

# **Regulatory and policy environment review**

Project: THE REPUBLIC OF UGANDA CONSULTANCY SERVICES FOR THE DEVELOPMENT OF  
A GOVERNMENT ENTERPRISE ARCHITECTURE (GEA) AND E-GOVERNMENT  
INTEROPERABILITY FRAMEWORK (E-GIF)

Project duration: 10 November 2020 – 09 September 2021

February 3, 2021, Version 1.1

## Change history

| Version | Date       | Summary of changes   |
|---------|------------|--|
| 1.0     | 2021-01-04 | Initial draft (Uuno Vallner, Katrin Nyman-Metcalf, Arvo Ott)                     |
| 1.1     | 2021-02-03 | Updates based on discussions during PIT meeting on 02.02.2021.<br>Clean version. |

## Document status

|              |   |
|--------------|---|
| Draft        |   |
| For approval | X |
| Approved     |   |

## Authors

| Name                    | Role                 |
|-------------------------|----------------------|
| Dr Uuno Vallner         | Enterprise architect |
| Dr Katrin Nyman-Metcalf | Legal expert         |
| Dr Arvo Ott             | Supervisor           |
| Tõnis Mäe               | Project Manager      |
| Anneli Piirat           | Project Secretary    |

## Contents

|   |    |
|---|----|
| Regulatory and policy environment review .....                          | 1  |
| 1. Legal issues related to e-government .....                           | 4  |
| 1.1. Introduction .....   | 4  |
| 1.2. Legal work for e-government.....                                   | 4  |
| 1.3. Uganda.....  | 7  |
| 1.4. Concluding remarks on the legal framework.....                     | 15 |
| 2. Policy environment review .....                                      | 17 |
| 2.1. Introduction .....   | 17 |
| 2.2. e-Government Master plan .....                                     | 18 |
| 2.3. ICT Sector Implementation Plan.....                                | 20 |
| 2.4. Feasibility Study Report for Integration of National Systems ..... | 21 |
| 2.5. National Information Security Framework .....                      | 22 |
| 2.6. Interim Interoperability Framework .....                           | 25 |
| 2.7. Integration of National Systems concept.....                       | 26 |
| 2.8. NITA-U Strategic Plan 2018/19 – 2022/23 .....                      | 27 |
| 3. Concluding remarks .....   | 30 |

# 1. Legal issues related to e-government

## 1.1. Introduction

The first component of this Report gives an overview of the legal issues related to e-government, which includes interoperability of databases and provision of electronic services within/between authorities and to the public. Legal work for the creation or improvement of e-government includes several different types of activities and areas of law that are similar in all countries, even if the exact steps vary. Section 1 of the Report provides a general background, highlights the current situation in Uganda and makes recommendations.

To simplify, law plays three distinct roles in the context of e-government:

- It helps to *create* e-government by mandating the use of digital data and new ways to perform administrative transactions, by creating and/or empowering institutions, and so on.
- It *enables* the use of electronic transactions by ensuring that these have legal validity, including recognising electronic ways to identify oneself and sign documents or other expressions of will.
- It *incentivises* the use of e-government through different measures like providing faster and cheaper service to people, by simplifying administrative tasks for officials, and similar.

Not only are technical solutions enabled and promoted through legal measures, but a proper legal framework ensures that the reforms lead to better governance in the form of more transparency, less risk of corruption, better protection of personal data and other positive steps to strengthen rule of law.

Uganda has in recent years adopted or amended a series of laws related to the digital society. Generally, the legal framework is well prepared for introduction of more e-government and other uses of ICT. The country has correctly included legal issues in its planning for e-government<sup>1</sup> and has already undertaken many of the necessary steps. The UN in its 2020 E-Government Survey presents Uganda as one of the success stories of Africa. It states that the success of Uganda<sup>2</sup> derives from having a comprehensive digital government strategy and forward-looking plans as well as quite well-developed online services. The robust legal framework is specifically mentioned as a positive factor.<sup>3</sup>

This section starts with a short general overview of the legal steps related to e-government. After this, the Ugandan situation is discussed. Finally, some concluding remarks are made, including reflections on future work. The Report is based on a study of publicly available material in the form of reports of international organisations, published articles, legal texts and similar. Any conclusions and suggestions made in the Report are those of the authors if not otherwise indicated.

## 1.2. Legal work for e-government

In this section the legal work linked the creation of e-government, including interoperability of databases (X-road) and use of e-services, is described. The same topics in the context of Uganda are

---

<sup>1</sup> Like already the 2010 Ministry of Information and Communications Technology *National Electronic Government (e-Government) Framework*.

<sup>2</sup> As well as of Rwanda and Tanzania, other successful African countries mentioned.

<sup>3</sup> UN Department of Economic and Social Affairs *E-Government Survey 2020* p. 83.

presented in the next section. The aim of this section is to explain why certain matters are relevant and what to look out for, so that the reader will be aware of this when reflecting on the specific Ugandan situation.

The legal work can be divided into three broad categories.

### *1.2.1. Analysis of existing legislation*

The analysis should include many areas of legislation and the aim is to identify any provisions that would create obstacles to e-government. The kind of provisions that cause obstacles normally relate to the following categories:

- Requirements of form: This includes rules on what documents or databases should look like (colour of paper or ink, etc.), stipulations on originals and copies, expressions like "raising the right hand", "attending during office hours", etc. assuming physical presence, and archiving rules assuming a physical archive. What to look out for is anything that is not easily and evidently replicable in electronic format.
- Procedural rules: Administrative or criminal procedure as well as sector-specific laws can include the same kind of things as in the point above, but sometimes in more detail and directly related to the validity of an act.
- Proof of payment, stamp duty, etc.: If laws require proof of payment in the form of a stamp or similar, this can cause problems in case of electronic payments.
- Rules on responsibility and competence: As the responsibility for databases and services is divided between different organisations and/or ministries, it has to be ensured that the law vests one specific organisation with the right to take binding decisions regarding interoperability and related matters. Organisations that are hierarchically parallel cannot take binding decisions for one-another without explicit competence in law.

If such obstacles are found, it needs to be determined what should be done:

- In some cases, the requirement of form is based on tradition rather than objective necessity and nothing would change in substance if removed.
- In other cases, a specific form shows something of relevance, like a specific nature of a transaction, and must in that case be replicated in an electronic manner.
- The determination must be made on a case-by-case basis.
- As for the question of responsibility and competence, this should be set out in law.

### *1.2.2. Drafting of specific legislation*

E-government does *not* require a lot of specialised legislation. Not only is it unnecessary to make special laws, but it can be harmful, as it risks creating a parallel system where the *form* of transactions or data rather than the substance becomes a legally determining factor. If you apply for a public service or grant, it should not matter if you apply electronically or on paper – the legal provisions on who can get the service and on what terms should be the same. Legislation should be technology-neutral to the greatest extent possible, to avoid becoming obsolete when technology changes. However, there are some matters that are different in an electronic world and need special laws and/or secondary legislation. These matters are horizontal, meaning that they are the same across different services and data sets. The most obvious one is the way to identify oneself electronically.

The areas in need of legislation are:

- Electronic identification and electronic signature: How these are made and certified as well as clear provisions recognising the legal validity.
- Data protection. This is not just for electronic data, but the protection in practice is different and clear rules on protection are important not least to gain trust among the population.
- Databases: These are the backbone of interoperability systems and need sufficient common standards. Data should only be collected once so it is essential to have rules on how to create or terminate databases and how to make it known what databases exist, in the form of a catalogue of databases. Specific rules on content should however be in the laws about the different areas that the databases concern and not in one central law, as the reasons and methods of data collection vary depending on the area.
- Archiving: What is kept, for how long, in what form, etc. In a digital world, it is the preservation of data and not some specific document that needs to be ensured.
- Access to information: This is not specific for electronic data, but in practice the way people can access data is different when it can be done electronically. Law and technology should cooperate so that the legal provisions on what data is public, what is secret (state secrets, business secrets etc.) or personal are taken into consideration in the technical possibilities to access data.

### *1.2.3. Drafting or amendment of indirectly connected legislation*

In addition to the mentioned areas there are topics with an indirect but still important connection to e-government.

