

HANDBOOK ON MINIMUM INFORMATION INTEROPERABILITY STANDARDS  
(MIOS)



\*

A BLUEPRINT TO GUIDE SEAMLESSNESS AND INTEROPERABILITY IN PUBLIC  
SERVICE AS PRESENTED BY THE DEPARTMENT OF PUBLIC SERVICE AND  
ADMINISTRATION

---

\* As adopted based on the United Kingdom Minimum Information Interoperability Standards in line with international trends and best practice

## PART 1: Technical Policies and Standards

Version 3

### Document History

Document Name	Revision Authority	Update	Revision Date
e-Gif		Adopted from UK Gov	July 2001
MIOS v1	SITA services Certification	Customised for RSA government	Sep 2001
MIOS v2	GITO Council MIOS workshop	Input from GITO Council	Nov 2001
MIOS3 16 April 2002.doc	SITA services Certification	Split MIOS into two Parts: Part 1 is Technical Policies and Standards  Part 2 is Implementation Support	April 2002

## Foreword

Information systems have the potential to transform Government and the services it provides to the public. But without consistent policies and standards to underpin those systems it will not be possible to work together to deliver collaborative services.

This policy discussion document suggests the technical standards and policies that will act as the foundation of our e-Government strategy. These standards will allow information to flow seamlessly across the public sector and will provide citizens and businesses with better access to government services. In addition, by adopting Internet and World Wide Web standards, the Framework aligns government with the rest of industry and serves as a basis for reducing the costs and risks associated with carrying out major IT projects.

We are aware that the electronic world is changing rapidly but thanks to foresight, continuous research and development that informs our Internet based change management process, we intend not only to keep pace with this change, but where necessary, to lead in the adoption of innovative market leading solutions. This is also why we will be publishing a series of handbooks, CD Roms, newsletters and online discussion forums in order to keep abreast with the very latest public sector standards and comment on these, and also provide us with innovative proposals for solving some of our generic IT problems.

Next to security and the availing of information infrastructure, the Interoperability Framework, as a cornerstone of the e-government strategy, will enable us to address the challenges of today's diverse systems and position ourselves for new opportunities in the future.

This document reflects our promise to stay ahead in the fast moving world of e-business, by reflecting new technologies and market developments. We intend to continue to update the framework, following continuous consultation, and to make it, and supplementary advice and guidance, available on the [www.dpsa.gov.za](http://www.dpsa.gov.za) website

## Tables of Components and Standards

Tables of Components and Standards .....	4
1 Overview.....	7
Introduction .....	7
Forecast Changes for future Versions .....	7
Scope .....	7
Main features.....	8
Policies and standards.....	8
Implementation support.....	9
Management processes .....	9
Relationships with other initiatives .....	<b>Error! Bookmark not defined.</b>
Security Framework .....	<b>Error! Bookmark not defined.</b>
Electronic service delivery.....	<b>Error! Bookmark not defined.</b>
Portals .....	<b>Error! Bookmark not defined.</b>
Metadata Framework .....	<b>Error! Bookmark not defined.</b>
Metadata Standard .....	<b>Error! Bookmark not defined.</b>
Government Information Technology Architecture(GITA) Framework....	<b>Error! Bookmark not defined.</b>
Your involvement .....	<b>Error! Bookmark not defined.</b>
2 Policies and Technical Standards .....	10
Introduction .....	10
Key decisions and drivers .....	10
Interconnection policies.....	11
Policy for Networks .....	11
Policy for Security .....	11
Policy for e-Mail.....	11
Policy for Directory .....	11
Policy for Domain Naming.....	11
Policy for File Transfer Protocol (FTP).....	11
Policy for Terminal Emulation .....	11
Interconnection standards and specifications.....	12
Table 1 Standards and specification for interconnectivity .....	12
Data Interoperability.....	14
Data Interoperability Policies.....	14
Data Interoperability standards and specifications .....	14
Table 2 Standards and specifications for data integration.....	14
Information access policies .....	15
Policies for Information Access are: .....	15
Standards and Specifications for Information Access.....	17
Table 3 Basic standards and specifications for information access - browsers and viewers.....	17
Table 4 Additional standards and specifications for information access - browsers and viewers .....	18
Content Delivery .....	18
WAP access standards and specifications.....	20
Table 5 Standards and specifications for information access - mobile phones	

