allow the easy expandability of e-services to the organizations.

The system should allow delegation for submitting service requests on behalf of other users for specific e-service requests (e.g: for laywers, other representatives)

- Support for Single Sign-On
- Single sign-on for Government Services allows citizens to be authenticated once on a certain channel (such as the web portal), and be able to access multiple services in the same session, even if these services are hosted on other locations or platforms. Without single sign on, citizens would have to remember multiple user names and passwords for multiple services, causing inconvenience as well as security issues in storing and managing passwords. Moreover, cases where services require going through forms across multiple government entities will not be possible to implement.
- While the vision may be to bring all online services on Irembo, this might not be feasible or practical, and as such the architecture should support multiple government services sites and should allow seamless navigation between them.
- Irembo currently provides a single credential to access many services. However:
- For the single sign-on to work, services currently need to be hosted on Irembo site.
- There is no provision for enabling access to other sites with the same credentials
- Other government sites require users to create and log in with different accounts : example is RISA, RRA
- Federated Identity is the enabler for single sign-on as it enables users from different trust domains to authenticate with their credentials in the home domain, but gain access to resources in other domains, based on established trust relationships between domains.



• The platform should support the following standards for enabling single sign-on though identity federation:

- WS-Federation
- SAML 2.0
- OAuth 2.0
- OpenID Connect

• All channels need to integrate with Single Sign-On using the agreed upon federated authentication protocol

Digital Signature

With the objective of paper-free digital government, it is essential to provide the facility for digital signature, and secure digital document exchange. Digital signature facilitates the transition to digital government whereby documents and transactions can be electronically signed. The objectives of this component are:

- **Confidentiality**: ensure that transactions passing between government entities as well as external entities are secured and confidential

- **Integrity**: ensure that no unauthorized modification to transaction is taking place through digital signature
- **Authentication**: ensure that parties can securely identify themselves through digital certificates
- **Non-repudiation**: ensure that transactions cannot be disputed and can be traced back to the originating entity

Currently, the Rwanda Electronic Transactions Law supports digital signature and makes it equivalent to hand-written signature. RISA has started the implementation of a National Public Key Infrastructure, which is currently used to issue certificate for government and private institutions for document signing purposes.

This infrastructure needs to be accredited so that its certificates are recognizable by common browsers and device

Governent Services

Overview

The Government Service Bus is a core component in the Digital Government Platform. It has the following main objectives:

- Accelerate the creation of new e-services through surfacing government data and processes
- Simplify the creation of services that span multiple government entities
- Reduce costs through removal of duplication of integration efforts
- Enforce security and privacy of message exchanges
- Standardize data integration and ensure interoperability
- Enable management and control over integration



It consists of the following main services:

- **Messaging & Routing Services** - responsible for managing messages that pass through the Bus: accepting, validating, and passing messages to the appropriate locations.
- **Application Integration Services** - connect to the target government organization services and routes messages and documents to and from them, handle the secure and reliable delivery of messages
- **Business Process Orchestration** – allows the aggregation of messages across multiple government entities to deliver combined processes

Messaging and Routing

Transactions which are initiated by government entities shall typically be submitted through either the Portal or by automated system interfaces. While the Portal provides a web-based interface allowing users to interact with the Gateway in a user friendly manner, automated system interfaces are required to allow external systems, inside and outside the Government, to submit transaction requests to the Bus without human intervention.

To support the above, the transaction and messaging services shall contain a transaction engine providing the following functionality:

- Service identification: In order to route a transaction request, the transaction engine must be able to determine which system(s) to route the transaction to. The target is typically based on the format of the transaction; however, it could be based on the data contained within the transaction itself.
- Transaction routing: The transaction engine shall be able to route a request to the proper recipient. Transactions may have multiple destinations or may come from multiple sources, depending on the specific process to be executed. The Gateway shall be able to route transactions between all supported sources and destinations.
- Auditing and Tracking: The transaction engine shall provide information on the transactions, which have been processed, for auditing and tracking purposes.
- Asynchronous Messaging: preferred to ensure reliability and scalability
- Synchronous Messaging: used to deliver near real-time services
- Publish/Subscribe Messaging: used to broadcast certain types of messages to subscribers
  The Bus should support international open standards for messaging including:
  - Message Formats : XML or JSON
  - Transport: HTTP / SOAP / REST
  - Security: SSL, SAML, WS-Federation, Oauth, OpenID Connect

