eID Interoperability for PEGS

NATIONAL PROFILE MALTA

November 2007

This report / paper was prepared for the IDABC programme by:

Author's name: Jos Dumortier - Hans Graux, time.lex

Company's name: Siemens - time.lex

Company's address (optional):

Company's logo (optional)

Contract No. 1, Framework contract ENTR/05/58-SECURITY, Specific contract N°3

Disclaimer

This paper can be downloaded from the IDABC website:

http://europa.eu.int/idabc/
http://ec.europa.eu/idabc/en/document/6484/5938

Executive summary

The project eID Interoperability for PEGS aims to propose a solution to the legal, technical and organisational issues related to the creation of an interoperable Pan-European identity management infrastructure. The EU Member States, Candidate Countries and EEA Countries are introducing more sophisticated ways to manage identities in the eGovernment area. Different member states are implementing different structures as their identity management solution. The main challenge for the eID Interoperability for PEGS project is to propose a general architecture that, while taking into account the existence of different models, is able to cope with them by obtaining the final goal of interoperability.

The project should conclude with several different proposals how to build interoperability without affecting member states' own existing infrastructures.

This document describes the current situation regarding the use of electronic authentication means in Maltese eGovernment applications.

Table of Contents

1 Documents

1.1 Applicable Documents

[AD1]	Framework Contract ENTR/05/58-SECURITY

1.2 Reference Documents

[RD1]	eGovernment in the Member States of the European Union – 5th Edition – May 2006 http://ec.europa.eu/idabc/servlets/Doc?id=24769
[RD2]	European Electronic Signatures Study http://www.law.kuleuven.ac.be/icri/itl/es_archive.php?where=itl
[RD3]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures http://europa.eu.int/information_society/eeurope/i2010/docs/esignatures/esignatures_en.pdf
[RD4]	Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council, OJ L 175, 15.7.2003, p.45 http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_175/l_17520030715en00450046.pdf
[RD5]	DIRECTIVE 2004/18/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_134/l_13420040430en01140240.pdf
[RD6]	IDABC Work Programme Third Revision http://ec.europa.eu/idabc/servlets/Doc?id=25302
[RD7]	DIRECTIVE 2004/17/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en00010113.pdf

2 Glossary

2.1 Definitions

In the course of this report, a number of key notions are frequently referred to. To avoid any ambiguity, the following definitions apply to these notions and should also be used by the correspondents.

- *Entity:* anyone or anything that is characterised through the measurement of its attributes in an eIDM system. This includes natural persons, legal persons and associations without legal personality; it includes both nationals and non-nationals of any given country.

- *eIDM system*: the organisational and technical infrastructure used for the definition, designation and administration of identity attributes of entities. This Profile will only elaborate on eIDM systems that are considered a key part of the national eIDM strategy. Decentralised solutions (state/region/province/commune…) can be included in the scope of this Profile if they are considered a key part of the national eIDM strategy.

- *eIDM token (or 'token')*: any hardware or software or combination thereof that contains credentials, i.e. information attesting to the integrity of identity attributes. Examples include smart cards/USB sticks/cell phones containing PKI certificates, …

- *Authentication*[1]: the corroboration of the claimed identity of an entity and a set of its observed attributes. (i.e. the notion is used as a synonym of "entity authentication").

- *Authorisation*: the process of determining, by evaluation of applicable permissions, whether an authenticated entity is allowed to have access to a particular resource.

- *Unique identifiers*: an attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context. Examples may include national numbers, certificate numbers, etc.

- *Official registers*: data collections held and maintained by public authorities, in which the identity attributes of a clearly defined subset of entities is managed, and to which a particular legal of factual trust is attached (i.e. which are generally assumed to be correct). This includes National Registers, tax registers, company registers, etc.

[1] For the purposes of this Profile, the notion of authentication is considered to be synonymous with 'entity authentication', as opposed to 'data authentication'. The notion of 'identification should be avoided to avoid confusion.

