Certification Practice Statement for the Government of Malta Electronic Identity System

OID : 2.16.470.4.1.1.1

Acknowledgments

This CA CP/CPS endorses in whole or in part the following industry standards:

- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework (obsoletes RFC 2527).
- RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.
- RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile.
- ISO/IEC 27001:2005 and related standards on information security and infrastructure.

This CA CP/CPS endorses in whole the following industry standards:

- ETSI TS 101 456 v1.4.3 (2007-05): Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Authorities issuing Qualified Certificates.
- ETSI TS 101 862 v1.3.3 (2006-01): Qualified Certificate profile.

Document Control

Reviewers

Current version	Name	Date
Prepared by	De La Rue / Verizon	
Reviewed by	SEALED / Arthur Cox / MITA	
Approved by	MECS Chairman	Effective 10.01.2013

Change Record

Version	Date	Author	Status/Description
1.0	10/01/2013	Malta Certification Authority	Issued for acceptance
1.1	15/07/2015	Malta Certification Authority	Updated to reflect • CRL partitioning and CRL publishing frequency change for Malta Citizen eID CA, and • CRL publishing frequency change for Malta Resident eID CA

1. INTRODUCTION

1.1. *Overview*

1.1.1. *Introduction to the Malta Government Identity System*

The Government of Malta operates a national identity card for citizens and residents as defined within the Identity Card Act, Chapter 258 Laws of Malta. This national identity card is currently used to facilitate interactions between Maltese citizens, residents between themselves, the Government of Malta, any private business relying on eID cards, within and beyond Malta.

The Government of Malta has launched the Electronic Identity Card project for Citizens, and an Electronic Resident Card for Residents, to provide them with the levels of trust and confidence necessary for them to interact with systems approved by the Government of Malta.

The Government of Malta supports the following cards within the national Electronic Identity Card scheme:

- National Electronic Identity Card, for use by Citizens;
- National Electronic Resident Card for use by Residents of Malta, and;
- Administrator Card for use by National Identity Management System administrators.

The National Identity Management System supports strong authentication and electronic signature by using a chip-embedded card that hosts two digital Certificates. One Certificate is dedicated for the authentication purpose and will be formatted according to the X509 standard [1]. The other Certificate is dedicated for the Electronic Signature purpose and is formatted according to the Qualified Certificate standards [3] and [6] and the Maltese Electronic Commerce Act [10]. The Certificates are embedded within cards that have been certified as meeting the control requirements defined within the Protection Profile for a Secure Signature Creation Device [13].

In this framework, the Certification Authorities that create and then manage the Certificates within the citizens and residents Electronic Identity Card are duly supervised by the Malta Communications Authority as per Articles 16 and 17 of the Maltese Law on ecommerce and Article 3.3 of the eSignature Directive 1999/93/EC [12].

The Certification Authorities that create and then manage the Certificates within the national Electronic Identity Card follow the certification practices described within this CPS and the associated Certificate Policies.

1.1.2. *CP and CPS Overview*

A CPS addresses the technical, procedural personnel policies and practices during the complete life-cycle of certificates as issued by a CSP.

A Certificate Policy is a "named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements".

This Certification Practice Statement (CPS) addresses the technical, procedural personnel policies and practices during the complete life-cycle of certificates as issued by the GOM eID PKI and is also a certificate policy in a broad sense. It meets the formal requirements of Internet Engineering Task Force (IETF) RFC 3647, dated November 2003 with regard to content, layout and format.

An RFC issued by IETF is an authoritative source of guidance with regard to standard practices in the area of Electronic Signatures and Certificate management. While certain section titles are included in this CPS according to the structure of RFC 3647, the topic may not necessarily apply in the implementation of the Certificate management services of the Government of Malta Electronic Identity Public Key Infrastructure (GOM eID PKI). These sections have been removed from this document. Where necessary additional information is presented as subsections added to the standard structure. Additional assertions on standards used in this CPS can be found in the “Acknowledgements” section.

The present CPS is used to convey legal conditions of usage to subscribers, relying parties, etc. The information contained in this document is also intended for personnel responsible for the management and operation of the GOM eID PKI, including the Government of Malta Root Certification Authority (GOM Root CA) and the subordinate Certification Authorities including the Malta Citizen eID CA, Malta Resident eID CA and the GOM Administrator CA.

The level of detail provided in the CPS is determined by the risk resulting from the possible harmful exploitation of the information disclosed. Within this CPS there are a number of references to documents that describe aspects of PKI activity or enforce compliance at a more detailed level. In addition, a number of other similar documents are implied, although not specifically referenced, in the CPS.

This information is part of internal Information Security Policy documentation set that Policy Management Authority uses to manage the PKI. These documents are not normally published or disclosed to the public. This information is made available to Auditors, Assessors and those that require to conduct detailed review of the PKI and its operations

As it is one of the roles of these Auditors to assess the PKI compliance against this CPS, the effectiveness of all these documents referenced in this CPS ensured through the audit process.

Should specific details of any such documents or content therein be required the Policy Authority shall, upon application make the appropriate information available to the applicant commensurate with the security controls of the PKI.

Request for information and any other inquiry associated with this CPS can be addressed to:

Malta Certification Authority
Gattard House
National Road
Blata l–Bajda
Malta

1.2. *Document name and identification*

This document is the Government of Malta Electronic Identity Public Key Infrastructure (GOM eID PKI) Certification Practices Statement (CPS).

It can be identified by any party through the following OID: 2.16.470.4.1.1.1

1.3. *PKI participants*

The PKI participants within the GOM eID PKI are identified as follows:

- Policy Management Authority as described in section 1.3.1
- Certification Authorities as described in section 1.3.2
- Registration Authorities as described in 1.3.4
- Revocation Authorities as described in 1.3.6
- Subscribers as described in 1.3.3
- Relying Parties as described in 1.3.7
- Other Participants as described in 1.3.8

The parties mentioned here above are collectively called the PKI Participants. All these PKI Participants are required to implement practices, procedures and controls meeting the requirements as stated in the present CPS.

The organisation responsible for the GOM eID PKI is the Malta Certification Authority (MCA). The MCA is the legal entity that acts as the Certification Service provider (CSP), as defined within the eSignature Directive 1999/93/EC

1.3.1. *Policy Management Authority*

The Policy Management Authority is the management team that acts on behalf of the Malta Certification Authority. Its main goal is to define, supervise and maintain the overall framework of Malta PKI system including the definition of the policies under which the Malta eID PKI system operates.