- Information and Communications Technology (ICT) legislation and competition law: Access to internet is essential if people are to be able to use e-services. Access is normally provided by private companies but given the importance, ICT is a regulated sector for which there are various rules and restrictions (in sector-specific and/or general competition law) also in market economies. The area of law is similar globally and normally well-developed in about the last 30 years, but if a country increases its dependence on electronic services, the good functioning of the legislation and the proper work of the relevant regulatory body are extra important.
- Public procurement and Public-Private-Partnership (PPP) legislation: PPP is often used in connection with e-government. If legislation allows for PPP, there is normally no need to amend laws or adopt new ones, but if PPPs are not possible, this area may need attention.
- Intellectual property legislation: Legislation protecting patents, copyrights and trademarks may influence the use of technologies, especially if the technologies used are under a restrictive licence.
- Incentives for use of e-services: If a country wishes to transition to e-government and get people to use e-services, it is necessary to think about how to make it attractive. Measures can include shorter handling times, lower fees, etc. Incentivising measures, if the internet access is poor, includes making free internet posts available (as is done in Estonia in the Law on Public Libraries). The issue of how to overcome problems with a digital divide between categories of people

and/or parts of the country or other educational issues, not least for the civil service, are also relevant.

- Cybersecurity and cybercrime legislation: Cybersecurity affects all areas of a digital society and cannot be dealt with in one law. Instead, different laws provide security, like rules on protection of critical infrastructure, data protection legislation, criminal law, etc.

### 1.3. Uganda

In this section, the situation in Uganda will be discussed related to the above-mentioned points.

#### 1.3.1. Analysis of existing legislation

Prior to the drafting of this report, the legal expert has not had direct contact with the Ugandan legal colleagues and consequently details of any analysis undertaken are not known. However, the fact that the legal issues have been included in planning and analysis indicate that the question has been considered. At the same time, this work is something that needs to continue throughout the introduction and improvement of e-government, as it includes many different areas of law and potential obstacles may be found in different places and in different form. It is thus an ongoing task that should go hand in hand with technological developments.

Requirements of form: The basic issue of recognising electronic format of transactions is taken care of by the Electronic Transactions Act, 2011,<sup>4</sup> which mentions that electronic form of documents and information as well as electronic signatures meet legal requirements, specifying what is regarded as an original message for example and what constitutes evidential weight (specifically Sections 5-8). One of the aims (Section 4) is to remove and eliminate the legal and operational barriers to electronic transactions. The Act proclaims technology neutrality and the aim of providing legal certainty and public confidence in the use of electronic communications and transactions. The Act specifies rules for electronic contracts and other transactions, including when offer or acceptance is regarded as legally made electronically. General contract law (like the 2010 Contracts Act) also recognises electronic format for contracts.

Electronic format of transactions and documents is recognised primarily through the 2011 Electronic Transactions Act.

The Electronic Transactions Act refers to the Electronic Signatures Act (2011),<sup>5</sup> see below. Additional rules are provided in the 2013 Electronic Transactions Regulations and the 2016 Certification of Providers of Information Technology Products and Services Regulations (as amended 2018). There are furthermore E-Government Regulations passed in 2015 and a national framework that provides guidelines for government organisations to develop their capabilities to use ICT for their internal organisation and service delivery.

Under the Electronic Transactions Act, it is made clear (Section 22) that where a law provides that a public body may accept the filing of a document or requires that a document be created or retained, that public body may accept that document in electronic form. Where a public

<sup>4</sup> <https://ulii.org/ug/legislation/act/2015/8-3>

<sup>5</sup> <https://ulii.org/ug/legislation/act/2015/7-6>

body may issue a permit, licence, or an approval, that public body may issue the permit, licence, or approval in electronic form. Similar rules apply to payments. Although this is a good way to legislate about form requirements, as it means that other laws can be read with this interpretation in mind and it is not necessary to amend every law that mentions documents or permits, it must be noted that the Act does not make it mandatory for government agencies to use the electronic format. Furthermore, additional rules can be issued, so until this is done, the legal certainty of what is required in specific circumstances may be lacking. The public body must make requirements known in the official gazette.<sup>6</sup> The real positive effect of this provision will depend on what the conditions will be and that sufficient public bodies make these known. It is at this point that unnecessary form requirements can be abolished, and relevant ones made suitable for a technology-neutral digital format.

The Electronic Transactions Act allows for public bodies to accept filings of documents and issue permits, etc., electronically but does not make this compulsory. The public bodies can issue additional rules for how this should be done, which means that the legal basis for electronic transactions exists, but the actual introduction of such transactions is a work in progress.

Requirements of a general nature about electronic signatures are provided. As has been commented by others, it may make sense in future legal reforms to merge the Electronic Transactions Act and the Electronic Signature Act, as the subject matter for these laws is very similar.<sup>7</sup>

The Electronic Transactions Act has a wide area of competence as it includes exchange of information or data and electronic sale or purchase of goods. It contains a section on consumer protection for e-commerce. As electronic ways of doing different things – governance, commerce, other communications – get more and more common and important in society, it is more difficult and often also less relevant to try to cover all aspects of such very different transactions in one law. The Act provides a good basis for progress on e-government as it makes clear that the electronic form is recognised legally, but in the future it may be more suitable to merge the law with the Electronic Signature Act and to have issues of e.g. consumer protection - for which the electronic form is only incidental - in legislation protecting consumers regardless of how they purchase goods or services (albeit with some specific rules adjusted to the type of transaction). [Reportedly, consumer protection legislation is under consideration by the Ministry in charge of trade.]

---

<sup>6</sup> It appears that different ministries have published different services, of varying complexity. As an example can be mentioned the Ministry of Agriculture e-Certification service for licences, permits and certificates related to livestock, fisheries and crop produce, for example, funded by a World Bank project. There are e-statistics for the same sector and an e-Voucher/m-Voucher, managed by NITA-U for subsidy distribution. A Knowledge Management Solutions Finder System Open Data Kit for animal disease reporting exists and other management systems to support more innovative tools, including use of AI to make agriculture more efficient. AESA *Uganda E-Services Assessment Report* (May 2020, ACP-EU Trade Com Programme) pp. 15-17. See also Barefoot Law *Cyber Laws of Uganda* (January 2019) pp. 26-27 and National Information Technology Authority Uganda *Feasibility Study for Integration of National Databases, Final Report*. (August 2015 Ernst & Young).

<sup>7</sup> Like the Commonwealth Telecommunications Organisation *Consultancy to Conduct a Gap Analysis of the Policy, Legal and Regulatory Framework for Uganda's Information & Communications Technology (ICT) Sector, Final Report* (January 2019) p. 9 and Barefoot Law (2019) p. 31.



The Electronic Transactions Act and the Electronic Signature Act could be merged. Consumer protection issues could be in a general law on consumer protection regardless of whether the transaction is electronic or not, to make law more technology neutral and more focused on content of transactions rather than form.

Procedural rules: The Electronic Transactions Act deal with various form requirements also in the procedural sense and in general ensures that electronic format may be used. The admissibility and evidential weight of electronic messages and records is specifically mentioned (Section 8). In addition to the above, electronic evidence is explicitly recognised in the Computer Misuse Act (2011). Evidence cannot be denied based only on its electronic format. Some of the studied reports mention challenges concerning the practical possibility for courts and administrative bodies to work with electronic data. Most probably educational activities need to continue and be intensified when e-transactions become more common

The legal basis appears to be appropriate and there should not be any question of the possibility to make electronic transactions with a legal value. However, in practice courts and administrative bodies throughout the country must also be competent and technically able to work with the new form of data.

Proof of payment, stamp duty, etc.: The Electronic Transaction Act stipulates that where there are provisions for payment, public bodies may make or receive payments by electronic means. This means that there is no basic legal obstacle to electronic payments. There is a Stamp Duty Act of 2014, with some amendments proposed in 2019. This does not appear to deal with the form for paying such duties.

