Ghana eGovernment Interoperability Framework (eGIF)

Version 2.0

TABLE OF CONTENTS

TABLES

FIGURES

1 INTRODUCTION

Government of Ghana IT systems have generally been acquired on a solution-by-solution basis, driven by the motivation to acquire the best solution for a specific purpose, within a specific sector. The result is the creation of a wide range of separate information and data islands across Government with no easy way of unlocking the valuable information assets they collectively contain to support more useful and productive processes.

Our quest to ensure delivery of better services in the public sector demands "joined-up" or interoperable ICT systems that work seamlessly and coherently across the public sector to provide good quality services to citizens and businesses. As different Ministries, Departments and Agencies (MDAs) develop IT systems supporting their business, a defined set of shared standards and policies to guide selection of technology, channels etc., - i.e., an *Interoperability Framework* - would prove very beneficial.

To address this issue, we are renewing our commitment to the development, implementation and ongoing maintenance of an Enterprise Architecture (EA) and an Interoperability Framework. The first iteration of the Government of Ghana Enterprise Architecture (GGEA) and accompanying eGovernment Interoperability Framework (eGIF) was adopted in 2008, but implementation was ineffectual and they are now out of date.

GGEA and eGIF v.2.0 reflect that renewed commitment and provide updates to account for changes in the technology context that have occurred since 2008, as well as a more comprehensive approach to organizational and human factors designed to strengthen implementation of the GGEA/eGIF framework.

1.1 The Business Case for Interoperability

Interoperability is both a prerequisite for and a facilitator of the efficient delivery of Government of Ghana Digital Services. Interoperability addresses the need for:

- ***cooperation*** between MDAs aiming at the establishment of public services;
- ***exchanging information*** between MDAs to fulfil legal requirements or policy commitments;
- ***sharing and reusing information*** among MDAs to increase administrative efficiency and reduce administrative burden on citizens and businesses;

resulting in:

- ***improved public service delivery*** to citizens and business by facilitating the one-stop shop delivery of public services;
- ***reduced costs*** for MDAs, businesses and citizens through more efficient delivery of public

services.

1.2 Purpose of this Document

The purpose of the Ghana eGovernment Interoperability Framework (eGIF) is:

- to promote and support the delivery of Government of Ghana Digital Services by fostering cross-sectoral[1] interoperability;
- to guide MDAs' efforts in providing Government of Ghana Digital Services to businesses and citizens; and
- to clarify interoperability policy and requirements to purchasers on the government side as well as system integrators and others involved with government IT projects on the supplier side.

The well-structured approach to interoperability defined in this updated eGIF Version 2.0 will help open up data and information silos and enable information to be exchanged more easily and usefully between systems, enabling MDAs to gain greater insight, better control and improved operational efficiency in information handling. The net outcome will be better-informed and timelier decision–making, improved cost efficiency, and improved satisfaction with public service delivery.

1.3 Target Audience and Scope

The eGIF is purposefully non-technical, and targets all stakeholder decision makers involved in the definition, design and implementation of Government of Ghana Digital Services.

The scope of the EGIF is to guide the design of Government of Ghana Digital Services at all levels of government. eGIF guidance should be adhered to when making decisions about the implementation of GGDS, and particularly during the procurement, development and deployment of new IT systems to support the implementation of policy initiatives.

1.4 eGIF Governance, Management and Maintenance

The eGIF is developed and maintained in the framework of the GGEA programme, in close collaboration between NITA and GGEA stakeholders. They have worked together in the spirit of Pillar 3 *Facilitating Government Administration and Service Delivery – Promoting Electronic Government and Governance* of the ICT4AD Policy to “support the modernization of the Civil and Public Service… to facilitate improvements in operational effectiveness, efficiency and service delivery”[1].

[1] *The Ghana ICT for Accelerated Development (ICT4AD) Policy*, p.8

As a Government of Ghana asset, the GGEA and eGIF must be effectively managed and maintained. NITA will act as the "owner" of the GGEA and eGIF, responsible for day-to-day operational aspects of the frameworks, with support from a GGEA/eGIF Working Group made up of staff from participating MDAs with the requisite technical skills.

Enforcement of eGIF standards will be part of the enterprise architecture compliance review process, as detailed in the GGEA, and involves assessing the compliance of a specific project against established architectural criteria and business objectives. eGIF compliance review will become an integral part of project funding reviews to ensure only projects compliant with eGIF standards are sanctioned to proceed.[2]

1.5 Key Definitions

Government of Ghana Digital Services (GGDS):

In this document, Government of Ghana Digital Services / GGDS refers to "*any cross-agency public sector IT enabled service supplied by MDAs, either to one another or to Ghanaian or International businesses and citizens by means of cooperation between those agencies.*"

(While not all Government of Ghana Digital Services are supported by ICT, most of them rely on some form of ICT support.)

***Interoperability*:**

The EGIF is concerned with interoperability in the very specific context of the provision of Government of Ghana Digital Services. Although in almost all cases, the provision of GGDS will involve the exchange of data between ICT systems, interoperability is a wider concept and encompasses the ability of organisations to work together towards mutually beneficial and commonly agreed goals. Therefore, the following definition is used in the eGIF:

"*Interoperability, within the context of Government of Ghana Digital Services delivery, is the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems*."

***Interoperability Framework*:**

Within the context of this document, an interoperability framework is "*an agreed approach to interoperability for organisations that wish to work together towards the joint delivery of public services. Within its scope of applicability, it specifies a set of common elements:*

[2] A waivers / exceptions process exists to allow non-compliance under a defined set of circumstances for a defined duration.

vocabulary, concepts, principles, policies, guidelines, recommendations, and practices".

1.6 Structure of this Document

In the following chapters, the eGIF addresses the key interoperability issues for the efficient and effective development and delivery of interoperable Government of Ghana Digital Services, arranged as follows:

Chapter 2 – Interoperability Principles defines eleven key principles on which Government of Ghana Digital Services shall be based. They reflect the expectations of MDAs, business and citizens with regard to public service delivery.

Chapter 3 – eGIF Digital Services Conceptual Model introduces the organising principle for the design of interoperable services focusing on how service components can be aggregated, and the technology options for service delivery.

Chapter 4 - Interoperability Levels covers the different interoperability aspects to be addressed when designing an interoperable Government of Ghana Digital Service and provides a common vocabulary for discussing issues encountered when establishing such a service.

Chapter 5 – Interoperability Agreements presents the approach proposed to facilitate the cooperation of MDAs working together to provide a given Government of Ghana Digital Service by introducing the concepts of interoperability agreements, formalised specifications and open specifications.

These are supplemented by seven ***Annexes*** focused on key interoperability areas including channel interoperability, business process interoperability, data interoperability, network interoperability, security interoperability, application and software interoperability, and Service Oriented Architecture. The annexes contain policy statements and the technical standards that will be used to assess compliance with the eGIF.

eGIF Recommended Approaches

Throughout the eGIF guidance and recommendations are provided that address specific interoperability requirements. Implementing the recommendations will create an environment in which MDAs organise themselves in order to establish new Government of Ghana Digital Services. This will help to grow an interoperability ecosystem with people familiar with interoperability, organisations ready to collaborate and common frameworks, tools and services facilitating the establishment of GGDS.

2 INTEROPERABILITY PRINCIPLES

The eGIF is anchored by 11 key Interoperability Principles relevant to the process of establishing Government of Ghana Digital Services. This chapter describes the context in which the principles should be applied during the design and implementation of GGDS. The key Interoperability Principles of the eGIF fall into three groups:

- The first two principles frame the context for GGDS design and implementation;
- Principles 3, 4, 5, 6 and 7 identify user needs and expectations that must be addressed;
- Principles 8, 9, 10 and 11 provide the technological foundation for collaboration between MDAs.

2.1 Interoperability Principle 1: Subsidiarity and Proportionality

The subsidiarity principle implies that Government of Ghana Digital Services decisions are taken as closely as possible to the citizen. In other words, the GoG does not take action unless national government action is more effective than action taken at the MDA, regional or local government level.

The proportionality principle limits GoG actions to what is necessary to achieve agreed policy objectives. This implies that the GoG opts for solutions that leave the greatest possible freedom for implementation to MDAs.

Subsidiarity and proportionality also apply to the delivery of GGDS and therefore to the exchange of information necessary for the delivery of such services. The exchange of information and the joint delivery of GGDS will occur either as a consequence of legislation or policy, or when MDAs willingly and proactively participate in coordinated initiatives.

2.2 Interoperability Principle 2: Effectiveness and Efficiency

MDAs should ensure that solutions serve businesses and citizens in the most effective and efficient way and provide the best value for taxpayer money.

There are many ways to take stock of the value brought by public service solutions, including considerations such as return on investment, total cost of ownership, increased flexibility, reduction of administrative burden, improvement of working methods, increased efficiency, reduction of risk, as well as increased transparency and simplification.

2.3 Interoperability Principle 3: User Centricity

Public services are provided to serve the needs of citizens and businesses. More precisely, those needs should determine what public services are provided and how public services are delivered. Generally speaking, citizens and businesses will expect:

- Access to user friendly services in a secure and flexible manner allowing personalization and with full respect of privacy;
- To provide any given piece of information only once to the government;
- To access a single contact point even when multiple administrations have to work together in order to provide the service;
- Multichannel delivery allowing access to services anyhow, anywhere, anytime. Interoperability

2.4 Interoperability Principle 4: Inclusion and Accessibility

The use of ICT should create equal opportunities for all citizens and businesses due to open, inclusive services that are publicly accessible without discrimination.

Inclusion aims to take full advantage of opportunities offered by new technologies to overcome social and economic disadvantages and exclusion. Accessibility aims at ensuring people with disabilities and the elderly access to public services so they can experience the same service levels as all other citizens.

Inclusion and accessibility have to be considered throughout the whole development lifecycle of a Government of Ghana Digital Service regarding design, information content and delivery.

Inclusion and accessibility usually encompass multichannel delivery. Traditional service delivery channels may need to co-exist with new channels established using technology, giving citizens a choice of access.

Inclusion and accessibility can also be furthered by the capability of a system to allow a third party to act on behalf of citizens who are unable, either permanently or temporarily, to directly make use of public services.

2.5 Interoperability Principle 5: Security and Privacy

Citizens and businesses must be assured that they interact with government in an environment of trust and in full compliance with the relevant regulations, e.g., on privacy and data protection. This means that MDAs must guarantee that the privacy of citizens and the confidentiality of information provided by businesses are respected.

Within the necessary security constraints, citizens and businesses should have the right to verify the information government has collected about them and to decide whether this information may be used for purposes other than those for which it was originally supplied.

Recommended Approach: MDAs should agree on an appropriate, common security and privacy policy for each Government of Ghana Digital Service they establish, (compliant with and providing detailed interpretation and application of National and MDA level security policies).

2.6 Interoperability Principle 6: Administrative Simplification

Businesses compile large amounts of information, often solely because of legal obligations, which is of no direct benefit for them and not necessary for achieving the objectives of the legislation imposing the obligations. This creates a considerable administrative burden that can be expressed as a cost incurred by businesses.

It is also widely recognised that there is a high redundancy in information to be provided by citizens to MDAs. Repeated requests by different administrations for the same information place a similar administrative burden on citizens who waste time compiling data and filling in forms with the same information over and over again.

When establishing Government of Ghana Digital Services, eliminating the request for unnecessary or redundant information should be a priority, even when it may require reorganisation and reengineering efforts in the MDAs' back-offices.

2.7 Interoperability Principle 7: Transparency

Citizens and businesses should be able to understand administrative processes. They should have the right to track administrative procedures that involve them, and have insight into the rationale behind decisions that could affect them.

Transparency also allows citizens and businesses to give feedback about the quality of the public services provided, to contribute to their improvement and to suggest the implementation of new services.

2.8 Interoperability Principle 8: Preservation of Information

Records and information in electronic form held by MDAs for the purpose of documenting procedures and decisions must be preserved. The goal is to ensure that records and other forms of information keep their legibility, reliability and integrity over time and can be accessed taking into account security and privacy.

In order to guarantee long-term preservation of electronic records and other kinds of information, formats should be selected so as to ensure long-term accessibility, including preservation of associated electronic signatures and other electronic certifications, such as mandates.

Recommendation Approach: MDAs should formulate together a long-term preservation policy for electronic records related to Government of Ghana Digital Services.

2.9 Interoperability Principle 9: Openness

Within the context of the eGIF, openness is the willingness of persons, organisations or other members of a community of interest to share knowledge and to stimulate debate within that community of interest, having as ultimate goal the advancement of knowledge and the use thereof to solve relevant problems. In that sense, openness leads to considerable gains in efficiency.

Interoperability involves the sharing of information and knowledge between organisations, hence implies a certain degree of openness. There are varying degrees of openness.

Specifications, software and software development methods that promote collaboration and the results of which can freely be accessed, reused and shared are considered open and lie at one end of the spectrum while non-documented, proprietary specifications, proprietary software and the reluctance or resistance to reuse solutions lie at the other end.

The spectrum of approaches that lies between these two extremes can be called the openness continuum.

MDAs need to decide where they wish to position themselves on this continuum with respect to the issues discussed in the eGIF. The exact position may vary, on a case-by-case basis, depending on their needs, priorities, legacy investments, budget and a number of other factors. While there is a correlation between openness and interoperability, it is also true that interoperability can be obtained without openness, for example via homogeneity of the ICT systems, which implies that all partners use, or agree to use, the same solution to implement a Government of Ghana Digital Service.

Recommended Approach: MDAs should favour openness when working together to establish a Government of Ghana Digital Service while taking into account their priorities and constraints.

2.10 Interoperability Principle 10: Reusability

Re-use is key to the efficient development of Government of Ghana Digital Services.

Re-use means that MDAs confronted with a specific problem seek to benefit from the work of others by looking at what is available, assessing its usefulness or relevancy to the problem at hand, and decide to use solutions that have proven their value elsewhere.

This implies that MDAs must be willing to share with others their service components.

Re-use and sharing naturally lead to collaboration, i.e. working together towards mutually beneficial and agreed common goals.

In the specific case of Open-Source Software, NITA will set up and maintain an Open-Source Repository, and provide consultation and support to facilitate MDAs to share and re-use open-source software components, and/or to collaborate on their development and improvement.

Recommended Action: MDAs are encouraged to reuse and share solutions and to collaborate on the development of common solutions when implementing Government of Ghana Digital Services.

2.11 Interoperability Principle 11: Technological Neutrality and Adaptability

Finally, and of great importance, when establishing Government of Ghana Digital Services MDAs should focus on functional needs and defer decisions on technology as long as possible in order to avoid imposing specific technologies or products on their partners and to be able to adapt to the rapidly evolving technological environment.

MDAs should render access to public services independent of any specific technology or product.

Recommended Action: MDAs should not impose any specific technological solution on citizens, businesses and other MDAs when establishing Government of Ghana Digital Services.

3 THE EGIF DIGITAL SERVICES CONCEPTUAL MODEL

This chapter proposes a conceptual model to describe the organizing principles underlying the construction and operation of Government of Ghana Digital Services. The conceptual model embodies common elements and best practices as a blueprint for future implementations of interoperable Government of Ghana Digital Services, to aid in developing a common vocabulary and understanding across MDAs about the main elements comprising a GGDS and their basic relationships to one another.

The conceptual model emphasizes a building-block approach to the construction of GGDS, allowing for the interconnection and reusability of components when building new services.

The conceptual model is generic by nature, to be applicable at any level of government providing GGDS, from the local level all the way up to the whole-of-government-level, and it illustrates the fact that any level of government can be a provider of both basic and aggregated digital services. In this sense, the model clarifies and rationalises the relationships between MDAs that are collaborating to deliver digital services.

The application of the conceptual model is intended to bring practical benefits in establishing Government of Ghana Digital Services. For example, the splitting of functionality into basic services with well-defined interfaces, conceived for reuse, will simplify and streamline the implementation of services and re-use of components to avoid duplication of effort.

3.1 Government of Ghana Digital Services Scenarios

The interoperability addressed in the eGIF comes into play in a number of interaction scenarios:

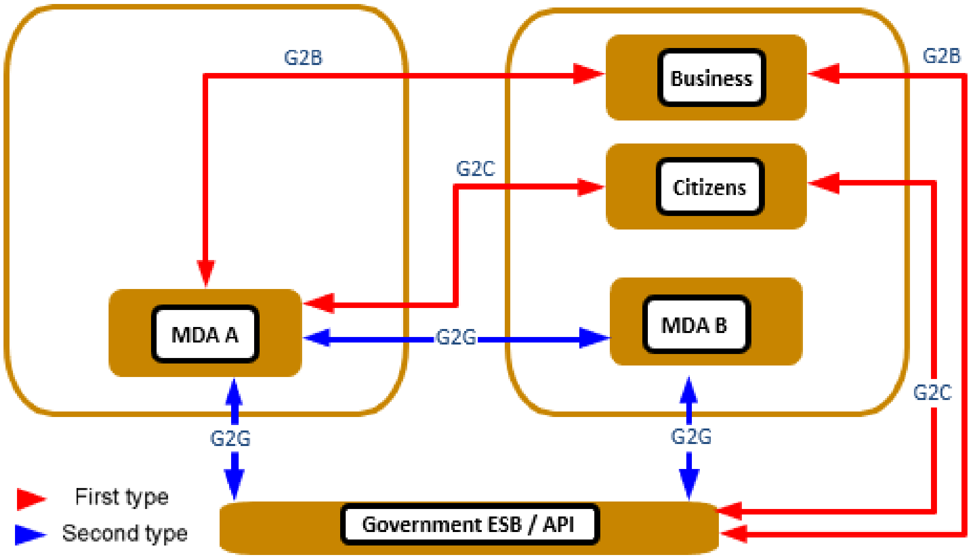


Figure 1 - eGIF Interoperability Scenarios

The GGDS covered by the eGIF can be subdivided into various interaction types as illustrated in the diagram above.