The Policy Management Authority on behalf of the Malta Certification Authority is responsible for:

- Specifying and validating the Malta eID CPS, supported CPs and their revisions;

- Supervising the correct implementation of the CPs in conformance with the CPS, and;

- The definition of the review requirements and processes relating to the implementation of the Malta eID CPS and supported CPs.

1.3.2. *Certification Authorities*

A Certification Authority is defined as an organisation that issues Certificates that are used in the public domain or within a business or transaction context.

The GOM eID PKI includes the following Certification Authorities:

- Government of Malta Root CA (GOM Root CA)
- Malta Citizen Electronic Identity CA (Malta Citizen eID CA)
- Malta Resident Electronic Identity CA (Malta Resident eID CA)
- Government of Malta Administrator CA (GOM Administrator CA)

The relationship between these Certification Authorities is illustrated in the following figure:

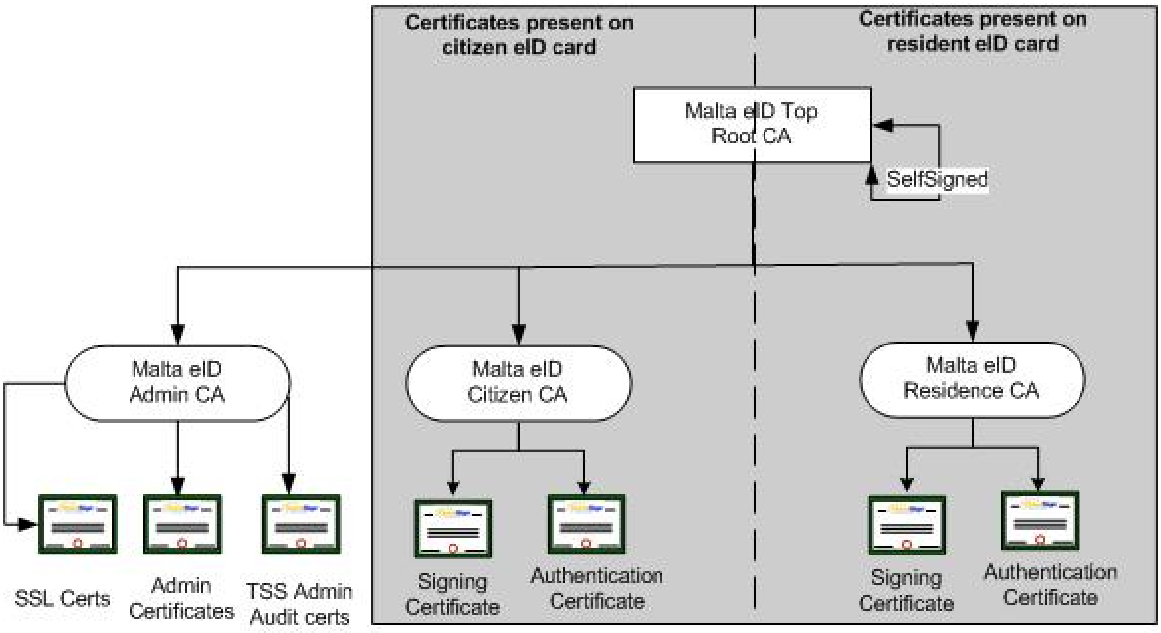

Figure 1: GOM eID PKI hierarchical architecture

1.3.2.1. GOM Root CA

The GOM Root CA is the highest trust point within the GOM eID PKI and certifies the other PKI entities within the GOM eID PKI.

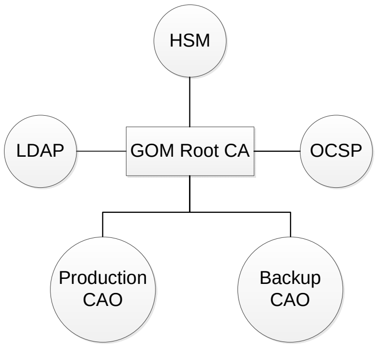

Figure 2 Logical structure for GOM Root CA

The GOM Root CA issues the following Certificates:

- GOM Root CA Certificate (self-signed)
- CA Certificates for the following Certification Authorities:
  - Malta Citizen eID CA
  - Malta Resident eID CA
  - GOM Administrator CA
- GOM Timestamp Server Certificate
- GOM OCSP Responder Certificate
- CA Officer Certificates for management of the GOM Root CA
- Internal Certificates used by the PKI software components

1.3.2.2. Malta Citizen eID CA

The Malta Citizen eID CA issues and then manages the (2) Certificates that are embedded within the Electronic Identity Card for the following usage:

- Authentication for persons over 14 years of age
- Electronic Signature (Qualified Certificate), for persons over 16 years of age

In addition, the Malta Citizen eID CA issues the following Certificates:

- Certificates for management of the Malta Citizen eID CA (keys stored on secure hardware)
- GOM OCSP Responder Certificate

1.3.2.3. Malta Resident eID CA

The Malta Resident eID CA issues and then manages the (2) Certificates that are embedded within the Electronic Resident Card for the following usage:

- Authentication for persons over 14 years of age
- Electronic Signature (Qualified Certificate) for persons over 16 years of age

In addition, the Malta Resident eID CA issues the following Certificates:

- Certificates for management of the Malta Resident eID CA (keys stored on Secure Hardware)
- GOM OCSP Responder Certificate

1.3.2.4. GOM Administrator CA

The GOM Administrator CA issues and then manages the (1) Certificate that is embedded within the Administrator Card for the following usage:

- Authentication

In addition, the GOM Administrator CA issues the following Certificates:

- Certificates for management of the GOM Administrator CA (keys stored on secure hardware)
- Internal SSL Certificates (client and server) for use by NIDMS
- Internal Signing Certificate
- GOM OCSP Responder Certificate

1.3.3. *Subscribers*

A Subscriber is the person who applies for a Certificate. Within the GOM PKI there are several types of Subscribers:

- Card applicant

A Subscriber “card applicant” is the person who applies for a Certificate. For the GOM eID PKI the Subscribers are also the holders of the appropriate Electronic Identity Card.

So within the GOM eID PKI there are the following classes of Subscriber:

- Citizens who are Subscribers to the Malta Citizen eID CA and who will hold a National Electronic Identity Card;
- Residents who are Subscribers to the Malta Resident eID CA and who will hold a National Electronic Resident card, and;
- Administrators who are Subscribers to GOM Administrator CA who will hold an Administrator card.