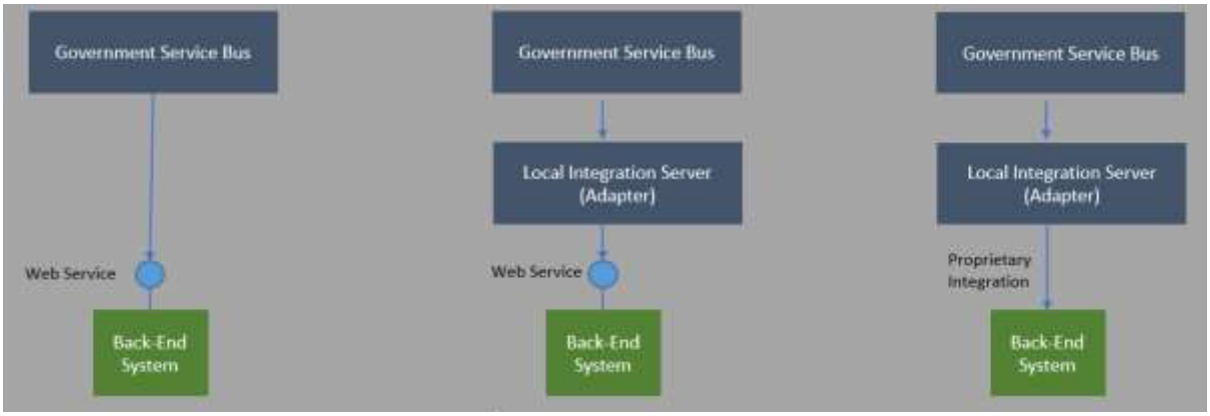
Application Integration

Integrating with the existing back-end systems, through the different protocols and access methods currently supported by these systems, is an important component that shall be implemented by the Government Service Bus. This component shall enable application integration by providing a standard and customized set of adapters for existing back-end systems.

The following integration patterns can be supported by the bus:

- Back-end systems should provide a Web Service interface (SOAP or REST)
- Using local integration servers (remote adapters) that connect to the bus

- Using adapters that can translate between canonical message formats and back-end systems in case a web service is not available



As the government is already in the process of building back-end systems to automate government functions, it would be useful to ensure that, as these systems are built, they facilitate future integration needs. Typical requirements for back-end systems for integration include:

- Systems should provide secure, well-documented Open APIs that are made available through standard interfaces that are accessible through REST or SOAP.
- The Open APIs should expose system data, provide the ability to initiate transactions and workflows, retrieve the status of transactions and workflows.
- Systems should support federated authentication and authorization through integration with Identity Management using OpenID Connect or WS-Federation. This would allow users to authenticate with single credentials on multiple systems

Business Process Orchestration

The Government Service Bus should provide the ability to model and execute customized business processes and rules that coordinate (through appropriate workflow) the execution of an e-Service with back-end systems.

While orchestration is a desire component of integration, it should be reviewed carefully due to the issue of ownership of the orchestration logic. The GSB as a central government component is not preferred to host and manage business logic related to other entities due to ownership and maintainability issues. It should allow the creation of orchestration logic that is created and maintained in the individual government entity, integrating with the GSB but not living in the central government GSB.

Secure Infrastructure

Overview

The Secure Infrastructure component provides the backbone of systems, hardware, networking and security that ensures a reliable, secure, and low cost operation of government services.