The first type is an interaction between businesses or citizens and MDAs (G2B and G2C), either directly or via the GoG Enterprise Service Bus or API infrastructure.

The second type is an interaction between different MDAs (G2G) either directly or via the GoG Enterprise Service Bus and/or API infrastructure. This second type of interaction may or may not involve services provided to businesses or citizens (G2B and G2C).

3.2 The Key Concepts of the Conceptual Model

The conceptual model promotes the reuse of information, concepts, patterns, solutions, and standards in MDAs and at whole-of-government level, recognizing that Government of Ghana Digital Services:

- are based on information from various sources located at different levels of administration, in different MDAs, and
- combine basic services constructed independently in different MDAs.

Therefore, the conceptual model highlights the need for modular, loosely coupled service components, interconnected through the necessary infrastructure, working together towards the delivery of Government of Ghana Digital Services.

It explicitly puts forward the government-wide adoption of a service-oriented architecture approach to system conception and development, as well as an ICT ecosystem that is broken down into consistent, and in some cases commonly developed, service components. Its service orientation is a specific style of creating and using business processes, packaged as services, throughout their lifecycle.

Recommended Approach: **MDAs should develop a component-based service model, allowing the establishment of Government of Ghana Digital Services by reusing, as much as possible, existing service components.**

There are well-known and widely-used technical solutions, e.g., web services, geared to ensure such connectability. MDAs will need to agree a common scheme on how to interconnect such components.

Recommended Approach: **MDAs should agree on a common scheme to interconnect loosely-coupled components and put in place the necessary infrastructure when establishing Government of Ghana Digital Services.**

The basic elements of the conceptual model are depicted in the diagram below:

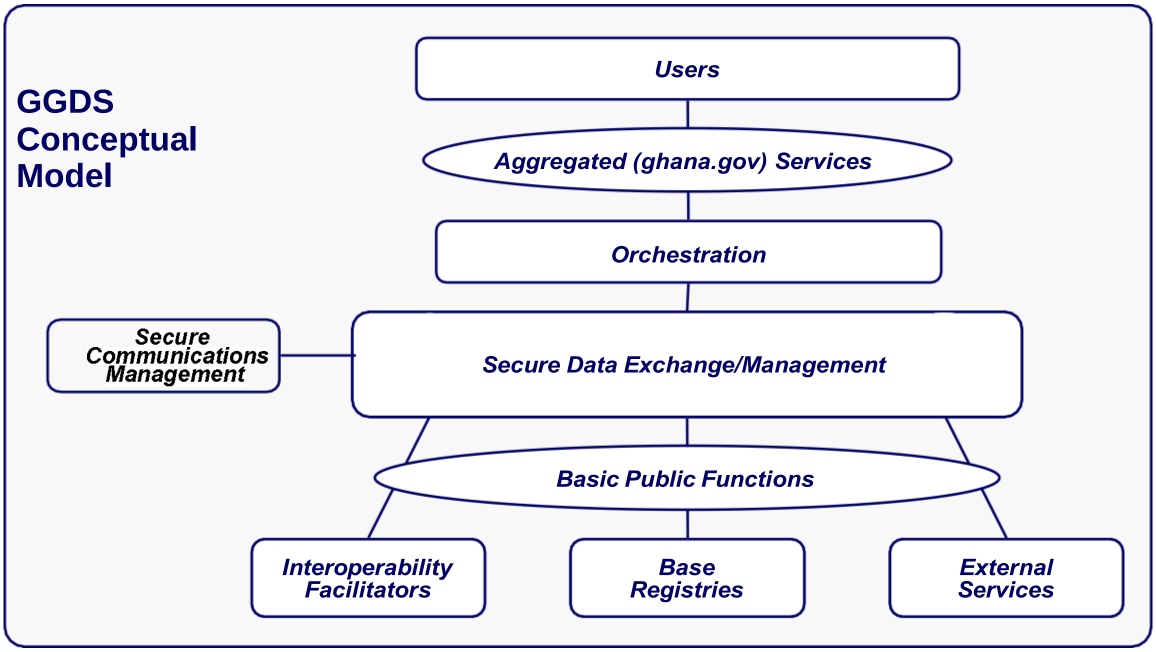

GGDS Conceptual Model
Users
Aggregated (ghana.gov) Services
Orchestration
Secure Communications Management
Secure Data Exchange/Management
Basic Public Functions
Interoperability Facilitators
Base Registries
External Services

Figure 2 - Basic Elements of the eGIF Conceptual Model

In order to understand this model, it is useful to subdivide it into three layers: basic public functions, secure data exchange and aggregate public services, detailed in the following sections.

3.2.1 The Basic Public Functions

The lowest layer of the Conceptual Model deals with the most basic components from which Government of Ghana Digital Services can be built. It groups three types of such basic components, namely interoperability facilitators, base registries, and external services, together calling them basic public functions.

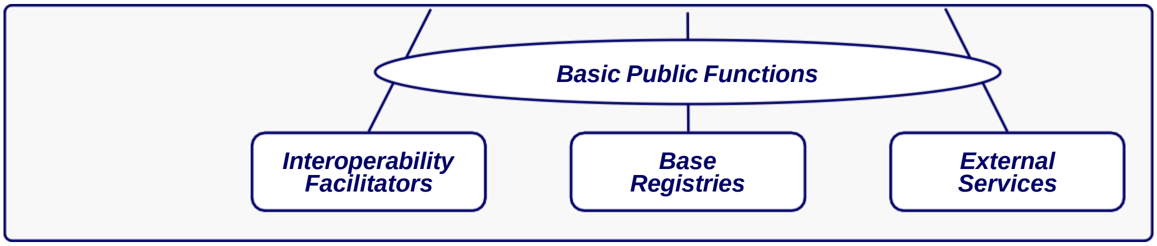


Figure 3 - Base Layer of the eGIF Conceptual Model

Some of these basic functions have been or will be developed primarily for the direct use by the MDA which has created them, or by their direct customers, i.e., the businesses and citizens, but are made available for reuse elsewhere with a view to being combined to provide aggregate public services. Others are generic and/or infrastructural in nature, while the remaining ones represent external services, i.e., services provided by third parties. The following sections describe in more detail each type of basic public function.

3.2.1.1 Base Registries

The most important components are the base registries which are reliable sources of basic information on items such as persons, companies, vehicles, licences, buildings, locations, roads, etc. Such registries are under the legal control of and maintained by a given MDA, but the information should be made available for wider reuse with the appropriate security and privacy measures.

The common thread running through all implementations of basic registries is the fact that they are authentic and authoritative in nature and are, separately or in combination the cornerstone of public services. Their content is, in general, not static; they also reflect the information lifecycle.

Recommended Approach: **MDAs should make their authentic sources of information available to others while implementing the appropriate access and control mechanism to ensure security and privacy as foreseen in the relevant legislation.**

One of the obstacles to the adoption of the conceptual model for Government of Ghana Digital Services implementation might be the existence of legacy systems. Such legacy systems, and their underlying data repositories, have specific characteristics limiting the possibilities for reuse (e.g. lack of published interfaces) and they might require extensive re-engineering efforts in order to make the information available for Government of Ghana Digital Services.

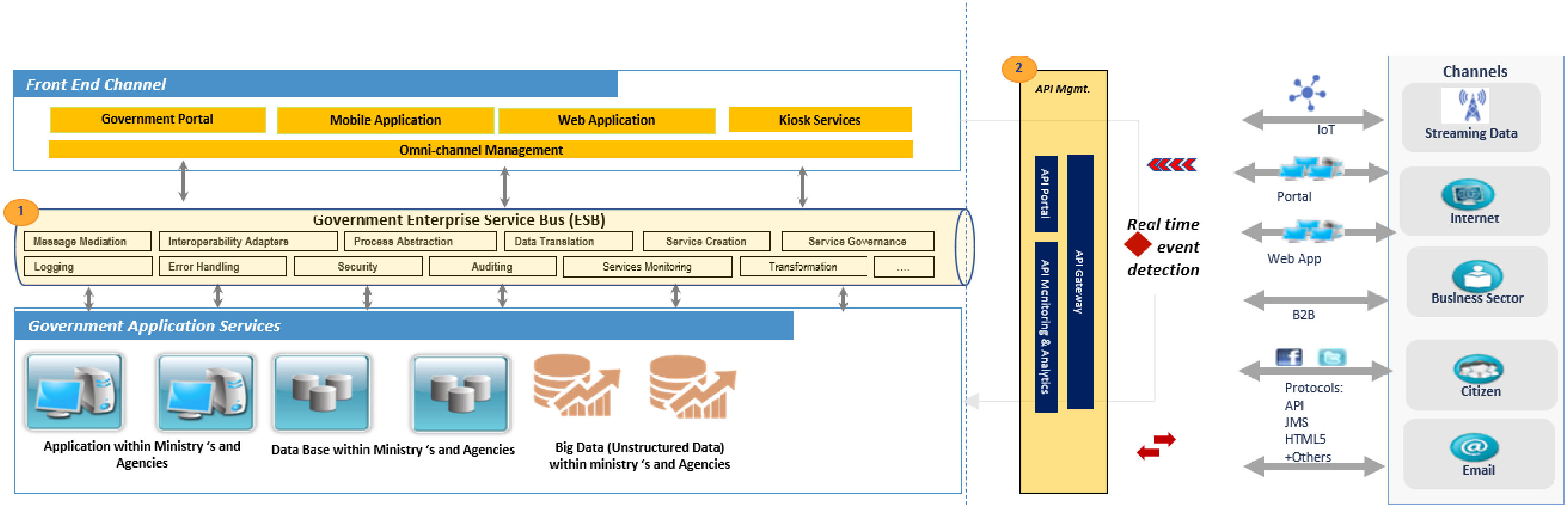
Access to authentic data sources across MDAs will be facilitated if the interfaces to these sources are published and harmonised, at both the semantic and technical level.

Recommended Approach: **MDAs, when working towards the establishment of Government of Ghana Digital Services, should develop the necessary interfaces to authentic sources and align them, at semantic and technical level.**

3.2.1.2 Interoperability Facilitators

Interoperability facilitators provide services such as translation between protocols, formats, languages or standards.

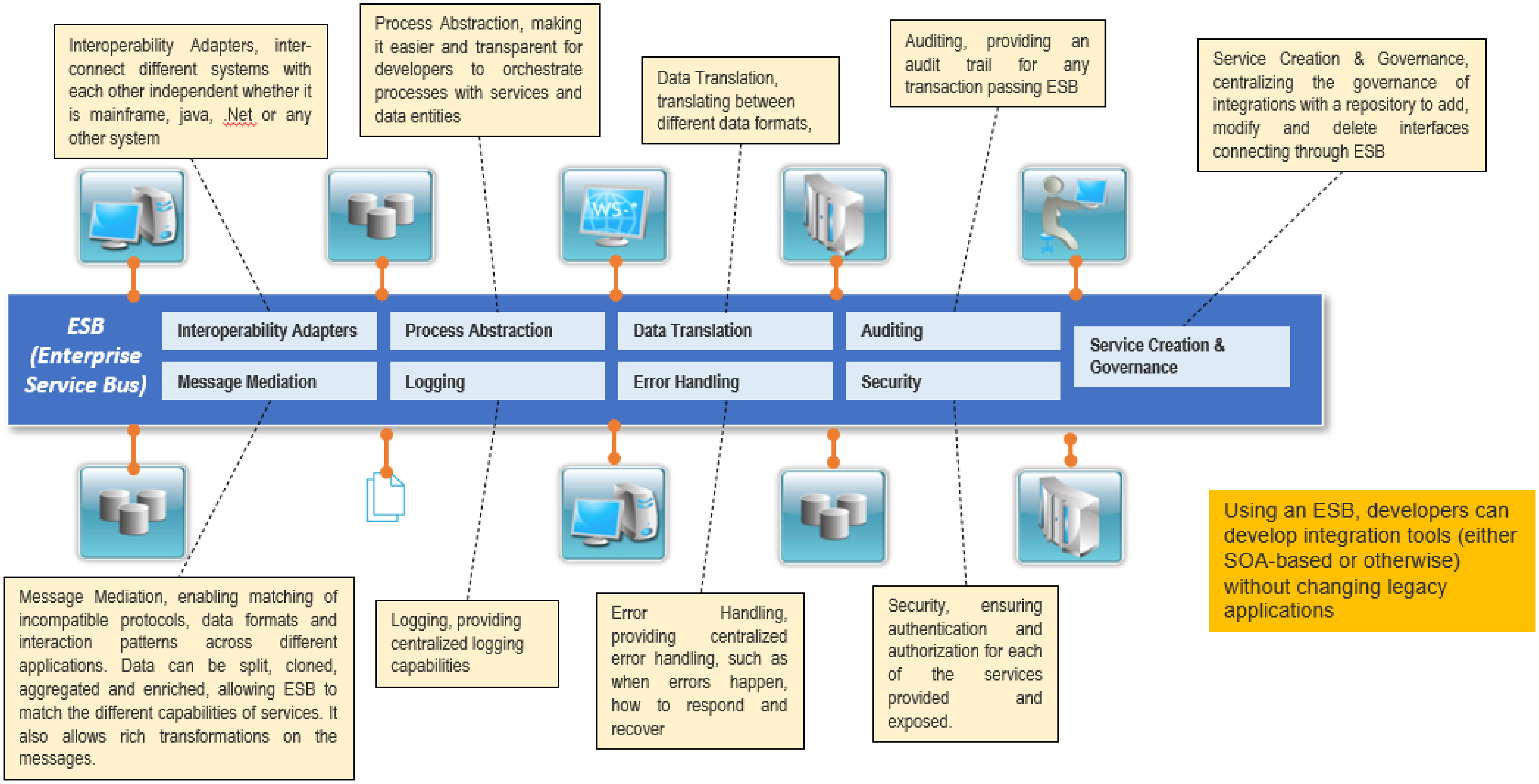
For our purposes, these will include Enterprise Service Bus (ESB) and Application Programming Interface (API) technologies, as illustrated on the following page.



An ESB provides interoperability between back-end systems (e.g., base registries or systems of record) within MDAs. Traffic is predictable, security is within MDA control and systems technologies (mainframe, Java, .Net etc) and data formats can be very different. Additionally, most of these interfaces may involve transactions that need roll-back and error handling mechanisms in place in case of failure. An ESB is used mainly for ***horizontal integration*** *as the interfaces are mainly between back-end systems.*

API Management is focused on ***vertical integration*** *between backend systems (systems of record) and front-end channels and third parties (citizen, businesses and external partners), the so-called systems of engagement. The features therefore are different as they need to handle and control large peaks of traffic, security and agility amongst others*

Figure 4 - Interoperability Facilitators - ESB and API



Interoperability Adapters, inter-connect different systems with each other independent whether it is mainframe, java, .Net or any other system

Process Abstraction, making it easier and transparent for developers to orchestrate processes with services and data entities

Data Translation, translating between different data formats,

Auditing, providing an audit trail for any transaction passing ESB

Service Creation & Governance, centralizing the governance of integrations with a repository to add, modify and delete interfaces connecting through ESB

Message Mediation, enabling matching of incompatible protocols, data formats and interaction patterns across different applications. Data can be split, cloned, aggregated and enriched, allowing ESB to match the different capabilities of services. It also allows rich transformations on the messages.

Logging, providing centralized logging capabilities

Error Handling, providing centralized error handling, such as when errors happen, how to respond and recover

Security, ensuring authentication and authorization for each of the services provided and exposed.

Using an ESB, developers can develop integration tools (either SOA-based or otherwise) without changing legacy applications

Figure 5 - ESB Functionality

3.2.1.3 External Services

This includes services provided by external parties such as, at business level, payment services provided by financial institutions, or at infrastructure level, connectivity services provided by telecommunications providers.

3.2.2 The Secure Data Exchange Layer

This layer is central to the Conceptual Model since all access to services passes through it.

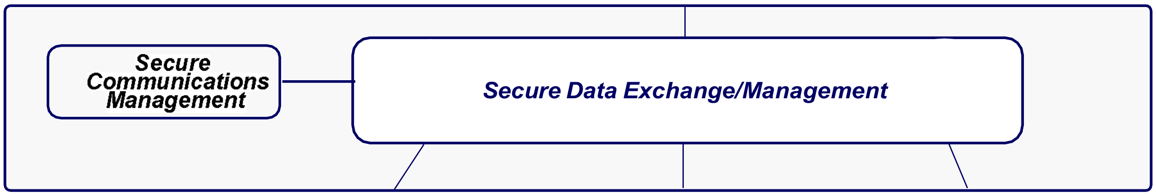

Secure Communications Management
Secure Data Exchange/Management

Figure 6 - The Secure Data Exchange Layer

3.2.2.1 Secure Data Exchange

From the business point of view, MDAs and other entities are exchanging official information, which might involve access to base registries. Such access should go through a secure, harmonized, managed and controlled layer providing information exchanges between administrations, businesses and citizens that are:

1) ***Signed and Certified*** – both sender and receiver have been identified and authenticated through agreed mechanism,
2) ***Encrypted*** – the confidentiality of the transported data is ensured,
3) ***Logged*** –the electronic records are logged and archived to ensure a legal audit trail.

In the eGIF conceptual model, those functions are grouped in the Secure Data Exchange layer.

This layer should allow secure exchange of certified messages, records, forms and other kinds of information among the different systems. In addition to the pure transport of data, specific security requirements such as handling of electronic signatures, certification, encryption, time-stamping, etc., should also be managed in this layer.

Security is one the most important barriers for interoperability if not applied in a harmonised and agreed way among organisations. The conceptual model intends to highlight this fact and draw the attention of all service providers to consider the security issues head-on, and to collaborate on a common framework to meet their respective security needs via compatible mechanisms and commonly agreed specifications, as well as to reach common understanding on essential characteristics such as authorisation levels and authentication strength.

