MINIMUM INTEROPERABILITY STANDARDS (MIOS) for Information Systems in Government

(version 4.1)

Foreword

Improved public service delivery tailored to citizen and business needs, as envisioned in the e-Government Strategic Framework: Accelerating Service Delivery 2014, published in 2007, requires the seamless flow of information across all tiers of Government. The Minimum Information Interoperability Standards (MIOS) sets out the Government's technical principles 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 an essential component in the overall e-Government strategy.

Adherence to the MIOS standards and policies is mandatory as set out in the proposed chapter five of the Public Service Regulations. They set the underlying infrastructure, freeing up public sector organizations so they can concentrate on serving the customer through building value added information and services. It is the responsibility of individual departments to improve their business processes so that they are more effective, and to take advantage of the opportunities provided by increased interoperability.

The main thrust of the framework (in line with international best practice), is the adoption of a structured approach with regard to information systems. To achieve this approach, and to ensure the enhancement of interoperability across Government, a minimum set of standards are included in this document as a required Government-wide standard. To this end, this updated version of MIOS contains an explicit definition of Open Standards as well as the inclusion of the ISO (International Standards Organisation) Open Document Format.

The objective of achieving interoperability must be managed as a long-term ongoing initiative. In this regard the Government Information Technology Officers Council, (GITOC) which consists of representatives from all Government Departments including provincial and local Government, are crucial and instrumental in carrying this objective forwards and through to implementation.

It is also essential to ensure that MIOS remains up to date and aligned to stakeholder requirements, so that it can embrace the potential of new technology as well as market developments. In this instance, collaboration becomes a critical success factor for the formulation of strategic synergies.

Minister Geraldine Fraser-Moleketi

Executive Summary

A key theme in Government is that all departments need to collaborate to improve citizen service delivery. National, provincial and local government departments are increasingly required to reach across portfolio boundaries to find collaborative, networked and multi-channel approaches to delivering information and services to business and to citizens.

The development of an Interoperability Framework underpins the provision of integrated services by articulating a set of agreed policies, principles and standards to facilitate the electronic flow of information and transactions seamlessly across government to all its stakeholders. Improving the capability of departments to confidently manage, transfer and exchange information and services is critical to achieving the benefits of 'connected' government.

This Interoperability Framework identifies those components that support an environment where business services and information generated and held by Government will be valued and managed as a strategic, national asset. The framework provides principles, guidelines, and standards that underpin sound management, and establish concepts, practices and tools that will drive the successful sharing of services across government boundaries.

An interoperability framework may focus on several interoperability layers, which may be broadly categorized as follows: the business process layer; the information management layer; and the technical interoperability layer.

This document focuses on interoperability at the technical level to enable the exchange of data and harmonisation of business transactions across government. The framework covers common methods and shared services for the communication, storage, processing and presentation of data.

Information systems have the potential to transform Government and the services it provides to the public. However, without consistent policies, principles and standards to underpin these systems, it is not be possible to deliver collaborative services.

This document recommends the technical principles and standards that form the foundation of e-Government integration efforts. Their adoption will facilitate the seamless flow of information across the public sector to provide citizens and business with improved access to Government services, and also improved service delivery.

Table of Contents

List of Tables

1 Overview

1.1 Introduction

1.1.1 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.

1.1.2 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.

1.1.3 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.

1.2 Scope

1.2.1 The scope of the MIOS comprises the exchange of data and information access between South African Government systems covering the interactions between:

- government and itself
- government and citizens
- government and employee
- government and external entities

1.2.2 "South African Government" includes National, Provincial and Local Government Departments and their agencies, and the wider public sector, i.e. organs of state and state-owned enterprises.

1.2.3 The MIOS standards are mandated on all new systems that fall within the scope defined in the paragraph 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.

1.2.4   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.

1.2.5   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.

1.3   Main Features

1.3.1   The MIOS comprises the technical principles and standards required to achieve interoperability. 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 principles and standards have also been chosen to interconnect and align Government to the Internet and its future development.

1.3.2   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.

1.3.3   In all of these areas, the main thrust of the specification has been to adopt 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 at a physical architecture level. This strategy includes provision of XML schemas for use throughout the public sector based on a set of agreed data standards.

1.4   Implementation Support

1.4.1   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.

1.4.2   Achieving data coherence across Government means that Government organizations need to agree upon data schemas for use throughout the public sector. This initiative will be managed and implemented by SITA.

