YEFI – Yesser Framework For Interoperability

Kingdom of Saudi Arabia

Riyadh, October 28, 2005

INTEROPERABILITY FRAMEWORK

Interoperability framework definition

- Set of policies to be adopted by government institutions that standardise the way the information is being exchanged and shared services are being used
- Interoperability framework will define
  - Data types and schemas
  - Metadata element and dictionaries
  - Technical policies, e.g.,
    - Integration approach and standards
    - Connectivity standards
    - Security standards
    - Information access and delivery standards

Interoperability framework importance

- If adopted, interoperability framework will decrease the effort (time and cost) required for developing the electronic exchange of information between government institutions, required for successful e-government implementation
- Shared, broadly adopted standards are the key in ‘decentralised coordinated’ approach, as proposed in National Action Plan

DOCUMENT CONTENT

Yesser Framework for Interoperability (YEFI) scope and general policies

YEFI components

YEFI development roadmap

Appendix - Proposed technical standards

SCOPE OF THE FRAMEWORK

The interoperability framework covers the exchange of information and the interactions between

- Saudi Arabian government and citizens
- Saudi Arabian government and foreign workers/expats with work permit
- Saudi Arabian government and business within and outside Saudi Arabia
- Organization/ministries/institutes of the Saudi Arabian government
- Saudi Arabian government to other governments (in the future)

GENERAL POLICIES

Key general policies decided

- **Alignment with the internet –** the universal adoption of common specifications used on the internet and world wide web for all information systems
- **Browser as the key user interface –** all information are to be accessible through browser-based technology; other user interfaces are permitted but only in addition to browser-based ones

The selection of the technical policy should be driven by

- **Interoperability –** only specifications that are relevant to systems interconnectivity, data integration and service access are specified
- **Market support –** the specifications selected are widely supported by the market in order to reduce cost and risk of the government systems
- **Scalability –** the specifications selected have the capacity to be scaled to satisfy changed demands made on the systems (e.g., data volume, number of transactions, number of users)
- **Openness –** the specifications are documented and available to the public
- **International standards –** preference will be given to standards with the broadest remit

DOCUMENT CONTENT

MAIN COMPONENTS FOR YEFI

	Elements	Explanation
A **Data standards**	• Data standards catalogue • Data schemas	• Defines data standards on business and logical level • Defines how data is exchanged between the systems
B **Metadata standards**	• Metadata standards • Metadata dictionaries	• Defines attributes to be used to ‘tag’ electronic document • Defines dictionaries for this attributes
C **Technical standards**	• Connectivity and networking standard • Integration standard • Security standards	• Sets all technical standards and policies to ensure interoperability on a technical level

Ⓐ THE COMMON PART OF THE DATA ACROSS GOVERNMENT INSTITUTIONS NEED TO BE STANDARDIZED

- The data schema of the same business object is different across ministries
- This is a major hurdle for interconnectivity as the diversity directly impacts the effort (cost and time) to establish intersystem connections
- In order to avoid that, the common parts of the different schemas should be standardized for all system interfaces for inter-ministry connectivity
- Moreover metadata should be introduced as part of the schema and schema versions should be recorded in a repository in order to achieve consistency under changing schemas
- A framework/process is proposed to achieve the appropriate standards

Ⓐ THE SCHEMA OF THE SAME BUSINESS OBJECT IS DIFFERENT ACROSS MINISTRIES

EXAMPLE

Example: The schema of a citizen across different ministries

	Ministry of Health		Ministry of Education		Ministry of Interior		Ministry of Labour	
	Attribute name	**Attribute type/format**	**Attribute name**	**Attribute type/format**	**Attribute name**	**Attribute type/format**	**Attribute name**	**Attribute type/format**
Specific additional attributes	• Disabled	Yes/no	• Profession	String	• Previously convicted	Yes/No	Job seeker	Yes/no
	• Level of disable-ment	Byte	• Academic degree	List	• Driver licence ID	Integer	Begin un-employment	mm.yy
Common part of the schemas	• Address	String (64)	• Home address	Address	• Address	String (128)	• Private address	String (64)
	• ID number	Integer	• Social ID	Integer	• ID	Integer	•Social ID	Double integer
	• Place of birth	String (16)	• –	–	• Place of birth	String	• Place of birth	String (16)
	• Date of birth	dd.mm.yyyy	• Date of birth	dd.mm.yy	• Date of birth	Mm/dd/yy	• Date of birth	dd.mm.yy
	• Last name	String (16)	• Last name	String (32)	• Surname	String (32)	• Title	List
	• First name	String (16)	• First name	String (32)	• Name	String (32)	• Name	String (64)