3.2.2.2 Secure Communications Management

The provision of secure, i.e., signed, certified, encrypted and logged, data exchange also requires several management functions, including:

1) ***Service Management**:* to ensure oversight of all communication activities relating to identification, authentication, and authorization, data transport, etc., including e.g., access granting, revocation, and audit.
2) ***Service Registry**:* to ensure, given proper authorization, access to available services through prior localisation as well as verification that the service is trustworthy.
3) ***Service Logging**:* to ensure that logging of all data exchanges for future evidence is adequately performed, including archiving when necessary.

3.2.3 The Aggregated Services Layer

Aggregated GGDS are constructed by grouping a number of basic public functions that are accessed in a secure and controlled way. Those functions can be provided by several administrations of any level, i.e., local, regional, or national level.

The typical aggregated service is intended to appear to its users (other MDAs, businesses or citizens) as one single service. Behind the scenes, transactions may be implemented across sectors and administrative levels, and even across borders.

Aggregation is accomplished via appropriate mechanisms according to the specific business requirements. In the most general case, some business logic would be required to implement the requirements and the implementation mechanism could take several forms, such as orchestration or workflow engines, all of them included in portal-(e.g., ghana.gov) access infrastructures.

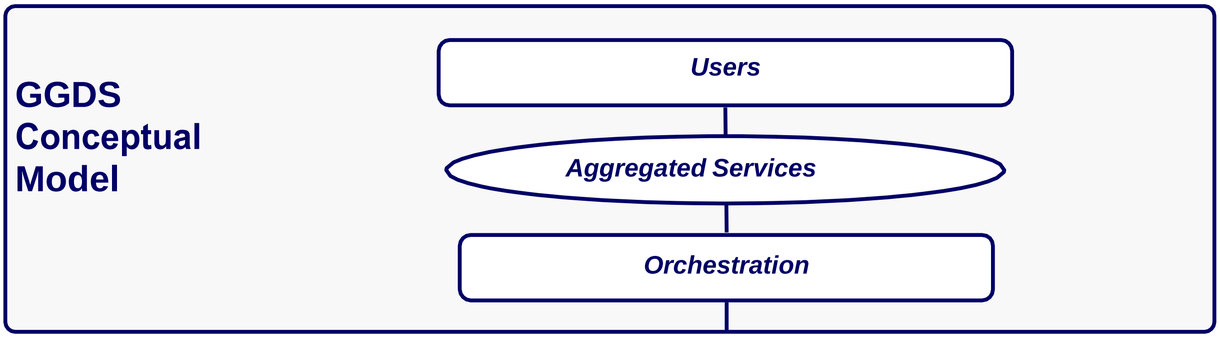


Figure 7 - The Aggregated Services Layer of the eGIF Conceptual Model

If aggregated public services are provided by intermediaries, MDAs should establish:

- a process of authorization in order to determine which public information may be disclosed to which intermediary, and
- a certification of intermediaries in order to establish trust between users and providers of the services.

3.3 Application of the Conceptual Model

The Conceptual Model's power comes from its flexibility to create different aggregated services by combining service components from a broad variety of providers. Using the Conceptual Model, the potential of further aggregating and combining the different services is unlocked.

A number of issues deserve highlighting in this regard:

Trust: The application of the conceptual model involves allowing external access base registries, hence requiring a high degree of security and trust.

Service levels and Government of Ghana Digital Services dependence on lower-level services: As the aggregated service depends on the basic functions provided by different entities, appropriate SLA's must be put in place in order to guarantee a secure and reliable provision of the service.

Common interface standards for basic public functions: The fact that basic functions, on which aggregated services are based, are developed by different MDAs highlights the need for common interface standards at technical and semantic level.

Privacy and Data protection: The Secure Data Exchange layer implements and enforces the security requirements for the aggregated service. As data originating from different MDAs may have attached to them different data protection requirements, a set of common requirements for data protection should be agreed in order to implement the aggregate service.

Recommended Approach: MDAs, when working together towards the development of aggregated GGDS, should collectively develop a common taxonomy of basic functions and agree on minimum service requirements for the secure exchange of data.

4 INTEROPERABILITY LEVELS

There are four interoperability levels that require special attention when a new Ghana Public Service is established.

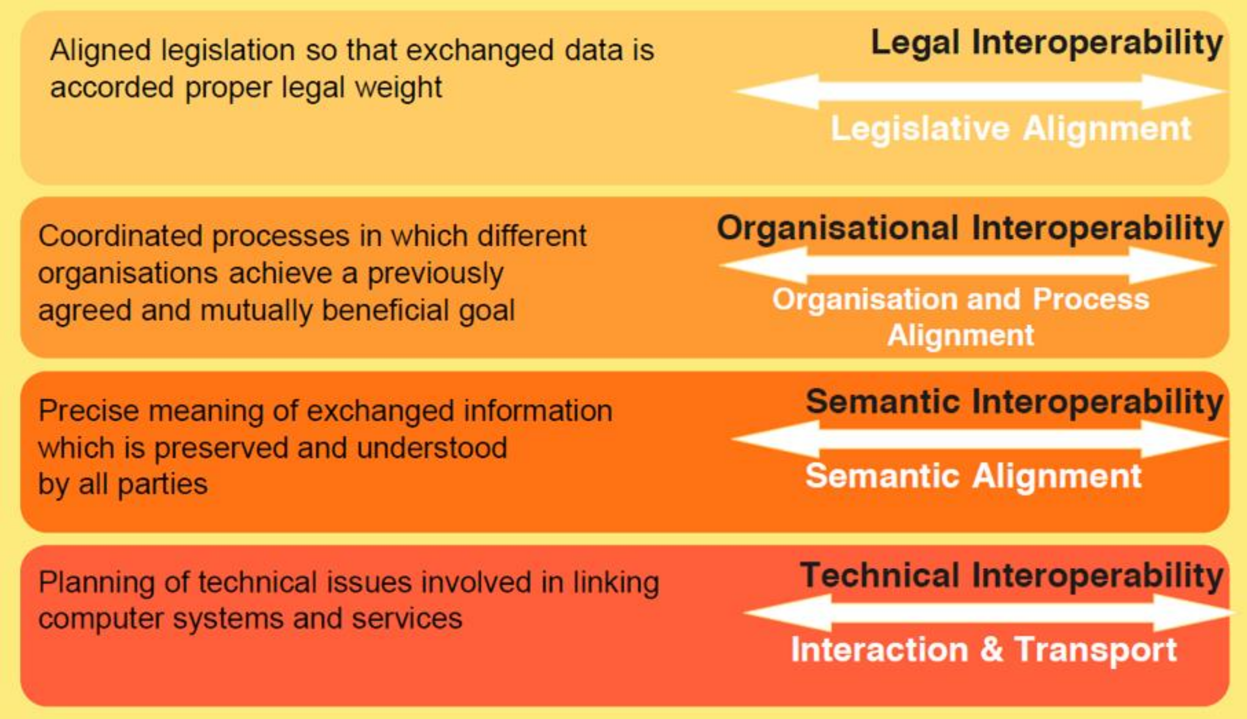

Aligned legislation so that exchanged data is accorded proper legal weight
Legal Interoperability
Legislative Alignment
Coordinated processes in which different organisations achieve a previously agreed and mutually beneficial goal
Organisational Interoperability
Organisation and Process Alignment
Precise meaning of exchanged information which is preserved and understood by all parties
Semantic Interoperability
Semantic Alignment
Planning of technical issues involved in linking computer systems and services
Technical Interoperability
Interaction & Transport

Figure 8 - The Four Levels of Interoperability

4.1 Legal Interoperability

Each MDA contributing to the provision of a Government of Ghana Digital Services works within its own legal framework.

Sometimes, incompatibilities between legislation governing different MDAs make working together more complex or even impossible. Legal initiatives may be needed to remedy such situations.

When exchanging information between MDAs in the context of the provision of a GGDS, the legal validity of such information must be maintained and the data protection policies in both originating and receiving MDAs must be respected.

Recommended Approach: **MDAs should carefully consider all relevant legislation and policy linked to the information exchange, including data protection legislation and policies, when envisaging the establishment of a GGDS.**

4.3 Organisational Interoperability

This aspect of interoperability is concerned with how MDAs in different sectors collaborate to achieve their mutually agreed goals. In practice, organisational interoperability is established through the integration of business processes and the related exchange of information.

4.3.1 Business Processes Alignment

In order for different MDAs to be able to work together efficiently and effectively to provide Government of Ghana Digital Services, they may need to align their existing business processes or even to define and establish new business processes.

Aligning business processes to contribute to GGDS implies documenting them, in a commonly agreed way, so that all MDAs contributing to the delivery of Government of Ghana Digital Services have a global view of the compounded business process and understand their role in it.

Recommended Approach: MDAs should document their business processes and agree on how these processes will interact to contribute to the delivery of a GGDS.

4.3.2 Establishment of Memoranda of Understanding and Service Level Agreements

Service orientation, on which the eGIF Digital Services conceptual model is built, requires the rigorous structuring of the relationships between service providers and service consumers.

Among other things, this involves the introduction of instruments to formalize the mutual assistance, joint activities, and interconnected business processes in the scope of services provision. These instruments can either be Memoranda of Understanding (MoU's) between MDAs on joint actions and cooperation and/or Service Level Agreements (SLA's) signed between participating MDAs.

Recommended Approach: MDAs contributing to the provision of GGDS should systematically define MoU's and SLA's for the part of the GGDS they provide and/or consume.

4.3.3 Change Management

Since the delivery of a Government of Ghana Digital Service is the result of the collective effort of a number of collaborating MDAs that produce or consume parts of the service, setting appropriate change management process is critical to ensure the accuracy, reliability and continuity of the service delivered to other MDAs, business and citizens.

Recommended Approach: MDAs collaborating on the provision of GGDS should define rigorous change management processes in order to ensure continuous delivery of such services.

4.4 Semantic Interoperability

Semantic interoperability enables MDAs to process information from external sources in a meaningful manner. It ensures that the precise meaning of exchanged information is understood and is preserved throughout the various exchanges between all communicating parties.

A starting point for achieving semantic interoperability is the establishment of sector-specific sets of data structures and data elements that can be referred to as semantic interoperability assets. Once these are established, the cooperating MDAs will need to agree on the meaning of the information to be exchanged. Due to the differing legal and administrative environments in the MDAs, reaching such agreements poses significant challenges.

In the context of the EGIF, the semantic interoperability level encompasses both of the following aspects:

- *Semantic Interoperability* is about the meaning of information elements and the relationship between such elements. It includes the development of the vocabularies used to describe information exchanges, and ensures that information elements are understood in the same way by communicating parties.

- *Syntactic Interoperability* is about describing the exact format of the information to be exchanged via grammars, formats, and schemas.

Achieving semantic interoperability in the Ghana context requires at least:

Agreed processes and methodologies for developing semantic interoperability assets;

Sector-specific and cross-sectoral communities to agree on the use of semantic interoperability assets at whole-of-government level, i.e., sector-specific and cross-sectoral elements.

Due to the complexity of the task, an organised effort towards harmonisation of both the processes and methodologies is needed.

Recommended Approach: MDAs should support the establishment of both sector-specific and cross-sectoral communities aimed at facilitating semantic interoperability and should encourage the sharing of results produced by such communities through GoG platforms.

4.5 Technical Interoperability

This aspect of interoperability covers the technical aspects of linking information systems. It includes aspects such as interface specifications, interconnection services, data integration services, data presentation and exchange, etc.

While MDAs have specific characteristics at the legal, organisational and partly at the semantic levels, interoperability at the technical level is not specific to MDAs. Therefore, technical interoperability should be ensured, whenever possible, via the use of the standards contained in this eGIF, or if such standards are not defined for a specific future use, either through standards endorsed by recognised standardisation organisations or technical specifications made available by industry consortia or other standardisation fora.

Recommended Approach: **MDAs should agree on the standards and specifications to be used to ensure technical interoperability when establishing Government of Ghana Digital Services.**

5 INTEROPERABILITY AGREEMENTS

This chapter presents the approach proposed to facilitate the cooperation of MDAs working together to provide a given Government of Ghana Digital Service.

As stated throughout this document, the provision of Government of Ghana Digital Services requires cooperation between different MDAs. Such cooperation takes place at the different interoperability levels described in the previous chapter. For each level, the MDAs involved should formalise their cooperation in interoperability agreements.

They should be drafted with sufficient level of detail so that they achieve the intended result – the provision of the GGDS in question – while leaving each organisation maximal internal autonomy.

At the legal level, interoperability agreements are expressed in concrete and binding terms via legislation, including Policy directives and their transposition into national legislation, whose details are outside the scope of the eGIF.

At the organisational level, interoperability agreements can take the form of MoU's or SLA's that specify the obligations of each party participating in cross-sectoral business processes. Interoperability agreements at the organisational level will define expected levels of services, support/escalation procedures, contact details etc., referring, when necessary, to underlying agreements at the semantic and technical levels.

At the semantic level, interoperability agreements take the form of, inter alia, reference taxonomies, schemes, code lists, data dictionaries or sector-based libraries.

At the technical level, interoperability agreements will include items such as communication protocols, messaging specifications, data formats, security specifications or dynamic registration and service discovery specifications.

While interoperability agreements at the legal and organisation level will normally be very specific to the GGDS to be provided, interoperability agreements at the technical level and, to a lesser extent, at the semantic can often be mapped onto existing specifications already formalised in the eGIF.

Recommended Approach: **When establishing Government of Ghana Digital Services MDAs should, as much as possible, base interoperability agreements on existing specifications already formalized in the eGIF.**

5.1 Assessing and Selecting Formalised Specifications

Because of their positive effect on interoperability, the use of open specifications, characterised by their potential for sharing and re-use, are encouraged in the context of Government of Ghana Digital Services delivery.

However, MDAs may decide to use less open specifications, especially in cases where open specifications do not meet the functional interoperability needs or the ones available are not mature and/or sufficiently supported by the market, or where all cooperating organisations already use or agree to use the same technologies.

Recommended Approach: **Other things being equal, MDAs should prefer open specifications when establishing Government of Ghana Digital Services.**

5.2 Contribution to the Standardisation Process

In some cases, MDAs may find that no suitable formalised specification is available for a specific need in a specific area. If consequently new specifications have to be developed, they may either develop the specifications themselves and put forward the result for formalization in the eGIF.

Even where existing formalised eGIF specifications are available, they evolve over time and, in general, revisions may take a long time to be completed. Active MDA participation in the eGIF standardisation process mitigates concerns about delays, supports a better alignment of the formalised specifications with MDA needs and can help GoG keep pace with technology innovation.

Recommended Approach: **MDAs should actively participate in the eGIF interoperability standardization activities that are relevant to their needs.**

TECHNICAL ANNEXES

Key Interoperability Area – Channels Interoperability

A channel is the means by which MDAs deliver services to their users. The formalised policies and standards listed below are intended to ensure that MDA systems to be deployed utilise channel technologies that can interoperate with other MDAs or users.

6.1 CHANNEL POLICIES

1. E-Government services should be designed to be accessible via multiple channels. MDAs' information systems should facilitate the use of various channels by citizens.

2. All government information systems providing e-Government services will support the Internet as a delivery channel, either directly or via third-party services.

3. Where middleware or plug-ins are required in using the Internet as a delivery channel it must be possible to upload and download without additional licensing fees or charges.

4. Systems employed by MDAs to provide Government of Ghana Digital Services must:

   - Be designed so that they are accessible through browser-based technology;

   - Provide services to the user (citizen and business) via a range of delivery channels and devices;

   - Be defined independently of any specific delivery channel;

6.2 CHANNEL STANDARDS

The formalised Channel standards listed below allow data to be interpreted and presented in consistent ways when shared between systems. Such standards include HTML (and XHTML) as well as selections from the wide range of image and streaming media formats. Also included are document encoding formats (e.g., RTF) and a range of specialised markup languages, including markup for mobile devices.

INTEROPERABILITY AREA	STANDARDS	DESCRIPTION	JUSTIFICATION
Portal	TCP, HTTP, HTTPS, SSL, TLS, SMTP XML, WML, voice XML v2.0, WSDL, UDDI, SOAP	Government & MDA Portals are Web based interfaces providing a comprehensive range of functionality including single point of access to various services, such as e-Payment, e- Forms and Identity management. Many Portals provide a Single Sign On capability to relevant structured and unstructured information, community of interest applications and collaboration. To be deployed for Internet, Intranet, Extranet.	HTTPS, SSL guarantees security for e-payments and password security.
Self Service Kiosks	TCP, HTTP, HTTPS, SSL, TLS, SMTP EXPAND ON STANDARDS LIST	A kiosk is a self-service device with onboard computer and a display screen. Kiosks are deployed at public buildings, used for information rendering as well as transaction services. Touch screens are the most common input method at self-service kiosk installations.	Plain/Formatted Text as files Hypertext documents as files
Fax	ITU-T Recommendations T.563, T.503, T.521, T.6, T.62, T.70, T.72	Used to create, examine, transmit and/or receive facsimile images	Became a standard in 1984 for digital facsimile devices to communicate over digital telephone lines.
Mobile Phone	GSM, CDMA, 3G, HSDPA, 4G, 5G, EDGE, GPRS, TDMA	Wireless phone used for mobile voice or data communication over a cellular network. Mobile (smart) phones are the most widely used channel for accessing the Internet in Ghana Additional services include SMS for text messaging, email, packet switching for access to the Internet, gaming, Bluetooth, infrared, camera with video recorder and MMS for sending and receiving image and video.	GSM is generally used by existing providers in the country. CDMA is still used by some operator such as: Verizon, US Cellular and old Sprint Network. Some of telco operator will shut down CDMA network in end of 2022.