1.5 Management Process

1.5.1   The task of integrating information systems across the public sector is a complex on-going process. The MIOS approach and technical standards must not only support and enhance Government's business processes, but must also ensure that new technological advances and innovations are leveraged to their full advantage.

1.5.2   The MIOS will be reviewed and updtaed on an annual basis through the GITOC Standing Committee on Architecture with due process of consultation.

1.6 Government-wide Enterprise Architecture (GWEA) Framework

1.6.1   The MIOS is an integral part of the envisaged GWEA. MIOS resides within the governance layer of the GWEA framework. The governance layer includes best practices, policies and standards. Interoperability standards are a special component of standards meant to define connectivity, integration, and interfaces between systems and users.

1.7 Stakeholder Involvement

1.7.1   Continual engagement of all MIOS stakeholders is a fundamental objective. Government Departments and their agencies, organs of state, local Government, industry and the citizen are all encouraged to comment and suggest ways of improving interoperability, and to provide support on the implementation of the MIOS.

1.8 Requirements for next release

1.8.1 In the interest of continuous improvement the MIOS for Government Information Systems the MIOS working group aspires to improve this normative product over time.

1.8.2   The following requirements have been noted for incorporation in future releases of the product:

- Introduce a Technical Reference Model to serve as reference and classification schema for all interoperability standards.
- Introduce government sector/cluster specific data interoperability and representation standards to ensure interoperability across information systems that are owned or shared across different government policy holders within the same sector/cluster.

- Introduction of data representation standards to support indigenous languages and the disabled and/or impaired staff.
- Add a motivation to comply to a particular interoperability standard where appropriate.
- Add implementation guidelines to improve the migration, selection and development of government information systems.
- Improve the MIOS development process and responsibilities.

2 Principles and Standards

2.1 Introduction

2.1.1 This section of the MIOS defines the minimum set of technical policies and standards necessary to achieve interoperability and seamless information flows across Government and the public sector.

2.1.2 The 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 principle statements as points of departure and secondly a table containing the specified standard including version numbers and notes.

2.1.3 Government is 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.

2.2 Drivers of Interoperability

The MIOS has been shaped by four key drivers:

- The universal adoption of common standards used on the Internet and World Wide Web for all public sector information systems.
- The adoption of XML as the primary standard for Data Interoperability and presentation tools for all public sector systems and the use of XML Schema to support Web Services through Web Services Description Language (WSDL) based interfaces.
- W3C compliant browser as the key human interface – all public sector information systems to be accessible through browser based technology.

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, freely implementable and available to the public at large.

- **Security**: all standards selected need to support a secure computing environment.

2.3 Open Standards

2.3.1 There are number of definitions of open standards which emphasise different aspects of openness, including of the resulting specification, the openness of the drafting process, and the ownership of rights in the standard. The list below contains frequently cited indicators of the openness of a standard. For the purposes of the MIOS, **a standard shall be considered open if it meets all of these criteria**. There are standards which we are obliged to adopt for pragmatic reasons which do not necessarily fully conform to being open in all respects. In such cases, where an open standard does not yet exist, the *degree* of openness will be taken into account when selecting an appropriate standard:

- it should be maintained by a non-commercial organization
- participation in the ongoing development work is based on decision-making processes that are open to all interested parties.
- open access: all may access committee documents, drafts and completed standards free of cost or for a negligible fee.
- It must be possible for everyone to copy, distribute and use the standard free of cost.
- The intellectual rights required to implement the standard (e.g. essential patent claims) are irrevocably available, without any royalties attached.
- There are no reservations regarding reuse of the standard.
- There are multiple implementations of the standard

2.4 Standards Development Organisations

2.4.1 There are a number of standards development organisations (SDOs) referred to in this document. The following table provides a brief reference – SDOs marked with an asterisk (*) indicate that standards are freely downloadable:

SDO	Description	URL
ISO	International Organisation for Standardization	http://www.iso.org/
IETF *	Internet Engineering Task Force	http://www.ietf.org
OASIS *	Organization for the Advancement of Structured Information Standards	http://www.oasis-open.org
W3C *	World Wide Web Consortium	http://www.w3c.org/
ITU	International Telecommunication Union	http://www.itu.int/
IEC	International Electrotechnical Commission	http://www.iec.ch
ECMA	Ecma International - European association for standardizing information and communication systems	http://www.ecma-international.org/
SABS	South African Bureau of Standards	http://www.sabs.co.za/
IEEE	Institute of Electrical and Electronics Engineers	http://www.ieee.org/
ANSI	American National Standards Institute	http://www.ansi.org/
OGC*	Open Geospatial Consortium	http://www.opengeospatial.org/
FIPS	Federal Information Processing Standards	http://www.itl.nist.gov/fipspubs/
ITU-T	International Telecommunication Union Standardisation Sector	http://www.itu.int/
ETSI	European telecommunications Standard Institute	http://www.etsi.org/

Table 1: Standards Development Organisations

2.5 Principle Statements as Points of Departure

2.5.1   A principle is a general rule or guideline for designing a system or architecture. By its nature a principle is *a restriction of design freedom*. Principles are the means to guide the design and evolution of systems.

2.5.2   The following general principle statements serve as points of departure for setting technical principles statements and standards:

- The funding of government IS/ICT projects and the purchasing of IS/ICT products and solutions is dependent on compliance to MIOS;
- Compliance to MIOS falls with in the scope of the PFMA and is therefore a responsibility of accounting officers and audited by the Auditor-general;

- When interconnectivity, data interoperability or information access is required, the cost of non-complying with MIOS rests with the non-complying entity, system or organisation.
- Government organisations' IS/ICT plans are based on the MIOS as well as acts and other relevant Government policy documents;
- The institution- and functional-based approach should be replaced by a service-centered approach;
- Government organisations that co-operate in order to ensure the provision of information and services for citizens or own officials need not know everything about the subordinating system or the division of roles therein;
- The development of information systems is based on an internet-centred approach;
- Access to public services should preferably be ensured via a web browser by different channels and devices;
- XML-based technologies are used for the integration of information systems and the presentation of data;
- Information systems provide and use services via a data exchange layer based on multilateral agreements; and
- In developing open information systems, open source based solutions are to be considered before proprietary ones

Principle Statement relating to Networks

2.5.3   Government organisations are to interconnect using Ipv4 (*noting that RSA Government is considering the adoption of IPv6 in due course. Peering agreements should investigated and considered where possible)*.

Principle Statements relating to Security

2.5.4   Protectively marked data is handled and transmitted in accordance with the provisions of the ISO 17799

2.5.5   Non-protectively marked data is handled and transmitted in accordance with the Public Service Information Security Framework

Principle Statements relating to e-Mail.

2.5.6   To use a product that supports interfaces which conform to the SMTP/MIME.

2.5.7   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.

Principle Statement relating to Directory

2.5.8   A government 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.

Principle Statements relating to Domain Naming

2.5.9   Projects are to follow the South African Government Domain Naming policy.

2.5.10   Domain Name Services (DNS) is to be used for Internet/intranet domain name to IP address resolution.

Principle Statements relating to File Transfer Protocol (FTP)

2.5.11   FTP should be used where file transfer is necessary within Government Intranets.

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

Principle Statement relating to Terminal Emulation

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

Principle Statement relating to Data Interoperability

2.5.14   Use XML and XML Schema for Data Interoperability;

2.5.15   Use RDF, OWL and RSS for Metadata framework. It provides interoperability between applications that exchange machine-understandable information on the Web;

2.5.16   Use UML and XMI for exchange of all business information and information system design modeling;

2.5.17   Use XSL for data transformation; and

2.5.18   Ensure XML products are written so as to comply with the recommendations of the World Wide Web Consortium (W3C). (*Where necessary base the work on the draft W3C standards but avoid the use of*

any product specific XML extensions that are not being considered for open standardisation within the W3C.)

Principal Statements relating to Information Access:

2.5.19   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.

2.5.20   Government information systems will be designed to be available, as appropriate, on the Internet, either directly, or via third party services

2.5.21   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

2.5.22   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

2.5.23   Additional middleware or plug-ins are to be used, when necessary, to enhance browser functionality

2.5.24   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, not withstanding the policy requirement that all public sector information systems be accesible through browser based technology, other interfaces are permitted in addition to browser based ones

2.5.25   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

Principle Statements relating to Content Delivery

2.5.26   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).

2.5.27   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.

2.5.28 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.

2.5.29 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).

Principle Statements relating to Web-Services

2.5.30 This is a crucial area for interoperability in which vendor neutral standards are emerging.

2.5.31 Implementations of web-services for government should adhere to the existing and evolving standards developed by W3C and OASIS.