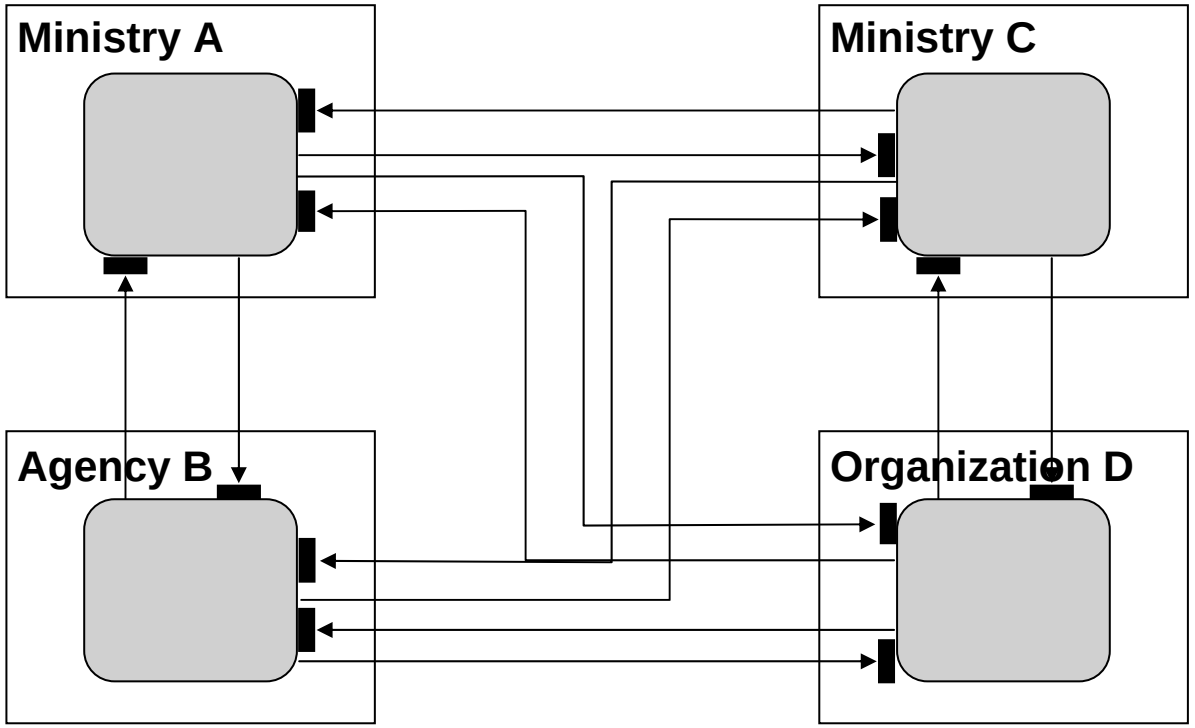
The common attributes have different names and types across ministries

Ⓐ WITHOUT STANDARD THE INTERCONNECTIVITY EFFORT SCALES NON-LINEAR WITH THE NUMBER OF INSTITUTIONS

Institution
Business object "citizen"
Adapter
Interface

- The common part of the business object schema differs across ministries
  - Attributes with same meaning have different name
  - Attributes with same meaning have different types
- Each interface of this business object requires an individual adaptor for each ministry in order to convert names and types of the attributes

The number of adaptors for the same business object scales non-linear* with the number of ministries



* N x (N -1) adapters are needed in this example, if N is the number of ministries