Wireless PDA	802.15.1 for Personal Area Network (PAN). WPAN	The IEEE 802.15 Working Group, a part of the IEEE 802® LAN/MAN Standards Committee, develops Personal Area Network consensus standards for short distance wireless networks: a.k.a. WPANs™. WPANs address wireless networking of portable and mobile computing devices such as PCs, Personal Digital Assistants (PDAs), peripherals, cell phones, pagers, and consumer electronics.	Most current standard for Wireless PDAs. It is also compactible with Bluetooth 1.1
Interactive Television	MHEG-5, MHP-DVB, DAVIC, OCAP/ACAP	iTV describes several techniques that allow viewers to interact with television content as they view it, enabling the television (with set top box middleware) to become a channel for government content delivery.	Most current and widely used open/public software standards for interactive television
eForms	XForms 1.2	Electronic form is a dynamic document that captures information and submits it in structured way to government agencies for processing. The form is a visual representation of complex application, powered by Adobe Reader, and widely used by governments worldwide.	Xform enables electronic process management. The future of web forms are process-centric not content-centric. Compatible to SOA. Xform supports multiple schemas.

Table 1 - Channels Interoperability Technical Standards

Key Interoperability Area - Business Process Interoperability (BPI)

To make government services and information more accessible and to improve the efficiency with which they are provided, government must build the interoperability capability of its agencies, harmonise policies and regulations, integrate programs and streamline business processes.

Business process interoperability is crucial in this regard because of the increasing need for cooperation between and within MDAs in the delivery of quality services, the development of policies and the implementation of programs or projects.

7.2 BUSINESS PROCESS INTEROPERABILITY POLICIES

1. **BPI must enable MDAs to achieve common goals or deliver similar services.** Interoperability is an enabling strategy for the achievement of high-level goals, such as connected government. It is not an end in itself, but a means to achieve higher levels, strategic goals and outcomes.

2. **Benefits of BPI can only be achieved by a whole government commitment and alignment.**
   The transition to interoperability of business processes should be driven by a common vision that is aligned with a whole of government approach to policy development, program management and service delivery. To be successful, MDAs must apply the consistent approach (with a common language, standards and agreed governance arrangements) to business process management and interoperability described in the Enterprise Architecture.

3. **Based on an approach that is practical, rigorous and flexible.**
   BPI should be simple and easy to manage, produce consistent and predictable outputs and allow individual agencies to operate unique or specific processes.

4. **Improvements in government policy formulation.**
   Service delivery should be based on a thorough understanding of user needs and expectations with the aim of developing and Driven by Users

   BPI should be driven by users‘ needs, with the aim of improving formulation of government policy and delivery of services to users maintaining trusted relationships and designing effective policy and policy instruments. It is critical that consumers experience consistent and effective service performance across government programs and services, equivalent to that received from private sector service providers. User needs should define the service and, in turn, the service should define technology support requirements.

5. **Recognising that people and culture are keys to successful change.**

The process of interoperability must embrace people and organisational culture as much as it relates to processes and systems if the whole of government objectives are to be achieved and successfully sustained.

6. **Commitment to agreed standards**
   Commitment to agreed standards, guidelines, reference models and frameworks ensures consistency and provides participants with confidence and credibility in decision-making and actions.

7. **Should ensure trust, confidence and security for customers and partners**
   BPI based on trusted relationships instils confidence in users and collaborating agencies and ensures respect for privacy, confidentiality, and intellectual property and security requirements.

8. **Relevant BPI techniques and tools**
   Relevant BPI techniques and tools adopted should provide capabilities to create, deploy, and execute workflow management, enterprise application integration (EAI), and trading partner integration (TPI)

7.3 BUSINESS PROCESS INTEROPERABILITY STANDARDS

Web Services are self-contained, modular business process applications that are based on the industry standard technologies of WSDL (to describe), UDDI (to advertise and syndicate), and SOAP (to communicate). They enable users to connect different components even across organisational boundaries in a platform- and language-independent manner.

However, none of these standards allow defining the business semantics of Web services and thus, Web services remain isolated and opaque. Breaking isolation means connecting Web services by specifying how they are jointly used to realize complex functionality - typically a business process.

A business process specifies the potential execution order of operations from a collection of Web services, the data shared between these Web services, which partners are involved and how they are involved, joint exception handling, and other issues involving how multiple services and organisations participate. Breaking the opaqueness of Web services means specifying constraints on how the operations of a collection of Web services and their joint behaviour can be used.

Business Process Execution Language for Web Services (BPEL4WS) allows specifying business processes and how they relate to Web services. This includes specifying how a business process makes use of Web services to achieve its goal, as well as specifying Web services that are provided by a business process. Business processes specified in BPEL are fully executable and portable between BPEL-conformant environments. A BPEL business process interoperates with the Web services of its partners, whether or not these are implemented based on BPEL, and supports the specification of business protocols between partners and views on complex internal processes.

INTEROPERABILITY AREA	STANDARDS	DESCRIPTION	JUSTIFICATION
Execution Language	WS-BPEL,BPELJ BPEL4People is the latest version Reference: http://www.oasis-open.org	The WS-BPEL process defines how multiple service interactions with these partners are coordinated to achieve a business goal, as well as the state and the logic necessary for this coordination. Business Process Execution Language (BPEL), short for Web Services Business Process Execution Language (WS-BPEL) is a modelling language for specifying business process behaviour based on Web Services	Enabling users to describe business process activities as Web services and define how they can be connected to accomplish specific tasks
	Business Process Execution Language for Web Services 1.1 (BPEL4WS)	Business Process Execution Language for Web Services 1.1(BPEL4WS) provides a language for the formal specification of business processes and business interaction protocols using Web Services	It extends the Web Services interaction model and enables it to support business transactions. Version 1.1 is the current version. It is supported by the industry.
Business Reporting	XBRL Meta Model v2.1.1 Reference: http://www.xbrl.org/XBRLandBusiness/	eXtensible Business Reporting Language - an XML language for business reporting. XBRL (eXtensible Business Reporting Language) is an open standard which supports information modelling and the expression of semantic meaning commonly required in business reporting. XBRL is XML based	XBRL is a standards-based way to communicate business and financial information. Provides specification documents, not in separate files but in a single file.
Choreography	WS-Choreography Model	WS-Choreography Model Overview defines the format and structure of the (SOAP) messages that are exchanged, and the sequence and conditions in which the messages are exchanged.	Choreography is used to guide the generation of Web services, and possibly to guide the generation of handling of units of work. The only Web Service with a global view of all the services working in a concert.

	Web Service Choreography Interface (WSCI) 1.0 WSFL8	Web Service Choreography Interface (WSCI) describes how Web Service operations can be choreographed in the context of a message exchange in which the Web Service participates. WSCI also describes how the choreography of these operations should expose relevant information, such as message correlation, exception handling, transaction description and dynamic participation capabilities.	WSCI describes the interdependencies among the Web Service‘s operations so that any client:- Can understand how to interact with such service in the context of the given process; and Can "anticipate" the expected behaviour of such service at any point in the process‘ lifecycle. Being able to describe the dynamic interface of a service in the context of a particular process enables the developer/architect to abstract from the implementation and to focus on the role the Web Service plays in such process.
	Web Service Choreography Definition Language (CDL4WS) · 1.0 www.w3.org/2004/12/ ws-chor/cdl	Web Service Choreography Description Language (CDL4WS) is to specify a declarative, XML based language that defines from a global viewpoint the common and complementary observable behaviour, where message exchanges occur, and when the jointly agreed ordering rules are satisfied.	WS-CDL can be used to specify truly interoperable, collaborations between any type of party regardless of the supporting platform or programming model used by the implementation of the hosting environment
Human Resource Management	HR-XML (Human Resources XML) HR-XML Consortium Reference: http://www.hr-xml.org/channels/home.htm	HR-XML is a library of XML schemas developed by the HR-XML Consortium, Inc. to support a variety of business processes related to human resource management. It includes schemas to represent résumés, payroll information, and benefits enrolment and so on.	Data interchange standards for Human Resources and spans a diverse number of business processes. The HR-XML was developed to enable e-business between arms-length HR service providers To be considered for Human Resources Exchange applications.
Business Object Documents	OAGIS (Open Applications Group Integration Specification) Open Applications Group, Inc. ebXML (Electronic Business using	OAGI uses XML as its implementation architecture and has developed the largest set of business messages and integration scenarios for	OAGI enables business and business applications to communicate. A modular suite of specifications that enables enterprises of any size and in

	extensible Markup Language) OASIS Reference: http://www.openapplications.org/ http://www.oasis-open.org	enterprise application integration and business-to-business (B2B) integration.	any geographical location to conduct business over the Internet
Business Process Management	BPML(Business Process Modelling Language) V1.0 , ebXML (Electronic Business Extensible Business) Reference: http://www.ebxml.org/ geninfo.htm	Business Process Management Language (BPML) provides a meta-language for expressing business processes and supporting entities. Addressing complementary aspects of e-Business process management. And provides a standard way to describe the Public Interface of e-Business processes,	BPML provides an abstracted execution model for collaborative and transactional business processes based on the concept of a transactional finite-state machine.
Process Definition Language	XML Process Definition Language (XPDL) Reference: http://www.ebpml.org/ xpdl.htm	The purpose of XPDL is to have an XML format for the storage of BPMN diagrams. If different vendors use XPDL as their file format, they can easily exchange process models. For example, Vendor A could be used for initial process modelling, Vendor B for process analysis, and Vendor C for process execution. XPDL is considered to be complimentary to WS-BPEL, rather than a competing standard.	They can be employed as an integration platform for the exchange of process models that are specified in proprietary languages.
Modelling Notation	BPMN(Business Process Modelling Notation) Reference: http://www.omg.org/spec/BPMN/	Business Process Modelling Notation (BPMN) to provide a standard notation for the process diagram. The Business Process Modelling Notation (BPMN) is a standardised graphical notation for drawing business processes in a workflow.	The Modelling notation gives an analytical representation of all the business processes or transactions within the system and the level of interoperability between the various agencies using the system. The use of the UML could be the appropriate tool for the modelling of inter-agencies business processes.

Finance	XBRL (eXtensible Business Reporting Language) RIXML (Research Information Exchange Markup Language) IFX (Interactive Financial exchange) OFX (Open Financial Exchange) Reference: http://www.xbrl.org http:www.rixml.org http://www.ifxforum.or g/ifxforum.org/index.c fm http://www.ofx.net/ofx /default.asp http://www.ifxforum.or g/standards/	Used for financial reporting. The IFX is well designed XML- based financial messaging protocol. RIXML is used financial content format, essentially financial analysis and reports.	(OFX) Open Financial Exchange is the financial services industry standard to exchange electronic financial data with consumers and small businesses. RIXML expedites searching and accessing content IFX is a financial transport and exchange format. For example between bank and enterprise
e-Commerce, Logistics and Purchasing	ebXML (Electronic Business using extensible Markup Language) OASIS UBLV2.0 (Universal Business Language) OASIS Reference: http://www.oasis-open.org http://www.ebxml.org http://www.oasis-open.org/committees/ubl	A modular suite of specifications that enables enterprises of any size and in any geographical location to conduct business over the Internet	Businesses in any geographical area can conduct business over the internet. XML standard of business documents such as purchase orders and invoices
WorkFlow	OASIS Business Transaction Protocol Business Process Management Language(BPML)version0.4 Reference: OASIS Wf-XML (Workflow XML) Reference: Workflow Management Coalition http://www.wfmc.org/ http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=business-transaction http://www.bpmi.org	This protocol allows coordination of application work between multiple participants owned or controlled by autonomous organisations This schema defines a language used to exchange information among Workflow Management Systems	BPMI intends to continue to develop and promote open standards specific to particular e-business needs. XML is a formal recommendation by the World Wide Web Consortium and are supported by the major browsers.

Table 2 - Business Process Interoperability Technical Standards

Key Interoperability Area - Data Interoperability

Data/information is a very crucial element in any system and hence the need to outline policies and standards to ensure best practises are used in handling data within MDAs to enable interoperability.

8.1 DATA INTEROPERABILITY POLICIES

1. MDAs shall utilise Data/Information Policies, methodologies, standards and best practices to develop, acquire, and/or implement application systems that collect, modify, and store data and report information.

2. The Government of Ghana owns all data collected by or for any MDA under any statutory provision or by a contract. Also, any business document created or collected by any MDA belongs to the government.

3. A Government of Ghana, Data Superintendent position should be created under GicTED/ NITA who will be responsible for keeping the integrity and security of government data.

4. MDAs will define requirements and develop agreements before sharing data between primary authoritative data sources, whether those sources are internal or external to the MDA. Ongoing interchange arrangements require a single agreement but regular reviews of its operation must be included. One time interchanges still require an agreement to ensure the process is documented.

5. XML (Extensible Markup Language) must be the universal and primary standard for the exchange of data between all the information systems in the MDAs, and relevant for administrative purposes.

6. Data/Information Architecture outcomes are expressed in the form of data models, information flows, and analysis of inputs/outputs and decision-making criteria for the activities of State government.

7. Data modeling produces an accurate model, or graphical representation, of the budget unit's information needs and business processes. The data model is a framework for business re-engineering and the development of new or enhanced applications to fulfill business requirements and processes. Data modeling describes the types of interactions and information exchanges that occur within and between MDA and their various customers, constituencies and business partners.

8. MDAs will create and implement policies and standards to identify and capture all business documents created or received in their processes. Identification and subsequent

management of all business documents reduces the risk of poorly informed or inconsistent decision-making, increases business reliability, reduces duplication of effort, and prevents ad-hoc management by individuals.

9. MDAs will identify data elements for which they hold custodial responsibility by defining and maintaining their metadata in a data catalogue in line with the metadata standards in the e-GIF.

10. MDAs will establish and maintain access rules for the categories of data and business documents under his/her control. Access rules must be based on the principle of public and equitable access to information unless explicit reasons preclude this. The size of the electronic data catalogue will depend on the relevant MDA.

11. Electronic interfaces between systems must use mechanisms based on open industry standards as specified in the government information technology policies and standards.

12. Interfaces based on closed proprietary standards are likely to be more expensive to run and are prone to becoming obsolete.

13. A directory of common schemas shall be kept by GICTeD. When individual MDAs are developing schemas for any project, they are required to adopt the Common Schemas that are considered mature whenever possible.

14. While the business analysts are performing business information modelling, they should search the Central Registry for suitable Common Schemas. The suitability of a Common Schema is determined by whether the data element specification of that Common Schema (specifically the definition, representation, and business contexts) meets the requirements of a particular data element identified in a business document.Since Project Schemas may affect a system‘s future integration with the systems of other MDAs and external parties, project teams are recommended to share Project Schemas with other MDAs and external parties where relevant.

8.2 DATA INTEROPERABILITY STANDARDS

INTEROPERABILITY AREA	STANDARD	DESCRIPTION	JUSTIFICATION
Data Integration/ Exchange	XML v 1.0 (Second Edition) and related W3C	XML is a markup language for documents containing structured information. It is a W3C Recommendation for marking up data that cannot be marked up using the HTML. It is a simple dialect of the Standard Generalised Markup Language (SGML) defined in ISO Standard 8879. The goal of XML is to enable SGML coded data to be served, received, and processed on the Web in the way that is as easy as that currently made possible by the use of the fixed SGML tag set provided by HTML. XML has been designed for ease of implementation and for interoperability with both SGML and HTML. XML is based on the ISO 10646 Universal Multiple-Octet Coded Character Set (UCS) so that it can be used in all major trading nations. **Reference:** XML v1.0 (Second Edition) is a W3C Recommendation. The specification is published at http://www.w3.org/TR/REC-xml.	XML is a global, matured and widely adopted standard on data integration. XML is extensively supported by a broad range of application development, software infrastructure, business application and industry-specific schema initiatives.
XML schema definition	XML Schema v1.0	XML Schema defines the structure, content and semantics of XML documents. It is appropriate for data-oriented message exchange and processing.	XML Schema is extensively supported by application development tools, application server, enterprise application integration, content management and business application products

Data transformation	XSL v1.0 (Extensible Stylesheet Language) as defined by W3C XSL Transformation (XSLT) as defined by W3C	XSL is a language for expressing stylesheets. It consists of two parts: a language for transforming XML documents, and an XML vocabulary for specifying formatting semantics. An XSL stylesheet specifies the presentation of a class of XML documents by describing how an instance of the class is transformed into an XML document that uses the formatting vocabulary. **References:** XSL (Extensible Stylesheet Language) as defined by W3C http://www.w3.org/TR/xsl XSL Transformation (XSLT) as defined by W3C http://www.w3.org/TR/xslt	XSL v1.0 (comprising XSLT and XPath) is widely supported by enterprise application integration, application server, application development and content management products.
MetaData Standards	WS-policy 1.5 http://www.w3.org/TR/ws-policy/	Web Services Policy Framework defines a base set of constructs that can be used and extended by other Web services specifications to describe a broad range of service requirements and capabilities.	The WS-Policy and WS-PolicyAttachment specifications extend the foundation of Web Services used for interoperability and offer mechanisms to represent the capabilities and requirements of Web services as Policies.
	WS-Discovery	This specification defines a multicast discovery protocol to locate services. By default, probes are sent to a multicast group, and target services that match return a response directly to the requester.	Its applicability is especially important on sensors and devices networks where nodes change location constantly. Typically, WS-Discovery is used in combination with UDP in order to broadcast discovery messages to different nodes.
	WS-Policy Assertions 1.1	WS-Policy Assertions provides an initial set of assertions to address some common needs of Web Services applications	WS-Policy Assertions is a building block that is used in conjunction with other Web service and application-specific protocols to accommodate a wide variety of policy exchange models.