2.5.32 Where standards are still emerging from industry consortia, such as WS-I, government should monitor standards development in this area and, where necessary, participate in national standards development.

Principle Statements relating to Enterprise Architecture

2.5.33 In terms of the Public Service Regulations, Government organisations are required to develop Information Plans, Infrastructure Plans and Operational Plans based on the Government organisations' business strategy;

2.5.34 Government organisations are required to develop plans based on a consistent enterprise architecture containing business architecture, application architecture, data architecture and technology architecture;

2.5.35 Business architecture contains a full business definition, including business motivation, services, business processes implementing these services, business units and locations and how these relate to each other;

2.5.36 Application, data and information technology architectures are consistent with the technology standards provided in the rest of this

document.

2.6 Interconnection Standards and Specifications

The RSA Government standards and specifications for interconnectivity are:

Component	Standard	Standards Body
Web transport	Hypertext Transfer Protocol HTTP v1.1 (RFC 2616)	IETF/W3C
Email transport	Simple Mail Transfer Protocol SMTP (RFC2821, RFC2822)	IETF
Internet message format	Multipurpose Internet Mail Extensions MIME (RFC 2045, RFC 2046, RFC 2047, RFC 2048 and RFC 2077)	IETF
Mailbox access	Internet Message Access Protocol IMAPv4.1 (RFC 3501)	IETF
Email 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.	IETF
Directory	X.500 core schema (ISO/IEC95948). Lightweight Directory Access Protocol LDAP V3 (RFC4510) is to be used for general-purpose directory user access.	ITU/IEC/ISO IETF
Domain Name System	DNS (RFC 1032 to RFC1035 and related updates)	IETF
File transfer protocols	FTP (RFC 959, RFC1579, RFC2428) Secure copy over ssh (OpenBSD reference implementation)	IETF
LAN/WAN interworking	Internet Protocol IPv4 (RFC 791)	IETF
IP security	IP-SEC (RFC2402/2404)	IETF
IP encapsulation security	Encapsulating Security Payload ESP (RFC2406)	IETF
Transport	Transport Control Protocol TCP RFC793 with extensions as referred in RFC4614 User Datagram Protocol UDP (RFC768)	IETF IETF
Transport security	TLS 1.1 (RFC 4346)	IETF

Component	Standard	Standards Body
Encryption algorithms	Stream Ciphers: RC4, Rabbit, Decim, TSC4 (ISO/IEC18033-4)	ISO
	Block Ciphers: AES (FIPS 197), Twofish, RC6, Blowfish, IDEA (ISO/IEC18033-3)	ISO
	Asymmetric: RSA (ISO/IEC18033-2); Elliptic Curve Cryptography (ECC SEC1) (ISO/IEC15946)	ISO
Hashing	SHA-256, SHA-512 (FIPS Pub 180-2);	FIPS
	SHA-384; RIPEMD-160; WHIRLPOOL-512 (ISO/IEC 10118-3)	ISO
Digital Signatures	With Appendix: RSA (ISO/IEC14888)	
	With Message Recovery: RSA (ISO/IEC9796-2/3); DSA (FIPS Pub 186-2), EC-DSA, Rabin, Nyberg-Reuppel (ISO/IEC14888))	
Key Management	Diffie-Hellman (ANSI X9.42 – DH-MQV); ElGamal, Nyberg-Reuppel, RSA (ISO/IEC11770-2/3))	

Table 2: Standards and specification for interconnectivity

2.7 Data Interoperability standards and specifications

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

Component	Standard	Standard Body
Metadata/MetaLanguage	XML (Extensible Markup Language)	W3C
XML MetaData definition	XML-Schema RelaxNG	W3C OASIS/ISO
XML Data transformation	XSL (Extensible Stylesheet Language)	W3C
XML Data query	Xpath	W3C
XML Signature	XML DSIG	W3C
XML Security mark-up	SAML v2.0 (Security Assertion Markup Language)	OASIS
Public Key Infrastructure	X509v3	ITU-T

Component	Standard	Standard Body
Minimum interoperable character set	Transformation Format – 8 bit UTF-8 (RFC3629), individual items in the XML schema may be further restricted in character set on a case by case basis.	IETF
Modelling and Description Language	UML (Unified Modelling Language) RDF (Resource Description Framework)	OMG W3C
Ontology-based information exchange	OWL (Web Ontology Language Semantics and Abstract Syntax)	W3C
Model exchange	XMI (XML Metadata Interchange), version 2.1	OMG
Form Representation and Data	Xforms	W3C
Geospatial data	GML (Geospatial Markup Language)	Open Geospatial Consortium

Table 3: Standards and specifications for data integration

It may be necessary to interface to legacy systems which do not have native XML support by using appropriate middleware.