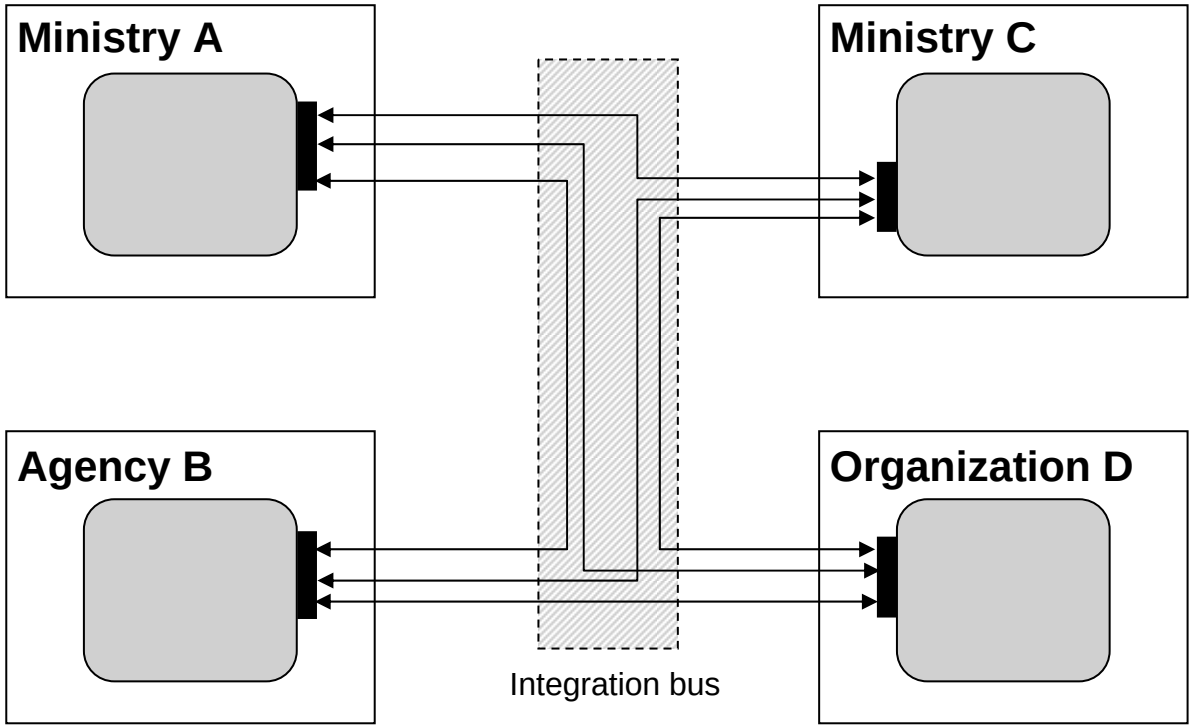
Source: Source

Ⓐ BY STANDARDIZATION THE INTERCONNECTIVITY EFFORT SCALES ONLY LINEARLY WITH THE NUMBER OF INSTITUTIONS

Institution
Business object "citizen"
Adapter
Interface

The number of adaptors scales only linear in case of standardization and encapsulation

- A facade adaptor enables standardized interconnectivity through encapsulation
- There is only one facade adaptor per business object for each ministry needed for all in- and outbound calls



- A standardization effort is needed for the common part of all shared business object across government institution in order to significantly reduce the interconnectivity effort
- This standardization effort should be done as part of the interface specification for the integration bus

* N adapters are needed in this example, if N is the number of ministries

Source: YESSER

Ⓐ THE FIRST STEP TO DATA STANDARDIZATION IS CREATION OF A GOVERNMENT DATA CATALOG

Government Data Catalogue:

- Is a key element in developing schemas for business **objects being exchanged**, but also can be used by government institutions to set up the **standards to store the data**
- Defines the standard for data on **logical level**, but not on the physical storage or display levels

Data Catalogue content:
Each data element described in catalogue should be defined through:

- **Name** of data element
- Business **definition**
- **Format** i.e., sequence and meaning of alpha/ digit characters
- **Validation** rules
- **Verification** – business steps required to verify data element
- **XML Schema ID** – references to schema (or schemas) where data element is used
- **Values** list of acceptable values (e.g., male, female)
- **Default value** (if any)
- **Owner** of the standard
- **Version**
- **Acceptance date**