Note that an Administrator will hold their Administrator card in addition to their National Electronic Identity card or National Electronic Resident card.

- Internal PKI certificates subscribers

In addition, a number of internal PKI roles are also defined (for example the CA Officer) where natural persons are issued Certificates for administrative and maintenance purposes purely within the eID PKI itself.

A number of the software components within the GOM eID PKI are also issued Certificates, for example, to establish a secure and authenticated connection. The

Subscriber for these Certificates will be the person responsible for the software component in whose name the application was made.

Details on the specific applicability, usage and community that apply to each End Entity Certificate class are described in the appropriate Certificate Policy documents.

- eID CAs

The GOM eID CAs request certificates to the GOM Root CA, which is the highest trust point within the GOM eID PKI and certifies the other PKI entities within the GOM eID PKI. This is detailed in the "eID CAs Certificate Policy.".

1.3.4. *Registration Authorities*

The Registration Authority is the entity that undertakes to identify and authenticate Subscribers on behalf of a CA.

The Registration Authority for the issuing Certification Authorities within the GOM eID PKI is linked directly to the National Identity Management System (NIDMS) in charge of the Citizens and Residents eID cards and related certificates issuance process, as the cards' Certificate key pairs are always generated within the card and remain embedded within it. NIDMS Cards issuance process is described in section 1.3.5.

The Certification Authorities within the GOM eID PKI also support a direct Registration Authority interface, for use solely for the issuance and maintenance of the internal GOM eID PKI certificates. For this purpose, the Certificate Authority Officer (CAO) will be permitted to perform manual registration only for Certificates used internally by the GOM eID PKI functions and devices (for example SSL certificates) using procedures approved by the GOM eID PKI. The GOM eID PKI has introduced a combination of physical, logical, procedural and cryptographic controls over the use of the CAO credentials to perform such certificate management. In addition, all actions performed using these credentials will be associated with a named individual and recorded within a secure log for subsequent management review.

1.3.5. *National Identity Management System*

1. Citizens eID card and related certificates issuance process

The Identity Management Office (IDMO) is responsible for the processes associated with the registration, validation and issuance of the Electronic Identity Cards in conjunction with their associated embedded Certificates and Private Keys.

1.1 Initial registration process

Citizens must apply for the Electronic Identity Card by completing an initial registration process at a Local Registration Authority Office where their credentials are validated and biometric data captured by the Local Registration Authority Officer (LRAO).

1.2 Request for card and keys generation

Upon successful completion of this initial registration process, the Local Registration Authority Administrator (LRAA) shall authorise the generation of an Electronic Identity Card.

1.3 Card personalisation

A card is then personalised for the Citizen using details entered into the system by the LRAO, approved by the LRAA. Keys for authentication and signing Certificates are generated within the card itself and two certification service requests are created and sent to the citizen eID CA.

1.4 Certification

The certification requests are processed by the Citizen eID CA and the generated certificates are returned to the card personalisation system.

1.5 Card completion and testing

Upon completion of the request the associated Public Key Certificates are then stored upon the card with their citizen eID Certification Authority Certificate chain to complete the trust chain. That is, the Public Key Certificates for the generated keys shall be stored along with the Public Key Certificates of the issuing sub-CA and GOM Root CA.

The card is tested from a functional quality point of view and if it passes, it is approved to be issued by the Central Registration Authority Administrator and transported to the registration office.

1.6 Hand over to citizen

The card is handed over to the citizen when (s)he returns to the registration office and signs the Subscriber Agreement that governs the card usage, obligations, security and functionality for the user to personally agree in writing for its safe handling.

1.7 PIN (or “activation data”) hand over to citizen

The Personal Identity Numbers (PINs) required to use the authentication and signing Certificates on the cards are sent independently to the registered address of the applicant.

Further information on the process can be found within the *Certificate Policy for Malta Citizen eID Digital Signature (QC) and Authentication Certificates.*

2.Residents card and related certificates issuance process

The Department of Expatriates and Citizenship / Ministry of Foreign Affairs (MFA) is responsible by delegation from the Identity Management Office (IDMO) for the processes associated with the registration, validation and issuance of the Resident Identity cards in conjunction with their associated embedded Certificates and Private Keys.

Applications for a Residents card follows a registration process similar at a high-level to the process described for applications by Citizens applying for a National Electronic identity card. In the case of resident cards, the details are passed to the Malta Residence eID CA and the certificates stored within the Electronic Resident Card.

Further information on the process can be found within the *Certificate Policy for Malta Resident Digital Signature (QC) and Authentication Certificates*.

3. Administrator cards

The Malta Certification Authority is responsible for the processes associated with the registration, validation and issuance of the Administrator cards in conjunction with their associated embedded Certificates and Private Keys.

Applications for an Administrator card follow a registration process similar at a high-level to the process described for applications by Citizens applying for a National Electronic identity card. In the case of administrators cards the approved details are passed to the GOM Administrator CA and the certificate stored within the Administrator Card.

Further information on the process can be found within the *Certificate Policy for GOM eID Administrator Certificate*.

1.3.6. ***Revocation Authorities***

The Suspension and Revocation Authority (SRA) is the authority that undertakes to validate requests for certificates suspension, unsuspension and/or revocation, and that transfers duly authenticated requests to the CA for action.

The Identity Management Office (IDMO) shall be the SRA for Electronic Identity Cards and Residence Permit Cards.

Requests for revocation / suspension / unsuspension of certificates can only be made by:

a) holders of e-ID Cards or of e-Residence Documents (hereinafter referred to as Identification Documents);
b) any person who has a power of attorney to manage Identification Documents on behalf of the holders;
c) any reliable third-party which shall be established as such by the IDMO – this applies, in particular (but not limited to) in cases when the holder is declared to be deceased or following the issuance of a court order).

when one or more of the circumstances for revocation detailed in Section 4.9.1 of this CPS are met. The revocation processes are described within the applicable separate Certificate Policy (CP).

The Certification Authorities within the GOM eID PKI also support a direct Revocation of internal PKI certificates interface: the Certificate Authority Officer (CAO) will perform manual suspension and/or revocation for certificates issued by the GOM eID PKI using procedures approved by the GOM eID PKI. The GOM eID PKI has introduced a combination of physical, logical, procedural and cryptographic controls over the use of the CAO credentials to perform such certificate management. In addition, all actions performed using these credentials will be associated with a named individual and recorded within a secure log for subsequent management review.

1.3.7. *Relying Parties*

A Relying Party is any natural person or legal entity that relies upon an Electronic Signature created using a Private Key, where the Public Key has been certified as being valid and genuine by a Certification Authority.