2.8 Standards for Web Services

Component	Standard	Standard Body
Web service request delivery	Simple Object Access Protocol SOAP v1.2	W3C
Web service request registry	Universal Description, Discovery and Integration UDDI v3.0	OASIS
Web service description language	WSDL 1.1	W3C

Table 4: Standards for Web Services

2.9 Standards and Specifications for Information Access

2.9.1 The Government standards and specifications for information access, browsers and viewers are defined in tables 5 and 6 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 5, this results in only a limited set of e-Government services being able to be offered via such

browsers.

2.9.2   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.

Component	Standard	Standard Body
Hypertext interchange formats	Those parts of Hypertext Markup Language HTML v4.0 and XHTML implemented in common by Firefox v2.0 or later, and MS Internet Explorer v6 or later, plus their interoperable extensions	W3C
Working Office Document formats (word-processing, spreadsheet, presentation)	UTF-8/ASCII Formatted Text Open Document Format (ODF) v1.0 (ISO26300) and later Oasis versions Comma-Separated Values (CSV) RFC4180	IETF OASIS/ISO IETF
Document formats for presentation view	XHTML markup PDF (version 1.6)	W3C Adobe[1]
Relational Database Access	Structured Query language SQL93	ANSI
Character sets and alphabets	UNICODE ISO/IEC 10646-1:2000	ISO/IEC
Graphical/still image information exchange	Joint Photographic Experts Group /ISO standards 10918 Portable Network Graphics (ISO/IEC15948:2001) For images that will not tolerate information loss use tag Image File Format (.tif)	ISO ISO Adobe

Table 5: Basic standards and specifications for information access

2.9.3   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

---

[1]   The full specification for pdf version 1.7 is available at http://www.adobe.com/devnet/pdf/pdf_reference.html, but is unreadable by the current linux acrobat reader. There are other issues with pdf which lead us to accept the format pragmatically but reluctantly whilst we monitor new emerging XML specifications (including Adobe's upcoming MARS and Microsoft's XPS).

Table 6.

Component	Standard	Standard Body
Multimedia audio/visual content	Moving Picture Experts Group (.mpg) MPEG-1 (ISO/IEC 11172) MPEG-2 (ISO/IEC 13818) MPEG-4 and ogg (http://www.xiph.org)	ISO
Browser scripting	JavaScript (ECMA 262)	ECMA
Internet Conferencing	H323 SIP (RFC3261)	ITU-T IETF
File compression	tar (POSIX.1-2001) gzip (RFC1951 and RFC1952) zip (http://www.pkware.com) bzip2 (http://www.bzip.org/)	POSIX IETF

Table 6: Additional standards and specifications for information access

2.10 Standards for Content Management Metadata

The South African Government standards for Content Management Metadata are:

Component	Standard	Standards Body
Content management metadata elements and refinements	Dublin Core	ISO15836
Metadata harvesting	Open Archives Initiative Protocol for Metadata Harvesting 2.0 (OAI-PMH) for metadata collection. Protocol Version 2.0 of 2002-06-14 Document Version 2003/02/21 T00:00:00Z Http://www.openarchives.org/OA/openarchivesprotocol.html	

Component	Standard	Standards Body
Content syndication	RSS (RDF Site Summary) Version 1 The RSS is a standard format for syndicating news content over the web using Dublin Core and RDF Published by the RSS-DEV Working Group http://web.resource.org/rss/1.0/	
	RSS (Really Simple Syndication) Version 2 The RSS was originally designed as an alternative standard format for syndicating news content over the web, however RSS can be and is being used to publish various types of data over the web, not just news data. The RSS 2.0 is offerred by Berkman Center for Internet & Society at Harvard Law School under the terms of the Attribution/Share Alike Creative Commons license http://blogs.law.harvard.edu/tech/rss	
Content-sensitive linking	OpenURL 0.1 (migrating to 1.0) for context-sensitive linking http://www.exlibrisgroup.com/sfx openurl.htm The openURL is designed to enable the transfer of the metadata from the information service to a service component that can provide context-sensitive services for the transferred metadata	
Distributed searching	Z39.50 or Search/retrieve Web Service (SRW) ISO 23950:1998 Information and documentation – Information retrieval (Z39.50) – Application service definition and protocol specification http://lcweb.loc.dov/z3950/agency/	

