

Common Technical Architecture Framework for Myanmar's eGovernment Interoperability in ASEAN Perspectives

Tun Tun Aung
Lecturer, Assumption University
tuntunaung@au.edu

Abstract

This paper proposes the common technical architecture framework for eGovernment Interoperability for Myanmar. It also recommends the interaction type/e-Government workflows in common for general e-government services and proposes the recommended data model, security model and network model for general e-government services. Many nations in ASEAN region are increasingly improving government services being given to citizens and businesses, accompanying increased economic globalization. Governments are trying to exploit information and communication technologies (ICT) to improve several public services with better quality, faster provision and accessibility of services. To enhance development of Myanmar eGovernment services in line with the unity development of ASEAN eGovernment services, Myanmar e-Government services development should adopt compatible mutual interoperability criteria. In this respect, the Common Technical Architecture Framework for E-Government Interoperability for Myanmar is necessary to be drafted in order to strive for meeting these demands.

1. Introduction

Interoperability is the ability of information and communication technology (ICT) systems used in

work processes for data exchange and the sharing of information and knowledge. A set of standards and guidelines will be defined in an interoperability framework to suggest how organizations make agreements with other different organizations for interaction with each other. In this respect, developing an interoperability framework has to go through periodic revision and adaption due to rapid changing technologies and standards and administrative requirements. The drafted interoperability framework in this paper consists of the core work procedures, data model, network model, and security model.

2. Interaction Type Related eGovernment Workflow in ASEAN Context

The interaction types between all related entities can be classified into 3 interaction types for the transactions within national boundaries and transactions related to the cross border activities as shown in the figure 1.

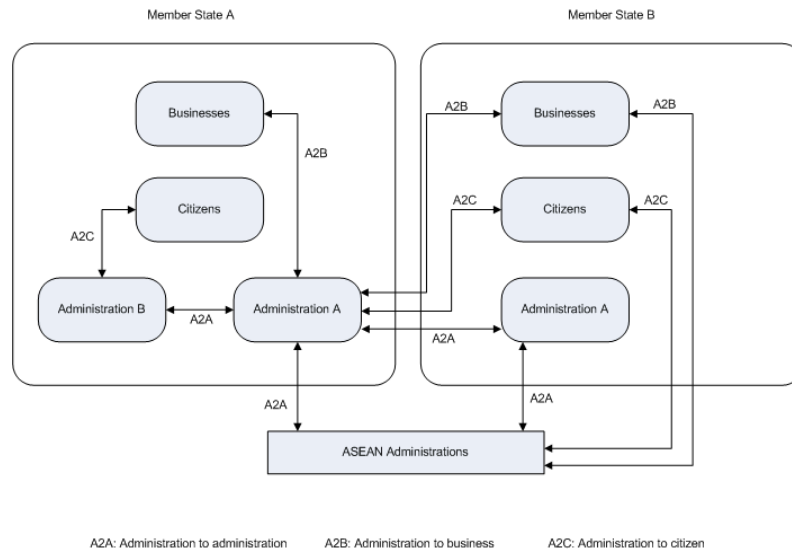


Figure 1. Overall Interaction Type

2.1 Citizen/Business to Administration

It is the interaction between citizens/business enterprises and government administrations in Myanmar. It can be applied for an exchange of data between citizens or business enterprises of Myanmar with administrations of other ASEAN member states and/or ASEAN institutions.

2.2 Administration to Administration

It is the data exchange between the administrations of Myanmar and the administrations of other ASEAN member states.

2.3 ASEAN Institutions to ASEAN Institutions and Administration to ASEAN Institutions

It is the data exchange between various ASEAN institutions or ASEAN institutions and administrations of ASEAN member states.

Table 1. List of Protocols for Data Model

Protocols			
Protocol/services with Legacy System	Middleware	Value Added Services	Network
EDI-based standards	Data integration and middleware	File and message transfer protocols	Distributed Application Arc
	XML-based standards	Message store services	Interconnection Services
	Web Services	Mailbox access	Message transport and security
	Directory and domain name services		Network services

International standard references are required for the data and information exchange format. Public administrations should be careful in perspective of independency by avoiding imposing specific technologies or products which may create constraints in future development. The following standards are necessary for data and information exchange formats which enhance interoperability:

3. Data Model

The following sets of protocols should be considered for the data model:

To establish e-Government services with the data interoperability at semantic and technical level, a mutual agreement such as vocabularies, schemas, exchange file formats, document templates, requisite ASEAN common e-forms, should be made in order to facilitate data and information harmonization.