## Executive Summary

1. Better public services tailored to the needs of the citizen and business, as envisioned in the e-government policy framework discussion document, require the seamless flow of information across all the tiers of government i.e. National, Provincial and Local. The Minimum Information Interoperability Standards (MIOS) sets out the Government's technical policies and standards for achieving interoperability and information systems coherence across the public sector. The MIOS defines the essential pre-requisite for joined-up and web enabled government. Next to security, it is a cornerstone policy in the overall e-government strategy.
2. Adherence to the MIOS standards and policies is mandatory as also set in the proposed chapter five of the Public Service Regulations. They set the underlying infrastructure, freeing up public sector organisations so that they can concentrate on serving the customer through building value added information and services. It will be for the government departments themselves to consider how their business processes can be changed to be more effective by taking advantage of the opportunities provided by increased interoperability. The State Information Technology Agency is setup to assist in these processes, thereby granting respective organs of state to streamline and focus of their areas of mandate and competency.
3. The main thrust of the framework (in line with international best practice), is to adopt the Internet and World Wide Web standards for all government systems. There is a strategic decision to adopt Extensible Markup Language (XML) and Extensible Stylesheet Language (XSL) as the core standard for Data interoperability and management of presentational data. This includes the definition and central provision of XML schemas for use throughout the public sector. The MIOS also adopts standards that are well supported in the global market place. It is a pragmatic strategy that aims to reduce cost and risk for government systems whilst aligning them to the global information society revolution
4. Specifying policies and standards in themselves is not enough. Successful implementation will mean the provision of support, best practice guidance, toolkits and centrally agreed data schemas. To provide this, the DPSA will be launching a series of publications through the Office of the Government Chief Information Officer (OGCIO). This is a Cabinet approved Office dedicated to deal with the whole issue of technology for improved governance, which entlists the generation of agreements pertaining to XML data schemas for use throughout the public sector. the OGCIO is also now being used for wide consultation on a number of other e-Government frameworks and processes.
5. The aims of the MIOS will not be achieved overnight. The strategy needs to be managed as a long-term ongoing initiative and must therefore be supported by robust processes. These processes, including the roles and responsibilities of key stakeholders, committees, management and working groups, are outlined in the document. Of particular significance is the establishment of a Government Information Technology Officers Council, (GITOC) which consists of representatives from all Government departments including provincial and local Government. Other stakeholders include, the Department of Communications (DoC), Department of Arts Culture Science and Technology (DACST), Department of Public Enterprises (DPE), National Intelligence Agency (NIA)etc.

6. It is also essential to ensure that the MIOS remains up to date and aligned to the requirements of all stakeholders and able to embrace the potential of new technology and market developments. In this instance, cooperation and collaboration becomes a critical success factor for the formulation of strategic synergies. The MIOS introduces an Internet based change management process which has been designed to engage and serve the stakeholder community in a dynamic way and to bring in innovations from industry on a global basis.

# 1 Overview

## *Introduction*

- 1.1 Modernising government and joined-up government demand joined-up information systems. Interoperable systems working in a seamless and coherent way across the public sector hold the key to providing better services tailored to the needs of the citizen and business and at a lower cost.
- 1.2 At the same time, clearly defined policies and standards for interoperability and information are also key to staying connected to the outside world and aligned to the global information revolution. This revolution is fuelled by the explosive growth of the Internet and its technologies.
- 1.3 The Minimum Information Interoperability Standards (MIOS) sets out the Government's policies and standards for achieving interoperability and seamless information flow across government as well as the wider public sector. The Minimum Interoperability Standards are fundamental in supporting the e-Government Policy published in April 2001.
- 1.4 The implementation and management process are defined in the MIOS Implementation Support document. This can be obtained from

## *Forecast Changes for future Versions*

- 1.5 Aspects currently under consideration for future versions include:
  - IPv6.
  - Standards for Video Conferencing and IP Telephony
  - Standards for Voice over IP
  - Standards for chat and instant messaging
  - Standards for Biometrics and Smart Cards
  - Detail of the compliance processes
  - Further detail on the implementation strategy
  - Identification and linkage to public sector communities' frameworks
  - Incorporation of ebXML standards
  - Standards for content delivery to:
    - Support the indigenous languages
    - the disabled

## **Scope**

- 1.6 The scope of the MIOS comprises the exchange of data and information access between RSA Government systems covering the interactions between:
  - RSA Government and citizens
  - RSA Government and employee
  - RSA Government and businesses (world wide)
- 1.7 "RSA Government" includes National and Provincial Government departments and their agencies, Local Government and the wider public sector, e.g. organs of state, state-owned enterprises etc.