	WS-MetadataExchange 1.1	WS-MetadataExchange enables a service to provide metadata to others through a Web services interface. Given only a reference to a Web service, a user can access a set of WSDL /SOAP operations to retrieve the metadata that describes the service.	Necessary for the exchange of metadata catalogues between entities.
Data description language	RDF (Resource Description Framework) as defined by RDF can be used with OWL for adding semantics.	RDF data model defines a simple model for describing interrelationships among resources in terms of named properties and values. RDF properties may be thought of as attributes of resources and in this sense correspond to traditional attribute value pairs. RDF properties also represent relationships between resources. As such, the RDF data model can therefore resemble an entity-relationship diagram. The RDF data model, however, provides no mechanism for declaring these properties, nor does it provide any mechanism for defining the relationships between these properties and other resources. The complete specification of the RDF consists of 5 components including RDF Model Theory, RDF/XML Syntax, RDF Schema, RDF Test Cases and RDF Primer. **References:** http://www.w3.org/TR/REC-rdf-syntax	RDF is a W3C framework for supporting resource description or *metadata* (data about data), for the Web. RDF provides common structures that can be used for interoperable XML data exchange. RDF is a matured W3C Standard – RDF Model and Syntax

	Universal Description, Discovery and Integration (UDDI) 3.0.2	Universal Description, Discovery and Integration (UDDI) defines a set of services supporting the description and discovery of businesses, organisations, and other Web services providers, the Web services they make available, and the technical interfaces which may be used to access those services.	UDDI is a core web service specification. And its seen as a central pillar for web services infrastructure.
	Web Service Description Language 2.0 SOAP Binding 2.0	Web Service Description Language SOAP Binding describes the concrete details for using WSDL 2.0 in conjunction with SOAP 1.1 protocol.	The SOAP protocol actual invokes the services of the WSDL. In a situation where two or more agencies know more about their business transactions, they can use the SOAP interfaces to enhance the exchange of data between them. The SOAP uses the web protocols that create a platform for a program on one computer to interact with a program on another computer by specifying how to encode the a HTTP and XML header.
Data modelling language	UML (Unified Modelling Language) v 1.5	UML is an industry standard language for visualising, specifying, constructing and documenting data and systems which has been accepted by the Object Management Group (OMG). UML offers a standard way to write a system's blueprints, including conceptual things such as business processes and system functions as well as concrete things such as programming language statements, database schemas, and reusable software components. **References**: UML is defined by OMG at http://www.omg.org/technology/documents/formal/uml.htm	UML is supported by a broad range of application development, enterprise application integration, CASE, application server and software testing products for visualising, specifying, constructing and documenting data and systems.

BWF	Broadcast wave format (BWF) RF64	It is a file and metadata format based on Microsoft‘s WAVE format for transferring files between digital audio workstations **Reference:** http://www.ebu.ch	Since the only difference between a BWF and a "normal" WAV is the extended information in the file header (Bext-Chunk, Coding-History, etc...), a BWF does not require a special player for playback.
GIF	gif v89a	The 'Graphics Interchange Format' (gif) allows high-quality, high-resolution graphics to be displayed on a variety of graphics hardware and is intended as an exchange and display mechanism for graphics images. **References:** *www.gif.com* http://en.wikipedia.org/wiki/Graphics_Interchange_Format	GIFs support sharp-edged line art (such as logos) with a limited number of colours. This takes advantage of the format's lossless compression, which favours flat areas of uniform colour with well defined edges (in contrast to JPEG, which favours smooth gradients and softer images). GIFs can also be used to store low-colours sprite data for games. GIFs can be used for small animations and low-resolution film clips.
JPEG	Jpeg version 1.5.8	Joint Photographic Experts Group is a common graphic image file format and image compression algorithm. JPEG provides a means of reordering information so that, after only a small part has been downloaded, a hazy view of the entire image is presented rather than a crisp view of just a small part **References:** http://www.jpeg.org/jpeg/	JPEG standard is widely supported by browsers and the majority of image processing, graphics design, photo processing and scanner accessory software.
MPEG-7	*MPEG-7 Version 1.0*	-Multimedia Content Description Interface‖ - Standard for description and search of audio and visual content. **References:** http://www.chiariglione.org/mpeg/standards/mpeg-7/mpeg-7.htm	MPEG7 plays a complementary functionality role to the previous MPEG standards, representing information about the content, not the content itself It also provides a fast and efficient searching, filtering and content identification method.

MXF	Mxf lib *version* 0.6.0.	Material eXchange Format – an open file format for the interchange of audio-visual material with associated data and metadata. MXF is a "container" or "wrapper" format which supports a number of different streams of coded essence, encoded with any of a variety of codecs, together with a metadata wrapper which describes the material contained within the MXF file **References:** http://en.wikipedia.org/wiki/MXF	MXF systems produce split-file A/V (that is, the video and audio stored in separate files), and use a file naming convention which relies on randomly generated filenames to link them. Not only does this exacerbate the issue of knowing exactly what is in an MXF file without specialised tools, but it breaks the functionality of standard desktop computer techniques which are generally used to manipulate data on a level as fundamental as moving, copying, renaming, and deleting
PDF(Adobe Specification)	PDF 9.0	Unlike other electronic file formats such as HTML or XML, the PDF captures all of the elements of a printed document as an electronic image and preserves the exact layout, font attributes, and formatting of the document from which it was created, ensuring that the electronic version of a document appears just like the original. Users can view, navigate, print and forward to other users.	PDF is a dominant format for document publishing which is extensively used on the Internet. It is supported by freely available Acrobat Reader and browser plug-ins.
PNG	(Portable Network Graphics) PNG Specification version 1.0	Portable Network Graphics – a format for storing bit-mapped images **References:** http://www.w3.org/Graphics/PNG/	It can be stored in interlaced order to allow progressive display. The purpose of this feature is to allow images to ―fade in‖ when they are being displayed on-the-fly. Interlacing slightly expands the file size on average, but it gives the user a meaningful display much more rapidly
RTF encoded document	RTF 1.6 RTF 1.8 RTF 1.9.1(newest version)	Rich Text Format is a method of encoding text formatting and documenting structure using the ASCII character set. **References:** http://en.wikipedia.org/wiki/Rich_Text_Format	Since there is no guarantee that the ―look and feel‖ of a document can be preserved 100% when the document is created, RTF ensures that the document is totally preserved

SVG	SVG Version 1.1	It is an XML specification and file format for describing two-dimensional vector graphics, both static and dynamic (interactive or animated **References:** http://en.wikipedia.org/wiki/Rich_Text_Format	The only available open standard that describes a two-dimensional vector graphics.
TIFF	TIFF *Version* 6.0	Tagged Image File Format A widely-supported tag-based bitmap image format **References:** http://en.wikipedia.org/wiki/TIFF_(disambiguation)	Today, TIFF is a standard file format found in most paint, imaging, and desktop publishing programs and is a format native to the Microsoft Windows GUI. TIFF's extensible nature, allowing storage of multiple bitmap images of any pixel depth, makes it ideal for most image storage needs.
XHTML	XHTML version 2.0	Extensible Hypertext Markup Language - A reformulation of HTML 4.0 in XML 1.0 **References**: http://en.wikipedia.org/wiki/XHTML	XML is a markup language where everything has to be marked up correctly, which results in "well-formed" documents. XML was designed to describe data and HTML was designed to display data. Therefore - by combining HTML and XML, and their strengths, we got a markup language that is useful now and in the future - XHTML.
Extensible Markup Language	Version 1.0 (Third Edition)	XML is a general-purpose specification for creating custom markup languages It is classified as an extensible language because it allows its users to define their own elements eXtensible Markup Language - a meta language (a way to define tag sets) that supports design of customized markup languages. It is also used in representing the signature of web resources and procedures for computing and verifying such signatures. **References:** http://www.w3.org/Signature/	Currently the best standard for data processing. Compatible with Service Oriented Architecture (SoA).

Primary Character set	Unicode UTF – 16 Bit encoded	The Unicode Standard [UNICODE] and ISO/IEC 10646 [ISO-10646] jointly define a coded character set (CCS), hereafter referred to as Unicode, which encompasses most of the world's writing systems. UTF-16, the object of this specification, is one of the standard ways of encoding Unicode character data; it has the characteristics of encoding all currently defined characters (in plane 0, the BMP) in exactly two octets and of being able to encode all other characters likely to be defined (the next 16 planes) in exactly four octets.	UTF-16 is a global, matured and widely adopted standard for character set.
Data Transformation	XSLT 2.0 the XML transformation language TXL - prototyping language-based descriptions using source transformation	A data transformation converts data from a source data format into destination data. **Reference**: http://en.wikipedia.org/wiki/Data_transformation	XSLT overlaps with XQuery 1.0 however, XSLT is stronger in its handling of narrative documents with more flexible structure, while XQuery is stronger in its data handling, for example when performing relational joins. XSLT therefore seems to be the only option for data rendering.
File Compression	Zip Rar	File compression is the practice of packaging a file or files to use less disk space. The File Compression category includes software programs that will archive your files and extract archived files.	Winzip and winrar has become a common file compression tools. It should be adopted for all file compression.

Formatted document file type for collaborative editing	.rtf v1.8 HTML and XHTML as implemented by commonly adopted versions of browsers .doc (Word 2007 file format which is used by Word 2007 and later versions).	Rich Text Format is a method of encoding text formatting and documenting structure using the ASCII character set **References:** http://en.wikipedia.org/wiki/Rich_Text_Format HTML is implemented by commonly adopted versions of browsers.	Since there is no guarantee that the –look and feel‖ of a document can be preserved 100% when the document is created, RTF ensures that the document is totally preserved. HTML is implemented by commonly adopted versions of browsers.
Presentation file type for collaborative editing	ppt (PowerPoint file format which is used by PowerPoint and later versions) .sxi OpenDocument 2.0	.ppt and .sxi presentation file types are the proprietary Microsoft PowerPoint presentation format and Open Office. These formats are to be used in inter-departmental information interchange between users of Microsoft PowerPoint and Open Document	Microsoft PowerPoint is one of the major presentation applications both in public and private sector. It is supported by open source alternatives .sxi also supports open source applications such as Open Document.
Spreadsheet file type for collaborative editing	.xls (Microsoft Excel file format) .sxc OpenDocument 2.0	.xls spreadsheet file type is the proprietary Microsoft Excel spreadsheet format. This format is to be used in interdepartmental information interchange between users of Microsoft Excel. .sxc is a spreadsheet format on an Open Office platform	xls and sxc are widely adopted file format for spreadsheet. They are extensively supported by dominant spreadsheet applications such as Microsoft Excel, Lotus 123, and OpenOffice Calc
E-mail format	Plain text emails HTML emails	These are the standard formats for store and forward method of writing, sending, receiving and saving messages over electronic communication systems. **References:** http://en.wikipedia.org/wiki/Email	There are different format for representing an e-mail. Therefore is becomes a pre-requisite for policies to be made to ensure that the e-mails that are sent or received does not pose any security risk.
Compressed files	.ZIP .RAR .TAR.GZ and .TGZ.	It is the conversation of source files in a single destination output file.	Winzip and Winrar has become a common file compression tools. It should be adopted for all file compression. Files made as one file and generally much smaller than the original size of all the files. This allows the file to be downloaded faster or more data to be stored on a removable media.

RDF		RDF data model defines a simple model for describing interrelationships among resources in terms of named properties and values. As such, the RDF data model can therefore resemble an entity-relationship diagram. The RDF data model, however, provides no mechanism for declaring these properties, nor does it provide any mechanism for defining the relationships between these properties and other resources. The complete specification of the RDF consists of 5 components including RDF Model Theory, RDF/XML Syntax, RDF Schema, RDF Test Cases and RDF Primer. **Reference:** www.w3.org/r df	RDF is a W3C framework for supporting resource description or *metadata* (data about data), for the Web. RDF provides common structures that can be used for interoperable XML data exchange. RDF is a matured W3C Standard – RDF Model and Syntax
UTF-16		ISO/IEC 10646-1 defines a multi-octet character set called the Universal Character Set (UCS) which encompasses most of the world's writing systems. Multi- octet characters, however, are not compatible with many current applications and protocols, and this has led to the development of a few so-called UCS transformation formats (UTF), each with different characteristics. UTF-8 has the characteristic of preserving the full US-ASCII range, providing compatibility with file systems, parsers and other software that rely on US-ASCII values but are transparent to other values. **Reference:** UTF-8 is a proposed IETF standard defined in RFC 2279–UTF-8, a transformation format of ISO 10646‖.	UTF-16 is a matured standard – an IETF standard since January 2004. It is widely supported by all dominant operating systems. UTF-16 preserves the full US- ASCII range, providing compatibility with file systems, parsers and software that rely on ASCII values

Table 3 - Data Interoperability Technical Standards

Key Interoperability Area - Network Interoperability

Network Interoperability refers to the functional inter working of a service across or between multi-vendor, multi-carrier inter-connections (i.e., node-to-node, or network-to-network) working under normal and stress conditions, and per the applicable standards, requirements, and specifications.

9.2 NETWORK INTEROPERABILITY POLICIES

1. Networks shall be operational, reliable, and available (24x7x365) for essential business processes and mission-critical business operations.

2. Networks shall be designed for growth and adaptability.

3. Networks shall use industry-proven, mainstream technologies based on pervasive-industry standards and open architecture.

4. Network access must be a function of authentication and authorization, not location.

5. All newly procured Network switches and other devices should support coexistence of IPv4 and IPv6.

6. All MDAs should use DNS for Internet/intranet domain names and for IP address resolution.

7. FTP should be used where file transfer is necessary within government intranets.

8. Restart and recovery facilities of FTP are to be used when transferring very large files.

9. Wireless LAN solutions must be based on the IEEE 802.11 series of standards.

10. IP-SEC must be used to secure wireless LANs deployed for restricted government information.

11. Network Interfaces: Internal networks using private, unregistered IP addresses for network workstations and appliances shall use reserved addresses as defined by the Internet Assigned Numbers Authority (IANA).

12. Internal networks using public, registered IP addresses for network workstations and appliances are acceptable for current use. External networks communicating outside the budget unit shall use public, registered IP addresses for all external ports on internetworking devices.

13. Cabling / Structured Cabling installations for new buildings, major cable plant additions or

modifications, building renovations or remodeling, shall meet all minimum requirements and mandatory criteria in the most recent Telecommunications Industry Association/Electronic Industries Association (TIA/EIA) standards.

9.3 NETWORK INTEROPERABILITY STANDARDS

INTEROPERABILITY AREAS	STANDARDS	DESCRIPTION	JUSTIFICATION
Wireless LAN	IEEE 802.11k or 802.r http://standards.ieee.org/getieee802/802.11.html	The 802.11g specification is a standard for wireless local area networks (WLANs) that offers transmission over relatively short distances at up to 54 megabits per second (Mbps)	Wireless LAN Device with Wi-Fi Certificate is recommended to establish interoperability between different manufactures and devices. And all new Access Points and new Client devices are highly recommended to support IEEE 802.11g
Mobile Device Internet Access	WAP v2.0 – for use with WAP devices www.openmobilealliance.org WML v2.0 – Wireless Markup Language version 2.0.	Wireless Application Protocol is a secure specification that allows users to access information instantly via handheld wireless devices such as mobile phones, pagers, two- way radios, smart phones, and communicators. WML allows the text portions of Web pages to be presented on mobile telephones and PDAs via wireless access. WML is under the Wireless Application Protocol (WAP)	The WAP protocol is based on Internet technology like IP and XML and is published by the WAP Forum. Today, all major mobile equipment manufactures support the WAP protocol. WAP defines a communications protocol as well as an application environment. In essence, it is a standardized technology for cross- platform, distributed computing.
Wireless LAN Security	802.11i WPA 2.0	**Wi-Fi Protected Access** (**WPA** and **WPA2**) is a certification program created by the Wi-Fi Alliance to indicate compliance with the security protocol created by the Wi-Fi Alliance to secure wireless computer networks. This protocol was created in response to several serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP).	WPA2 replaced WPA; like WPA, WPA2 requires testing and certification by the Wi-Fi Alliance. WPA2 implements the mandatory elements of 802.11i. It introduces a new AES-based algorithm, CCMP, which is considered fully secure. WPA 2.0 is recommended.

LAN/WAN Internetworking	IPv4 – http://www.ietf.org/ rfc/rfcs791.txt,762, txt, 919.txt, 922.txt, 1 112.txt IPv6 – Internet protocol version 6. http://www.ietf.org/rfc/rfc	The Internet Protocol (IP) is part of the Transmission Control Protocol/Internet Protocol suite which is the basic communication protocol used on the Internet. IPv6 - Internet *Protocol version 6* is the second version of the Internet Protocol to be used generally across the virtual world.	Internet Protocol version 4. The protocol by which data is sent between interconnected packets switched computer communication networks. Internet protocol version 6 is a new version of IP which is designed to be an evolutionary step from IPv4. It provides longer address capabilities therefore creating many internet addresses to support users and servers. Also, IPv6 provides additional security features that do not exist in IPv4. For example, Authentication Header (AH) is introduced for data integrity in IPv6 transmission. IPv6 is recommended
LAN/WAN Transport Protocol	TCP –RFC 793 http://www.ietf.org/ rfc/rfc793.txt	TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet.	Transmission Control Protocol. Used along internet protocol in the provision of data communication on the Internet.
	UDP –RFC 768 http://www.ietf.org/ rfc/rfc768.txt	UDP (User Datagram Protocol) is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP)	User Datagram Protocol. Alternative transport protocol to TCP that offers minimal transport service for applications using multicast broadcast delivery DNS, routing information for network management. Both TCP and UDP are adopted standards.