Public/ National Cloud

The Smart Rwanda Master Plan advocates for a “Cloud-First” approach, stating that, while setting up new systems and applications, public sector organizations shall prioritize business models and solutions that are cloud-based over stand-alone or individually hosted services. Cloud Services provide the capability to quickly deploy IT infrastructure and software to deliver government services. It provides:

- Fast time to market for services, due to the readily available virtualized resources that can quickly be deployed, the government can accelerate the pace it delivers services to citizens.
- Cost efficiency through economies of scale as multiple government entities are able to host their services on consolidated hardware, software, and infrastructure.
- Enabling innovation and modernization of services: through making
- Scalability on demand: to match demand, especially in seasonal scenarios, the cloud provides the capability to increase available resources to scale the service.
- Public Cloud Operators utilize advanced security mechanisms to ensure the privacy and security of data, and as such can provide better security commitments than data hosted within the government entity data centers.

The Government of Rwanda has the option to leverage existing Public Cloud offerings as well as the expanding a National Cloud based on the existing national data center. While the National Cloud provides the ability to store data within the borders of the country, the Public Cloud provides significant benefits leveraging the innovation and scale of international technology vendors.

Cyber Security

With the Government of Rwanda going Digital, more and more government systems and services are open on the Internet. The Government of Rwanda has openly recognized the importance of Cyber Security in ensuring that all Digital Services and connected systems are properly protected.

It has identified the following related objectives (based on Rwanda Cyber Security Policy):

- Build **cyber security capabilities** for detection, prevention and response to cyber security incidents and threats
- Establish an **institutional framework** to foster cyber-security governance and coordination;
- Strengthen **legal and regulatory frameworks**, as well as promote compliance with appropriate technical and operational security standards
- Promote **Research and Development** in the field of cyber security
- Promote **Cyber Security Awareness** in all sectors and at levels in order to build a culture of security within country
- Promote National, Regional and International Cooperation in the field of cyber security.

As the government seeks to build **cyber security capabilities** for detection, prevention and response to cyber security incidents and threats, it can leverage the following services within the cyber security component:

- Security Risk Assessment
  - Regularly review cyber security people, processes, technology covering four categories of assets:
    - **Identities** – Critical element to security as all assurances are based on authentication and authorization provided by identity systems
    - **Applications and Data** – The stores of business value whose confidentiality, integrity, and availability must be protected.
    - **Infrastructure** – A critical security dependency for most apps and data that adversaries are exploiting to get at them
    - **Devices** – the front line of the security battle that collectively protects access to all assets
- Continuous infrastructure protection, hardening and remediation.
- Conduct continuous Cyber Security Threat Detection and Analytics and response.

Communication and Collaboration Services

In order to be able to deliver on digital government needs, government employees need to be able to collaborate and communicate efficiently. Currently, most government entities maintain mail servers at their premises, while some government entities utilize the services of the Government Data Center for mail hosting. While some government entities utilize video conferencing technology mainly for conferencing with remote offices, there is no unified communication platform(mail, voice, video, instant messaging) in most government entities.

The Communication and Collaboration Services in the Digital Government Platform:

- Provide a scalable government-wide communication and collaboration platform that facilitates employee-employee interactions
- Support unified real-time communication within and across entities covering:
    - E-mail
    - Instant messaging
    - Audio conferencing
    - Video conferencing
    - Collaboration and Information sharing
    - Community and forum discussions
- Integrates with the Digital Government Notification Services to facilitate citizen interactions

Ownership and Governance

As described earlier, the Rwanda Digital Government Platform (RDGP) should not beconsidered as one monolithic solution that can be deployed at once. It is rather a set of technology systems, components, architecture artefacts, and guidelines that are most likely going to be deployed and operated by separate organizations at various points of time. The most critical success factor of this Platform is ensuring that all components integrate and work together towards the common vision.

This section lists the recommended ownership and governance framework for the platform. The key principles related to governance of the platform are listed below:

1. RDGP Global Ownership

- The overall ownership of the Rwanda Digital Platform belongs to the GoR.
- MiTEC has the responsibility of overall oversight, setting policies around information sharing and protection as well as overseeing the implementation of different components.
- RISA has the responsibility to ensure that the architecture is maintained and evolved. Also to ensure interoperability of all components under it, and coordinating all the initiatives stemming from it as well as compliance.

2. RDGP Component Ownership

Each component of the platform must have one single accountable government entity as owner but still ensure that the implementation of the component is aligned to the global strategy and quality requirements of the overall RDGP.