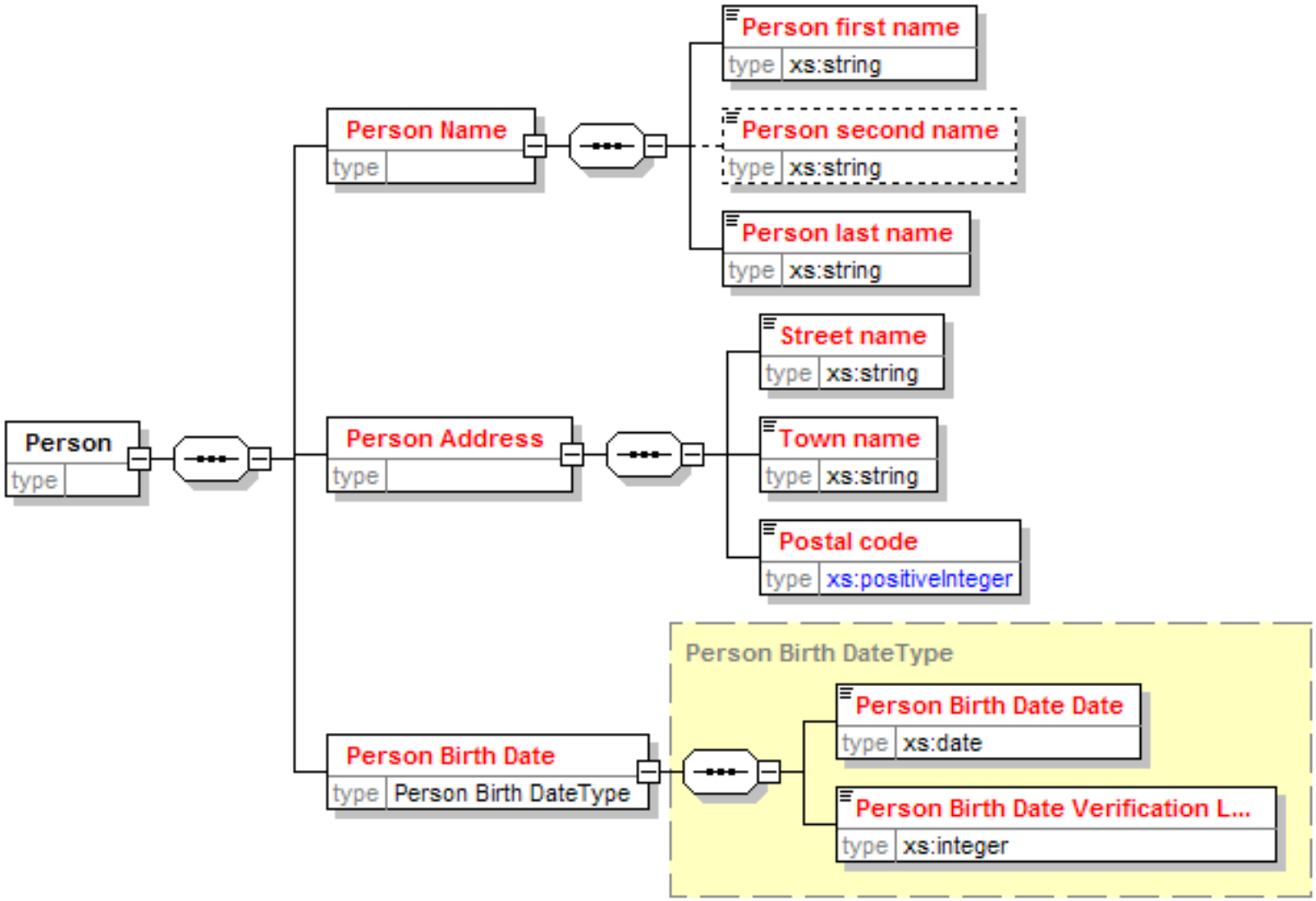
Source: UK eGIF

Ⓐ EXAMPLE FOR GOVERNMENT DATA CATALOG ENTRY

Attribute	Value
Name	Person Birth Date
Business definition	The date on which a person was born or is officially have been deemed to have been born
Format	1. See *Date* definition
Validation	1. See *Date* definition 2. Date must not be in the future. 3. Date must not be later than Person Death Date where held.
Verification	Level 0: no verification Level 1: verified with one of following documents: passport, national id, driver license
XML Schema IDs	Person Information v. 1.0
Values	N/A
Default value	N/A
Owner	eGovernment Unit
Version	1.0
Acceptance date	2006-01-01