- *eGovernment application*: any interactive public service using electronic means which is offered entirely or partially by or on the authority of a public administration, for the mutual benefit of the end user (which may include citizens, legal persons and/or other administrations) and the public administration. Any form of electronic service (including stand-alone software, web applications, and proprietary interfaces offered locally (e.g. at a local office counter using an electronic device)) can be considered an eGovernment application, provided that a certain degree of interactivity is included. Interactivity requires that a transaction between the parties must be involved; one-way communication by a public administration (such as the publication of standardised forms on a website) does not suffice.

- *eSignature*: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication with regard to this data. Note that this also includes non-PKI solutions.

- *Advanced electronic signature*: an electronic signature which meets the following requirements:

  (a) it is uniquely linked to the signatory;

  (b) it is capable of identifying the signatory;

  (c) it is created using means that the signatory can maintain under his sole control; and

  (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

  Again, this definition may cover non-PKI solutions.

- *Qualified electronic signature*: advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, as defined in the eSignatures Directive[2].

- *Validation*: the corroboration of whether an eSignature was valid at the time of signing.

[2] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

2.2 Acronyms

A2A ..... Administration to Administration

A2B ..... Administration to Businesses

A2C ..... Administration to Citizens

CA ..... Certification Authority

CRL ..... Certificate Revocation Lists

CSP ..... Certificate Service Provider

eID ..... Electronic Identity

eIDM ..... Electronic Identity Management

IAM ..... Identity and Authentication Management

IDM ..... Identity Management

OCSP ..... Online Certificate Status Protocol

OTP ..... One-Time Password

PKCS ..... Public-Key Cryptography Standards

PKI ..... Public Key Infrastructure

SA ..... Supervision Authority

SOAP ..... Simple Object Access Protocol

SCVP ..... Server-based Certificate Validation Protocol

SSCD ..... Secure Signature Creation Device

USB ..... Universal Serial Bus

TTP ..... Trusted Third Party

XAdES ..... XML Advanced Electronic Signature

XML ..... eXtensible Markup Language

XML-DSIG ..... XML Digital Signature

3 Introduction

3.1 General status and most significant eIDM systems

The Government of Malta had embarked on eID implementation in March 2004, when the Ministry for Information Technology and Investment presented an eIDM system allowing citizens to gain personalised access to online government services. The Maltese electronic identity is based on a secure network key that can be used to securely access online services requiring authorisation, thus enabling the secure provision of value-added transactional e-services.

The Ministry responsible for Government eIDM systems and for eID in general is the Ministry for Investment, Industry and Information Technology ("the Ministry"). It is the main body creating the strategy, objectives and the implementation plans for eIDM systems. The creation of a horizontally integrated eIDM system is at the heart of this project.

The implementation of eID program is undertaken by the Government in phases. Currently, in its first phase of implementation, the eIDM systems as implemented are positioned at Level 1 within the accepted 4-tier authentication assurance classification[3] and, accordingly, utilise login, password and PIN issued upon completion by entities of the application procedure.

One must note, however, that in addition to the Level 1 authentication currently used in eID systems by the Government, a number of e-Government services deploy digital certificates. These services are generally those offered to commercial entities as clients, where the Government is a relying party. Digital certificates used for these purposes are procured by the Government. Such certificates are used as eIDM tokens for authentication purposes. None of the services offered at this time requires digital certificates for qualified signatures.

e-Government services using eIDM systems are application-based offered by various departments and authorities and include services on national level by:

- Inland Revenue Department;
- VAT Department;
- Malta Environment and Planning Authority;
- Malta Transport Authority;
- Malta Financial Services Authority

amongst others and accessible via the relevant ministry/authority website. The later are also accessible via the generic government website www.gov.mt

[3] Level 0: no authentication; Level 1: restricted authentication (login, password and PIN); Level 3: confidential authentication (digital certificate); Level 4: maximum authentication (qualified digital certificate).

Decentralised services are now also provided by local councils which act as agents to Government. Government is also working to offer a set of services on mobile telephone, via a call centre, through public internet access points and the front offices of local councils and post offices.

It has been announced that in 2007 the Government will implement Level 2 authentication generally enabling the use of digital certificates for its eID system. Moreover, a national electronic identity card (eID Card) – a chip-embedded card containing *inter alia* a unique identifier for every resident in Malta and digital certificates – is envisaged to be implemented also in 2007. It has also been stated that the structure of Government eIDM systems will be streamlined and integrated to provide a horizontally integrated coherent platform across all e-Government services and to enable access to all such services from a single portal.