For the Certificates and associated Private Keys embedded within the National Identity Cards, the Relying Parties will include all who rely upon Electronic Signatures created using the Private Key associated with the Qualified Certificates or using the Private Key associated with the authentication certificate held within the Electronic Identity Card and/or Electronic Resident Card.

The Certification Authority does not authenticate the content of any message signed using an Electronic Signature and accordingly does not entertain any liability or risk in relation thereto.

1.3.8. *Other Participants*

The GOM eID PKI includes the following other entities:

- The GOM Timestamp Server, signed by the GOM Root CA. The GOM Timestamp Server is linked to a predictable and consistent time source to ensure that it maintains accurate time, and;
- OCSP Server. The GOM eID PKI supports the use of the Online Certificate Status Protocol to provide Certificate status details to Relying Parties.

1.4. *Certificate usage*

1.4.1. *Appropriate Certificate uses*

The GOM eID PKI currently supports the use of the following main types of Certificates.

GOM eID PKI Certificates:
- Root CA Certificate (self-signed);
- CA Certificates;
- OCSP Certificates;
- Certificate Authority Officer (CAO) Certificates.

End Entity Certificates:
- Electronic Identity Card Authentication Certificates;
- Electronic Identity Card Digital Signing Qualified Certificates;

- Residence Card Authentication Certificates;
- Residence Card Digital Signing Qualified Certificates;
- Administrator Authentication Certificates, and;
- SSL Client and Server Certificates (for NIDMS).

These certificates are briefly described below. For each class of End Entity Certificate, the specific usage, applicability and community is defined within a separate Certificate Policy (CP). Further details about the Root CA Certificate, CA Certificates and the CAO Certificates are defined later within this CPS.

The Root CA Certificate is a special class of self-signed Certificate that is generated by the GOM Root CA to itself, as the highest trust point within the GOM eID PKI. They may not be used for any other purpose.

The Root CA Certificate is embedded within the Electronic Identity Cards or Electronic Resident Card.

CA Certificates are a special class of Certificates that are issued to the GOM eID Certification Authorities by the GOM Root CA. CA Certificates are used by the Certification Authority to sign the Certificates for other PKI entities (for example an OCSP server), sign Certificates from the Subscribers and to sign Certificate Revocation Lists. They may not be used for any other purpose.

The following Subscribers are issued with CA Certificates by the GOM Root CA:

- Malta Citizen eID CA
- Malta Resident eID CA
- GOM Administrator CA
- GOM Time Stamp server
- GOM Online Certificate Status Protocol (“OCSP”) responder

The issuing CA Certificate is embedded within the Electronic Identity Cards or Electronic Resident Card.

OCSP (Online Certificate Status Protocol) Responder Certificates are generated by the Certification Authorities that publishes Certificate status information to the GOM OCSP Responder.

Within the GOM eID PKI the following CAs will generate a Certificate for the GOM OCSP Responder:

- GOM Root CA
- Malta Citizen eID CA
- Malta Resident eID CA
- GOM Administrator CA

CAO Certificates are a special class of Certificates that are issued to natural persons who are performing the role of Certification Authority Operator. This administrative role is responsible for the maintenance of the GOM Root CA and associated PKI Entities. They may not be used for any other purpose.

Identity card Authentication Certificates are Certificates that are embedded within the Electronic Identity Card issued to Citizens that must only be used for the purpose of user authentication for persons of 14 years of age and above.

The Certificates are issued by the Malta Citizen eID CA following a successful application made by a Citizen through the National Identity Management System.

The authentication Certificate on a Citizen eID card must be used only by the approved card holder and only for the purpose of authenticating the owner of that card into systems approved by the Government of Malta. The authentication Certificate has a single key usage of Digital Signature which is used to guarantee the authenticity of the card holder.

Identity card Digital Signing Certificates are Certificates that are embedded within the Electronic Identity Card issued to Citizens that may only be used for digital signing for persons of 16 years of age and above.

The Certificates are issued by the Malta Citizen eID CA following a successful application made by a Citizen through the National Identity Management System.

Identity card digital signing Certificates are Qualified Certificates as defined within Chapter 426, Laws of Malta.

The Digital Signature (Qualified) Certificate on a Citizen eID card must be used only by the approved card holder and only for the purpose of signing data being submitted into systems approved by the Government of Malta. This Certificate has a single key usage of non-repudiation which means that any signature made on data by the card holder cannot later be disowned by the card holder.

Resident Authentication Certificates are Certificates that are embedded within the Electronic Resident Card issued to Residents that must only be used for the purpose of user authentication for persons of 14 years of age and above.

The Certificates are issued by the Malta Resident eID CA following a successful application made by a Resident through the NIDMS.

The authentication Certificate on an Electronic Resident Card must be used only by the approved card holder and only for the purpose of authenticating the owner of that card into Government of Malta approved systems. The authentication certificate has a single key usage of Digital Signature which is used to guarantee the authenticity of the card holder.

Resident Digital Signing Certificates are Certificates that are embedded within the Electronic Resident Card issued to Residents that may only be used for digital signing for persons of 16 years of age and above.

The Certificates are issued by the Malta Resident eID CA following a successful application made by a Resident through the NIDMS.

Electronic Resident Card Digital Signing Certificates are Qualified Certificates as defined within Chapter 426, Laws of Malta [10].

The Digital Signature (Qualified) Certificate on an Electronic Resident Card must be used only by the approved card holder and only for the purpose of signing data being submitted into systems approved by the Government of Malta. This Certificate has a single key usage of non-repudiation which means that any signature made on data by the card holder cannot later be disowned by that card holder.

Administrator Certificate is a Certificate that is embedded within the Administrator Card issued to natural persons who have the role of Administrator within the National Identity Management System. The Certificate may only be used for Subscriber authentication.

The Administrator Certificates are issued by the GOM Administrator CA following a successful application made by an authorised natural person.

1.4.2. *Prohibited Certificate uses*

The Certificates issued within the GOM eID PKI may only be used for the purpose(s) defined within their respective Certificate Policy and CPS. All other usage outside of this CPS and their Certificate Policy is prohibited.

1.5. *Policy administration*

1.5.1. *Organization administering this CPS*

The Organisation administering this document is the Malta Certification Authority.