However, the practical question of how payments are made should also be kept in mind. Uganda has a low level of formal banking. Mobile money is frequently used. This was first introduced in 2009 and by now there are a number of different systems. In 2020 the National Payment Systems Act was adopted. Previously mobile money was regulated e.g., by guidelines (from 2013) by the Central Bank.<sup>8</sup> A government payment platform has been developed. The Payment Systems Act permits innovative payment systems, regulating existing ones and introducing a "sandbox" system for innovation. It is not known if this will entail changes to the stamp duty act or any other acts regarding how payments are made and shown, but it provides a legal basis for different payment systems with an important role for electronic payment systems. Such systems are comprehensively regulated, taking into account the fact that traditional banking is not widespread but alternative systems predominate for a large part of the population. There is a governmental electronic payment platform in use allowing for different payment options, including mobile money..

In this context it may also be mentioned that use of data should normally not entail a cost if a system of interoperability is to function well.<sup>9</sup> In the Regulations on e-government it is stipulated that public bodies are obliged to pay for the connection to and the use of the National Data Transmission Backbone Infrastructure (NBI). The Board of NITA-U (see below)

---

<sup>8</sup> Barefoot Law (2019) p. 11. The 2013 Guidelines set out respective responsibilities, stipulating that licenced financial institutions are responsible together with mobile operators. In addition to consumer protection provisions, the Guidelines contain provisions to enable competition in the sector e.g. by requiring technological interoperability. Consumer protection guidelines of the Bank of Uganda (that e.g. contain rules on protection of privacy) also apply to mobile money services.

<sup>9</sup> NITA-U is mandated to charge for its services, which in case of licensing (in case the licensing is reasonable, see below) is in line with best international practice. However, the competence to charge should not be used to charge for data exchange or similar.

may set the rates. The 2019 National Databank Regulations mention the possibility of a fee for access to data.

It should be considered to what extent services like the use of the National Data Transmission Backbone Infrastructure, access to data or other concepts of interoperability should be subject to payment..

Rules on responsibility and competence: The National Information Technology Authority-Uganda (NITA-U) is an autonomous statutory body established under the NITA-U Act 2009, to coordinate and regulate Information Technology services in Uganda. NITA-U is under the general supervision of the Ministry of ICT and National Guidance. Further rules are found in National Information Technology Authority-Uganda (E-Government) Regulations, ~~from~~ 2015. NITA-U has the mandate to coordinate, promote, monitor, and support IT use; plan and implement e-governance infrastructure and backbone; and regulate the IT environment in the public and private sector. This latter tasks includes supporting the private sector to integrate services on shared platforms (like the government payment platform).<sup>10</sup>

NITA-U is engaging with different partners to develop digital skills curricula and provide various standards on matters such as Arbitration and Certification of IT Professionals and IT Training Institutions, Business Process Outsourcing Standards and Accreditation guidelines, Social media guide; Guidelines for development and management of Government websites and so on.<sup>11</sup>

Among its many tasks NITA-U regulates the electronic signature infrastructure and related matters. It has the task to certify businesses that provide ICT products or services. It is important to keep in mind that there should not be a need for special permits and certificates to provide services, unless there is an objective reason for such limitations and the process is proportional to that reason..

Although it appears as if NITA-U has the kind of mandate that is required for successful e-governance introduction, some studies<sup>12</sup> suggest that its role regarding e-government should be clarified and it should be given an increased role to enforce rules, including the power to sanction as well as to deal with consumer complaints and different disputes, including offering mediation.

### *1.3.2. Drafting of specific legislation*

Electronic identification and electronic signature: As mentioned Uganda has an Electronic Signatures Act from 2011<sup>13</sup> as well as an Electronic Transactions Act from 2011.<sup>14</sup> The electronic signature is based on public key infrastructure (PKI). The Electronic Signatures Act contains detailed provisions on various types of electronic signatures, signature creating devices, trust services, etc. plus the very important points of ensuring the legal validity of the signature. The law includes many notions know from best international practice. There is thus

<sup>10</sup> <https://www.nita.go.ug/> See also AESA *Uganda E-Services Assessment Report* (May 2020, ACP-EU Trade Com Programme).

<sup>11</sup> <https://www.nita.go.ug/service/regulatory-services>

<sup>12</sup> Commonwealth (2019) pp. 9-10, 13.

<sup>13</sup> <https://ulii.org/ug/legislation/act/2015/7-6>

<sup>14</sup> <https://ulii.org/ug/legislation/act/2015/8-3>

a legal basis for this essential element of a digital society. For this Report, we have not studied how the signature works in practice.

Of relevance for identification is also the Registration of Persons Act 2015, which harmonizes and consolidates the law on registration of persons to establish a national identification register and a national registration and identification authority and to provide for the issue of national identification cards. The information held within the register can be used for specific purposes based on law.<sup>15</sup>

On the regional level, the East African Community (EAC) is in the process of developing harmonised legislation on electronic transactions and signatures. Studies point out that there may be a need to amend provisions to harmonise with any such rules. This may also be an occasion to introduce such elements that are not in the law, like rules on seals and full legal recognition of trust services and certification services (plus registered electronic delivery).<sup>16</sup>

Data protection: Data protection legislation exists in the shape of the Data Protection and Privacy Act, adopted in 2019 and in force since March 2019.<sup>17</sup> The law sets up a Personal Data Protection Office reporting to the NITA-U Board, but it is not yet fully functioning. A Regulation was proposed in 2020 and awaits approval. Data protection has constitutional protection under Article 27 (2) of the 1995 Constitution, which protects the right to privacy.

The 2015 E-Government Regulations include rules to ensure the security of information and protection of personal data for e-government services. Government agencies are allowed to share personal data with other public and private organisations, but they are not allowed to disclose the information without a person's consent. Thus, data protection rules existed also before the recently adopted law.<sup>18</sup> Furthermore, there are data protection provisions in special legislation for different sectors. The Registration of Persons Act for example requires that a registration officer treats the personal data as confidential and does not disclose this data unless required by law. Financial legislation also contains data protection provisions.

Data protection legislation exists but is very new. Its proper implementation is very important for the creation of trust in electronic transactions.

Archiving: Uganda has a National Records and Archives Act from 2001. The Act mentions records in electronic form, as the functions of the Records and Archives Agency (Article 5) includes to ensure that organs of the state follow good practices of managing public records in any form, including electronic. Apart from this mention, the law does not specify how records are made or kept, but rather deals with procedures and responsibilities. The Electronic Transactions Act contains rules on retention of information or records, which can be done electronically (Article 9).

There is a legal basis for keeping records electronically. Practical and technical conditions are necessary to enable this also in practice, which is a work in progress for most countries.

Access to information: The Constitution (from 1995) defines a basic right to access to information which has been shaped by court cases that in general have defined the various possibilities to limit access. The African Charter on Human and People's Rights contains the principle of access to information. In 2005 an Access to Information Act was adopted. There

<sup>15</sup> Feasibility Study (2015) p 28.

<sup>16</sup> Commonwealth (2019) p 9.

<sup>17</sup> <https://ulii.org/ug/legislation/act/2019/1>

<sup>18</sup> Barefoot Law (2019) p 27.

are regulations from 2011 that serve to further clarify what information that should be accessible and in which cases there can be limitations. The regulations stipulate the form for requests, meeting these requests and so on. The key principle is one of openness.

A government body may provide electronic forms that can be used for making requests. In addition, persons have a right to make requests in various electronic formats, e.g. by e-mail. People can normally request the form in which they want to receive the information, which can be in electronic form, if this is available (or can be converted to this format). Some reports find that there could be more provisions on government proactively publishing information. Regulations on e-Government make it compulsory to have websites and the regulations allow NITA-U to establish websites if authorities do not.<sup>19</sup>

### *1.3.3.Databases*

Given the nature of the Project, which is focused on interoperability of databases, the legal issues linked to databases are of specific importance and are given extra attention in this Report. As mentioned above, specific rules on what data is collected in different contexts should be in legislation on the area in question, but certain common rules and a sufficient level of common standards is necessary.