While entities have been encouraged to obtain eID (at Level 1) to enable them to use e-Government services, at this stage obtaining eID is not compulsory.

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

The Ministry for Investment, Industry and Information Technology is responsible for strategy, implementation and coordination in respect of eIDM systems.

Except as stated below, all tasks necessary for the development of the strategy and implementation of eIDM systems are done on the national level. The Ministry's role involves collaboration with a number of public and private entities involved in the implementation of eIDM systems and eGovernment services.

In particular, technical implementation and integration is carried out by Malta Information Technology and Training Services Limited ("MITTS"), a government-owned IT agency in charge of providing and maintaining IT infrastructure for the Government.

At this time, the Government is finalising a selection, by tender, of a strategic partner for the implementation of the eIDM systems in general.

Moreover, in May 2007, the Government also issued a call for the expression of interest inviting commercial entities wishing to undertake development of one or more e-Government service applications to register for this purposes. The register of commercial entities created on the basis of this call for the expression of interest will be used to select a contractor for the development and implementation of each new e-Government service.

Currently the administration of eGovernment is not horizontally integrated and, each department providing an eService still carries out its own authentication processes. Horizontal integration will mean implementation of the 'single authentic source' which will allow the various departments to share the information for a citizen rather than having separate processes. However, even at this stage only one time registration is required to obtain eID login, password and PIN. The information collected during this initial eID registration is validated by the Registration Authority and then stored in a repository administered by a central body for access by all other eGovernment service providers and beneficiaries.

3.2.2 National eGovernment cooperation and coordination

The majority of eGovernment processes occurs at the national Government level. The Government is currently carrying out an integration and rationalisation exercise with respect to eIDM systems, so that the departmental systems administered by various departments are integrated into a common system, with common infrastructure and administration across the Government. This program is being carried out largely by MITTS, an IT agency for the Government.

Local government (local councils) are involved only in certain tasks. One of such tasks is assisting of the registration of entities for the purposes of obtaining an eID. Another example of Local Councils' involvement is their role in the eVERA system that provides the Maltese citizens with the facility to renew their vehicle road licence on-line, to pay any outstanding contraventions and to check their vehicle roadworthiness test from any place with an internet connection. This web application is integrated with the Local Enforcement System (managed by Local Councils) and allows traffic wardens that are out on duty to register and manage traffic contraventions of various kinds. The Maltese Government considers that the partnership with Local Councils '*aims at empowering Local Councils, providing them with the necessary capacity and a framework for action that will position them as centres of ICT-excellence in their locality*'.[4] The involvement of Local Councils is thought to be a way of making eServices more easily understandable and accessible to the Maltese Citizen.

3.2.3 Traditional identity resources

The major traditional identity resources that eGovernment services rely upon for the purposes of authentication of entities are the common national database (Public Registry) and a National Identity Card (ID Card). A National ID Card was introduced by the Identity Card Act in 1975. It is mandatory in Malta from the age of fourteen. The card takes the form of a small plastic card, similar to a credit card, containing the person's full name, manual signature, address of current residence, date and place of birth, nationality, gender and photo. Data included in the National Identity Card is a subset of data held in the common national database. The older form of the Identity Card was in paper from and contained other data such as marital status and names of children. These are no longer included.

[4] Government Website: http://www.gov.mt/egovernment.asp?p=114&l=1

Each ID Card has a unique Identity Number, based on a combination of (a) a sequential registration number in the relevant year; (b) the relevant year number (2 digits), where the year is the year of birth (for Malta-born persons) or year of registration (for non-Malta born persons), and (c) a letter designating the geographic origin of the person ('M' for the mainland of Malta, 'G' for the Maltese island of Gozo, 'A' for aliens (non-Maltese citizens)). This number is the main identification feature in the Maltese system and any form of identity request within the Government will normally require the identity number.

Non-Maltese citizens are required to apply for a Maltese Identity Card if they stay in Malta for over 6 months. In order to apply for this, non-EU citizens also have to show that they are in possession of a renewable work permit or along-term visa. EU citizens require the presentation of their passport.