1.5.2. *Contact person*

Contact Person	**The CA Manager**
Postal Address	**Gattard House** **National Road** **Blata l-Bajda** **Malta**
Phone:	(356) 2123 4710
Fax:	(356) 2123 4701

1.6. *Definitions and acronyms*

Definitions:

Administrator: A natural person who performs a function within the National Identity Management System for the enrolment of individuals and the issuance of the appropriate National Identity Card.

Administrator Card: A card that is issued to natural persons who have the role of Operators and administrators within the National Identity Management System. The Administrator Card contains an embedded Certificate for authentication.

Advanced Electronic Signature: an Electronic Signature that meets the following requirements:

- It is uniquely linked to the signatory;
- It is capable of identifying the signatory;
- It is created using methods that the signatory can maintain under his sole control; and
- It is linked to the data to which it relates to in such a manner that any subsequent change of the data is detectable.

Agreements: The Subscriber Agreement and the Relying Party Agreement, each of which incorporates the terms of this CPS by reference.

Certification Authority (CA): has the meaning set out in paragraph 1.3.1.

Certificate: An electronic attestation which links signature verification data to a person and confirms the identity of that person.

Certificate Authority Operator (CAO): A person who has an administrative role within the Certification Authority.

Certificate Policy (CP): A named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements.

Certificate Validity Period: The time interval during which the CA warrants that it will maintain information about the status of the Certificate. (Time interval between start validity date and time and final validity date and time).

Certificate Revocation List (CRL): A signed list indicating a set of Certificates that are no longer considered valid by the relevant Certification Authority.

Certificate Trust Chain: An ordered list of Certificates that contains the end-entity Certificate, intermediary Certificates and the Certificate for the Root CA such that a Relying Party may follow the trust chain up to and including the top level trust anchor. Within the national identity cards the full Certificate Trust Chain is embedded within the card at the time of issuance and is not subsequently updated on the card. For example, the Certificate Trust Chain for the authentication Certificate contained on an Electronic Identity Card would comprise the Public Key Certificates for the authentication Certificate, the Malta Citizen eID CA and the Malta Root CA.

Certification Service Provider (CSP): An entity or a legal or natural person who issues Certificates or provides other services related to Electronic Signatures.

Certification Practice Statement (CPS): This document. A formal statement of the practices which a Certification Service Provider employs in issuing, managing, revoking, and renewing or re-keying Certificates.

Citizen: A person who resides in Malta and has Maltese nationality.

CRL Distribution Point: A directory entry or other distribution source for CRLs; a CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of Certificates issued by one CA or may contain revocation entries for multiple CAs.

Digital Signature: is an electronic signature created through the use of public key cryptography

Electronic Signature: means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication

Electronic Identity Card: A National Identity Card that is issued to Citizens through the National Identity Management System. The identity card contains an embedded Certificate for authentication for persons over 14 years of age and an embedded Qualified Certificate for signing for persons over 16 years of age.

Electronic Resident Card: A National Identity Card that is issued to residents of Malta through the National Identity Management System. The residence card contains an embedded Certificate for authentication for persons over 14 years of age and an embedded Qualified Certificate for signing for persons over 16 years of age. The Electronic Resident Card may take a number of physical forms, including the Resident Permit and Resident Document as determined by the Government of Malta.

End Entity Certificate: has the meaning set out in paragraph 1.4.1.

GOM eID Certificate Authority: The term used to refer to the subordinate certification authorities within the Government of Malta Electronic Identity Public Key Infrastructure (GOM eID PKI). This term will include the Malta Citizen eID CA, the Malta Resident eID CA and the GOM Administrator CA.

GOM eID PKI: The term used to refer to all of the participants that are required to follow the practices defined in this CPS. The participants within the GOM eID PKI are:

- Certification Authorities (Root and subordinate);

- Registration Authorities;
- Subscribers;
- Relying Parties, and;
- Other participants such as the OCSP responder and Time Stamping Authority.

Malta Certification Authority: means the Malta Electronic Certification Services (MECS) Ltd, a limited liability company and any replacement or successor Certification Authority appointed by the Maltese Government to act as the Certification Service Provider under this CPS from time to time.

National Identity Card: The collective term used to refer to the cards that are issued under the National Identity Management System. This term includes the Electronic Identity Card, the Electronic Resident Card and the Administrator Card.

National Identity Management System: The system implemented by the Government of Malta to manage the registration, issuance and other aspects of the Electronic Identity Card, Electronic Resident Card and Administrator Card.

Object Identifier (OID): a sequence of numbers that uniquely and permanently references an object.

Policy Management Authority: the management team that acts on behalf of the Malta Certification Authority and is responsible for the compliance of the Malta Certification Authority with this Certification Practices Statement.

Public Key: That key of an entity's asymmetric key pair that can be made public.

Private Key: That key of an entity's asymmetric key pair that should only be used by that entity.

Qualified Certificate: A Certificate that has been issued in accordance with Chapter 426, Laws of Malta also known as the Electronic Commerce Act III of 2001 (amended 2002, 2004, 2005 and twice in 2007).

Qualified Signature: is an Advanced electronic Signature based on a Qualified Certificate and created by means of a Secure Signature Creation Device.

Relying Party: means any natural person or legal entity that relies upon an Electronic Signature created using a Private Key, where the Public Key has been certified as being valid and genuine by a Certification Authority.

Relying Party Agreement: The contract between Relying Parties and the Malta Certification Authority which contains the legal terms and conditions governing acceptance and use of Certificates and Qualified Certificates by Relying Parties. The Relying Party Agreement incorporates the terms of this CPS by reference.

Resident: A person who resides in Malta and does not have Maltese nationality.

Secure Signature Creation Device: is a secure device handling the private key of the user and complying with the eSignature Directive Annex III and Chapter 426, Laws of Malta also known as the Electronic Commerce Act III of 2001 (amended 2002, 2004, 2005 and twice in 2007). The smartcards used for the national Electronic Identity card and the National Electronic Resident card are examples of a Secure Signature creation Device and have been assessed against the appropriate Secure Signature creation Device Protection Profile (PPSSCD) [13].

Signature Creation Data: means unique data, such as codes or private cryptographic keys, which are used by the Signatory to create an Electronic Signature.

Signature Creation Device: means configured software or hardware used to implement the Signature Creation Data.

Signature Policy: requirements imposed / committing the GOM PKI actors with respect to the application of electronic signatures on documents and data that should be signed in the context of a particular transaction, process or business in order for these signatures to be considered as valid (technical) signatures

Signature Verification: a process performed by a Verifier either soon after the creation of an Electronic Signature or later to determine if an Electronic Signature is valid against a Signature Policy implicitly or explicitly referenced.