Through the Ministry of ICT, NITA-U has put in place the National Databank Regulations (2019). The 2019 Regulations define the national databank as the information system technology system implemented and managed by NITA-U resulting from the integration of various databases to facilitate real time access and retrieval of information by authorised persons. Section 3 stipulates the creation of such a databank and that every data controller shall link its database as prescribed by NITA-U. A register of databases shall be maintained by NITA-U (Section 8) while every data controller is responsible for keeping its database updated (Section 7). In general, the Regulations set up a good system of dividing tasks between the authority with overall responsibility (NITA-U) and the data controllers. [A feasibility study undertaken by NITA-U in 2015 indicated that at the time a small fraction of public bodies used the mentioned infrastructure.<sup>20</sup>

In NITA-U E-Government Regulations from 2015, in Regulation 2 , e-government is defined as the use of ICT to deliver public services in a convenient, efficient customer-oriented and cost-effective way. Integrated service delivery is defined as the provision of government information or services integrated according to function or topic rather than separated according to the boundaries of agency jurisdiction. A government web portal is defined as a website or interface that offers a range of resources and services, including email, a search engine and an integration of websites. These definitions provide a good basis on which to build the more detailed provisions of e-government.

The Regulations are based on the authority given by the 2009 Act on the National Information Technology Authority Uganda to the Minister responsible and passed in consultation with the Board of NITA-U. The 2009 Act provides an appropriate legal basis for taking decisions related to e-government, including interoperability, and these Regulations are an example of the exercise of these powers.

---

<sup>19</sup> Barefoot Law (2019) pp 22-23.

<sup>20</sup> Nine out of 32 were using it at the time of the study. Feasibility Study (2015) pp 82, 87.

By the Regulations, details of the National Databank are established. This is an information technology system managed by NITA-U resulting from the integration of various databases. Data controllers shall link their databases to the system as prescribed. The definition of the National Databank stipulates that this is an information technology system implemented and managed by NITA-U resulting from the integration of various databases established by different data controllers to facilitate real time access and retrieval of information by authorised persons. From this definition and other provisions, we can see several important elements. The databases are managed by different controllers, thus there is no creation of one centralised database. The aim of the databank is to make it possible to use data across different organisations, but this is to be for authorised persons only.

The 2019 Regulation includes many relevant provisions for databases. Definitions of what constitutes processing and so on largely follow best international practice. The Regulation sets out tasks for the authority – NITA-U – in relation to the system of interoperability, including to take appropriate security measures, ensure a system for resolving complaints, cooperate internationally and issue relevant codes of practice or guidelines. Data controllers are responsible for the integrity and confidentiality of their databases and for taking reasonable technical, security and organisational measures in this respect. The division of responsibilities appears appropriate although the real functioning will be fully seen only when the various acts presupposed are taken and the practical cooperation and division of tasks is seen. The Regulation includes the important provisions on notification of any data security breaches.

Access rights to the Databank are given by NITA-U in accordance with the relevant access rights and access levels. These remain to be set out in further acts. The access should be limited to what is needed and be as specific as possible, to avoid excessive possibilities to access personal data, especially sensitive data. As Uganda only has very recent data protection legislation, it is essential to ensure that the understanding of providing access to data in a restrictive manner permeates the interoperability system.

There is a provision on the need to have a catalogue of databases, which is very important. The Regulation sets out that there shall be a register of databases in the National Databank and among information listed is the purpose for which data is collected.

The Regulation is an appropriate legal act for the creation of a functioning system of interoperability. It includes relevant provisions for an interoperable system of databases, which however will be completed with additional guidelines etc. to firmly establish the division of roles, access levels and so on.

The Regulation mentions the possibility that there is a charge for data access, which is something that should be re-evaluated from a policy viewpoint – whether payment for use of data is appropriate.

The Regulation does not define, what the “linking” means. It means collecting metadata about registries or centralised access point to the registries.

Although providing a basis, the Regulation needs additional discussions. It may not be reasonable to centralise access to the registries. The centralisation of access to the registries can cause single point of failure for Ugandan e-government.

#### *1.3.4. Drafting or amendment of indirectly connected legislation*

Information and Communications Technology (ICT) legislation and competition law: The current Communications Act from 2013<sup>21</sup> consolidated the 2000 Communications Act and the Electronic Media Act. One of the aims of the 2000 law was to introduce more competition in the sector following its liberalisation. The Uganda Communications Commission,<sup>22</sup> the competent regulator, was set up as a consolidated regulator by the 2013 Act, as a successor to the initial regulator created by the 2000 law. The law is supplemented with a series of regulations, on licensing, equipment, type approval and so on. The Ugandan telecommunications market is one of the most liberalised in Africa and competition is regarded as working well. Among problems mentioned by reports<sup>23</sup> is a minimal sharing of infrastructure, lack of access of affordable broadband and a quite significant digital divide.

Public procurement and Public-Private-Partnership (PPP) legislation: Uganda has legislation on PPP since 2015 but has used PPPs even earlier. There is a special unit for PPP under the Ministry of Finance, Planning and Economic Development.<sup>24</sup> A Bill with various amendments to the Public Procurement and Disposal of Public Assets Law was proposed in May 2019. Among other things, it provides for electronic records and communication. Private sector engagements and concerted efforts to move to a digital economy are aspects of the Ugandan national development plans.<sup>25</sup> This issue thus appears to be properly regulated and allowing for projects in the ICT sphere.

Intellectual property legislation: Uganda recently adopted a National Intellectual Property Policy. The idea is to design different measures to enhance innovation, which may include amendments to legislation. What is in need of more efforts is commercialisation of IP. There is a national IP office, the Uganda Registration Services Bureau. The legislation includes the Copyright and Neighbouring Rights Act 2006, the Trade Secrets Protection Act 2009, the Trademarks Act 2010, the Geographical Indications Act 2013, and the Industrial Property Act 2014.

Incentives for use of e-services: The Electronic Transactions Act lists a number of aims (Article 4), including to enable and facilitate electronic communication and transactions and promote e-government services as well as to encourage investment and innovation in ICT to promote electronic transactions and develop a safe, secure and effective environment for the consumer, business and the Government to conduct and use electronic transactions. Such aims are reflected in various programmes and projects to further e-government and support ICT.<sup>26</sup> To facilitate practical access, NITA-U provides free wi-fi services in many locations.

---

<sup>21</sup> <https://www.ucc.co.ug/files/downloads/UCC%20Act%202013.pdf>

<sup>22</sup> <https://www.ucc.co.ug/> (see also <https://ict.go.ug/about-us/agencies/uganda-communications-commission/> )

<sup>23</sup> Commonwealth (2019); AESA (2020).

<sup>24</sup> <https://www.pppunit.go.ug/content/overview-ppp-projects-uganda>

<sup>25</sup> AESA *Uganda Assessment Report of Digital Skills, Entrepreneurship & Innovation* (May 2020, ACP-EU Trade Com Programme) p. 11.

<sup>26</sup> The Ministry of ICT and National Guidance website provides a heading of e-governance with updates on progress and plans: <https://ict.go.ug/initiatives/e-governance/>

NITA-U has developed different regulations to promote use of electronic services within government agencies as well as increased citizen participation in government.<sup>27</sup>

Uganda has a number of tools in place to make e-services available to the public. There is an e-Citizen portal<sup>28</sup> as well as a Mobile Service Delivery Gateway (called uConnect). The e-Citizen Portal is a one-stop-shop for 178 different systems/applications and 71 services like e-passport or tax. There is an "Ask Your Government" website (from 2014), designed to facilitate for people to ask questions from government and authorities under the government.<sup>29</sup> Despite these efforts of outreach, there is a considerable digital skills gap and a digital divide in the Ugandan society.

There appears to be room for improvement regarding overview of e-government services that are currently available and the relevant conditions and requirements for such services. With such information readily available, it would be easier to raise awareness among businesses and citizens about the availability of e-government services.<sup>30</sup>

Cybersecurity and cybercrime legislation: Uganda has a Computer Misuse Act from 2011 and a Regulation of Interception of Communication Act from 2010. Normally, such specific laws supplement general provisions on what constitutes crimes, which may be relevant for cybercrimes even if drafted with different things in mind. The Penal Code and Penal Procedure Code in force are from 1950. The process to join the Budapest Convention was initiated in 2018,<sup>31</sup> but the country has not yet joined. In addition to laws, NITA-U has developed a National Information Security Policy which outlines the mandatory minimum security controls that all public and private sector organisations that handle official communications, process personal data or perform similar functions must apply to reduce vulnerability to cyber threats.<sup>32</sup> There are probably additional regulations and rules in various contexts, like protection of critical infrastructure. It is not necessary to go into detail, as it can be seen that a basic legal framework does exist. As always, proper implementation – for which sufficient knowledge and understanding among relevant persons – is the key to success, with no need for too detailed laws on every possible threat.