- 1.8 The MIOS standards are mandated on all new systems that fall within the scope defined in paragraph 1.5 above. In order to address some of the interoperability challenges identified by e-Government Policy, all other systems ( which deliver citizen and/or business centric services and are part of departmental electronic service delivery) and legacy systems will need to comply with these standards.
- 1.9 For systems that fall outside the scope and mandate, the MIOS is recommended in all public sector procurements and major upgrades to other departmental legacy systems. Guidance on complying with this mandate is given in the MIOS Implementation Support document.
- 1.10 The MIOS does not standardise the appearance of information on the human interface which can be provided by various user channels e.g. web browsing, public kiosks, Digital TV and WAP phones. The MIOS does standardise the interchange requirements for the delivery of data to interfaces and tools for the management of the presentation of data.

### ***Main features***

- 1.11 The MIOS comprises three major components: policies and standards, a strategy for XML schemas provision. Policies and standards are outlined below. The management processes and the strategy for XML schema provision are defined in the MIOS Implementation Support document. The logical separation of the components was done to ensure manageable maintenance of components. This would ensure that update or modifications in one component does not necessarily affect the other component e.g. if the management structure changes, this would not necessarily affect the standards. Although MIOS implementation is not covered here, an overall picture is provided to ensure continuity between the components.

### **Policies and standards**

- 1.12 The technical policies and standards for interoperability across the public sector are specified in Section 2 of this document. These are the minimum set necessary to support the range of transactions and services provided by government and to integrate information systems within government. These policies and standards have also been chosen to interconnect and align government to the Internet and its future development.
- 1.13 The policies and standards in the MIOS cover three key areas of technical policy, which are essential for interoperability. These are Interconnectivity, Data Interoperability and Information Access.
- 1.14 In all of these areas, the main thrust of the specification has been to adopt the Internet and World Wide Web standards for all government systems. There is also a strategic decision to adopt XML as the main standard for data integration. This strategy includes provision of XML schemas for use throughout the public sector based on a set of agreed data standards, e.g. BS 7666 for property addresses.



## **Implementation support**

- 1.15** The adoption of XML (Extensible Mark-up Language) and XSL (Extensible Stylesheet Language) form the cornerstone of the government data presentation and integration strategy. However adopting these standards, in themselves, is not sufficient.
- 1.16** Achieving data coherence across government means that government organisations need data schemas that have been agreed for use throughout the public sector. They also need information, best practice guidance and toolkits to make implementation easier. In order to meet these demands, the RSA Government has embarked on an initiative to propose mechanisms and standards for achieving interoperability based on best practice and lessons learned from other countries. This initiative, managed by SITA e-Services, will publish on the Internet the draft and agreed XML data schemas which can then be applied to any public sector system. The group will also make available on the RSA MIOS web site the best of breed toolkits, guidance and information on XML implementation.

## **Management processes**

- 1.17** The work of integrating and evolving information systems across the public sector is a complex on-going process. The MIOS approach and policies must not only support and enhance government's business processes but also ensure that it stays tuned to the possibilities of new technological advances and innovations.
- 1.18** The MIOS management processes are described in MIOS Implementation Support for MIOS document covering the following:
- a governance process that describes the roles and responsibilities, committee structures and compliance processes
  - an Internet based change management process that is designed to introduce a global consultation and change process for capturing maximum stakeholder involvement and innovation.

## 2 Policies and Technical Standards

### *Introduction*

2.1 This section of the MIOS defines the minimum<sup>1</sup> set of technical policies and standards necessary to achieve interoperability and seamless information flows across Government and the public sector.

2.2 The current specification for the MIOS is given below and covers the areas of interconnectivity, Data Interoperability and Information Access. Each area is presented in two parts, first the key policy decisions and then a table containing the specified standard including version numbers and notes. Government is, however, committed to ensuring that these policies and standards are kept aligned to the changing requirements of the public sector and to the evolution of the market and technology.