- Exchanging and/or integrating business processes
 - BPMN 2.0 – Business Process Modeling Notation
- Exchanging Images and Multimedia
 - JPEG 2000 – Lossy Compression
 - PNG ISO/IEC 15948 – Lossless Compression
 - ODF – Document Type for Editable Document with Formatting, Presentation and Spreadsheet

- PDF v1.7 ISO32000-1 – Non-Editable Document
- PDF/A ISO19005-1 – Scanned Document
- OGG Vorbis – Audio Compression Format
- OGG Theora – Video Compression Format
- Media Streaming – .wmv, rm, mp4
- Animation - .swf, .avi, .mov
- XFORMS with XHTML – E-Forms
- MS Office 2010 - Microsoft Office Format for Editable Document (.docx), Presentation (.pptx) and Spreadsheet (.xlsx)
- CSV – Comma Separated Variable / Delimited File Format (.csv)
- Zip – Compressed file Format
- XML v1.0 – Default Document/ Message Formatting Language
- XML Schema v1.0 – Default Schema Definition
- XSL v1.0 – Default Data Transformation and Vocabulary for Specify formatting schema
- Xpath v2.0 – Content searching and navigation in an XML document
- SQL ISO/IEC 9075 – Relational Database Query Language
- WML v2.0 – Mobile Devices Markup Language
- UTF-8 – Minimum Interoperable Character Set ISO/IEC 10646-1
- ISO/IEC 1179: Information Technology – Metadata Registries (MDR)
- CSS 2 – Style Sheets
- XSL 2.0 – Extensible Style Sheets

4. Network Model

Computer network systems are necessary in the first place for interconnectivity.

Interconnection is the communication linkage set up among several agencies using network model.

Most common channel to delivering e-Government services to citizens and businesses is to set up a common portal in front of the entire set of applications. In addition, as the mobile devices such as smart phones, tablet computer becomes significant, mobile application of portal handles should support for a multitude of services involving provision or collection of data to and from the user and

government. Specific middleware component connection is required for the support of portal and application communication. Network and Computer System for interoperability should have a mutual compliance for mature communication.

The Network and Computer Systems require international standard references. Public administration should be careful in perspective of independency by avoiding imposing specific technologies or products which may create constraints in future development. The following standards are recommended for network and computer systems enhance interoperability:

- Layer Model

Table 2. Seven Layers Model

Open System Interconnection (OSI) Model ISO/IEC 7498-1			
	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption and decryption, convert machine dependent data to machine independent data
		5. Session	Interhost communication, managing sessions between applications
	Segments	4. Transport	End-to-end connections, reliability and flow control
Media layers	Packet/ Datagram	3. Network	Path determination and logical addressing
	Frame	2. Data link	Physical addressing
	Bit	1. Physical	Media, signal and binary transmission

- Networks
 - SSL v3.0 128bit – Secure Socket Layer
 - IPv4 – 32 bit Internet Protocol
 - IPv6 – 128 bit Internet Protocol
 - TCP – Transmission Control Protocol
 - UDP – User Datagram Protocol
 - TLS 1.2 – Transport Layer Security
 - LAN/WAN – IEEE 802.3
 - IEEE 802.11 – Wireless LAN Security Implementation
 - WAP v2.0
- Mail

- SMTP/MIME – Simple Mail Transport Protocol/ Multipurpose Internet Mail Extensions – Secure Electronic Mail
- POP3 – Server/Client Protocol permit a workstation to dynamically access a mail held on server – Mail Box Access
- Directory
 - LDAP v3 – Provide access to X.500 or other directories
- File Transfer
 - HTTP – Hypertext Transfer
 - HTTPS – Hypertext Transfer Protocol over Secure Socket Layer
 - SFTP – Secure File Transfer Protocol
 - SIP2
 - OAI-PMH
 - DES ANSI X3.92 and 3.106 (FIPS 46-3 and 81) – Data Encryption Standard
 - 3DES ANSI X9.52 (FIPS46-3): Triple Data Encryption
- Web Service
 - WSMML – Web Service Modeling Language
 - DNS – Domain Name Services
 - SOAP v2.0 – Web Service Request Delivery
 - WSDL v3.0 – Web Services Description Language
 - UDDI v3 – Web Registry
 - NNTP – Network News Transfer Protocol
 - HTML 5 – Hypertext Web Content
- Application
 - FTAM – File Transfer and Access Management Protocol
 - Z39.50 – Information Retrieval: Application Service Definition and Protocol Specification

5. Security Model

The e-Government public service contains all official entities' exchanged data and information, so it is necessary to be secured, managed, monitored, controlled and harmonized, allowing secure access and exchange between administrations, businesses,

and citizens to enhance trustworthiness in order to create sustainability and integrity to the ASEAN community. The classification of users can be specified as follows:

- Individual – An individual can access data or services on his own behalf.
- Agent – An agent is an individual or organization that can access data or services on behalf of another individual/s or organization/s provided that consent is granted to the agent by the data subject (an individual or organization).
- Organization Representative – An organizational representative is an individual who can access data or services on behalf of an organization/s provided that consent is granted to the data subject (representative by the organization).