#### 1.4. Concluding remarks on the legal framework

Uganda has a legal framework for e-government in place. This is positive and provides Uganda with an advantage over many countries and a good basis for increase and improvement of e-government in the country. There should not be too much detailed law on digital issues, as these form a part of all aspects of society rather than a separate unit. In Uganda, the focus of the legal work related to e-government should be on ensuring that the existing laws are properly implemented.

Uganda has a designated authority with competence for e-government in the form of NITA-U, with adequate competence for further development in the area. Some commentators suggest that the mandate of the organisation could be modernised, both in the sense of having an even clearer mandate to promote e-government but also so as to avoid excessive regulations in the ICT sector. The basic legal framework for enabling interoperability appears

---

<sup>27</sup> Feasibility Study (2015) p. 82.

<sup>28</sup> <https://ecitizen.go.ug/content/ecitizen-portal>

<sup>29</sup> <https://askyourgov.ug/>

<sup>30</sup> Barefoot Law (2019) p. 28.

<sup>31</sup> Barefoot Law (2019) p.18.

<sup>32</sup> Feasibility Study (2015) p. 84.

to be in place, including essential rules about databases and their interoperability. However, some reports mention that the implementation may lag behind and that there is a need for a better overview of what electronic services exist. Although the essential basic issue of recognising electronic transactions and identities is handled via the relevant laws, as has been pointed out, the laws do not make it mandatory for government agencies to use the electronic format and additional rules need to be issued. In this process, which will presumably be ongoing for some time, it remains necessary to pay attention to what form requirements that are finally made and how these are made the most suitable for each situation as well as easy to use. The laws on Electronic Transactions and Electronic Signatures could be merged, as the core issues are the same. Consumer protection rules for electronic transactions would be more suitable in general consumer protection legislation, rather than a law only for electronic transactions and reportedly, this is in the process

Regarding form requirements and the possibility to use electronic transactions, although the legal framework is in place, it is essential that courts and administrative authorities have the ability in practice (which includes the proper competence of staff) to use this new form of transactions. Another practical question is how it is possible to present proof of payment electronically, for transactions that carry a charge, on which there have been recent developments. In this context, it can be mentioned that there should be as few costs and charges for transactions and data use as possible.

Uganda has recent data protection legislation, which introduces the modern best practice of one general data protection legal framework rather than provisions in various sectoral legislation. The implementation of the legislation is in a very early phase. Given that many reports mention the problem of low awareness of digital legislation in general, there is a need for attention to the data protection question as such legislation plays a very important role when it comes to strengthening people's trust in digital services.



## 2. Policy environment review

### 2.1. Introduction

The concepts of information society and the recently more often used one of digital transformation of society focus on all levels and all fields of society. Consequently, topics related to the use of technology in society should be reflected in all policy documents. Within the scope of the current review, it is not realistic to include all different policy aspects, but we focus directly on the issues related to the interoperability framework and architecture of e-government. In addition, it is important to mention that Uganda 2040 is emphasizing the importance of digital transformation in Ugandan society and this is also relevant for the government interoperability framework (GIF).

The Ministry of ICT and Guidance is explaining on its web site<sup>33</sup> the Digital Uganda Vision, based on Uganda 2040:

“Digital Vision is a National Policy and Strategic Framework that reviews, integrates, consolidates, and improves all the existing ICT strategies, policies and plans into one overarching digital Vision for Uganda by providing a unified direction for ICT development and an Integrated ICT project implementation approach.”

The aim of this vision is

- to have a consolidated and integrated strategic direction of how ICT shall support the delivery of Vision 2040,
- to review, align, harmonize and synergize the existing fragmented policies and strategies into one overarching document,
- to align ICT initiatives to major objectives of the different Sectors,
- to encourage the involvement of key stakeholders,
- to institute central implementation, coordination and monitoring and evaluation of ICT initiatives, etc.

Digital Uganda Vision is available still in draft version but there are some conceptual descriptions very actual for GIF:

- **Equity:** All citizens shall have the same consideration in the enjoyment of rights and freedoms, attainment of access to affordable ICT, services and content.
- **Technology neutrality and Open Access:** The development of our ICTs shall be technology neutral and use common, interoperable, open access standards and protocols and foster infrastructure sharing.
- **Environmental protection and safety:** The design, utilization, and disposal of ICTs shall maintain the integrity of the environment and safety of the community.
- **Good governance:** The implementation of the DUV shall adhere to the highest standards of good governance including accountability, transparency and ethical behavior among others;
- **Collaborations and Whole of Government approach:** Engage and collaborate across Government and with industry and other stakeholders in the implementation of the

---

<sup>33</sup> <https://ict.go.ug/initiatives/digital-uganda-vision/>

Vision;

- Promotion of local content: Promote the use of local solutions in the realisation of the Vision.

Many of these aims are important with regard to the e-Government Interoperability framework and Enterprise Architecture but due to the scope of the current project it is not possible to study all available policy documents.

During this policy review, we focused on the following important materials about Ugandan e-government. On the basis of these documents, we have identified areas for further discussion. The materials reviewed include:

- E-Government Master Plan
- ICT Sector Implementation Plan
- Feasibility Study Report for Integration of National Systems
- National Information Security Framework
- Information sharing principles
- Interim Interoperability Framework
- Integration of National Systems concept
- Strategic Plan 2018/19 - 2022/23 (not included in the TOR initially, but suggested by NITA-U)

## 2.2. e-Government Master plan

The Master plan<sup>34</sup> was outlined during a project carried out by the National IT Promotion Agency (NIPA) of Korea. A goal of the project was to achieve good governance and social and economic development by establishing effective, systematic, and productive e-government. The final report comprises the following four points to achieve the goal.

- Establishing the vision, strategy and framework
- Selecting quick win projects and drawing a long-term roadmap
- Defining a governance framework to regulate and control e-government initiatives
- Defining the direction of restructuring the legal framework

According to the authors of the Master Plan, establishing an e-government Master Plan is a long-term project, which requires more than a ten-year period. However, it is better to shorten the project period and make periodic modifications to the plan.

The Master Plan comprises five parts:

1. Project Overview
2. Research & Analysis
3. Vision & Strategy
4. Implementation Strategy
5. Action Plan

---

<sup>34</sup> National IT Industry Promotion Agency of Korea *2012 Uganda e-Government. Master plan.* (276 p.)

Two countries, Korea and UK, are taken as templates for building the Ugandan e-government. Both countries are highly ranked. Both governments have been analysed deeply. The approach of both countries was found to be appropriate for Uganda.

The Master Plan highlights four main goals:

- G4C: Provide citizen-oriented and customized services
- G2B: Provide transparent and prompt services
- G2G: Networked and knowledge-based government
- Infrastructure: Management of integrated ICT infrastructure and establishment of the legal framework

The Master plan brings out 25 important strategic initiatives for Uganda

1. National IT Standard Framework
2. e-Learning
3. Recruitment and Employment Information System
4. National Medical and Health Information System
5. Single Window for Online Business Service
6. Government Business Reference Model (BRM)
7. Architectural Administration Information System
8. Government Work Management System
9. Customs Information System
10. National Integrated Logistics
11. Electronic International Trading System
12. Government Representative Portal
13. Groupware (e-Document, e-Approval, Knowledge Management System)
14. Digital Archiving
15. Electronic Procurement System
16. Government Data Centre
17. Online Citizen Participation Portal
18. Integrated Civil Service Call Centre
19. Informatisation of City/Province Administration
20. e-Foreign Affairs
21. e-National Assembly
22. National Finance Information System (NAFIS)
23. PKI
24. Administration Information Sharing Centre
25. National Identification (N-ID)

The following are identified as priority projects in order to establish e-government in Uganda:

- ❖ Digital Archiving
- ❖ National Identification (N-ID)
- ❖ National Finance Information System (NAFIS)
- ❖ Government Data Centre
- ❖ PKI
- ❖ Groupware (e-Document, e-Approval, Knowledge Management System)
- ❖ Electronic Procurement System
- ❖ Administration Information Sharing Centre
- ❖ National IT Standard Framework
- ❖ Government Representative Portal
- ❖ Government Work Management System
- ❖ Single Window for Online Business
- ❖ Online Citizen Participation Portal

The Master Plan sets clear goals, concrete strategic topics and highlights priority projects for Ugandan e-government.