### *Key decisions and drivers*

2.3 At the highest level, the MIOS has been shaped by three key policy decisions; these are:

- alignment with the Internet – the universal adoption of common standards used on the Internet and World Wide Web for all public sector information systems,
- adoption of XML – as the primary standard for Data Interoperability and presentation tools for all public sector systems
- adoption of OMG Metadata Interchange Specification (XMI) for Metadata interchange and
- W3C compliant browser as the key interface – all public sector information systems to be accessible through browser based technology. Other interfaces are permitted but only in addition to browser based ones.

2.4 The selection of MIOS standards has been driven by:

- **Interoperability** – only standards that are relevant to Systems Interconnectivity, Data Interoperability and Information Access are specified
  - **Market support** - the standards selected are widely supported by the market, and are likely to reduce the cost and risk of government information systems
  - **Scalability** – standards selected have the capacity to be scaled to satisfy changed demands made on the system, such as changes in data volumes, number of transactions or number of users.
-

- **Open Standards** -- the specifications for the standards are documented and available to the public at large.

### *Interconnection policies*

2.5 The policies for systems interconnection are defined below:

#### **Policy for Networks**

- Departments are to interconnect using IPv4, noting that RSA Government is considering the adoption of IPv6 in due course. Peering agreements should be investigated and considered where possible.

#### **Policy for Security**

- Protectively marked data will be handled and transmitted in accordance with the provisions of the ISO 17799
- Non-protectively marked data will be handled and transmitted in accordance with the Public Service Information Security Framework

#### **Policy for e-Mail.**

- To use a product that supports interfaces which conform to the SMTP/MIME.
- Within government, the norm will be to use the intrinsic security to ensure e-mail confidentiality. Outside secure government networks, S/MIME V3 should be used for secure messaging.

#### **Policy for Directory**

- A Directory schema should be developed to support a range of communication services including message handling, telephone and facsimile services as well as interactive access to a range of other applications.

#### **Policy for Domain Naming**

- Projects are to follow the RSA Government Domain Naming policy. Domain Name Services(DNS) is to be used for Internet/intranet domain name to IP address resolution.

#### **Policy for File Transfer Protocol (FTP)**

- FTP should be used where file transfer is necessary within Government Intranets. Restart and recovery facilities of FTP are to be used when transferring very large files.

#### **Policy for Terminal Emulation**

- Web based technology is to be used in applications that previously used Terminal Emulation whenever possible.

## ***Interconnection standards and specifications***

2.6 The RSA Government standards and specifications for interconnectivity are:

*Table 1 Standards and specification for interconnectivity*

Component	Standard
Hypertext transfer protocols	HTTP v1.1 (RFC 2616) Hypertext standards include on-line wide-area publishing services.
E-mail	E-mail products that support interfaces that conform to the SMTP/MIME. This includes RFC 821; RFC 822; RFC 2045; RFC 2046; RFC 2047; RFC 2048; RFC 2049 NB. E-mail attachments may conform to the file types for browsers and viewers as defined in table 3. The file types in table 4 may also be attachments when support for the extensive functionality provided by such components is essential.
E-mail security	S/MIME V3 shall be used where appropriate for pan government messaging security unless security requirements dictate otherwise. This includes RFC 2630 to RFC 2633.
Directory	X.500 core schema . LDAP V3 is to be used for general-purpose directory user access.
Domain name services	DNS (RFC 1035)
File transfer protocols	FTP (RFC 959) (with restart and recovery) and HTTP (RFC 2616) for file transfer
Newsgroup services	NNTP (RFC 977) where required, subject to security constraints
LAN/WAN interworking	IPv4 (RFC 791)
Security	National government departments should refer to the security policy at <a href="http://www.dpsa.gov.za">www.dpsa.gov.za</a> . This policy is based on ISO 17799.
IP security	IP-SEC (RFC2402/2404)
IP encapsulation security	ESP (RFC2406)
Transport security	SSL v3/TLS (RFC 2246)

Transport

TCP (RFC 793)

UDP (RFC 768) where required, subject to  
security constraints

Note: Copies of the IETF RFCs can be found at [www.ietf.org/rfc.html](http://www.ietf.org/rfc.html)

## Data Interoperability

### Data Interoperability Policies

2.7 RSA Government Policy is to use:

- XML and XML Schema for Data Interoperability
- RDF for Metadata framework. It provides interoperability between applications that exchange machine-understandable information on the Web.
- XML Metadata interchange using UML using XMI Data Type Definition (DTD), for exchange of all business, information and information system and information technology designs modeling.
- XSL for data transformation.