Signatory: A person who holds a Signature Creation Device and uses it to apply an Electronic Signature either on his own behalf or on behalf of the natural legal person or entity he represents.

Subject: Entity to which a Certificate issued.

Subscriber: Entity that request and subscribes for a Certificate and for which it is either the Subject or not as more particularly described in paragraph 1.3.4 below.

Subscriber Agreement: The contract between Subscribers and the Malta Certification Authority which contains the legal terms and conditions governing the use of Certificates and Qualified Certificates contained in Electronic Identity Cards which are held by Citizens and Residents. The Subscriber Agreement includes a Subscriber application form and incorporates the terms of this CPS by reference.

Time Stamp: A proof-of-existence for a datum at a particular point in time, in the form of a data structure signed by a Time Stamping Authority, which includes at least a trustworthy time value, a unique integer for each newly generated time stamp, an identifier to uniquely indicate the security policy under which the time stamp was created, a hash representation of the datum, i.e. a data imprint associated with a one-way collision resistant uniquely identified hash-function.

Validation Data: additional data, collected by the Signatory and/or a Verifier, needed to verify the Electronic Signature in order to meet the requirements of the Signature Policy. It may include: Certificates, revocation status information or time-stamps.

Verifier: an entity that validates or verifies an Electronic Signature. This may be either a Relying Party or a third party interested in the validity of an Electronic Signature.

Acronyms:

CA Certification Authority
CAO Certificate Authority Operator
CP Certificate Policy
CPS Certification Practice Statement
CRAO Central Registration Authority Officer
CRL Certificate Revocation List
CSP Certification Service Provider
HDO Help Desk Officer
HSM Hardware Security Module
IDMO Identity Management Officer
IDMOA Identity Management Office Administrator
IETF Internet Engineering Task Force
ISO International Organisation for Standardisation
ITU International Telecommunications Union
LCP Lightweight Certificate Policy
LDAP Lightweight Directory Access Protocol
LRAA Local Registration Authority Administrator
LRAO Local Registration Authority Officer
MFA Ministry of Foreign Affairs
MFA Administrators
NIDMS National Identity Management System
OID Object Identifier
OPM Office of Prime Minister Administrators
PIN Personal Identification Number
PKCS Public Key Certificates Standard
PKI Public Key Infrastructure
PKIX Public Key Infrastructure (X.509) (IETF Working Group)
QCP Qualified Certificate Policy
RA Registration Authority
RAO Registration Authority Officer
RFC Request for Comments
RMAA Residence Card Management Authority
RMAO Residence Card Management Authority Officer
RMIO Residence Card Management Identity Officer
RSA A specific Public Key algorithm invented by Rivest, Shamir, and Adleman
SRAO Suspension and Revocation Authority Officer
URL Uniform Resource Locator

2. Publications and Repository Responsibilities

2.1. *Identification of entities operating repositories*

The GOM eID repositories are made of the GOM eID Directory and its associated web site. The GOM eID Directory and its associated web site publish the GOM Root CA Certificate, the Citizen, Resident and Administrator CA Certificates and their associated CRLs in order to provide the various Subscribers and Relying Parties within the GOM eID PKI with access to those pieces of information.

The GOM eID Directory publishes the Certificate Revocation Lists (CRL) that are created by the GOM eID Certificate Authorities within the GOM eID PKI to a public LDAP (the GOM eID Directory)

As such, the GOM eID Directory is responsible for:

- Providing the entities that have been defined within the GOM eID PKI with access to Certificates and CRL in accordance with the policies and procedures defined in this CPS and the related Certificate Policies;
- Limiting access to the GOM eID PKI Certificates and CRL that it maintains in accordance with the policies and procedures defined in this CPS and the related Certificate Policies;
- Maintaining an archive of all Certificates and CRLs that it has published in accordance with the policies and procedures defined in this CPS and the related Certificate Policies;
- Providing access to archived Certificate and CRL data as specified in this CPS and in the other relevant contracts (i.e. the Subscriber Agreement and the Relying Party Agreement), or otherwise required by law;
- Creating and maintaining an audit journal that records all significant events related to the GOM eID Directory’s fulfilment of the above mentioned responsibilities;
- Providing selective access to audit journal records as specified in this CPS and in the other relevant contracts (i.e. the Subscriber Agreement and the Relying Party Agreement), or otherwise required by law;
- Implementing other operational controls as specified in this CPS, and;
- Ensuring that the information that it stores and processes is handled in a manner that is consistent both with the policies and procedures defined in this CPS and with applicable law.
- Publishing the present CPS, the related CPs and the Agreements or any amendments or additions thereto that would be required for any actors to understand and abide his/her rights and responsibilities.

2.2. *Distribution of Certification Information*

The GOM Root CA publishes the following information to the GOM eID Directory:

- A copy of the self-signed GOM Root CA CRL and CA signing Certificate.

The GOM Root CA certificate and associated CRL are located at http://crt.qca.gov.mt/RootCA_rs.crt and http://crl.qca.gov.mt/RootCA.crl respectively.

The Malta Citizen eID CA publishes the following information in the GOM eID Directory:

- A copy of the Malta Citizen eID CA Certificates that correspond to each Malta Citizen eID CA Private Key used in creating Certificates within the GOM eID PKI ;
- A copy of the Certificate issued by the Malta Citizen eID CA, during the validity of that Certificate, and;
- A copy of the most recent CRLs that have been issued.

The Malta Citizen eID CA certificates are located at http://crt.qca.gov.mt/CitizenCA.crt.

The Malta Citizen eID CA CRLs are located at:

- http://crl.qca.gov.mt/CitizenCA.crl.
- http://crl.qca.gov.mt/CitizenCA_2015_001.crl
- http://crl.qca.gov.mt/CitizenCA_2015_002.crl
- ...
- http://crl.qca.gov.mt/CitizenCA_YYYY_NNN.crl

The Malta Citizen eID CA partitions its CRLs to manage their size and increase performance, by periodically changing the CRL location.

When using a CRL to check the validity of any End Entity Certificate issued by the Malta Citizen eID CA, the Relying Party must consult the CRL indicated in the CRL Distribution Point of that End Entity Certificate.

The Malta Resident eID CA publishes the following information in the GOM eID Directory:

- A copy of the Malta Resident eID CA Certificates that correspond to each Malta Resident eID CA private key used in creating certificates within the GOM eID PKI ;
- A copy of the Certificate issued by the Malta Resident eID CA, during the validity of that Certificate, and;
- A copy of the most recent CRLs that have been issued.