Selected templates (Korea and UK) have been appropriate for starting to build e-government in Uganda.

Many goals of the Master plan have been achieved. It is now time to renew the Ugandan e-government approach. It may be reasonable to put the main emphasis on interoperability and on building a holistic e-government architecture.

### 2.3. ICT Sector Implementation Plan

The five-year ICT sector Implementation Plan (ICT-SIP)<sup>35</sup> is developed to guide planning, budgeting and investment in the sector. In addition, the Plan will strengthen mechanisms for quality, effective and efficient service delivery. The Plan is in conformity with the National Planning framework including the National Development Plan II, and the National Vision 2040.

The Action Areas for ICT-SIP are as follows:

- ❖ Policy, Legal and Regulatory Framework
- ❖ Institutional Framework
- ❖ ICT Infrastructure
- ❖ Human Capital Development and Planning
- ❖ Information Security

---

<sup>35</sup> Ministry of Information and Communications Technology *ICT Sector Strategic and Investment Plan* (2015/16 – 2019/20). ConnectedUganda@2020 (214 p.)

- ❖ Research, Innovation and Development
- ❖ Health, Safety and Environment
- ❖ Promotion and Coordination of ICT in other Sectors
- ❖ Promotion of e-Services and Local Content
- ❖ e-Government
- ❖ ICT Industry Promotion in Target Markets

The ICT-SIP is divided into six chapters as follows:

Chapter 1: Introduction covering the background of the ICT Sector, institutional setup within the sector, rationale and process for development of the plan;

Chapter 2: Sector Achievements highlighting how far the sector has come and its achievements;

Chapter 3: Situational Analysis providing an assessment of the current situation of the ICT Sector and the challenges or gaps faced;

Chapter 4: Strategic Direction pointing out the Strategic Direction for the ICT Sector, namely the Vision, Mission, Strategic Themes, Strategies and Strategic Interventions for the next five years;

Chapter 5: Implementation Mechanism indicating how the ICT-SIP will be implemented through the monitoring and evaluation framework, and communication strategy; and

Chapter 6: Investment Plan highlighting the funding framework and cost of the ICT-SIP.

The five-year ICT-SIP provides a coherent set of strategies, interventions, actions and attendant resource requirements to enable ICT to play a pivotal role in the country's socio-economic transformation and development as envisaged in the NDP II and Vision 2040.

#### 2.4. Feasibility Study Report for Integration of National Systems

The Government of the Republic of Uganda acting through NITA-U identified the need to integrate national databases and systems to provide standard e-Government Services Integration Framework for the development of G2G, G2B and G2C services. Ernst & Young (EY) was contracted by NITA-U to carry out a feasibility study<sup>36</sup> for integration of the national databases.

**Overview of Best Practices.** Countries looked at included Estonia, Moldova, Singapore, USA and the Republic of South Korea. Each case study was analysed at a high level. The overview is focused on the functionality of these e-governments. Requirements and conceptual architecture aspects have been dealt with in less detail. Data exchange on G2B level is not analysed. The need of cross-border data exchange is not mentioned.

Functionalities of best practices are adequately covered in the best practice overview. Conceptual aspects have been dealt with in less detail.

**Identification of priority e-services.** The top three priority e-services recommended by the report:

- ❖ E-registration. This service will support citizen registration for various Government

<sup>36</sup> NITA-U *Feasibility Study for Integration of National Databases*. Final Project. 2015. (378 p.)

services. The service will reduce the time taken by citizens to physically queue in lines while registering for Government services.

- ❖ E-verification. This service will support identity verification of people to businesses and Government bodies. This enables quick service delivery, since currently validating identity and authenticity of documentation before providing services takes a long time.
- ❖ E-citizen. Using this e-service, the citizen is able to view their entire online profile from a single place. A citizen is able to view information about their identity, request modifications, pay utilities and taxes, view asset information e.g., land owned and view their criminal records.

**Technical Solution Proposal.** Proposed integration illustrated

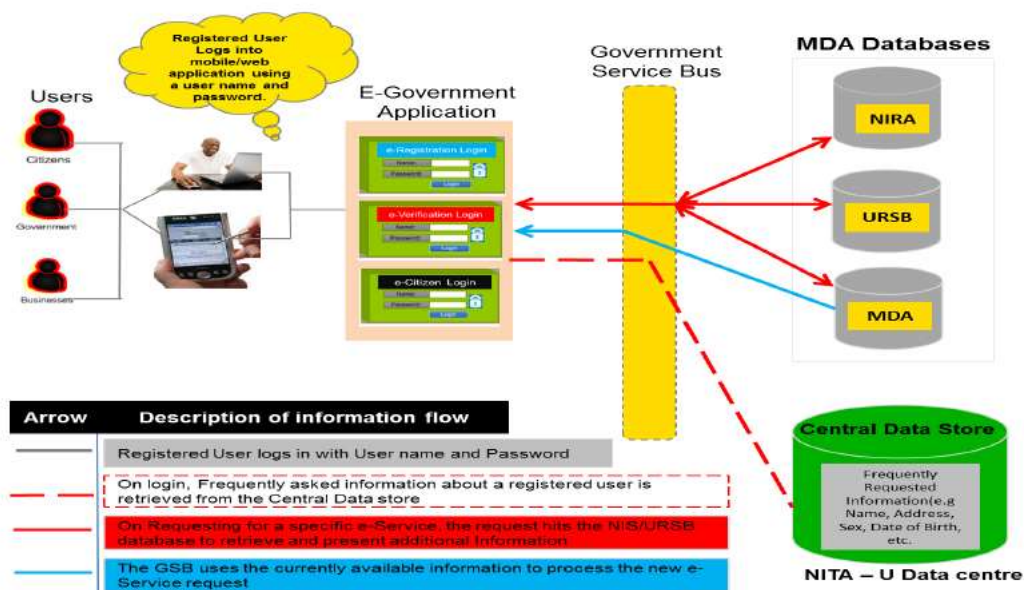


Figure 1 Proposed by EY integration

Some important topics need additional discussion, like centralised vs decentralised, commercial vs open-source platform, involving private sector, cross-border data exchange, single point of failure, centralisation vs decentralisation of e-service orchestration and choreography.

The chosen architecture is based on the Enterprise Service (ESB) architecture, open-source software is avoided, the recommendation was mapped against Oracle, IBM and Microsoft technologies. The use of ESB architecture is accepted on MDA level.

The problems of use of ESB architecture on interagency level should be discussed during the current project.