2.8 XML products will be written so as to comply with the recommendations of the World Wide Web Consortium (W3C). Where necessary the government will base the work on the draft W3C standards but will avoid the use of any product specific XML extensions that are not being considered for open standardisation within the W3C.

### Data Interoperability standards and specifications

2.9 The RSA Government standards and specifications for Data Interoperability and transformation are:

Table 2 Standards and specifications for data integration

Component	Standard
Metadata/Meta language	XML (Extensible Markup Language) as defined by W3C <a href="http://www.w3.org/XML">www.w3.org/XML</a>
Metadata definition	XML-Schema
Data transformation	XSL (Extensible Stylesheet Language) as defined by W3C <a href="http://www.w3.org/TR/xsl/">www.w3.org/TR/xsl/</a>
Modelling and Description Language	XMI (XML Metadata Interchange) using UML (Unified Modelling Language) DTD <a href="http://www.omg.org/technology/documents/formal/omg_modeling_specifications_a_vai.htm">www.omg.org/technology/documents/formal/omg_modeling_specifications_a_vai.htm</a>
RDF (Resource Description Framework) as defined by W3C	<a href="http://www.w3.org/TR/REC-rdf-syntax/">www.w3.org/TR/REC-rdf-syntax/</a>
Data definition and schema standardisation process	Government Data Standards

Minimum interoperable character set

Transformation Format – 8 bit UTF-8 (RFC 2279), individual items in the XML schema may be further restricted in character set on a case by case basis.

Geospatial data

GML (Geospatial Markup Language) as defined by Open Geographic Council. [www.opengis.org/techno/specs.htm](http://www.opengis.org/techno/specs.htm)

Note: Copies of the W3C specifications can be found at: [www.w3.org/TR](http://www.w3.org/TR)

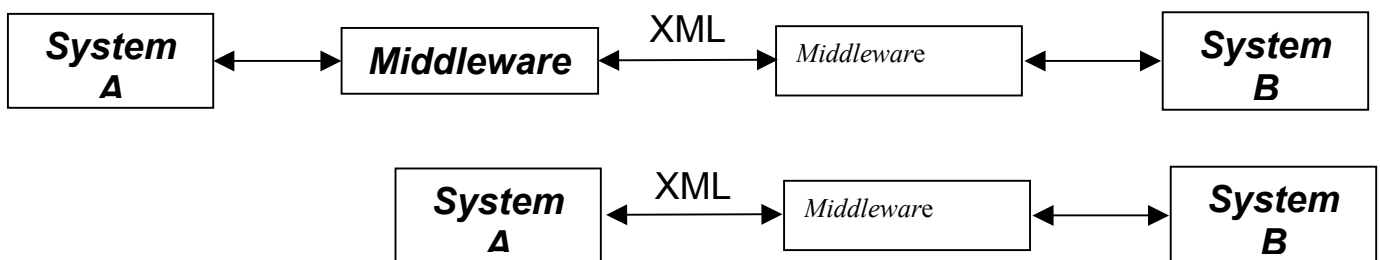
Notes on XML and middleware: not all systems are required to be directly XML enabled where appropriate it is acceptable to use middleware as illustrated below.

2.10 Note: although the configurations below present potential solutions, it should be clear that new procurements should strive to use the direct XML model as shown.

Figure 1 Direct XML Model



Figure 2 Interchanges via middleware



### Information Access Policies

#### Policies for Information Access are:

2.11 The Government Policies for information access are

- government information systems will be designed so that as much information as possible can be accessed and manipulated from common commercial browsers through utilisation of functionality freely supported and available within the browser community.

- government information systems will be designed to be available, as appropriate, on the Internet, either directly, or via third party services
- government information systems will support the standards and specifications listed in the browser standards and specifications tables below using, where necessary, freely available browser plug-ins or dedicated viewers
- government information systems will be designed to provide protection against security risks of connection to the Internet, including the ability to protect against the vulnerability of downloading executable content code that is not authenticated
- additional middleware or plug-ins are to be used, when necessary, to enhance browser functionality
- browser standards adopted for conformance should support those features that a business or citizen may be assumed to have available or can easily download without incurring a licensing fee, notwithstanding the policy requirement that all public sector information systems be accessible through browser based technology, other interfaces are permitted in addition to browser based ones
- government information access systems will be designed to provide the ability to support the citizen in their own time and at their own pace i.e. for asynchronous operation as well as synchronous



## Standards and Specifications for Information Access

2.12 The Government standards and specifications for information access, browsers and viewers are defined in tables 3 and 4 below. The services to be delivered to the citizen will dictate the expected standards required to be supported by the browser. However, as some browsers may only support the basic standards listed in table 3, this results in only a limited set of e-Government services being able to be offered via such browsers.