Source: UK eGIF

Ⓐ DATA SCHEMA CONSIST OF DATA ELEMENTS OF TYPES DEFINED IN DATA CATALOG



Source: UK eGIF

Ⓐ DATA CONSISTENCY REQUIRES META DATA AS PART OF THE OBJECT DATA SCHEMA AND A CENTRAL SCHEMA REPOSITORY

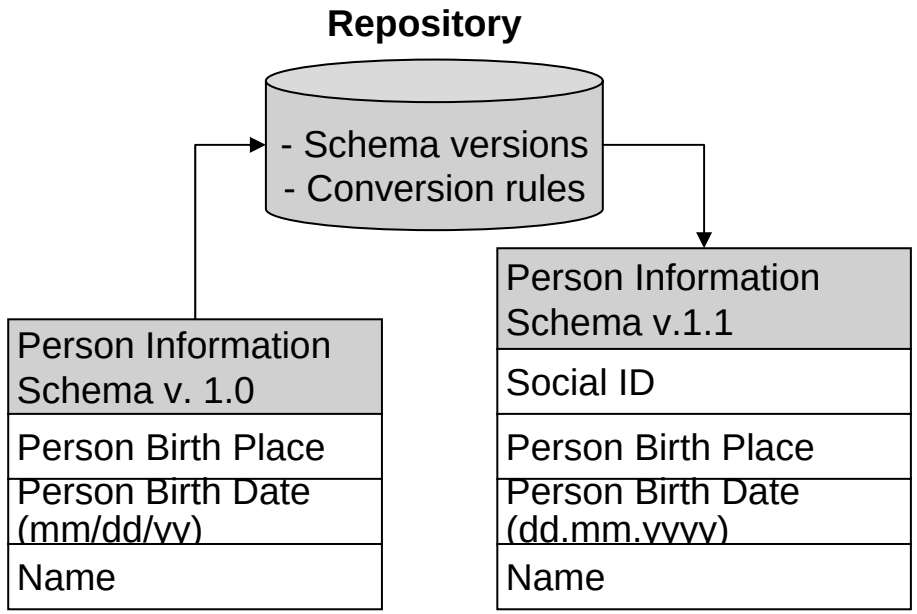
The standardized schema consists of header and data body

Example: Attributes of the business object “Person”

Business object created	meta data are part of the header
Business object updated	
Owner	
Data schema ID	
Global unique object ID	
Person Birth Place	Business data are part of the body
Person Birth Date	
Person First Name	
Person Last Name	

A central repository for the standardized schemas is required to handle persistent data of outdated schemas

Schemas will evolve over time. Hence there will be persistent business objects of outdated schemas. In order to convert this object into the latest schema, the latest schema and conversion rules needs to be retrieved from a repository



Business object with outdated schema

Business object converted to the latest schema

Ⓐ A STANDARDIZATION PROCESS NEEDS TO BE ESTABLISHED AS PART OF THE INTEROPERABILITY EFFORT

	Identify shared business objects	**Develop standard for common attributes**	**Sign-off standard by the government institutions**
Activities	• Identify shared business objects • Identify list of government institutions using the business object	• Identify common attributes of the business object schema • Develop standard catalogue entries for the common attributes of the schema • Assign ownership to a institution • Send request for standardization to all government institutions	• Sign-off standard by the government institutions as part of the activities of the interoperability committee • Take necessary actions to implement the standard and to avoid a potential bypass of the standard
Deliverables	• Matrix of shared business objects	• Standardization request	• Sign-off • Action plan

Source: YESSER

Ⓑ METADATA STANDARDS

What is metadata?	**"Data about data"**
Where it is important?	**Content management** – describe the content of documents
Why this is important	• Allow for easy access to information and documents (e.g., searching, browsing by category) being published by different government institutions
What are typical metadata elements?	• Typically describe goal, origin, content and history of document, e.g., *Addressee*, *Creator, Contributor, Date issued, Description, Format, Identifier, Language, Publisher, Copyright, Source/URL, Status, Subject, Title, Type* • Often based on Dublin Core standard