The security model(s) will make sure that confidentiality, availability, integrity, authenticity, and non-repudiation of information traversing the framework is maintained and consistent with its classification/sensitivity. This should be in accordance with government policies/requirements. The security model(s) for interoperability in authentication, authorization, and accounting should be recommended and considered with standard references as follows:

Authentication – Transaction Transport Security required preventing stolen, misused, modified, or denied (non-repudiation). Security authentication will be used to correctly authenticate user and effectively encrypt the data transfer over public network. For secure authentication, the following standards and protocols should be considered as a minimum:

- CA (Certificate of Authentication)
- PKI X.509 digital certification
- Secure Socket Layer (SSL)
- Internet Protocol Security (IPsec)
- Username Token Profile (UTP)
- SAML – Wireless LAN Authentication
- DSA (FIPS 186-3) – Digital Signature Algorithms
- XML Signature – XML message signing

Authorization – Accessibility through all transaction activities should define the level of permit access and activities, limit authorization which enable

access allowance from various channels which additionally offer flexible support on handicap facilitation, multilingualism, or assistive technology. Assurance of authentication shall match the level of risk associated over transaction. The following lists are recommended as concerned subjects in application development:

- Multiple Channel Access
- Collective Authoring
- Interface for Accessibility
- Level of Data Presentation and Exchange
- Level of Authorization
 - Government Agency
 - o Approval
 - o Verify
 - o Record
 - o Review
 - o Evaluate
 - o Track
 - Business
 - o Submission
 - o Clarify
 - o Report
 - o Certified
 - o Track Progress
 - Individual
 - o Submission
 - o Certified
 - o Track Progress.

Accounting – All accessing activities shall be monitored, controlled, managed and logged with identifiers to prevent jeopardization and misappropriation of e-Government resources.

6. Recommendations

6.1 Data Interoperability

For each e-Government service, the data elements should be interoperable as agreed semantic criteria. The following requisites are recommended to be complied with:

- The responsible administrations should establish the proposal on data model including data elements and prior data dictionaries development at national and ASEAN level. This should be performed on mutual data and data elements required by e-

Government core service activities. The agreed data elements should be defined.

- For the agreed ASEAN data elements, all responsible administrations should establish a multilateral mapping table between national and ASEAN data element.
- Every concerned administration need to publish information on detailed data elements as part of requirements for a use of service to be offered at national level.

Common semantics on the XML basis performed should be complied with and correspond to existing international standards. In particular, the following elements should be complied with ASEAN common infrastructure:

- Mutual agreed core/specific of the XML vocabularies used for e-Government data elements,
- Mutual agreed specific ASEAN schemas and Definition,
- Mutual agreed standard of data, file type, file compression and document format.

For the content, forms, instruction, and communication ability to support users in all levels, the following aspects of multilingualism should be considered:

- Minimum of 2 Languages Support (Myanmar and English)
- Translation Middleware

6.2 Network Interoperability

At the national level, all concerning public administrations' agreement should be made on a mutual scheme to loosely-coupled components when establishing Public Services Infrastructures.

Public administrations should favor openness for integration while taking into account their priorities and constraints. Specific technological solution should not be imposed.

For interconnectivity solutions development, Myanmar public administrations should consider multi-layers supported Bilateral Solutions and Multilateral Solutions when establishing ASEAN Public Services Infrastructure.

At the back-office level, interconnectivity solutions for technical interoperability should consider the following fields:

- Layer Model
- Network Protocol
- Mail and Communication channel/access
- Directory
- File Transfer
- Web-Services (Lightweight client software of internet standards (Web Browser))
- Application

For applicable Internet Protocol (IP) development consideration aspect, the following perspectives should be taken into consideration:

- All IPv4 must be gradually migrated to IPv6 maintaining coexistence with IPv4.
- New procurement required to support coexistence of IPv4 and IPv6 networks
- Cost effective procurement must consider Dual IPv4 and IPv6.
- Infrastructure Architecture

The following security aspects should be taken into consideration for all layers;

- Security Services
- Public Key Infrastructure (PKI)
- Web Service Security
- Firewall
- Protection against viruses, worms, Trojan horses, e-mail bombs, phishing

6.3 Security Interoperability

Public administrations should develop a long-term preservation policy for electronic records for public eGovernment services at both national level and ASEAN level.

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

- Service Management – to make sure oversight of all communication activities in regards to data transport, identification, authentication, and authorization, etc., including e.g. access right grant, revocation, and audit.

- Service Registry – to grant authorization, access right to services offered through localization and verification.
- Service Logging – to make sure that it adequately functions data exchange logging for future evidences including archive.

Public administrations need to make agreement on common security and privacy policy for a public service to be offered to both citizen and business.

6. Conclusions

Development of interoperability architecture needs long-term planning and communication among concerning administrations. Detailed considerations on possible impact on all business transaction between the systems to be integrated, is utmost necessary. Standardization and interchangeability of processes require different authorities' supports and efforts. Public administrations in Myanmar need to collaborate with eGovernment agencies and administrations from other ASEAN Member States and ASEAN eGovernment Institutions to be part of AEC network by which necessary eGovernment services can be provided to not only Myanmar citizens/businesses but also citizens/businesses of other ASEAN member states.

References

- [1] EUROPEAN INTEROPERABILITY FRAMEWORKS FOR PAN-EUROPEAN EGOVERNMENT SERVICES, IDABC Version 1.0.
- [2] Information Economy Report 2007-2008, Science and Technology for development: the new paradigm of ICT, UNCTAD.