3. Public-Private-Partnership

Whenever possible, implementation and operation of RDGP components will prioritize a PPP model while keeping the ownership structure as articulated in points 1 and 2 above.

The following table provides the recommended ownership model. This is presented for discussion only.

Top-Level Component	Sub- Component(s)	Ownership	Implementation	Opera
RDGP Global Ownership		GOR (MiTEC/RISA)	RISA (Coordination)	RISA (Coor

Integrated Digital Channels	Web portal e-forms engine Life evens Gov. yellow pages Service catalog Appointment scheduling Kiosks	RISA	RISA/ROL	RISA/I
	Online chat engine Map/location services Search			
	Mobile services	RISA	• Creation of guidelines and templates by RISA • Mobile App implementation will be done by various private or public- sector organizations depending on the service to be provided	RISA/I
	Social Media Services	OGS	GOR's entities	GOR's
	Call Center	RISA	To be outsourced	To be
	Citizen Experience Management	MINALOC	RGB	RGB

	IoT Services	RISA	RISA	RISA
Digital Government Enabling Services	Payment Gateway	BNR	BNR/RISA/RURA	BNR
	Notification Gateway	RISA	RISA/ROL	RISA/I
	Data Services	RISA	RISA/ROL	RISA/I
	Employee Portal	RISA	RISA	RISA
Government Services Bus	Government Services Bus	RISA	RISA	RISA
Secure Infrastructure	Communication & Collaboration Services	RISA	RISA	RISA
	Cyber Security	RISA	RISA	RISA

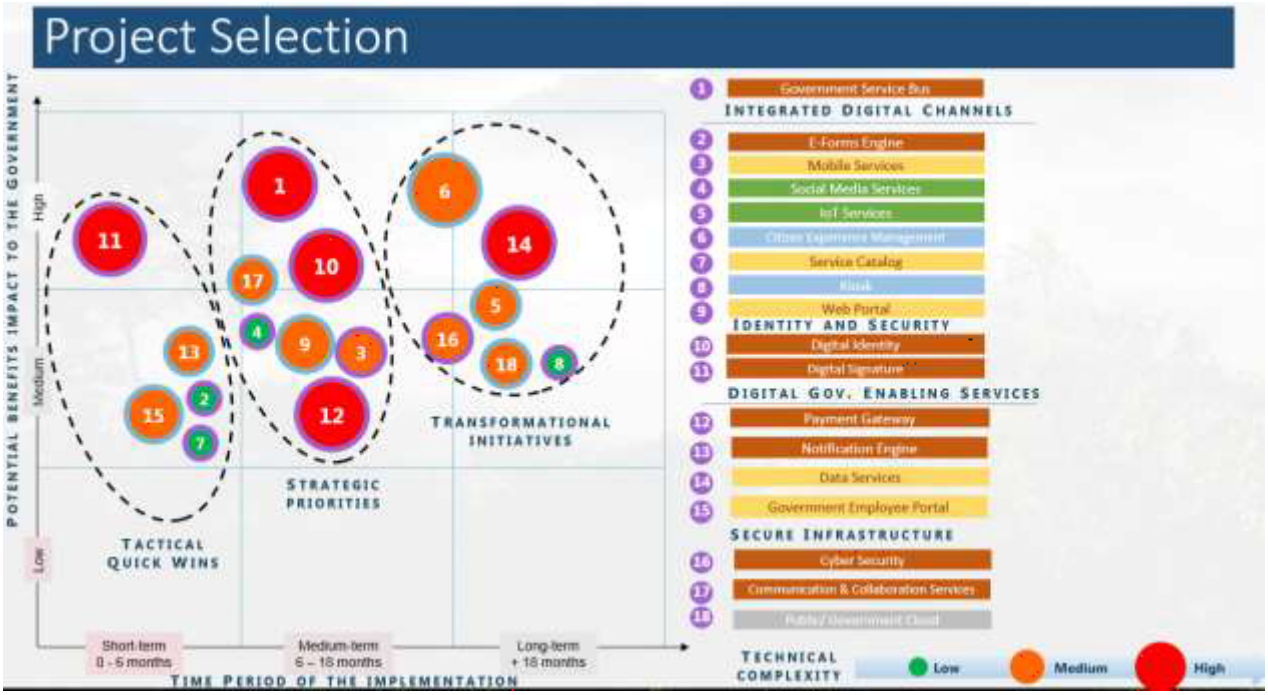
	Operation management	RISA	RISA	RISA
Digital Identity and Security	Digital Identity, Single Sign-On	RISA	RISA	RISA
	Digital Signature	RISA	RISA	RISA