Directory Access	LDAPv3 http://www.ietf.org/ rfc/ rfc2830.txt, 1777.txt, 2251.txt, 1274.txt,1 276.txt, 1308.txt, 1492.txt, 2116.txt	Lightweight Directory Access protocol version 3. Protocol for accessing online directory services. It is both a network protocol and a standard architecture for organizing the directory data.	LDAP is the dominant directory access protocol supported by all the major directory software providers. Version 3 is the latest version of LDAP and has been widely adopted.
Domain Name Service DNS	http://www.ietf.org/ rfc/ rfc1035.txt, 1035.txt	Domain Name Service used for Internet/Intranet domain for IP resolution. A service for mapping domain names and corresponding IP Address	Facilitates addressing of computers with names instead of IP Address. It is the dominant names to IP resolution standard on the internet. DNS is widely adopted.
Mailbox Access	POP3 http://www.ietf.org/ rfc/rfc1939.txt, 2449.txt	for basic mailbox (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail	POP3 is widely used and will remain in the email standards, and is known for its simplicity and ease of implementation. Should only be used on basic mail exchange.
	IMAP4 rev1 RFC 2060 RFC 2342 RFC 2971	IMAP - Internet Message Access Protocol is a standard protocol for accessing e-mail from your local server, for more advanced clients; manipulation of messages on the server	IMAP provides the user more capabilities for retaining e-mail on the server and for organizing it in folders on the server. Should be adopted for higher functionality of mail exchange. Better option.
E-mail Transport	SMTP, POP v3, IMAP, http://www.ietf.org/ rfc/ rfc2821.txt, 2822.txt	(SMTP) Simple mail Transport Protocol. (POP) Post Office Protocol, (IMAP) Internet Message Access Protocol. Protocol used to send e-mail on the internet. Host to Host Protocol	Is the most popular E – mail Transport Protocol used by most Internet Email Servers and Email Clients. SMTP is widely adopted.
E-mail format	MIME rfc2045.txt,2046 .txt, 2047.txt, 2048.txt, 2049.txt, 2231.txt, 3023.txt , 2557.txt, 2392.txt, 2387.txt	**Multipurpose Internet Mail Extensions** (**MIME**) is an Internet standard that extends the format of e-mail to support: • Text in character sets other than ASCII • Non-text attachments • Message bodies with multiple parts • Header information in non-ASCII character sets http://www.ietf.org/rfc/	For the embedding of binary data into e-mail handled by ordinary electronic mail interchange protocols. MIME is widely adopted for SMTP e-mails.

	S/MIME	E-mail Secured Format	Secured Multipurpose Internet Mail Extension used for secured mail attachment.
Hypertext transfer protocol	HTTP V1.1 http://www.ietf.org/ rfc/ rfc2616.txt www.w3.org/protocols	Application-level protocol for world wide web.	Provides a simple standard for transferring text base documents across various devices of different architecture HTTP is a worldwide, established and widely accepted internet standard used since 1990. Supported by all web servers and browsers.
Secured hypertext transfer protocol	HTTPS http://www.ietf.org/rfc/rfc2818.txt	A secured version of HTTP using secured socket layer TLS.	Provides a secured version of the HTTP to transfer sensitive data across the internet
File Transfer	FTP http://www.ietf.org/ rfc/rfc765.txt, rfc114.txt	File transport protocol internet protocol for transferring files from one computer to another.	FTP is a communication protocol that supports transmission of all types of digital files over the Internet, irrespective of their size. And supported by all relevant products.
	SFTP	Secure FTP, uses SSH to transfer files as well as commands by encrypting the data	
WAN Internetworking	BGP4	Border Gateway Protocol is a protocol for exchanging routing information between gateway hosts (each with its own router) in a network of autonomous systems.	Provides a system of sharing routing information among different network devices
Remote Services Delivery Protocol	SOAP v1.2 http://www.w3.org/ TR/soap12-part0/ http://www.w3.org/ TR/soap12-part1 http://www.w3.org/ TR/soap12-part2	SOAP – Simple Object Access Protocol states the definition of an XML document for the exchange of information, based on a one-way message exchange between a sender and receiver. Applications can combine SOAP messages to provide more sophisticated interactions, including remote procedure calls (RPCs) and conversational document exchange. SOAP	SOAP is one of the main technologies that drives web services and has significant industry support for a broad range of infrastructure and application providers. SOAP v1.2 standards was published as W3C Working Drafts since been used by Application server vendors, Enterprise application integration vendors,

		messages can be exchanged using a variety of protocols, including application layer protocols, such as HTTP and SMTP	Application development tool vendors, application vendors, like SAP and Oracle and Enterprise portal vendors
IP security	IP-SEC Authenticated header RFC 2402/2404	Internet Protocol Security is a framework for a set of protocols implementing security at the network and/or packet processing layers of network communication	For site-to-site Virtual Private Networks (VPNs) IPSec is preferred for secure communication. It provides both confidentiality and integrity of data. IPSec is widely adopted for site-to-site VPNs. SSL should be used for remote access VPNs.
IP encapsulation security	VPN requirements ESP RFC 2406	Virtual Private Network (VPN) is a network that uses a public telecommunication infrastructure or medium, such as the Internet, to establish a secured network to offices or individual to have a secure access to their organization’s network.	For site-to-site Virtual Private Networks (VPNs) IPSec is preferred for secure communication. It provides both confidentiality and integrity of data. IPSec is widely adopted for site-to-site VPNs.
Transport security	SSL v3, TLS, TLS 1.3, RFC 2246	SSLv3/TLS is a form of VPN that can be used with a standard Web browser.	SSL should be used for Remote Access VPNs. Access between a client computer to a secure network will be best implemented using SSLv3. There is low payload on the encrypted traffic unlike using IPSec VPNs.
Secure Shell	SSH File Transfer Protocol, SSH Transport Layer Protocol, SSH Authentication Protocol, SSH Connection Protocol, SSH Protocol Architecture, Generic Message Exchange Authentication For SSH http://www.ietf.org/ids.by.wg/secsh.ht ml	For securely administering a remote computer. Provides encrypted session between clients and servers for secure remote administration of systems.	Telnet provides an unsecure remote access to computer systems and should only be used within a secure infrastructure. SSH, however, provides a secure remote access. SSH is widely adopted.

Encryption algorithms	3DES	Encryption algorithm that encrypts data three times. Three 64-bit keys are used, instead of one, for an overall key length of 192 bits.	At minimum all implementation of encryption should support 3DES. Provides effective 128 bits key length.
	AES (FIPS 197 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf	Advanced Encryption Standard (AES), an encryption algorithm for securing sensitive but unclassified material by U.S. Government agencies and It may eventually become the base encryption standard for commercial transactions in the private sector.	Where optimum security is required, AES should be recommended. AES provides 256 bits key length.
For signing & Key Transportation	RSA	Internet encryption and authentication system	The RSA algorithm is the most used encryption and authentication algorithm and is mostly integrated into standard Web browsers. RSA is widely adopted.
	DSS FIPS 186-2 http://www.itl.nist.gov/fipspubs/fip186.htm	Digital Signature Standard (DSS) is the digital signature algorithm (DSA) developed by the U.S. National Security Agency (NSA) to generate a digital signature for the authentication of electronic documents.	
For hashing	SHA-512, SHA- 256 FIPS 180-2		A minimum of SHA-256 should be used for data integrity.
Structured Cabling System	TIA/EIA 568-B.1, ANSI/TIA-586-C, ISO/IEC 11801	A standard for telecommunications pathways	Widely used for cable installations for new buildings, major cable plant additions or modifications, building renovations or remodeling.
	The TIA/EIA 569-A	Standard for telecommunications pathways and spaces addresses floor loading, ceiling and perimeter pathways	
	TIA/EIA 606	Standard provides a uniform administration scheme to manage telecommunication infrastructure	

	TIA/EIA 607	Standard provides grounding and bonding requirements for telecommunications circuits and equipment	
Copper Network Cabling	Category 6, Category 5e, UTP Category 7 www.siemon.com/ us/standards	Cabling is certified to carry up to 10 Gbps of data up to 100 meters	Widely used for Structured Cabling System installations for new and/or renovated buildings without cabling shall be Category 6 Unshielded Twisted Pair (UTP) as specified by TIA/EIA 568-B.2.1 Commercial Building Telecommunications Cabling Standards. Category 6 link and channel requirements are backward compatible to Category 5e.
Fibre Network Cabling:	TIA/EIA-568-B series standards.	TIA/EIA-568-B is a set of three telecommunications standards from the Telecommunications Industry Association. The standards address commercial building cabling for telecom products and services.	Is suited for Structured Cabling System installations for new buildings, major cable plant additions or modifications, building renovations or remodelling.
Network Link Layer Access Protocol	(CSMA/CD) IEEE 802.3	Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method	Ethernet standards provide 10 / 100 / 1000 (1 Gbps) / 10,000 (10 Gbps) Mbps operation progressively providing higher bandwidth and improved performance. Standards provide an upgrade path resulting in a consistent management model across all operating speeds.
Logical Network Topology	IEEE 802.3	Ethernet standards support star-wired Local Area Network (LAN) designs using point-to- point links and structured cabling topologies	802.3 is the widely adopted Logical Network Topology. BUS and Token Ring network topologies are no longer in use. IEEE 802.3 is widely adopted.

Switching Technologies	IEEE 802.1p/Q	standards and IETF Multi-Protocol Label Switching (MPLS) .	Is secured and used to achieve LAN network device connectivity in Open Systems Interconnection (OSI) Layers 2, 3, and 4 Should be considered when implementing a LAN.
	IP QoS	Enables networks to support existing and emerging multimedia service/application requirements	
	IEEE 802.1p	Enables network traffic prioritisation and the seamless integration of data, voice, and video into converged services	
	IEEE 802.1Q	Trunking support to enables segmentation of individual data, voice, and video client platform devices into separate logical virtual networks (VLANs)	
Converged Services Client Platform Devices	SIP	Session Initiation Protocol (SIP)	Shall be capable of accepting and processing voice, video, and data applications within a single, secure, client platform device using the most currently approved versions of open, industry-standards for signalling protocols, compression, and media stream
	H.323	H.323 is a standard approved by the International Telecommunication Union (ITU) in 1996 to promote compatibility in videoconference transmissions over IP networks.	
	Integrated Services Digital Network (ISDN)	Integrated Services Digital Network is a set of CCITT/ITU standards for digital transmission over ordinary telephone copper wire as well as over other media.	
	codec	Standard compression/decompression (codec) techniques	

Inter-Network Transport Services	Resilient Packet Ring (RPR) 802.17x	A network topology developed as a new standard for fiber optic rings.	Suitable for generally and commercially available transport services, commonly referred to as carrier services and incorporate open, secure, scalable, industry- standards-based
	SONET	Standards for synchronous data transmission on optical media.	
	Frame Relay	Frame relay is a telecommunication service designed for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between end-points of wide area network (WAN).	
Network Time Protocol	NTP architecture	Network Time Protocol (NTP) to securely obtain time information needed to synchronize network devices and computer clocks.	All Microsoft Windows versions since 2000 include the Windows Time Service, which can sync the computer clock to an NTP server. Synchronized time is required for a good system audit. NTP is widely adopted.

Table 4 - Network Interoperability Technical Standards

Key Interoperability Area - Service Oriented Architecture

The underlying principle behind the concept of a Service Oriented Architecture (SOA) is the idea that IT systems, software, devices and services can be integrated even if they were not specifically designed to communicate with each other in the first place.

As SOA is implemented using Web Services, applications are constructed as sets of re-useable, co-operating services with each being responsible for one or more clearly identified and bounded user tasks, business processes or information services.

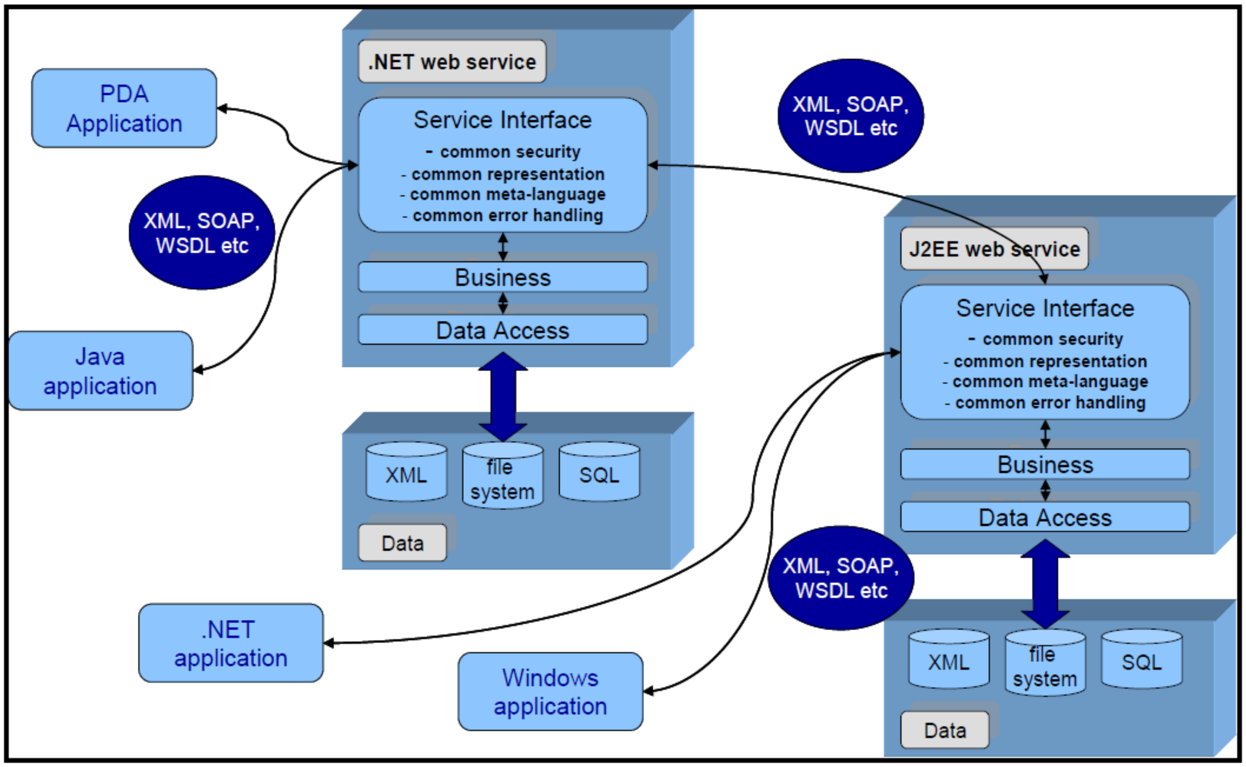


Figure 9 - Service Oriented Architecture (SOA)

SOA encompasses multiple dimensions which must work in concert for it to be successful. Adopting service-based technologies alone will not enable agencies to achieve the benefits associated with SOA.

Rationale for SOA

The adoption of a broad-based SOA capability throughout the GoG will enable:

- **Improved government responsiveness:** By employing services to establish a flexible architecture centered on business and technology capabilities, the impact of change can be isolated and business processes can be more easily and rapidly modified to meet business and mission performance requirements.

- **Simplified delivery of enhanced government services:** SOA and the "service" business model enable collaboration by simplifying access to services and streamlined value chains across organizational boundaries.
- **More efficient government:** SOA facilitates mutually leveraged public and private sector investment; reuse of capability; elimination of undesirable redundancies; and a more focused model for on-going IT recapitalization.
- **Information sharing:** SOA provides an effective and efficient approach to implementing reusable data exchanges - taking logical interoperability coming from multiple data modeling activities and rapidly evolving it into physical interoperability.
- **Transparency, security, and resilience:** SOA is predicated on a shared, standards-based infrastructure. This will enable consolidation, simplification, and optimization of IT Infrastructure, which in turn will enable greater transparency and audit-ability, as well as improved continuity of operations.

The primary risk of SOA occurs when its application is not effectively governed with purposeful intent - in other words, the business agility SOA promises cannot be achieved through ad-hoc application of SOA technologies.

Business agility must be purposefully designed into each MDA's Enterprise Architecture, IT Governance, and IT Policy framework and implemented incrementally with each step tied to delivery of business value. MDA and government-wide policy must ensure that this formalized, structured approach is incorporated into SOA implementations and evaluated through Assessment Frameworks.

Keys to Implementing the Service Oriented Architecture:

- Identify critical business objectives. Perform business process analysis and reengineering and sustain accurate service-based business models for business automation requirements.
- Identify and define the target service architecture. Establish a layered service architecture that directly supports the business performance objectives. Introduce "service" as a first order concept in your MDA architecture. Integrate existing and emerging cross-Government and cross-MDA services, ideally driven out of GGEA v.2.0 segment architecture activities.
- Enable and empower autonomous compliance and alignment. Define and publicize the enterprise service portfolio plan and phased transition strategy. Note that this works best where you have the most detailed roadmaps, thus start with the core mission or business activities, or cross cutting services where you have developed segment architectures.
- Adopt model-driven architecture and pattern-based design. Establish model-based reference architectures and reference implementations. Start by bridging from segment to specific solution architectures.

- Establish a service-oriented infrastructure that addresses security/privacy, scalability, and interoperability. In particular, leverage secure virtualization approaches to clearly separate the shared security, transport, storage, and compute capabilities from individual services and solutions.
- Study critical transactions to develop a trust and semantic model. Invest to develop standard government security services; test and certify adaptively and continuously. In particular, look to align with and adopt existing and emerging cross-Government solutions, and improve them as needed via established governance models. Isolated MDA-based solutions, no matter how good, run the risk of impeding downstream cross-Government interoperability.
- Introduce run time service monitoring tools. This includes monitoring and management across all relevant targeted attributes — security, privacy, reliability, serviceability, and availability. This is another area where it is important to align with and adopt existing and emerging cross-Government approaches to ensure that creation of artificial boundaries for sharing, reuse, and interoperability are avoided.
- Establish performance-based service levels and service level management processes and cost and performance accounting processes to facilitate the effective sharing of services. Look to express these service level agreements in shared, Government-wide structured IT policy frameworks.

While ICT has provided greater efficiencies in government, it has been an impediment for the most part in providing greater flexibility and creativity in crossing MDA application boundaries for common services and service reuse, which is the next step of automation delivery. Therefore, the following GoG-wide policies shall be followed in support of SOA implementation for greater effectiveness and added benefits and value for the state.

10.1 SERVICE ORIENTED ARCHITECTURE (SOA) POLICIES

The Ghana.gov portal and MDAs web services applications have positioned the government, more than ever before, for architectural creativity and the development and implementation of new/reuse enterprise services for citizens, communities of interest, and other third-party organisations.