Ⓑ CONTENT MANAGEMENT METADATA IN THE EXAMPLE

Metadata	Information
Addressee	Member of YEFI coordinating committee
Creator	Dr. Ricco Deutscher
Contributor	Ali Saleh Al Soma, Marcin Warszewski
Date issued	28 October 2005
Description	Outlines the Interoperability framework to be established in the e-Government of the Kingdom of Saudi Arabia
Format	Powerpoint
Identifier*	LOX-MCB001-20051029-PSMW-P1
Language	English
Publisher	<not published>
Copyright	Reserved to the Yesser Group, Kingdom of Saudi Arabia
Source/URL	<not available>
Status	Version 1.0
Subject	Interoperability
Title	e-Government Interoperability Framework
Type	Standard

This metadata should be part of each documentation which is made available publicly or exchanged between government agencies

* Persistent identifiers shall conform to the ANSI/NISO Z39.84 standard http://www.niso.org/

Ⓒ TECHNICAL POLICIES WILL CONSIST OF 3 SUBSECTIONS

Technical subsections	Description
Integration	• It specifies the integration approach, middleware technologies and standards necessary to integrate the different applications in the different ministries
Interconnection	• It specifies network and transport protocols should be used for information exchange, access, and delivery
Security	• It specifies the security approaches, technologies, and standards in the different e-government services

Ⓒ IN ADDITION TO THE INTEGRATION STANDARDS A SYSTEM INTEGRATION STRATEGY NEEDS TO BE OUTLINED

Key elements of an integration strategy	Description
Integration approach	• The integration approach outlines two things along the different phase, – The topology, e.g. point-to-point, hub-and spoke and bus – The architecture layer of integration, e.g. data, application layer
Specification of technology standards	• Specification of all technical standards relevant to the integration (see Appendix proposed technical standards)
Specification of semantics	• **Application integration:** All interfaces/services to be interconnected should be listed, specified and described in order to achieve consistency and high reuse* • **Data integration:** All major business objects/data to be transmitted between systems across organization should be specified in order to achieve consistency**