The plastic identity card currently in use is ready for the inclusion of a chip. These ID cards will continue to be used once the eID cards will be introduced by adding the chip with digital certificates.

Other major entity identity resources include:

- a social security register, including a unique social security number for every working person in Malta. This information is shared by several departments and authorities;
- a register of commercial partnerships and companies administered by the Registry of Companies. Every company/partnership has a unique identified used throughout the life of the entity consisting of a letter identifying the legal form (e.g., "C" for a company) and a sequential registration number. The database contains details of the company's shareholders (past and present), directors (past and present), company secretary (past and present), annual returns, annual accounts and some other details. This information is publicly available;
- a register of employers. Every employer (regardless of type of entity) has a unique employer registration number. This information is shared by several departments and authorities;
- a register of taxpayers. For every physical person, his/her ID card number serves also as a taxpayer's number. For every other entity, it is given an income tax number.

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

In Malta, eGovernment applications were launched in 2004, offered on the basis of a secure network key, enabling citizens to access a number of interactive and transactional eservices.

The Government promotes e-services system characterised by client-centred features, whether the services are for physical persons or for other entities.

Malta is currently at the first phase of the project and has implemented eID Level 1. Services for businesses for advanced eGovernment services requiring digital certificates do exist at this stage but require the Maltese Government to procure digital certificates from a commercial certification

authority. None of the eGovernment services actually require the user to sign electronically, however, as digital certificates are used for the purposes of authentication rather than for signing.

In order to get access to eGovernment services (at Level 1) a person must register and obtain an eID.

The eID is applied for by presenting the ID Card and a valid e-mail address to a Local Council office. The ID Card is photocopied at the Local Council and a digital photo of the person is also taken. Details submitted are then forwarded to the Registration Authority (Accerta), which performs validity checks and sends the applicant a first-time password through the registered e-mail address and an activation PIN number by post. These passwords and activation PIN numbers enable citizens to activate eID-related services that are currently available.

The unique identifier that is the basis for identification for the provision of an eID is therefore the National Identity Card.

It has been recently announced that Level 2 and Level 3 authentication – based eIDM systems will be implemented in the very near future (in 2007). Level 2 will involve the general distribution of digital certificates, and Level 3 – the implementation of smart ID Card – ID Card with embedded digital certificates, that will replace the current ID Card. The Government PKI infrastructure, including the setting up of the Certification Authority, is expected to be set up very shortly in line with the move to Level 2.

The Government has recently announced that it is carrying out a reorganisation exercise with respect to its eIDM systems. The main aim of this exercise is to rationalise the systems and to create a more manageable, integrated eIDM platform. The plan is to integrate the systems, to launch the Certification Authority in order to move to Level 2, as well to launch an integrated eServices portal.

The Government site (www.gov.mt) currently used as the main government portal through which ministries', departments', and authorities' websites can be reached for e-services provided via such other websites will shortly be replaced by another portal. The Government has just announced that this new portal (www.mygov.mt) will be launched shortly for an integrated, one-point entry access to all eGovernment services. This portal will contain links to all eservices, will build up the profile of services used by entities and will also recommend relevant e-services to the users. The new portal will be used, unlike in the current scenario, by entities to apply for eIDs and also to manage e-services.

The amended eIDs will allow entities to manage their identities, including their involvement with other entities. Thus, a person will be able to register for eID and to manage various capacities in which that person accesses eGovernment services (i.e., personal, as a director of a company, etc). Delegation, in a particular capacity, to a trusted person will also become possible.

As far as organisations are concerned, the new approach to eID will allow all kinds of organisations to have access to relevant eGovernment services. The organisation would nominate one person as the authorised manager authorised to act as such. The manager would then be able to create groups with various access levels and manage them.

Within the reorganised eIDM system, all identities will be issued and managed within the integrated core infrastructure and the authentic source principle will be adhered to.