## 2.5. National Information Security Framework

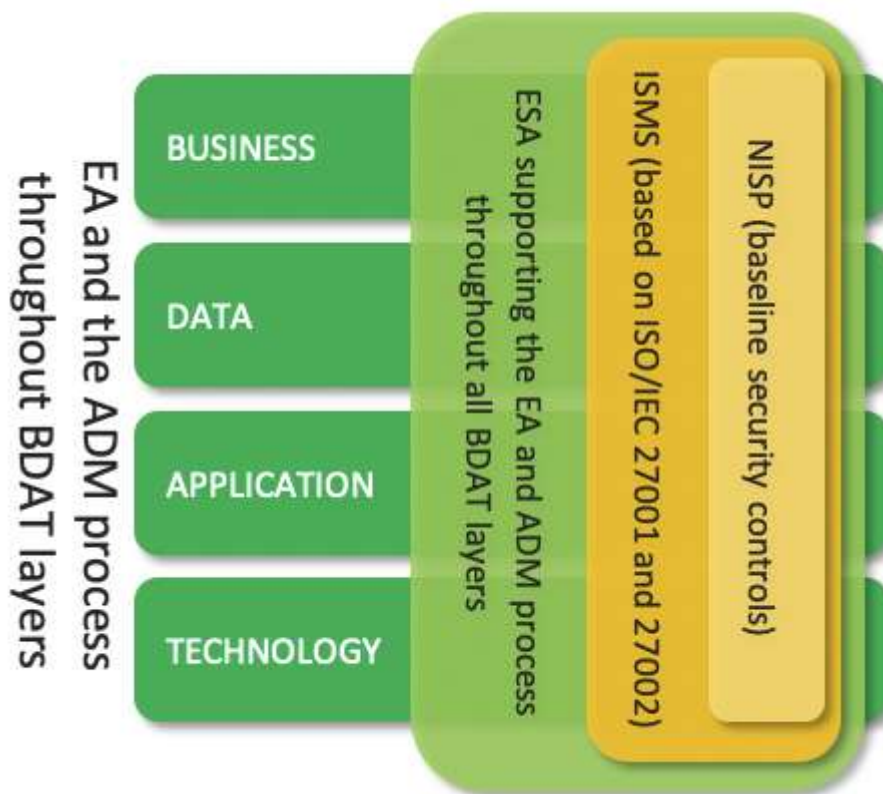
### 2.5.1 Introduction

The draft version of the National Information Security Policy (NISP), a publication of the National Information Security Framework, was issued in February 2014. The NISP is carrying the main idea of mandatory minimum collection of security controls (the baseline) for any

Uganda private or public sector organisation processing personal data, owning or operating protected computers or official communications. More precise applicability is defined as:

- Computers used directly in connection with or necessary for Uganda's:
  - Security, defence, diplomacy
  - Law enforcement
  - Communications infrastructure
  - Banking and financial services
  - Public utilities
  - Public key infrastructure and public safety
- Information that Ministries, Departments, Agencies and Local Governments (MDALs) create and process during their day-to-day business activities
- Critical infrastructure and Critical Information Infrastructure.

NITA-U has accepted ISO/IEC 27000 family security standards as a part of their Standards Catalogue.<sup>37</sup> The relationship between Enterprise Architecture (EA), Enterprise Security Architecture (ESA), Information Security Management System (ISMS), ISMS security standards and NISP can be visualised with the following simplified diagram:



To successfully and completely integrate NISP minimum security controls with ESA and EA, the NISP must align with ISMS (ISO/IEC 27001) requirements and support ESA and EA concepts throughout the full Architecture Development Method.

### 2.5.2 NISP alignment to ISO/IEC 27001

As mentioned above, the baseline controls and the mandatory minimum-security requirements of the NISP apply to a large audience in Uganda. This allows us to compare its content to the

<sup>37</sup> <https://www.nita.go.ug/publication/nita-u-standards-catalogue-2017>

ISO/ IEC 27001:2013 standard that is similarly applied across a wide range of organisations, regardless of their needs and objectives, security requirements, processes used and the size and structure. Both the NISP and ISO 27001:2013 aim at creating a system, or a model that manages key functional security areas in an organisation:

|  |   |
|--|---|
| <p>NISP uses <b>Security Governance</b> to manage:</p> <ul style="list-style-type: none"> <li>- Information Security</li> <li>- Personnel Security</li> <li>- Physical Security</li> </ul> | <p>ISO 27001 uses <b>ISMS Requirements</b> to manage:</p> <ul style="list-style-type: none"> <li>- Information Security Policies</li> <li>- Organisation of Information Security</li> <li>- Human Resource Security</li> <li>- Asset Management</li> <li>- Access Control</li> <li>- Cryptography</li> <li>- Physical &amp; Environmental Security</li> <li>- Operations Security</li> <li>- Communications Security</li> <li>- System Acquisition Development &amp; Maintenance</li> <li>- Supplier Relationships</li> <li>- Information Security Incident Management</li> <li>- Information Security Aspects of Business Continuity Management</li> <li>- Compliance</li> </ul> |
|--|---|

The fact that the NISP refers to ISO/IEC 27001 in a number of its controls points out that the Policy itself does not diverge greatly from the ISO standard. In our mapping, whilst the NISP and the ISO/IEC 27001 standard do not count the security controls in the same way, all NISP controls were covered by the ISO standard.

Where the two diverge is in areas such as support, performance evaluation or improvement. Although the NISP did not dedicate an entire control to cryptography – as ISO/IEC 27001 does – the Policy stresses the importance of encryption on several occasions. The starkest contrast is in the approach that ISO/IEC 27001 takes to ensure that activities related to system acquisition, development and maintenance are part of the ISMS, while the NISP omits this area.

### *2.5.3 NISP alignment to ESA*

NISP and its baseline controls are not contradicting ESA concepts in any way. There are directly linkable topics between NISP and ESA, but also through the ISMS of ISO/IEC 27001.



The most remarkable deficiency of NISP is not the NISP itself, but the surrounding processes and principles to implement NISP in any specific organisation. For example, the following questions are not getting answers:

- How to align the organisation's security strategy to the business strategy?
- How to define the organisation's security objectives and requirements?
- How to design the organisation's own information security policy?
- How to ensure that the organisation's own information security policy is effective in terms of the security controls effectively controlling the organisation's security risks?
- How to identify and manage security risks?

During the current review, it was not possible to acquire a copy of the National Information Security Framework to analyse the presence of missing strategical and implementation level processes. However, ESA's fundamental goal is to find the desired future state of security and design the implementation steps.

#### 2.5.4 NISP current status

The 1.0 version of the NISP draft document was issued in the year 2014. During the inception report preparation phase, it was not possible to obtain evidence about putting the NISP into practice, including approving, establishing and implementing the policy.

In addition, the NISP document does not reflect its own requirement to be reviewed and updated at least annually, even though the NISP says "*NITA-U shall review this policy, at least annually*" (page 7).

The NISP core does not require any major changes, but minor modifications to fix expired references. The main focus should be invested on applying ESA principles supporting the NISP and ISMS application. These principles can be applied by documenting, approving and implementing the other tiers or levels of the National Information Security Framework (NISF) that are currently missing.

#### 2.6. Interim Interoperability Framework

NITA-U has developed the e-Government Interoperability Framework (e-GIF)<sup>38</sup> to guide the smooth implementation of interoperable e-government systems and to enhance capability of government institutions to deliver services effectively.

e-GIF main topics are:

- Principles
- Organisational interoperability
- Information and semantic interoperability
- Technical Interoperability
- Interoperability governance

When a new version of e-GIF is needed, this document can be used as a basis for it.

<sup>38</sup> NITA-U *Uganda e-Government interoperability framework* (E-GIF) 2017 (27 p.)

## 2.7. Integration of National Systems concept

The report "UgHub. Application and Data Integration Platform for the e-Government of Uganda"<sup>39</sup> is focused on developing a common platform through which data shall be shared between MDAs in a cost effective, secure, harmonised and reliable manner to improve e-service delivery, expedite decision making and implementation of Government Programmes.

The introduction part gives background information and highlights the need for an integrated platform. The Report includes case studies of four countries with integration platforms: Kenya, Estonia, Bahrein, Moldova. A comparison of architectures is not provided in the report. It seems WSO2 is chosen as basis for integration in Uganda. In the report<sup>40</sup> of the project "e-Governance Support to Ukraine", financed by the Swedish International Development Agency and the Estonian Ministry of Foreign Affairs, a comparison of WSO2 and X-Road in-depth analysis and real testing was performed by Michiel Malotaux, Innovation Guide, The Vision Labs (The Netherlands). The Report says: "WSO2 is an Open Source SOA middleware platform providing data services, business process management, ESB routing/transformation, rules, security, throttling, caching, logging and monitoring. WSO2 is primarily used within the enterprise/ministry domain (i.e., within a controlled environment). WSO2 mainly uses the organization's private Intranet. Security facilities include: identification, authentication, encryption and logging. Missing, but important between independent organizations, are: certification and non-repudiation. WSO2 is a centralized facility and therefore less scalable and resilient (24x7 availability cannot be guaranteed). In the tests, the load balancer seems to be a single point of failure, and it is also a performance bottleneck. WSO2 provides message transformation and processing, but this is not needed for the UIS between Government organizations. Ministries could be expected to even reject the UIS due to its central processing ambitions. WSO2 can be used message-agnostic, which was proven in the tests."