* This should be part of the future application architecture

** The specification and description of the business data should comply to metadata standards

DOCUMENT CONTENT

Yesser Framework for Interoperability (YEFI) scope and general policies

YEFI components

YEFI development roadmap

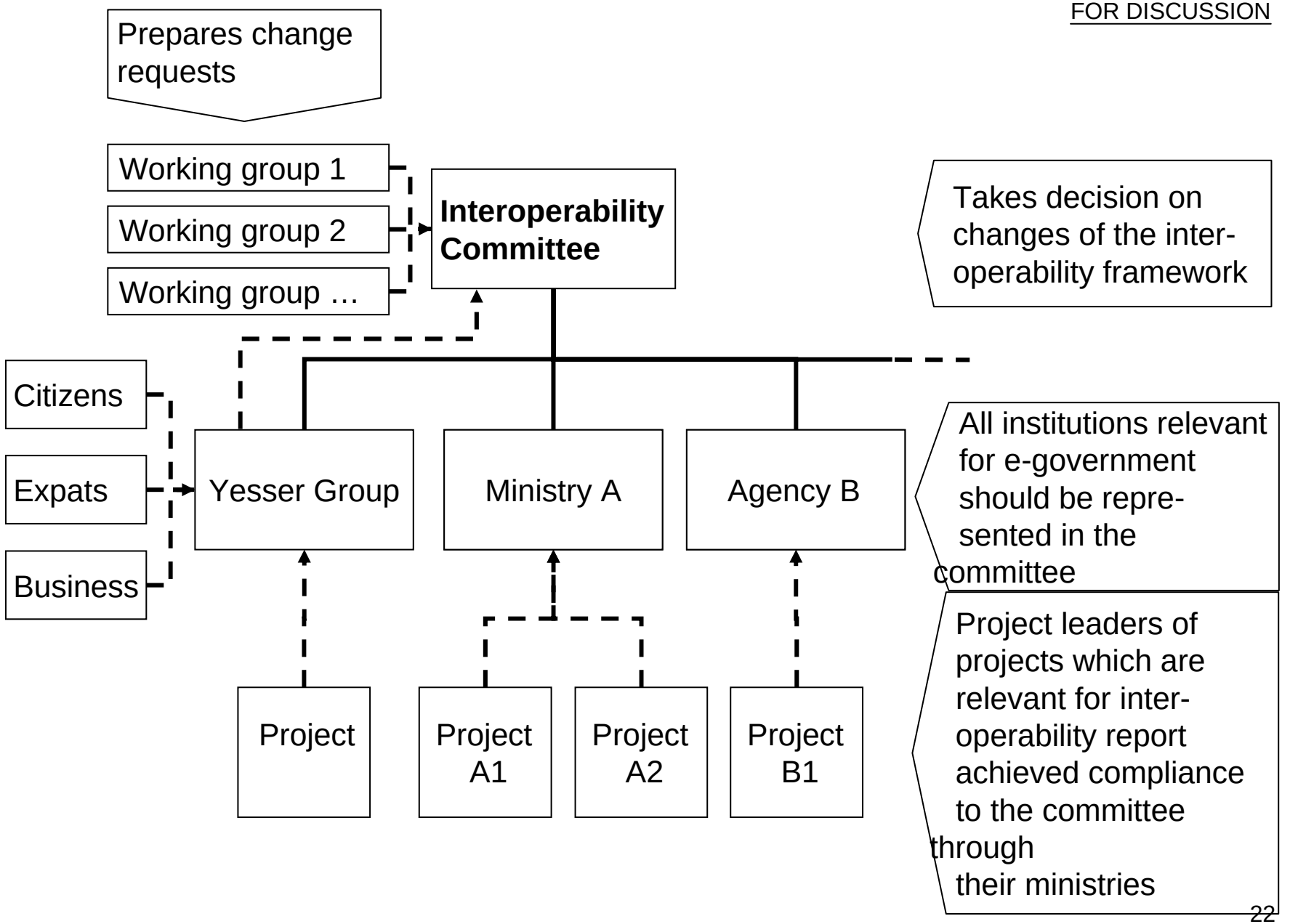
Appendix - Proposed technical standards

TWO MAIN WORKSTREAMS TO BE LAUNCHED

	The goal of workstream	Next steps
Data and metadata standards	• Develop and agree on definition of types and structures of common/shared data to be exchanged between government institutions • Develop and agree on set of metadata tags (and relevant dictionaries) to be used to categorise electronic document	• Launch working group ('Data group') with the goal to: – Identify common/shared business objects (e.g., citizen, company) – Identify object's attributes and agree on their definitions – Develop XML Schemas to define structures in which data is being exchanged • Launch working group ('Metadata group') to work on tags definition and dictionaries
Technical standards	• Define and agree on key technical standards (like integration, connectivity, security)	• Launch technical standards working group (with relevant sub groups, e.g., security sub group) to work on technical standards definition