The Malta Resident eID CA certificates and associated CRLs are located at http://crt.qca.gov.mt/ResidentCA.crt and http://crl.qca.gov.mt/ResidentCA.crl respectively.

The GOM eID certification Authorities also publishes Certificate status information via OCSP. Certificate status information is available at http://ocsp.qca.gov.mt.

This CPS and related certificate Policies is published to a central repository: http://repository.qca.gov.mt.

2.3. *Time and Frequency of Publication*

The GOM Root CA will create new CRL at least every 3 months. The new CRL(s) will be added to the GOM eID Directory and its associated website at the time following each new CRL entry's creation.

The Malta Citizen eID CA and Malta Resident eID CA will create a new CRL every six (6) hours, namely at 00:00hrs, 06:00hrs. 12:00hrs and 18:00hrs, and publish to the locations detailed above immediately after. The CRL will have a validity of 6 days. The new CRL(s) will be added to the GOM eID Directory and its associated web site at the time following each new CRL entry's creation. Certificate status information will be published to OCSP at the time immediately following creation of the CRL(s).

The Administrator CA will create a new CRL at least every 6 days. The new CRL(s) will be added to the GOM eID Directory and its associated web site at the time following each new CRL entry's creation. In addition, a new CRL set will be generated and published to the GOM eID Directory and its associated web site following the revocation of any Certificate that was previously issued by this CA. Certificate status information will be published to OCSP at the time following creation of the CRL.

2.4. *Access Control on Repositories*

Only Trusted Staff functions, as specified in section 5 of this CPS have write and change access on these repositories, with strong PKI Credentials based access control. The GOM eID PKI has ensured that appropriate security measures have been implemented to protect these repositories and to monitor access and maintenance.

3. IDENTIFICATION AND AUTHENTICATION

3.1. *Naming*

3.1.1. *Types of names*

The GOM uses a genuine, unambiguous, clearly distinguishable and unique X.500 Distinguished Name (DN) in the certificate subject name fields in accordance with RFC 5280.

The detailed structure of the Certificates Subject attributes is provided in section *3.1.2* of this CPS (including X.500 distinguished names and RFC-822 names.

3.1.2. *Need for names to be meaningful*

The names used under this CPS shall be meaningful and follow the following structure, where Malta as country is used (Country codes MUST follow the format of two letter country codes, specified in *ISO/IEC 3166, Codes for the representation of names of countries and their subdivisions – 1997)*:

3.1.2.1. GOM Root CA

Malta Top Root CA Certificate Profile		
Issuer	CN	Government of Malta Root CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Subject	CN	The same as the issuer
	OU	
	O	
	C	

3.1.2.2. Malta Citizen eID CA

Malta Citizen eID CA Certificate Profile		
Issuer	CN	Government of Malta Root CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Subject	CN	Malta Citizen Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT

3.1.2.3. Malta Resident eID CA

Malta Resident eID CA Certificate Profile		
Issuer	CN	Government of Malta Root CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Subject	CN	Malta Resident Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT

3.1.2.4. GOM Administrator CA

GOM Administrator CA Certificate Profile		
Issuer	CN	Government of Malta Root CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Subject	CN	Government of Malta Administrator CA
	OU	Class Qualified
	O	Government of Malta
	C	MT

3.1.2.5. Malta Citizen eID CA Electronic Signature Certificate (Qualified Certificate)

Malta Citizen eID Electronic Signature Certificate Profile		
Issuer	CN	Malta Citizen Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Subject	Citizen DN	The Citizen Distinguished Name will be derived from the citizen Certificate service request created by the National Identity Management System during the registration process. It is made up of the following components: 1. Country [C=MT] 2. Common Name [First name Known as Name (if available) Surname Known as Surname (if available) (Signature)] 3. Surname 4. Given Name 5. Title 6. Serial number = MBUN (meaningless but unique number)

3.1.2.6. Malta Citizen eID Authentication Certificate

Malta Citizen eID Authentication Certificate Profile		
Issuer	CN	Malta Citizen Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Subject	Citizen DN	It is made up of the following components: 1. Country [C=MT] 2. Common Name [First name Known as Name (if available) Surname Known as Surname (if available) (Authentication)] 3. Surname 4. Given Name 5. Title 6. Serial number = MBUN (meaningless but unique number)

3.1.2.7. Malta Resident eID Electronic Signature Certificate (Qualified Certificate)

Malta Resident eID Electronoc Signature Certificate Profile		
Issuer	CN	Malta Resident Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT

Subject	Resident DN	The Resident Distinguished Name will be derived from the Resident Certificate service request created by the National Identity Management System during the registration process. It is made up of the following components: 1. Country [C=MT] 2. Common Name [First name Surname (Signature)] 3. Surname 4. Given Name 5. Serial number = MBUN (meaningless but unique number)

3.1.2.8. Malta Resident eID Authentication Certificate

Malta Resident eID Authentication Certificate Profile		
Issuer	CN	Malta Resident Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Subject	Resident DN	The Resident Distinguished Name will be derived from the Resident Certificate service request created by the National Identity Management System during the registration process. It is made up of the following components: 1. Country [C=MT] 2. Common Name [First name Surname (Authentication)] 3. Surname 4. Given Name 5. Serial number = MBUN (meaningless but unique number)

3.1.2.9. GOM Administrator Certificate

GOM Administrator Certificate Profile		
Issuer	CN	Government of Malta Administrator CA
	OU	Class Qualified
	O	Government of Malta
	C	MT

Subject	Administrator DN	The Administrator Distinguished Name will be derived from the Administrator Certificate service request created by the National Identity Management System during the registration process. It is made up of the following components: 1. Common Name (First name, Surname) 2. Organisational Unit (Role Type) 3. Country [C=MT] 4. Serial number = MBUN (meaningless but unique number)

3.1.2.10. OCSP Certificate profile signed by Citizen CA

GOM OCSP Responder Certificate signed by Malta Citizen CA		
Issuer	CN	Malta Citizen Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Subject	CN	Government of Malta OCSP Responder
	OU	Class Qualified
	O	Government of Malta
	C	MT

3.1.2.11. OCSP Certificate profile signed by Malta Resident CA

GOM OCSP Responder Certificate signed by Malta Resident eID CA		
Issuer	CN	Malta Resident Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Subject	CN	Government of Malta OCSP Responder
	OU	Class Qualified
	O	Government of Malta
	C	MT