The second part focuses on understanding integration of government systems. It outlines rationales and focus of projects. Sections that talk about P2P integration are questionable. Eight weaknesses of P2P connections are listed in this document. Are these shortcomings inherent on the Internet (and www, Skype) as a typical P2P network? We can use architecture where interfaces/proxy are standardised, and every MDA will open all services over this proxy and get services from other providers over this proxy. For example, the Estonian X-Road architecture in the figure has no issues listed in the reviewed document.

---

<sup>39</sup> NITA-U *UgHub. Application and Data Integration Platform for the Government of Uganda*. May 2020 (73 p.)

<sup>40</sup> Michiel Malotaux *Ukraine Interoperability Solution*. UIS Test Report (44 p.)

## X-ROAD ARCHITECTURE

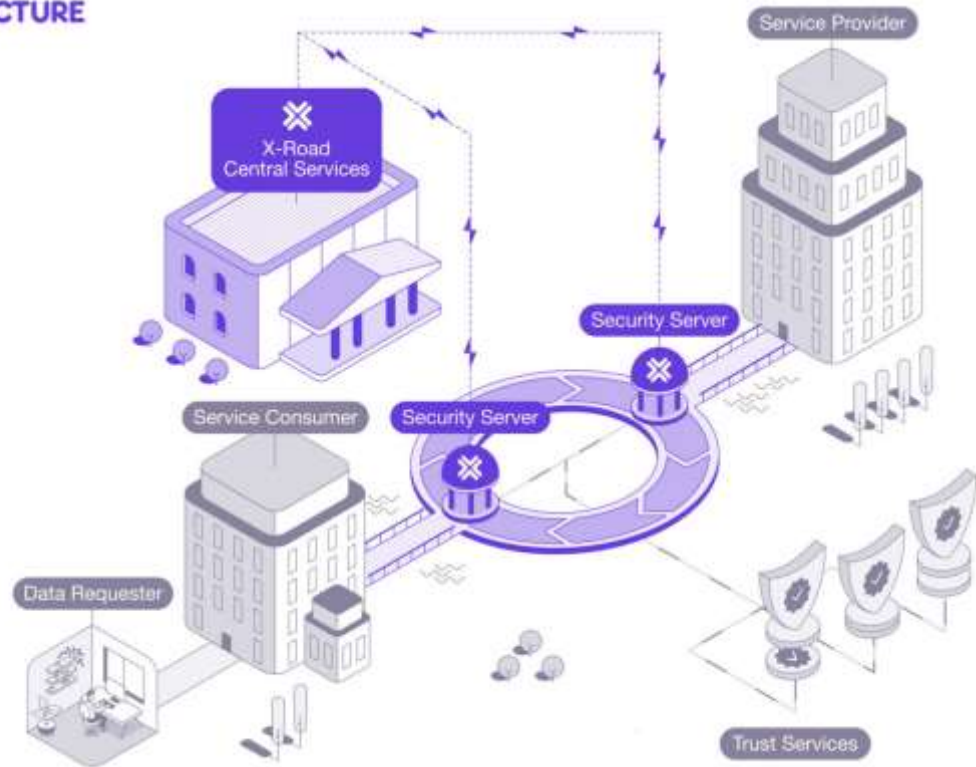


Figure 2. Example of P2P architecture (<https://x-road.global/architecture>)

The P2P issues raised in the report can be avoided as illustrated by the X-Road example

Other parts of the Report are dedicated to the WSO2 platform. WSO2 is an excellent platform for public and private institutions. The platform can be used for building a citizen portal. The use of WSO2 on interagency and cross-border level is questionable. WSO2 includes components (like identity and access management, AI, data mining, analytics, etc), which it is not needed to centralise. These tasks are important to perform under control of data owners. A more detailed analysis of WSO2 issues can be found in chapter **Error! Reference source not found.** of the Inception Report. WSO2 does not support cross-border data exchange.

The issues of the WSO2 platform for the interagency and cross-border level are discussed in chapter **Error! Reference source not found.** of the Inception Report.

If Uganda will choose WSO2, additional tools are needed to alleviate weaknesses. Some internal components (identification, digital signing, timestamping) will need to be replaced with third party components. Data owners will be granted full control over their data.

### 2.8. NITA-U Strategic Plan 2018/19 – 2022/23

Dr Aminah Zawedde said "The new NITA-U Strategic Plan 2018/19 – 2022/23<sup>14</sup> is one that transitions NITA-U from an IT infrastructure-based model to an IT service delivery model. The new Strategic Plan highlights three fundamental pillars on which NITA-U will base to achieve our vision. These are:

- service delivery excellence,
- operational excellence and
- relationship excellence.

The vision of the Strategic Plan is to ensure that 80% of Government services in the key priority sectors are available online and accessed by 60% of the target population.



Figure 3: The three strategic focus areas of the Strategic Plan

#### Strategic objectives:

- SO 1: Improve Customer Satisfaction
- SO 2: Improve Products and Services
- SO 3: Improve Financial Performance
- SO 4: Improve compliance with IT legislations and standards
- SO 5: Increase uptake of service
- SO 6: Risk Management
- SO 7: Improve communication and flow of information
- SO 8: Improve distribution of Products and Services
- SO 9: Optimize utilization of infrastructure
- SO 10: Improve use of technology
- SO 11: Improve Skills and Competencies
- SO 12: Improve Performance Management

The plan proposes eleven initiatives cut across the different strategic objectives and cater for all the perspectives i.e. customer, financial stewardship, internal processes and organizational capacity:

- Strengthen customer relationship management through strategic marketing and communication.
- Implement a Sensitization and compliance Program.
- Capacity building and skilling for e-Government services.
- Implement the IT Service Delivery Model.
- Implement an equitable employee management program.
- Develop and roll out e-Services and M-Services
- Develop and Implement the NITA-U revenue growth program.
- Automation of key NITA-U processes.
- Implement an Information Security Program.

- Implement Research and development program.

The project for the development of a Government Enterprise Architecture and E-Government Interoperability Framework for Uganda will be aligned to the objectives and activities of the Strategic Plan.

### 3. Concluding remarks

Uganda has produced a number of strategies, policies and plans for use of ICT for governance and the introduction and strengthening of e-government. Many relevant specific legal acts have been adopted and necessary amendments made to other laws. A number of comparative studies have been undertaken to learn from good examples of other countries and use these as a basis for implementing ideas derived from best international practice. Thus, Uganda has undertaken several of the steps necessary related to e-government.

There is a National Information Technology Authority-Uganda (NITA-U), which is an autonomous statutory body with the task to coordinate and regulate Information Technology services in Uganda. NITA-U is under the general supervision of the Ministry of ICT and National Guidance. It is set up by law with specific duties and responsibilities according to regulations. NITA-U has the mandate to coordinate, promote, monitor, and support IT use and plan and implement e-governance infrastructure. Uganda has a National Data Transmission Backbone (NBI) managed by NITA-U.

However, as pointed out in the Digital Vision, there is a need to harmonize the different policy papers and strategies. The multitude of documents makes it difficult to assess to what extent the plans overlap, what is implemented and what is overtaken by more recent plans and documents. In the legal field, it may be recommended to consolidate legal acts in order to make legislation technology neutral to a greater extent.

In order to evaluate the successful digitalisation of society, for legal, technical as well as practical issues much is dependent on how the existing tools are used in practice. For example, there is a need for public bodies to adopt further rules on some issues and to address potential weaknesses in the integration of systems. Some important topics need additional discussion, like centralised vs decentralised, commercial vs open-source platform, how to involve the private sector, questions of cross-border data exchange, how to avoid creating a single point of failure, centralisation vs decentralisation of e-service orchestration and choreography, payment of data use, to mention but a few. Issues in need of attention are highlighted in this Report and recommendations made.