2.13 As such, the essential minimal level of information required to be accessed and viewed by the citizen should either be conveyed or be capable of being converted using personalization technologies, e.g. transcoders, through the use of the basic standards in table 3.

*Table 3 Basic standards and specifications for information access - browsers and viewers*

Basic Component	Standard
Hypertext interchange formats	Those parts of HTML v4.0 and XHTML commonly implemented by Netscape Navigator v4 or later, and MS Internet Explorer v4 or later, plus their interoperable extensions
Document file types	Adobe Acrobat as (.pdf), minimum viewer version 3 Rich Text Format as (.rtf ) files Plain/Formatted Text as(.txt) files Other product viewer as (.htm) files where the HTML generated conforms to the standard for Hypertext interchange format components
Spreadsheet file types	Proprietary product viewer as (.htm) files where the HTML generated conforms to the standard for Hypertext interchange format components Delimited file as (.csv) files
Presentation file types	Proprietary viewer products as (.htm) files where the HTML generated conforms to the standard for Hypertext interchange format components
Character sets and alphabets	UNICODE ISO/IEC 10646-1:2000 Transformation Format for 16 planes of group 00 (UTF-16)
Graphical/still image information exchange	Joint Photographic Experts Group /ISO standards 10918 (.jpg)

Graphics Interchange Format (.gif)  
 Portable Network Graphics (.png)  
 For images that will not tolerate  
 information loss use  
 Tag Image File Format (.tif)

2.13 Some services to be delivered to the citizen will require more extensive functionality in the browser. Where such extensive functionality is required the standards used should be selected from those listed in table 4.

Table 4 Additional standards and specifications for information access - browsers and viewers

Additional Component	Standard
Extended Document file types	Lotus Notes Web Access (.nsf) Microsoft Word Viewer (.doc)
Moving Image and audio/visual Information exchange standards	Moving Picture Experts Group (.mpg) MPEG-1/ISO 11172 Conversion is provided by most mainstream packages
Audio/video streaming data	Real Audio, Real Video Shockwave Windows Media Format (.wmf, .wmv and .wma) Apple Quicktime, Waveform Audio File Format (.wav). 8µ Law H263
Animation	Macromedia Flash (.swf) Dynamic html (.dhtml)
Scripting	ECMA 262 Script Java Virtual Machine – for browser enhancements
General purpose file compression	File types (.tar), (.zip) and (.gz) file types

**Content Delivery**

2.14 The design aim is for the content to be independent of the delivery mechanism, hence the strategic direction is to use XML and XSL (see table 2).

2.15 The full range of services to be delivered to the citizen will dictate the standards required. Content management techniques and personalisation technologies can be used to support various delivery channels e.g. low function web browsers, public kiosks, Digital TV, WAP phones, etc.

2.16 Transcoding services, as an example of personalisation technologies, can deliver web content to a variety of destination environments within greatly

reduced timescales and at significantly reduced cost. The principle is that transcoding can be used to dynamically filter, convert and reformat web content to match the requirements and display capabilities of the destination device. Transcoding technology is server-side software that modifies Web page content based on data protocols, markup languages, device and network parameters and user preferences.

2.17 Personalisation technologies may also be used to support groups such as ethnic minorities or visually impaired or blind people (i.e. by using text translation, larger fonts and graphics, audio, etc. via a transcoder).

### **WAP access standards and specifications**

2.18 The services to be delivered to the citizen via mobile phones will conform to the WAP Specification Suite, published by the WAP Forum as implemented to interoperable standards by the WAP providers.

2.19 The issues of security, relating to transactions undertaken through mobile phones, are complex and depend on emerging industry standards. Work in this area will be undertaken in due course. In the meantime the lack of standards does not imply that security issues can be ignored. Decisions will need to be made on a case by case basis depending on the nature of the transaction in question.

*Table 5 Standards and specifications for information access - mobile phones*

Component	Standard
WAP specifications	The specifications to be used are defined by the WAP Forum, see <a href="http://www.wapforum.org/what/technical.htm">www.wapforum.org/what/technical.htm</a>