3.3.2 Legal framework

Legislation relevant to eIDM is as follows:

- The Electronic Commerce Act,[5]
- The Electronic Commerce (General) Regulations 2006 (L.N. 251 of 1006)
- The Electronic Communications (Income Tax) Regulations[6] constituting the legal framework to support the validity of some electronic services that can be provided by the Inland Revenue Department
- The Public Contracts Regulations: Legal Notice No. 177 Public Contracts Regulations 2005 and Legal Notice No. 178 Public Procurement of Entities operating in the Water, Energy, Transport and Postal Services Sectors Regulations, 2005 both published in the Government Gazette No. 17775 dated 3rd June 2005. These Legal Notices complete the legislative framework for the use of electronic signatures in public procurement and provide for the opportunity to use electronic auctions and dynamic purchasing systems.
- The Data Protection Act
- The Criminal Code: amendments have been made to the Criminal Code in order that computer misuse has been rendered a criminal offence.
- The Electronic Commerce Act,[7] (hereinafter referred to as the eCommerce Act) entered into force in 2002. It lays down the main regulatory framework encapsulating eCommerce legislation and was modelled on the UNICTRAL[8] Model law for Electronic Transactions and the EU Directives for Electronic Commerce and Electronic Signatures respectively. The eCommerce Act establishes the legal equivalence of paper-based transactions with electronic ones, the parameters within which electronic contracts are to be concluded, and the regulatory frameworks for the provision of electronic signature certification and intermediary services.

The currently used ID cards are mandated by the Identity Card Act, but the Act does not have any provision relating *specifically* to the eID card. The Act, whcih mandates identity cards for every person from the age of fourteen, provides that “an identity card shall be made of such material and in such manner as in the opinion of the authorised officer provide adequate security against forgery, tampering or alteration thereof, and it shall, in any case, include a limited area where machine readable coded information may be inserted”. This provision, in our view, can serve as an enabler for eID.

[5] Chapter 426 of the Laws of Malta, subsequently amended by Legal Notice 251 of 2006.

[6] Subsidiary Legislation 372.23.

[7] Chapter 426 of the Laws of Malta, subsequently amended by Legal Notice 251 of 2006.

[8] United Nations Commission for International Trade Law.

The Identity Card Act explicitly specifies the information to be stated on the card and allows for any additional details to be included "as the authorised officer may deem appropriate". However, it also provides that machine readable information contained in the card cannot contain any information not included in the card. This provision may need to be amended in view of any additional data that the eID card may have in machine readable format.

The Electronic Commerce Act deals with electronic signatures and provides for the existence of certification authorities, but does not deal with authentication per se.

Whilst all Maltese citizens over the age of fourteen are required to have an Identity Card, this need not be electronic. Therefore electronic authentication systems are not mandatory to anyone at the current time; users are free to choose whether or not to use eGovernment services, and will only be required to provide authentication at such time of usage. Authentication systems currently operate at Level 1 (username and password only); however there are some which require a different authentication system as explained above.

It is to be noted that all major eGovernment applications (including PKI based applications) currently operate using the abovementioned authentication mechanisms as a substitute for e-signatures; and that e-signatures in the strict sense of the word are not currently in use, since no data is actually signed.

The Electronic Communications (Income Tax) Regulations[9] constitute the legal framework to support the validity of some electronic services that can be provided by the Inland Revenue Department. These relate to the use of electronic communications to the use of electronic communication:

- to make and deliver income tax returns;
- to pay provisional tax;
- to submit payee statements of earnings and payer's annual reconciliation statements.

Access to such requires an eID and electronic registration with the Inland Revenue Department. Article 9 of the Subsidiary Legislation states that electronic communication of returns, forms and documents pursuant to the Income Tax Act and the Income Tax Management Act, shall be considered valid and treated in the same way as paper copies of the same. However the article gives discretion to the Commissioner for Inland Revenue to request paper copies of the submission, the receipt of which should take place within 48 hours of the request being lodged.

With regard to data protection issues, The Data Protection Act (Cap 440 of the Laws of Malta) states that the Office of the Prime Minister (OPM) is responsible to ensure that Data Protection compliance is achieved in all Government Departments. Subsequently, a collaboration agreement was signed between the OPM and the state-owned services company, MITTS Ltd. This agreement relates to a joint effort to coordinate, advise and assist all Government Departments in the implementation of the

[9] Subsidiary Legislation 372.23.