1. SOA must be designed based on a thorough understanding of existing business strategies/initiatives and IT systems;
    - SOA must be built on existing application and information systems;
    - SOA must be built on existing common data repositories, whenever and wherever possible, to improve the verification and validation of public and private information;
    - SOA must be based on loosely coupled service components that provide the most flexibility at the lowest cost.

2. Implementation of SOA must be based on open standard web services.

3. Business Process Modelling (BPM): BPM shall be performed by MDAs to collectively define business processes/services and application resources to achieve business objectives and services for e-government. BPM efforts should be developed incrementally and discretely when developing modelling strategies and controls over business processes/services.

4. Integrated Service Environment (ISE): MDAs shall develop their ISE with integrated development tools and technologies (application suites, workbenches, tool/sets) that are non-proprietary, interoperable, and scalable.

5. Service components shall be built on existing application and information systems and loosely coupled without dependency upon other services/programs/modules, to provide the most flexibility, at the lowest cost.

6. Service Oriented Business Applications (SOBA): SOBAs are business applications that provide discrete units of business-level functionality through well-defined services utilizing web service standards for web-based messaging application access and interfaces. SOBAs shall be deployed as composite services via the GoG‘s Web Portal and/or MDA web sites within the SOA Blueprint. MDAs shall share SOBA applications with other MDAs and third-party organisations to promote reuse of services and information assets.

7. Enterprise Service Bus (ESB): All MDAs shall use the GoG‘s Enterprise Service Bus (ESB) for SOA applications that cross inter-MDA and other third party organisation application boundaries. It is at the discretion of the MDA‘s ICT Department whether to use the state‘s ESB for crossing intra-MDA application boundaries.

10.2 SERVICE ORIENTED ARCHITECTURE (SOA) STANDARDS

A service-oriented architecture (SOA) is an architectural pattern in computer software design in which application components provide services to other components via a communications protocol, typically over a network. The principles of service-orientation are independent of any product, vendor or technology. SOA key principles include:

1. **Standardized Service Contract** – Services adhere to a service description. A service must have some sort of description which describes what the service is about. This makes it easier for client applications to understand what the service does.

2. **Loose Coupling** – Less dependency on each other. This is one of the main characteristics of web services which just states that there should be as less dependency as possible between the web services and the client invoking the web service. So if the service functionality changes at any point in time, it should not break the client application or stop it from working.

3. **Service Abstraction** – Services hide the logic they encapsulate from the outside world. The service should not expose how it executes its functionality; it should just tell the client application on what it does and not on how it does it.

4. **Service Reusability** – Logic is divided into services with the intent of maximizing reuse. In any development company re-usability is a big topic because obviously one wouldn't want to spend time and effort building the same code again and again across multiple applications which require them. Hence, once the code for a web service is written it should have the ability work with various application types.

5. **Service Autonomy** – Services should have control over the logic they encapsulate. The service knows everything on what functionality it offers and hence should also have complete control over the code it contains.

6. **Service Statelessness** – Ideally, services should be stateless. This means that services should not withhold information from one state to the other. This would need to be done from either the client application. An example can be an order placed on a shopping site. Now you can have a web service which gives you the price of a particular item. But if the items are added to a shopping cart and the web page navigates to the page where you do the payment, the responsibility of the price of the item to be transferred to the payment page should not be done by the web service. Instead, it needs to be done by the web application.

7. **Service Discoverability** – Services can be discovered (usually in a service registry). We have already seen this in the concept of the UDDI, which performs a registry which can hold information about the web service.

8. **Service Composability** – Services break big problems into little problems. One should never embed all functionality of an application into one single service but instead, break the service down into modules each with a separate business functionality.

9. **Service Interoperability** – Services should use standards that allow diverse subscribers to use the service. In web services, standards as XML and communication over HTTP is used to ensure it conforms to this principle.

This document contains primarily conceptual and logical level standards to help MDAs and Agencies ready SOA-based services and enable SOA governance. Physical level design standards and guidelines are expected to evolve as more Tier One services are deployed and the multi-agency governance teams collaborate.

INTEROPERABILITY AREA	STANDARDS	DESCRIPTION	JUSTIFICATION
Business Service Listings and Discovery Registry	Universal Description Discovery Integration (UDDI)	The Universal Description, Discovery and Integration (UDDI) protocol is one of the major building blocks required for successful Web services. UDDI creates a standard interoperable platform that enables companies and applications to quickly, easily, and dynamically find and use Web services over the Internet (or Intranet).	UDDI is a cross-industry effort driven by major platform and software providers, as well as marketplace operators and e-business leaders within the OASIS standards consortium [uddi-oasis-open-org]. UDDI has gone through 3 revisions and the latest version is 3.0.2 [uddi-v3].
Web Services	Web Services Reliable Messaging (WS-RM)	Web Services Reliable Messaging (WSRM) is a specification that allows two systems to send messages between each other reliably	The aim of this is to ensure that messages are transferred properly from the sender to the receiver
	Simple Object Access Protocol (SOAP)	The Simple Object Access Protocol (SOAP) is a lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. By combining SOAP-based requests and responses with a transport protocol, such as HTTP, the Internet becomes a medium for applications to publish database-backed Web services	SOAP requests are easy to generate, and a client can easily process the responses. One application can become a programmatic client of another application's services, with each exchanging rich, structured information. The ability to aggregate powerful, distributed Web services allows SOAP to provide a robust programming model that turns the Internet into an application development platform.

	JavaScript Object Notation (JSON)	JSON (JavaScript Object Notation) is a lightweight data-interchange format. It is easy for humans to read and write	It is easy for machines to parse and generate. It is based on a subset of the JavaScript Programming Language Standard ECMA-262 3rd Edition - December 1999. JSON is a text format that is completely language independent but uses conventions that are familiar to programmers of the C-family of languages, including C, C++, C#, Java, JavaScript, Perl, Python, and many others. These properties make JSON an ideal data-interchange language.
	Extensible mark-up language (XML)	Extensible Markup Language (XML) is a flexible markup language for structured electronic documents. Extensible Markup Language (XML) is a programming language commonly used by data-exchange services (like blog feeds) to send information between otherwise incompatible systems	It is readable by both humans and computers and is based on SGML (standard generalized markup language), an international standard for electronic documents. Many other languages, such as RSS and XHTML, are based on XML
	XML Schema Definition (XSD)	XML Schema Definition (XSD) language is the current standard schema language for all XML documents and data. On May 2, 2001, the World Wide Web Consortium (W3C) published XSD in its version 1.0 format	The XML Schema definition language (XSD) enables you to define the structure and data types for XML documents. An XML Schema defines the elements, attributes, and data types that conform to the World Wide Web Consortium (W3C) XML Schema Part 1: Structures Recommendation for the XML Schema Definition Language. The W3C XML Schema Part 2: Datatypes Recommendation is the recommendation for defining data types used in XML schemas. The XML Schema Reference (XSD) is based on the W3C 2001 Recommendation specifications for

			Datatypes and for Structures.
Geospatial data standards	OGC Geography Markup Language (GML)	The Geography Markup Language (GML) is an encoding specification defined by the Open Geospatial Consortium (OGC) to express geographical features. GML serves as a modeling language for geographic systems as well as an open interchange format for geographic transactions on the Internet.	GML is an extensive XML based language designed to express any geographic concept in common usage. The GML specification defines (a) a language for expressing application schemas for feature types and (b) predefined properties and schemas commonly required to describe geographical features, such as polygons, curves, points, coordinate reference systems, units of measure, observations, coverages, etc. Profiles and application schemas are smaller subsets of the GML schema designed by specific information communities to tailor the more extensive GML for a smaller number of users and more targeted uses
	OGC City Geography Markup Language (CityGML)	CityGML is an open data model and XML-based format for the storage and exchange of virtual 3D city models. It is an application schema for the Geography Markup Language version 3.1.1 (GML3), the extendible international standard for spatial data exchange issued by the Open Geospatial Consortium (OGC) and the ISO TC211	The aim of the development of CityGML is to reach a common definition of the basic entities, attributes, and relations of a 3D city model. This is especially important with respect to the cost-effective sustainable maintenance of 3D city models, allowing the reuse of the same data in different application fields.

	OGC GeoSPARQL	The OGC GeoSPARQL standard supports representing and querying geospatial data on the Semantic Web	GeoSPARQL defines a vocabulary for representing geospatial data in RDF, and it defines an extension to the SPARQL query language for processing geospatial data. In addition, GeoSPARQL is designed to accommodate systems based on qualitative spatial reasoning and systems based on quantitative spatial computations
	OGC KML	KML is an XML language focused on geographic visualization, including annotation of maps and images. Geographic visualization includes not only the presentation of graphical data on the globe, but also the control of the user's navigation in the sense of where to go and where to look	From this perspective, KML is complementary to most of the key existing OGC standards including GML (Geography Markup Language), WFS (Web Feature Service) and WMS (Web Map Service). Currently, KML 2.2 utilizes certain geometry elements derived from GML 2.1.2. These elements include point, line string, linear ring, and polygon
	OGC Network Common Data Form (NetCDF	netCDF is a set of software libraries and self-describing, machine-independent data formats that support the creation, access, and sharing of array-oriented scientific data	The conventions for climate and forecast (CF) metadata are designed to promote the processing and sharing of netCDF files. The conventions define metadata that provide a definitive description of what the data represents, and the spatial and temporal properties of the data.

	GeoXACML	GeoXACML stands for Geospatial eXtensible Access Control Markup Language	It defines a geo-specific extension to XACML Version 2.0, as it was ratified by OASIS standards organization on 1 February 2005. GeoXACML version 1.0.1 is standardized by the Open Geospatial Consortium (OGC).
	OGC Web Service (OWS)	Open Geospatial Consortium (OGC) Web Services (OWS) are services defined by the OGC, allowing all kinds of geospatial functionality	Open Geospatial Consortium (OGC) include services for data access, data display and data processing. OWS requests are defined using the Hyper Text Transfer Protocol (HTTP) protocol and are encoded using key-value-pairs (KVP) structures or Extensible Markup Language (XML). The most widely known OWS is the Web Map Service (WMS).
	OpenGIS Web Feature Interface Standard (WFS)	The OGC Web Feature Service (WFS) Interface Standard defines a set of interfaces for accessing geographic information at the feature and feature property level over the Internet	A feature is an abstraction of real-world phenomena, that is it is a representation of anything that can be found in the world. The attributes or characteristics of a geographic feature are referred to as feature properties. WFS offer the means to retrieve or query geographic features in a manner independent of the underlying data stores they publish. Where a WFS is authorized to do so, the service can also update or delete geographic features. An instance of a WFS is also able to store queries in order to enable client applications to retrieve or execute the queries at a later point in time.
Messaging Transportation	Extensible Style sheet Language Transformation (XSLT)	Stands for "Extensible Style Sheet Language Transformation."	While XML is supposed to be a standardized language, not all XML documents use the same type of formatting. Therefore, the documents sometimes need to be "transformed," or modified so that another script or program will be able to

			read them. XSLT make this transition possible
Database Access and Manipulation Language	Structured Query Language (ANSI SQL)	SQL is an ANSI (American National Standards Institute) standard computer language for accessing and manipulating database systems	SQL is the most popular computer language used to create, retrieve, update and delete data from relational database management systems. There are many different versions of the SQL language, but to be in compliance with the ANSI standard, they must support the same major keywords in a similar manner (e.g., SELECT, UPDATE, DELETE, INSERT, WHERE, and others).
	W3C XML Query (XQuery)	XQuery is a standardized language for combining documents, databases, Web pages and almost anything else	It is very widely implemented. It is powerful and easy to learn. XQuery is replacing proprietary middleware languages and Web Application development languages. XQuery is replacing complex Java or C++ programs with a few lines of code. XQuery is simpler to work with and easier to maintain than many other alternatives.
Web Services Description Language	Web Services Description Language (WSDL)	WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information	The operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are combined into abstract endpoints (services). WSDL is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate, however, the only bindings described in this document describe how to use WSDL in conjunction with SOAP 1.1, HTTP GET/POST, and MIME.

Web services message exchange	Web Services Addressing (WS Addressing)	Web Services Addressing (WS-Addressing) provides a standard framework for specifying the endpoints of a SOAP message. This framework is transport-neutral and improves the interoperability of web services that use different transport mechanisms. The WS-Addressing specification introduces message addressing properties and endpoint references	Web Services Addressing (WS-Addressing) is a Worldwide Web Consortium (W3C) specification that improves interoperability between web services by defining a standard way to address web services and provide addressing information in SOAP messages
	Web Services Enumeration (WS Enumeration	WS-Enumeration describes a general SOAP based protocol for enumerating a sequence of XML elements that is suitable for traversing logs, message queues, or other linear information models	WS-Enumeration enables an application to ask for items from a list of data that is held by a Web service. In this way, WS-Enumeration is useful for reading event logs, message queues, or other data collections. WS-Enumeration defines a single operation, Pull, which allows a data source, in the context of a specific enumeration, to produce a sequence of XML elements in the body of a SOAP message.
	Web Services Metadata Exchange (WS-MetadataExchange)	WS-MetadataExchange handles the exchange of information about a web service. It is a protocol used by a web service to describe itself.	Web Services Metadata Exchange (WS-MetadataExchange) defines three request-response message pairs to retrieve three types of metadata: one retrieves the WS- Policy associated with the receiving endpoint or with a given target namespace, another retrieve either the WSDL associated with the receiving endpoint or with a given target namespace, and a third retrieves the XML Schema with a given target namespace. Together these messages allow incremental retrieval

			of a Web service's metadata.
	Dublin core metadata	The Dublin Core metadata element set is a standard for cross-domain information resource description	In other words, it provides a simple and standardized set of conventions for describing things online in ways that make them easier to find. Dublin Core is widely used to describe digital materials such as video, sound, image, text, and composite media like web pages. Implementations of Dublin Core typically make use of XML and are resource description framework based.
Information Exchange Services Compliance	Web Services Policy (WS-Policy)	WS-Policy provides a flexible and extensible grammar for expressing the capabilities, requirements, and general characteristics of entities in an XML Web services-based system. WS-Policy defines a framework and a model for the expression of these properties as policies	WS-Policy defines a policy to be a collection of policy alternatives, where each policy alternative is a collection of policy assertions. Some policy assertions specify traditional requirements and capabilities that will ultimately manifest on the wire (e.g., authentication scheme, transport protocol selection). Other policy assertions have no wire manifestation yet are critical to proper service selection and usage (e.g., privacy policy, QoS characteristics). WS-Policy provides a single policy grammar to allow both kinds of assertions to be reasoned about in a consistent manner.
	Web Services Security Policy (WS-SecurityPolicy)	The recently updated Web Services Security Policy Language (WS-SecurityPolicy) specification defines a set of security policy assertions which apply to Web Services Security: SOAP Message Security, WS-Trust, and WS-SecureConversation	WS-Policy defines a framework for allowing web services to express their constraints and requirements. Such constraints and requirements are expressed as policy assertions. Flexibility with respect to token types, cryptographic algorithms and mechanisms used, including using Transport Level Security (TLS) is part of the design and allows for evolution over time.

			The intent is to provide enough information for compatibility and interoperability to be determined by web service participants along with all information necessary to actually enable a participant to engage in a secure exchange of messages
	Web Services Distributed Management (WSDM)	WSDM is a web service standard for managing and monitoring the status of other services.	The goal of WSDM is to allow a well-defined network protocol for controlling any other service that is WSDM-compliant. For example, a third-party digital dashboard or network management system could be used to monitor the status or performance of other services, and potentially take corrective actions to restart services if failures occur. Some aspects of WSDM overlap or displace functionality of Simple Network Management Protocols (SNMPs).
Web services Message Security	Web Services Interoperability Basic Security Profile (BSP	The BSP is an interoperability profile that addresses transport security, SOAP messaging security and other security considerations. Specifically, the BSP1.0 focuses on the interoperability characteristics of two technologies: HTTP over TLS and Web Services Security: SOAP Message Security. HTTP over TLS is a point- to-point technology that protects the confidentiality of all information that flows over an HTTP connection.	Web Services Security: SOAP Message Security provides security protection for SOAP messages and applies even when a message passes through several intermediary waypoints, allowing differing levels of protection for selected portions of a message. The BSP describes a way to apply SOAP Message Security to attachments. The BSP also incorporates Web Services Security: Username Token Profile, Web Services Security: X.509 Certificate Token Profile, Web Services Security: Kerberos Token Profile, Web Services Security: SAML Token Profile and Web Services Security: XRML Token Profile.

Table 5 - Service Oriented Architectue (SOA) Technical Standards

Key Interoperability Area - Security Interoperability

Information security is the process of ensuring the confidentiality, integrity and availability of government information. The policies and standards below are designed to ensure security in an interoperable environment.

11.1 SECURITY INTEROPERABILITY POLICIES

Network Infrastructure and Services

Email

1. Mail clients are not configured securely by default upon release by manufacturers and are vulnerable to attack. MDAs must ensure that all default configurations are changed to secure settings.
2. Email messages must adhere to classification standards. All Email clients deployed in MDAs must support encryption, and encryption must be applied to messages that require confidentiality.
3. Email messages which require non-repudiation must be digitally signed. MDAs‘email systems must support digital signature.
4. Mail servers must be configured not to report mail server and operating system type and version.

Network Level Security

1. All MDA networks must be designed within the defence in depth concept to ensure an appreciable level of security in all government systems.
2. All MDA network perimeters must be protected by using an application proxy firewall.
3. Network devices must be configured with stringent packet filtering rules.
4. All external connections into an MDA network should be routed through gateways.
5. Intrusion detection strategies or tools should be used to enhance network security.
6. Network and host vulnerability scanners should be used to test for vulnerabilities of internal systems and of network perimeter defences.