ORGANIZATIONAL STRUCTURE OF THE INTEROPERABILITY Committee

FOR DISCUSSION



FOR DISCUSSION

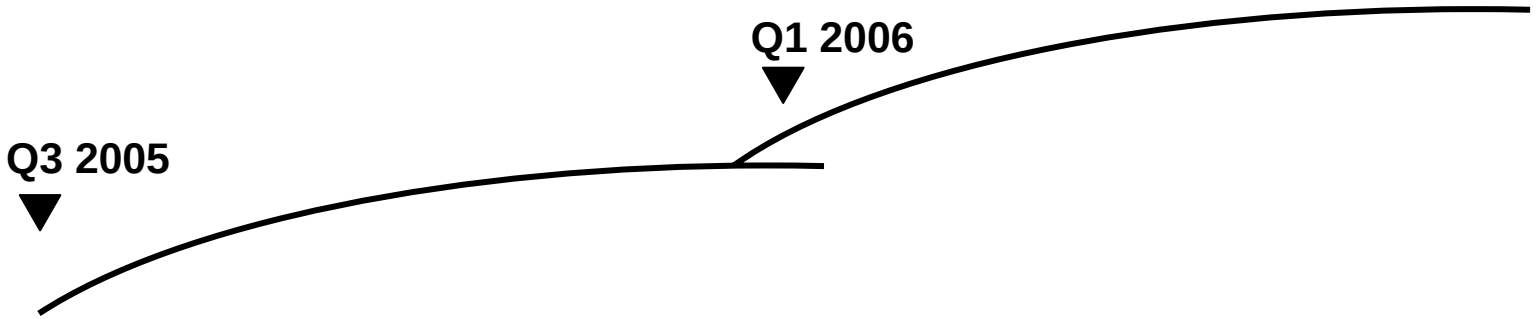
THE MANAGEMENT PROCESS ENSURES THAT THE FRAMEWORK REMAINS UP TO DATE

Lifecycle of the interoperability standards

	Requirement management	Decision on changes to the standards	Roadmap and compliance
Activities	• Review changes in the international interoperability standards • Collect/analyze feedback from all relevant stakeholders	• A change request will be sent to all other committee members • Decide changes to the standards according to the new requirements • Disseminate the new standards/decisions	• Specify and agree on a roadmap for implementation of the standards • Review compliance of the implementation projects
Deliverables	• Requirement catalogue including change requests	• Updated standards and policies	• Mutual agreed roadmap • Compliance reports of individual projects
Responsible	• Working group of the interoperability committee	• Interoperability committee	• Working group of the interoperability committee

THE ORGANIZATIONAL STRUCTURE SHOULD GROW OVER TIME

FOR DISCUSSION



Focus	• Specifications of the most important and urgent parts of the framework and standards	• Further refinement within the sections of the framework
Organization	• 1 working group for all topics	• 6 working group – 1 for the overall framework – 1 for each of the 5 technical area
Working mode	• Biweekly meeting of the working group • Monthly meeting of the interoperability committee	• Monthly meetings for the individual working groups • Quarterly meeting of the interoperability committee

DOCUMENT CONTENT

Yesser Framework for Interoperability (YEFI) scope and general policies

YEFI components

YEFI development roadmap

Appendix - Proposed technical standards

GUIDING PRINCIPLES FOR THE SPECIFICATION OF THE FIRST VERSION OF THE TECHNICAL STANDARDS

Guiding principles

- Outdated available standards should not be considered
- All available standards which are not outdated and in operations should be considered, e.g. Microsoft .NET, however gradual migration to a narrower set of preferred standards should be started
- All state-of-the-art standards should be considered even if they are currently not in operations, e.g. JAR, WML
- Technology areas which do not have standards yet and are not in use should not yet have standard policies, e.g. metadata management technology
- Localized standards should be taken into consideration, e.g. AR8MSWIN 1256

Source: YESSER survey

INTEGRATION TECHNOLOGY STANDARDS

Bold - preferred standard

Middleware technologies

- Microsoft .NET
- IBM MQService
- BEA Tuxedo
- Java RMI
- **Web services**
- Java J2EE

Character sets

- ASCII
- ISO 8859-1/Latin1
- Unicode
  - UTF-8
  - **UTF-16**
- AR8MSWIN 1256

WebService/ XML Technologies

- Data structure: **XML**
- Data format: **XSL**
- Data schema:
  - DTD
  - **XML Schema**

Resource description framework

- **RDF**

Source: YESSER survey

CONTENT FORMATS

Web content formats	Document formats	Image formats	Audio formats	Video formats	Compression technologies	Mobile device content formats
• HTML	• **DOC**	• TIF	• WAV	• DivX	• ZIP	• WML
• DHTML	• RTF	• GIF	• MP3	• MPEG	• CAB	
• **XHTML**	• TXT	• JPEG/JPG	• Real audio/RA	• AVI	• RAR	
• Flash	• PPT	• Bitmap/BMP	• AAC	• QuickTime	• JAR	
	• XSL		• MPEG-4	• MMS/gp3		
	• **PDF**		• MIDI	• WMV		
	• MMP					

Source: YESSER survey

INTERCONNECTION STANDARDS

Email outbound	Email inbound	Other transport protocols	Directory protocols	Network protocols/ services	File transfer protocol	Mobile device network protocol	WLAN network protocols
• SMTP	• POP3 • IMAP	• http • SOAP • Telnet • FTP • RTP	• LDAP • Microsoft Active Directory Service	• **TCP/IP** • IPX/SPX • HSRP • Frame Relay • ATM • OSPF • RIP • EIGRP • IGRP • BGP • IS-IS • SONET • X.25 • DNS	• FTP • TFTP	• WAP • GPRS • UMTS • CDMA • GSM • WLL • TDMA	• IEEE 802.11b • IEEE 802.11a • IEEE 802.11g

Source: YESSER survey

SECURITY STANDARDS

Email security	Transport protocol	Network protocol	Encryption algorithm, digital signature
• S/MIME	• SSL	• IPSec	• RSA
• PGP	• TLS		• DSA
• PKI			• DES
• SMM			• 3DES

Source: YESSER survey