Table 7: Standards and specifications for content metadata

2.11 Standards for Identifiers

The South African Government standards for Identifiers are:

Component	Standard	Standards Body
Persistent and unique logical identifiers	z39.84 provides a syntax for unique identification for digital content	ANSI/NISO

Table 8: Standards and specifications for Identifiers

2.12 Standards for Mobile Phones

Component	Standard	Standard Body
WAP specifications	WAP2.0	WAP Forum http://www.openmobilealliance.org/
GPRS	The General Packet Radio Service specifications for Mobile Stations including: EN No: 310 113, 301 344, 301 347 and TS 101 297, 101 351	European telecommunications Standard Institute (ETSI)
SMS	The Short Message Service specifications for Mobile Stations including ETS 300 536, 537, 300 559, 300 560, see www.etsi.org	European Telecommunications Standards Institute (ETSI)
MMS	The Multimedia Messaging Service specifications for Mobile Stations including: TS 122 140, 123 140, 126 140	European Telecommunications Standards Institute (ETSI)

Table 9: Standards and specification for mobile phones

2.13 Standards for Biometric Data Interchange

The South African Government standards for Biometric Data Interchange are:

Component	Standard	Standard Body
Secure XML Encoding for exchanging biometric data	OASIS XCBF 1.1 Specification. Secure XML encodings for the patron formats specified in CBEFF, the Common Biometric Exchange File Format (NISTIR 6529).	OASIS
Data Element Specification	ISO/IEC 19785-1 Information Technology – Common Biometric Exchange Formats Framework – Part 1: Data Element specification	ISO/IEC
Interchange format framework	ISO/IEC 19794: Information Technology Biometric data interchange formats – Part 1: Framework	ISO/IEC
Interchange formats for finger minutiae data	ISO/IEC 19794: Information Technology Biometric data interchange formats – Part 2: Finger minutiae data	ISO/IEC
Interchange formats for Finger pattern spectral	ISO/IEC 19794: Information Technology Biometric data interchange formats – Part 3: Finger pattern spectral	ISO/IEC
Interchange formats for Finger image data	ISO/IEC 19794: Information Technology Biometric data interchange formats – Part 4: Finger image data	ISO/IEC
Interchange formats for Face image data	ISO/IEC 19794: Information Technology Biometric data interchange formats – Part 5: Face image data	ISO/IEC
Interchange Formats for Signature/sign behaviour data	ISO/IEC 19794: Information Technology Biometric data interchange formats – Part 7: Signature/sign behaviour	ISO/IEC
Graphical/still image information exchange specifications	ISO/IEC 10918-1:1994 Information technology – Digital compression and coding of continuous- tone still images: Requirements and Guidelines ISO/IEC 10918-1:1994/CD Cor 1 ISO/IEC 10918-2: 1995 Information technology – Digital compression and coding of continuous-tone still images: Compliance testing ISO/IEC 10918-3: 1997 Information technology –Digital compression and coding of continuous-tone still images: Extensions ISO/IEC 10918-3:1997/Amd 1:1999	ISO/IEC

Component	Standard	Standard Body
	ISO/IEC 10918-4:1999 Information technology –Digital compression and coding of continuous-tone still images: Registration of JPEG profiles, SPIFF profiles, SPIFF tags, SPIFF colour spaces, APPn markers, SPIFF compression types and Registration Authorities (REGAUT)	

Table 10: Standards and specification biometric data interchange

Document History

Document Name	Revision Authority	Update	Revision Date	Originating application
e-Gif		Adopted from UK Gov	July 2001	
MIOS v1	SITA services certification	Customised for RSA Government	Sep 2001	
MIOS v2	GITOC MIOS Workshop	Input from GITOC	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	
MIOS_30June_2007.odt		Included ISO26300 odf document standard. Minor maintenance revisions. Reformatted.	July 2007	OpenOffice2.2.0
MIOS_v4_final.odt		Incorporated revisions from SITA workshop	August 2007	OpenOffice2.2.0
MIOS_v4.1_final.odt	GITOC	Minister's Foreward	Sept 2007	OpenOffice2.2.0

Table 11: Document History