Data Protection requirements in the Public Service so as to bring all Departments in compliance with the Data Protection Act.[10]

Under the Data Protection Act, an ID Card number, which is a unique identifier for every person in Malta, in the absence of consent, can only be processed when such processing is clearly justified having regard to:

(*a*) the purpose of the processing;

(*b*) the importance of a secure identification;

(*c*) some other valid reason as may be prescribed.

The current eID system is available for certain eGovernment applications and is not applicable to the private sector. It is presumed that when the eID that will replace plastic identity card will be issued in such a way as to make it also usable in the private sector. However, no details are available at this stage.

3.3.3 Technical aspects

As explained above, only Level 1 of the project has been implemented so far. This works upon the use of a username and password to be used for the purpose of accessing the eServices which require authentication (described below). There are currently no tokens and no smart cards used. The system is currently not PKI based.

Level 1 has been implemented built on Microsoft Windows Server™ 2003, a multipurpose operating system capable of handling a diverse set of server roles in either a centralized or distributed fashion. It offers a number of security benefits, including capabilities available for public key infrastructure and smart card login. Active Directory®, a central component of the Microsoft Windows® platform, provides a central repository for data and single log-on capability across multiple Web sites. For extra scalability and robustness, Microsoft `SQL Server™ 2000 was also implemented and linked to Active Directory. Active Directory was chosen as it will be able to handle digital certificates and a PKI infrastructure, and even biometric recognition when these parts are implemented. The architecture is scalable and extensive, with XML enabling all future integration capabilities.[11]

The e-Government Technical Architecture is works on a three tier based framework and supports these type of interaction:

[10] Preliminary Study on the Mutual Recognition of eSignatures for eGovernment applications, European eGovernment Services (IDABC).

[11] Preliminary Study on the Mutual Recognition of eSignatures for eGovernment applications, European eGovernment Services (IDABC).

- citizen-to-Government, for which the main paradigm may be HTML and forms. These will be converted by the e-public service portal to XML and XSL – based interactions for e-filing, e-lookup, expectation management etc;
- business-to-government, for which the main paradigm may be XML and XSL data packages and file transfer protocols;
- Government-to-business, for which the main paradigm may be XML and XSL data packages and file transfer protocols.[12]

The current applications use a set of pre-defined web services which were issued by the Maltese Government IT Agency (MITTS), and all applications, which use inbuilt encryption, have to conform to these standards.

The Citizen (or front end) element provides the medium for connectivity by customers to the e-Government Portal. The architecture is premised to provide the ability to add new access channels without technological constraint or implications on the service delivery architecture.[13]

The middle tier is to house the Middleware and will provide the common infrastructure to support the transportation of messages to obtain the appropriate level of authentication and access the services or information. Common information-based services will also be housed within the middle tier including, for example, common search facilities to provide information across the range of services contained within the Portal service set. Other components could include, for example, a feed mechanism identifying the next appropriate service or other appropriate delivery channels for the customer based on sample usage. Data Protection auditing should also be provided in the Middle tier to ensure that information relating to specific services is only sent to the appropriate Department to safeguard the rights of the individual.[14]

The Government element (back end) provides for the connectivity from the Departmental systems, including legacy systems, to the Transaction Management System, hosted within the Middleware layer, through appropriate interface systems. This layer will “ring fence” existing systems. Its isolation layer should allow ongoing development of the Departmental systems without a knock-on development requirement on the Portal architecture.[15] The main back-office components are a centralised repository of identity attributes linked to the Common Data Repository application maintained by the Maltese Government.

Previously, an consortium ‘Accerta’ was declared by the Government as the entity to perform the functions of Certification Authority. However, in 2007 the Government announced that Accerta would only perform the functions of a Registration Authority (and, in fact, it has been carrying out these functions with respect to eID registration process), while MITTS, the Government IT agency will perform the functions of the Certification Authority.