Wireless LAN Security

1. Risks to WLAN should be assessed regularly and often due to the greater effort required to ensure adequate protection.
2. Bluetooth devices should not be allowed to operate in insecure mode.
3. All MDA wireless networks and hand-held devices shall be managed and inventoried as a

state asset to further protect confidential and sensitive state information.

4. All diagrams and topologies of wireless networks must be documented and maintained with specific details of underlying structures for a complete understanding of the wireless network.

Cryptography

1. All sensitive state information residing on any storage media must be encrypted.
2. All critical state databases must be encrypted.
3. All classified traffic (voice, video and data) must be encrypted.

Data Security

1. The privacy of the citizen information must be protected at all times. All government Web sites and databases storing system information must be protected to guarantee maximum protection of the privacy of information.

Data Classification

1. A risk assessment process must be established that addresses the sensitivity and the criticality of information.
2. An asset classification scheme must be designed to on a 'need to know' basis so that information will be protected from unauthorised disclosure, use, modification and deletion, and include strict guidelines for the implementation of labelling, handling and destruction procedures according to the asset‘s classification.
3. Government information must be consistently protected throughout its life cycle, from its origination to its destruction.
4. The assets of government must be listed in an information asset inventory.
5. Each information asset must have a nominated trustee/steward.
6. The trustee/steward of the information asset must identify /approve of the controls that should be implemented to provide appropriate protection to the asset.
7. Information assets must be classified in accordance with a specific asset classification scheme and related guidelines to be developed for this purpose.
8. The classification of each information asset is to be reviewed at periodic intervals and may be amended in accordance with the asset classification scheme and related guidelines in force at the time.
9. All information assets shall be labelled physically or electronically in accordance with their asset classification

Identity Management

MDAs will be required to comply with the identity-proofing, registration, issuance and maintenance processes. Credentials will be issued only to individuals under their true identity and after a proper authority has authorised issuance of the credential.

MDAs should practice card management throughout the card lifecycle.

Individual MDAs are responsible for determining the proper level of identity assurance required for access to their physical and logical assets.

Wireless Policies

1. Wireless Security must be implemented using the defence-in-depth approach.
2. Where wireless networks are deployed, steps must be taken to ensure that appropriate management and monitoring tools are implemented to define rights to control network devices and clients.
3. MDAs must only implement Wireless Ethernet Compatibility Alliance (WECA) certified devices in a wireless network to ensure interoperability.

11.2 SECURITY INTEROPERABILITY STANDARDS

Security spans all the layers described in the e-GIF. The standards listed below cover the three key facets (CIA Triad) of Information security:

- *Confidentiality*: Ensuring that only authorised user will have access to view data
- *Integrity*: Ensuring the integrity of information will involve restricting changes to only authorised users.
- *Availability*: Ensuring that information is available to legitimate users all the time.

INTEROPERABILITY AREA	STANDARDS	DESCRIPTION	JUSTIFICATION
Web Services Security	WS-Security 1.1.1 http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-SOAPMessageSecurity-v1.1.1-os.doc	**WS-Security** is a communications protocol providing a means for applying security to Web Services. The protocol contains specifications on how integrity and confidentiality can be enforced on Web services messaging. The WSS protocol includes details on the use of SAML and Kerberos, and certificate formats such as X.509.	In point-to-point situations confidentiality and data integrity can also be enforced on Web services through the use of Transport Layer Security (TLS), for example, by sending messages over https. WS-Security however addresses the wider problem of maintaining integrity and confidentiality of messages until after a

INTEROPERABILITY AREA	STANDARDS	DESCRIPTION	JUSTIFICATION
			message was sent from the originating node, providing so called end to end security.
	WS-Federation 1.2 http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.doc	**WS-Federation** describes how to manage and broker the trust relationships in a heterogeneous federated environment including support for federated identities. A federation is a collection of realms (security domains) that have established relationships for securely sharing resources. A Resource Provider in one realm can provide authorised access to a resource it manages based on claims about a principal (such as identity or other distinguishing attributes) that are asserted by an Identity Provider (or any Security Token Service) in another realm.	WS-Federation works with WS-Security, WS-Trust, and WS-SecurityPolicy provide a basic model for federation between Identity Providers and Relying Parties. It provides the transformational model.
	WS-Trust 1.4 Errata 01 http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/errata01/os/ws-trust-1.4-errata01-os.doc	WS-Trust describes a framework for trust models that enables Web Services to securely interoperate. It uses WS-Security base mechanisms and defines additional primitives and extensions for security token exchange to enable the issuance and dissemination of credentials within different trust domains.	An integral part of the WS Security standards. Widely used by Microsoft etc for trust implementation within web services.
	WS-Security: X.509 Certificate Token Profile 1.1.1 http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-x509TokenProfile-v1.1.1.doc	**WS-Security: X.509 Certificate Token Profile** describes the use of the X.509 authentication framework with the WS-Security: SOAP Message Security specification.	The only specification that describes the use of the X.509 authentication framework with the Web Services Security: SOAP 133 Message Security specification [WS-Security].

INTEROPERABILITY AREA	STANDARDS	DESCRIPTION	JUSTIFICATION
	Information technology - Biometric Identity Assurance Services (BIAS) https://www.iso.org/standard/53228.html http://docs.oasis-open.org/bias/soap-profile/v1.0/biasprofile-1.0.doc	A system in which a user is authenticated to a resource wherein the user is coupled to a biometric sensor. It is therefore a system in which a user is authenticated to a resource wherein the user is coupled to a biometric sensor. BIAS is a framework for deploying and invoking identity assurance capabilities that can be readily accessed using services-based frameworks (e.g. Web services)	Biometric systems are better used for verification rather than identification. In general, that is, they are better suited for a one-to-one match assuring that the individual in question is who he says he is and has the requisite authorisation to engage in the activity in question. Biometric systems provide a substantially higher level of security beyond current means of identification
	BioAPI Specification https://www.iso.org/standard/70866.html	BioAPI defines the Application Programming Interface (API) and Service Provider Interface (SPI) for standard interfaces within a biometric system that support the provision of that biometric system using components from multiple vendors. It provides interworking between such components through adherence to this and to other International Standards.	
Smart cards	Contact smart card (eg.SIM Cards) Contactless smart card (eg. Hong Kong's Octopus card, South Korea's T-money(Bus, Subway, Taxi)) Cryptographic smart cards are often used for single sign-on (eg. PKCS#11)	A smart card, chip card, or integrated circuit card (ICC), is any pocket-sized card with embedded integrated circuits which can process data. **Reference**: http://en.wikipedia.org/wiki/Smart_card	

INTEROPERABILITY AREA	STANDARDS	DESCRIPTION	JUSTIFICATION
Email Security	S/MIME v4.0 – Secure Multi- purpose Internet Mail Extensions version 4.0 https://datatracker.ietf.org/doc/html/rfc8551	S/MIME provides a method to send and receive secure MIME messages by sending e-mail that uses the Rivest-Shamir-Adleman (RSA) encryption system. S/MIME is included in the latest versions of the email clients from Microsoft and has also been endorsed by other vendors that make messaging products. **References:** RFC 8551: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification	S/MIME is a matured standard. Version 4.0. S/MIME is a well supported standard and has been selected over the alternatives such as PGP (not suited to large user communities), PEM and MIME Object Security services (neither of these standards has gained significant industry support). S/MIME v4.0 is widely supported by the latest versions of the market leading email products.
Certificate	On-line Certificate Status Protocol https://datatracker.ietf.org/doc/html/rfc6960	Enables the current status of a digital certificate to be determined without the use of a certificate revocation list. This protocol can be used by applications, typically for high-value or highly sensitive transactions, to perform an online check of the status of a digital certificate, rather than relying on a periodic certificate revocation list (CRL).	RFC 6960 is an IETF standard, and the only viable one for on-line certificate status protocol.
	Certification Request	Defines the format of a request to a certification authority (CA) for a public-key certificate to enable the use of digital certificates issued by multiple certification authorities.	*De facto* standard from RSA Security for a request for certification of a public key, a name and an optional set of attributes. Published as an Informational RFC.
	Certificate Profile	Defines the format and semantics of digital certificates to be used within government, to ensure that certificates issued by multiple CAs can be used across government applications.	RFC 6818 profiles both the X.509 v9.0 certificate and CRL for use in the Internet.

INTEROPERABILITY AREA	STANDARDS	DESCRIPTION	JUSTIFICATION
	Certificate Revocation List Profile	Defines the format and semantics of certificate revocation lists (CRLs) to enable the status of digital certificates issued by different certification authorities (CAs) to be verified. CRL-based status checking is commonly adopted, although it does not provide the most up-to-date status of a certificate.	
	Certificate Import / Export Interface PKCS #12 v1.1	Provides a mechanism for storing private keys and certificates and allows for import and export of certificates. This would allow, for example, users to import certificates provided on diskettes by Certification Authorities or allow certificates to be imported onto tokens or smart cards.	De facto standard from RSA Security for a portable format for storing or transporting a user‘s private keys, certificates, secrets etc.
Transport Level Security	TLS v1.3 – Transport Layer Security version 1.3. https://datatracker.ietf.org/doc/html/rfc8446	TLS has replaced SSL. The primary goal of the TLS Protocol is to provide privacy and data integrity between two communicating applications	The successor of the now-deprecated Secure Sockets Layer (SSL), is a cryptographic protocol designed to provide communications security over a computer network. The protocol is widely used in applications such as email, instant messaging, and voice over IP, but its use as the Security layer in HTTPS remains the most publicly visible.
Network Level Security	IPsec – Internet Protocol Security. https://datatracker.ietf.org/doc/html/rfc6071	IPsec is a general mechanism for securing IP. It is a standard for security at the network or packet processing layer of network communication. It builds security into the fabric of the Internet so that anyone who chooses to communicate securely can do so, as easily as they can do anything else on the net.	IPsec is the only viable standard for IP network-level security. IPsec is widely adopted by all IP VPN products, for example, those provided by market leaders such as IBM, Cisco Systems IOS and Checkpoint Software

INTEROPERABILITY AREA	STANDARDS	DESCRIPTION	JUSTIFICATION
Network Level Encryption	IP ESP – IP Encapsulating Security Payload https://datatracker.ietf.org/doc/html/rfc4303	IP ESP provides confidentiality, data origin authentication, connectionless integrity, anti-replay services and traffic flow confidentiality with IPv4 and IPv6 networks. ESP may be applied alone, in combination with the IP Authentication Header (AH), or in a nested fashion (using tunnel mode).	IP ESP is widely used in VPN products which are supplied by numerous vendors, including all of the leading Firewall vendors such as IBM, Cisco, Computer Associates, HP, and Symantec.
Encryption Algorithms	Advanced Encryption Standard https://www.iso.org/ standard/81564.html	AES is a symmetric-key algorithm and is included in the ISO/IEC 18033-3 standard.	AES has been adopted by U.S. government. It supersedes the Data Encryption Standard (DES)
Digital Signature Algorithms	DSA – Digital Signature Algorithm; and RSA for Digital Signature http://nvlpubs.nist.gov/ nistpubs/FIPS/NIST.FIPS.186-4.pdf https://nvlpubs.nist.gov/ nistpubs/FIPS/ NIST.FIPS.186-4.pdf https://nvlpubs.nist.gov/ nistpubs/FIPS/ NIST.FIPS.186-5-draft.pdf	NIST published the DSA in the Digital Signature Standard (DSS), which is a part of the U.S. government's Capstone project. DSS was selected by NIST, in co-operation with the NSA to be the digital authentication standard of the US Government. RSA for Digital Signatures is an alternative method for generating and checking digital signatures. It is recognised by the NIST as an alternative to DSA. RSA is a proprietary public-key cryptography system, from RSA Security, that provides both encryption and digital signatures. RSA uses the public key of the recipient to encrypt data which can only be decrypted by the recipient using their private key.	Together with RSA, DSA is a widely accepted standard for digital signature algorithms. RSA is a matured security standard – it was first developed in 1997 and has been extensively tested. RSA for Digital Signature is a proprietary standard introduced in February 2000, which has gained wide acceptance. RSA is the most widely used digital signature algorithm.

INTEROPERABILITY AREA	STANDARDS	DESCRIPTION	JUSTIFICATION
XML Message Signature and Encryption	XML Signature Syntax and Processing https://www.w3.org/TR/xmlsec-reqs2/ XML Encryption Syntax and Processing https://www.w3.org/TR/xmldsig-core/	XML Signature is a standard for digital signing of XML and its applications. The standard defines a schema for capturing the result of a digital signature operation applied to arbitrary (but often XML) data. Like non-XML-aware digital signatures (e.g., PKCS), XML signatures add authentication, data integrity, and support for non-repudiation to the data that they sign. However, unlike non-XML digital signature standards, XML signature has been designed to both account for and take advantage of the Internet and XML. A fundamental feature of XML Signature is the ability to sign only specific portions of the XML tree rather than the complete document. An XML signature can sign more than one type of resource.	XML Signature is a joint W3C/IETF standard, and the only one available for XML message signing. Currently, only one version of XML Signature exists. Publicly available toolkits and software development kits are provided by market leading security vendors, including IBM, HP, Microsoft, RSA and VeriSign.
Hashing Algorithms for Digital Signatures	SHA-2 – Secure Hash Algorithms 2. SHA-3 – Secure Hash Algorithms 3. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf	SHA is a message digest algorithm (and cryptographic hash function) designed by the National Security Agency (NSA) and published by the National Institute of Standards and Technology (NIST).	SHA-3 is the first cryptographic hash algorithm NIST has developed using a public competition and vetting process that drew 64 submissions worldwide of proposed hashing algorithms. SHA-3 is not the only family of hash functions that NIST approves for hashing electronic messages; the SHA-2 family, specified in FIPS 180-4 that NIST approved for use in 2002, remains secure and viable.

Table 6 - Security Interoperability Technical Standards

Key Interoperability Area - Applications & Software Interoperability

12.1 APPLICATION AND SOFTWARE INTEROPERABILITY POLICIES

1. MDAs shall utilize current, commonly recognised best practice system development methodologies and standards to develop, implement, and/or acquire application systems.

2. Application architecture must support open, interoperable solutions that make government information, programs, and services shareable.

3. Applications architecture must be agile, enabling rapid modification as business requirements change.

4. Enable Re-use of information from single authoritative source. Information must be collected and shared in line with GoG Data Policy to enable a single authoritative government data source. The principle of re-use, wherein information is created once and is available to be used for different purposes with confidence, is fundamental.

5. Client software on a terminal device which makes use of a service offered by the middle tier must be web-based, except under exceptional conditions (i.e., Java script/applets with appropriate safeguards and formal Compliance Exemption granted through GGEA governance process).

12.2 APPLICATION AND SOFTWARE INTEROPERABILITY STANDARDS

INTEROPERABILITY AREAS	STANDARDS	DESCRIPTION	JUSTIFICATION
Simple functional integration in an open environment (e.g., information retrieval from a remote application)	SOAP v1.1	SOAP - Simple Object Access Protocol is a system to enable program running in one kind of operating system to communicate with a program in the same or another kind of an operating system. Standards such as World Wide Web's Hypertext Transfer Protocol (HTTP) and its Extensible Markup Language (XML) is used as a mechanism for information exchange.	
	WSDL v1.1	A WSDL provides a comprehensive technical description of services. It describes what the service does in terms of its operations and message formats. And how to interact with it.	WSDL is defined in XML and is therefore strictly implementation independent. WSDL v1.1 is currently supported by various tools on different platform and referenced by the WS – 1 Basic profile v1.1.
	UDDI v3	UDDI - Universal Description, Discovery, and Integration is an XML-based registry for businesses worldwide to list themselves on the Internet For the publication and discovery of remote service descriptions	

Reliable document exchange between application systems in an open environment for business document-oriented collaboration	ebMS v2	ebXML (ebMS) Message Services is the messaging standard defined within the ebXML framework and is sometimes abbreviated as ebMS, for secure and reliable messaging over the Internet.	MDAs exchanging business data using ebMS may take advantage of it to provide: Privacy Encryption of data via SSL Authentication User authentication via SSL or Digital Signature Reliable Messaging Once-and-only-once message delivery validated through SSL or Digital Signature Flexibility Messages of any data type, including binary graphics, EDI or XML
Secure exchange of messages in a Web Services environment	WS-Security 1.0	WS-Security 1.0 defines mechanisms for signing and encrypting SOAP messages.	The new WS-Security v1.1 standard is an important milestone that includes significant enhancements to the original specification. It also profiles and adds support for several new security token types, such as SAML, Kerberos, X.509 certificates, and others
Applications which use Middleware	Java 2 Platform, Enterprise Edition (J2EE) v1.4 Java 2 Platform, Standard Edition (J2SE) v1.4		The development and integration of integrated applications on the middle tier require the use of Java 2 Platform, Enterprise Edition (J2EE) for applications which directly integrate basic components or libraries provided for this purpose, and applications designed, as a whole or in part (components), for re-use (porting) If an application does not require the full J2EE functionality either initially or on a permanent basis, J2EE technologies should be used

			individually as an alternative via the Java 2 Platform, Standard Edition (J2SE), in accordance with J2EE Specification 1.4 in order to create a compatible migration path to J2EE.
	Java Database Connectivity (JDBC) v3.0		JDBC should be used for access to databases.
	Java Message Service (JMS) v1.1, J2EE Connector Architecture v1.5		Either the Java Message Service (JMS) or the J2EE Connector Architecture should is suitable for integrate external systems.
	.NET Framework	.NET Framework is a middleware technology which was developed by Microsoft.	The system architecture of .NET includes a runtime environment for different programming languages and a development environment. It supports major web standards (including SOAP, WSDL, UDDI, XML).
Application Standards without Middleware	PHP: Hypertext Preprocessor (PHP) v4.x		PHP can be used for applications without an integration requirement, i.e., non- distributed stand-alone applications which do not communicate with one of the basic components, legacy systems or other special e-government applications).

Table 7 - Application and Software Interoperability Technical Standards