Implementation Roadmap

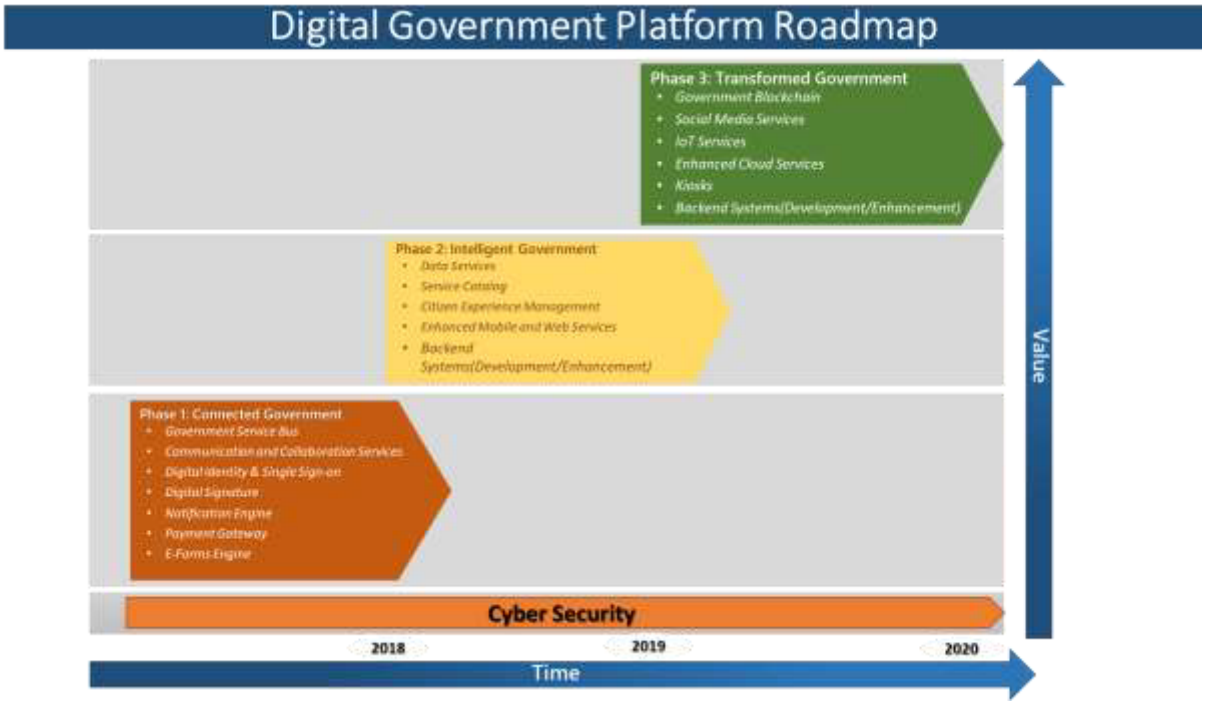
Considering the gap between the current status and the expected future status, the RDGP's components are further classified into three categories:

- Tactical quick wins
- Strategic priorities
- Transformational initiatives.

The matrix below is a summary of the project prioritization process.



For implementation, the roadmap focuses first on high value items. Components that already exist in some form are shifted forward as per the diagram below:



- **Phase 1 "Connected Government**" focuses on ensuring that connected government services are feasible through ensuring the implementation of a Government Service Bus, Communication and Collaboration, and others.
- **Phase 2 "Intelligence Government**" focuses on data-driven government including big data services, open data, citizen experience management, and others.
- **Phase 3 "Transformed Government**" builds on the previous phases to deliver modern experience based on social media, IoT, as well as provide more robust payment and cloud services.