The Certification Authority (CA) would be issuing digital certificates upon the approval of an entity by the Registration Authority. The Certification Authority duties will include the establishing of the PKI

[12] Governement Website: The Government Technical Architecture Framework: http://www.gov.mt/egovernment.asp?p=111&l=1

[13] ibid

[14] ibid

[15] ibid

infrastructure and hierarchy, technical security controls, physical, management and operational controls and putting in place certificate revocation mechanism. The PKI hierarchy will include the government root CA, which will be self-signed and signing the intermediate CA. It has been announced that software certificates will be used. Digital certificates will be used for authentication and for signatures.

The PKI infrastructure will be complaint with FIPS 140-2 security requirements for cryptographic modules. It has been announced that the CA will not keep in its possession the private key of the key-pair. The CA will be hosted at the Government data centre.

The CA will implement and maintain the Certificate Revocation Lists, which will be signed and time-stamped. It is planned to have the real time status checking facility and the relying parties will be able to presume that the certificate is not revoked when it is not on the List.

It is planned that the information to be made available to relying parties will include the name, surname, the digital certificate information and its unique number, which will be linked to the unique identifier (ID card number), however the ID card number itself will not be visible.

No biometric information is currently used.

MITTS maintains the ICT and eGovernment standards and policies which are publicly available at http://ictpolicies.gov.mt

3.3.4 Organisational aspects

The eID is applied for by presenting a copy of the plastic ID card and a valid e-mail address to a Local Council office. Details are submitted to the Registration Authority, which performs validity checks and sends the applicants a first-time password through their registered e-mail address and an activation PIN number by post. These passwords and activation PIN numbers enable citizens to activate eID-related services that are currently available.

No federated identities are in use. Role management is not used at this time, but each service (e.g. VAT services or tax return services) can have service-specific information associated with it. For example, a system is in place for a corporate entity to authorise its tax practitioner for the purposes of electronic submission of returns to the Inland Revenue Department.

The eID user can view his/her account details and inform the eID administrator and/or the purposely set-up Help Centre if any discrepancies are noted. The eID user further has to opt-in to each eID service, thus implicitly giving permission for the use of eID data.

Please refer to the section above for the proposed amendments / improvements.

3.4 Interoperability

The fact that each and every Maltese citizen already has a national ID Card facilitates the implementation of the eID system. Since Malta is a small country, the entire eID system can be treated as a single system without any real interoperability issues. Currently only individual citizens use the eID system.

As mentioned above, the eIDM structure currently in use is a Level 1 authentication system consisting of username and password available to Maltese citizens on presentation of their national Identity Card. At this time there is no official information as to whether and in what way interoperability of foreign eID cards will occur. The Electronic Commerce (General) Regulations 2006 however provide that the use of signature products originating from outside Malta and which comply with the Electronic Signature Directive shall not be subject to any restrictions.[16] It should also be noted that foreign citizens can also apply for a Maltese Identity Card as mentioned above.

3.5 eIDM Applications

There are in total 21 e-services offered by the Government. The services represented below are those requiring eID authentication and are categorised by Ministry.

- **Ministry for the Family and Social Solidarity**

  eServices www.mfss.gov.mt and through Automated Call Centre
- **Ministry for Health, the Elderly and Community Care**

  eHealth Portal www.ehealth.gov.mt
- **Ministry for Justice and Home Affairs**

  Online Renewal of Passports http://www.passaporti.gov.mt
- **Ministry of Finance**

  Corporate taxes Online Services http://www.ird.gov.mt

  Order of Fiscal Receipts Books http://www.vat.gov.mt

  Final Settlement System http://www.ird.gov.mt

  VAT Online Services http://www.vat.gov.mt

The following eGovernment services, which use a different authentication system to the username and password authentication system:

[16] Section 10(2) Electronic Commerce (General) Regulations 2006

(i) the Inland Revenue Department's (IRD) eGovernment services[17] for:
   a. on-line submission of social security forms (for employers who employ ten or more employees)
   b. on-line submission of tax and social security forms and the related payments of tax contributions (for Tax Practitioners for their corporate taxpayers)

(ii) the Vehicle Licenses Online[18] for:
   a. vehicle-owners who wish to pay their road license online
   b. vehicle-owners who wish to check the due date of the next Vehicle Roadworthiness Testing
   c. Insurance agents who wish to provide the road-license payment to their clients through an authenticated login

Online completion of a personal income tax return and the payment for the self-assessment are accessed using eID. All the other services require a digital certificate, which is supplied by the department upon application from employers and tax practitioners. Similarly the Malta Transport Authority offers the same type of digital certificates to Insurance agents. These digital certificates are procured by Government from a Commercial certification authority as already mentioned.

In April 2006 the Malta Transport Authority launched 'Vehicle Licenses Online' this does not use eID as its method of authentication but requires the user to enter the following information:

- Vehicle Registration Number
- ID Card/Passport Number
- Last 4 characters of Engine Number

Specific emphasis is made on Public Procurement and the status of eSignatures in related processes. The use of eSignatures is central to establishing operational eProcurement systems across the EU. eProcurement is expected to constitute one of the major fields of eSignature application, especially the more advanced ones. The challenge lies in implementing eSignatures across Europe for eProcurement without creating barriers to cross-border trade. As outlined above the use of electronic means for communications in the public procurement procedures is regulated by Chapter 174 of the Laws of Malta.

The eGovernment online system for public procurement is found at http://www.contracts.gov.mt. This site is however an information site with dynamic content being restricted to Adobe PDF documents which are published regularly to give updates on latest adverts and notifications and awarded contracts and no authentication or electronic signing is required.

The e-Procurement eGovernment service (www.e-procurement.gov.mt) is restricted to the request for quotation of IT Desktop Equipment which costs less than Lm2,500. This eGovernment service is intended for use by Quality Mark Suppliers, and Purchasing Officers from Government Ministries, Departments and Public Sector entities connected to the Malta Government Wide Area Network (MAGNET), who may request quotations for the required equipment. The suppliers may then submit

[17] Website available at: http://www.ird.gov.mt and eGovernment may be accessed directly from http://ird.gov.mt/secureservices.aspx

[18] Services available online from: http://www.licenzji-vetturi.gov.mt

their quotations. The website does not use eID authentication but a username and password sent to suppliers upon approval of their application to become authorised vendors.

The only major applications involving eID are those used by the banks and they do not rely on the eIDM systems of the Government.

3.6 Future trends/expectations

Future plans for eIDM systems will bring about stronger authentication levels by implementing Level 2 and Level 3 authentication eIDM systems. This is likely to be in the form of a chip placed within the plastic ID, containing details and an electronic signature. This will probably be used in for private and public services. An additional number of eServices are likely to be rolled out concurrently. Horizontal integration will be in place so that a citizen need not apply and submit his details twice.

The Government is in the process of identifying a Strategic Partner for National Identity Management Systems (NIDMS). The NIDMS will be used for core identity management processes, including the issuance of eID Card and electronic passports. It will also be used to develop national electronic register of persons, to be populated during the registration process for the eID Card. No further information is publicly available at this time. It is likely that, due to the fact that a national ID card is compulsory, the eID Card will also be mandatory, possibly after a transitory period.

3.7 Assessment

The Maltese approach has a number of advantages and disadvantages, which can be briefly summarised as follows.

3.7.1 Advantages:

The eID system in Malta is still in the initial stages. However plans are in place for the implementation of an all-encompassing system, allowing additional features to be added in stages. The eID should be applicable to both private and public services and when implemented will bring about a high degree of practicality amongst Maltese citizens.

3.7.2 Disadvantages:

The system as it currently stands cannot be said to be fully catering to users' needs or be very practical. The level of authentication required at this stage is still very basic, and therefore the number of eServices requiring authentication is not large; moreover, the lack of horizontal integration means the process is not a practical one.

This has resulted in a slow up-take of the eID process. It is also submitted that the Maltese citizen is not sufficiently aware of the services available, of the registration procedure and of the security features of the eID. In our view, the Maltese citizen therefore tends to be sceptical of these measures.

Accessibility to non-nationals is also problematic at this stage. It is submitted that eID is not required for non-nationals currently, as most of the eServices requiring authentication are not relevant to most non-Maltese citizens. However, as the process in Malta enters further stages, the matter will have to be dealt with specifically. Unfortunately there is no information publicly available as to how this will be implemented in the future.