3.1.2.12. OCSP Certificate profile signed by Malta Administration CA

GOM OCSP Responder Certificate signed by Malta Administrator CA		
Issuer	CN	Government of Malta Administrator CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Subject	CN	Government of Malta OCSP Responder

	OU	Class Qualified
	O	Government of Malta
	C	MT

3.1.2.13. Time Stamp Certificate profile

GOM Timestamp Server Certificate signed by GOM Root CA		
Issuer	CN	Government of Malta Root CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Subject	CN	Government of Malta Timestamp Server
	OU	Class Qualified
	O	Government of Malta
	C	MT

3.1.2.14. Time Stamp Administrator Certificate

GOM Timestamp Administrator Certificate		
Issuer	CN	Government of Malta Administrator CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Subject	CN	Timestamp Administrator
	OU	Class qualified
	O	Government of Malta
	C	MT

3.1.2.15. Time Stamp Auditor Certificate

GOM Timestamp Auditor Certificate		
Issuer	CN	Government of Malta Administrator CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Subject	CN	Timestamp Auditor
	OU	Class qualified
	O	Government of Malta
	C	MT

3.1.3. ***Uniqueness of names***

The Distinguished Name shall be unique and shall be constructed as described in section 3.1.2 of this CPS and the associated Certificate Policy.

3.1.4. ***Recognition, authentication, and role of trademarks***

All product or company names that may be mentioned in this publication are trademarks or registered trademark of their respective owners.

If the Distinguished Name of a Certificate relates to a natural person, the name is as defined by the Malta IDMO established under the control of the ID Management Officer. For these certificates Trademarks do not need to be recognized.

In all other cases, it is solely the Subscriber's responsibility that their choice of name does not violate any trademark and copyright or Intellectual Property infringement of any person or entity, whether fraudulently, negligently, innocently or otherwise. The GOM eID Certificate Authorities are not obligated to check such rights. If a GOM eID Certificate Authority is notified of a violation of such rights, it has the right to revoke the Certificate.

3.2. *Initial identity validation*

3.2.1. *Method to prove possession of private key*

The National Identity Management System will generate the Certificates' Key Pairs upon the card and create Certificate Service Requests for Subscribers' End Entity Certificates. This request is built upon a standard industry format that provides cryptographic evidence that the entity submitting a public key to be certified by a CA has possession of the corresponding Private Key.

3.2.2. *Authentication of organization identity*

End Entity Certificates shall only be issued to natural persons. The registration processes for these Certificates are briefly explained in section 1.3.5 and further detailed in applicable CPs.

Certificates issued for infrastructure components (for example, SSL Client and Server Certificates) shall only be issued to the GOM eID PKI components. The subscriber in this case must be a duly authorised personnel member of the GOM eID PKI. The Registration Authority will authenticate the Subscriber as being a person responsible for the maintenance of this infrastructure component through face-to-face meetings and other validation procedures, as described in section 1.3.4 and detailed in a confidential and internal document.

3.3. *Identification and authentication for re-key & update requests*

Certificate re-key and Certificate update requests are not allowed for End Entity Certificates. All update requests for Certificates embedded upon a National Identity Card are treated as an initial request and shall result in the issuance of a new National Identity Card and associated embedded keys and Certificates.

The Root CA and sub-CAs support Certificate re-key and this will be undertaken through a formal witnessed internal signing ceremony described in a confidential and internal document.

3.4. *Identification and authentication for revocation request*

Requests for revocation of Certificates embedded within the National Identity Card, National Electronic Resident Card or Administrator Card shall only be supported through a request authenticated by the National Identity Management System as described in the applicable CP.

The revocation of all other Certificates shall only be accepted from the Policy Management Authority on behalf of the Malta Certification Authority.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. *Certificate Application*

4.1.1. *Who can submit a Certificate application*

The Malta Citizen eID CA will only accept certification requests from the Malta National Identity Management System following the successful application for a new Electronic Identity Card by a Citizen and the approval of the request by a Local Registration Authority Administrator (LRAA).

The Malta Resident eID CA will only accept certification requests from the Malta National Identity Management System following the successful application for a new Electronic Resident Card by a Resident of Malta and the approval of the request by a Residence Card Management Authority Administrator (RMAA).

The GOM Administrator CA will only accept certification requests from the Malta National Identity Management System following the successful application for a new Administrator card by a duly authorised personnel member of the GOM eID PKIs. Details of the registration process for an Administrator are described in a confidential and internal document.

4.1.2. *Subscriber Registration Process*

The Subscriber Registration Process for the Malta Citizen eID CA, Malta Resident eID CA and Administrator CA is described within this document in section 1.3.5 as part of the description of the National Identity Management System (NIDMS) and further detailed in the applicable CPs.

4.2. *Certificate application processing*

4.2.1. *Performing identification and authentication functions*

The National Identity Management System operates the identification and authentication processes that are followed for the issuance of a Citizen, Residence or Administrator National Identity Card and associated embedded keys and Certificate issuance according to section 1.3.5, and according to procedures described in a confidential and internal document.

4.3. *Certificate issuance*

4.3.1. *CA actions during certificate issuance*

The CA is configured in such a manner that it will only accept certification requests relating to the National Identity Cards from NIDMS that have been entered by the appropriate Officer and approved by the appropriate Adminstrator.

The National Identity Management System supports the issuance of the certificates associated with the National Electronic Identity card, the national Electronic Resident card and the Administrator card. In each case the request will be entered and approved by authorised personnel using the appropriate local interface. The approved details will be passed to the appropriate dedicated card management system component where the key pair(s) will be generated upon the appropriate card and the certificate request(s) will be created using the correct format.

The NIDMS card management system component dedicated to the production of the Citizen National Electronic Identity cards will only have access to the cryptographic credentials required to submit requests to the Malta Citizen eID CA.

The NIDMS card management system component dedicated to the production of the National Electronic Residents cards will only have access to the cryptographic credentials required to submit requests to the Malta Resident eID CA.

The NIDMS card management system component dedicated to the production of the Administrator cards will only have access to the cryptographic credentials required to submit requests to the Malta Citizen eID CA.

4.3.2. *Notification to Subscriber by the CA of issuance of Certificate*

Subscribers will be notified at the time of application by their RAO of the timescales within which their Electronic Identity Card will be ready for collection.

Where the Subscribers are Citizens applying for an Electronic Identity Card, the Certificates will be provided to them embedded inside their Electronic Identity Card when collected from the LRA office and accepted by the Citizen in accordance with the terms of the Subscriber Agreement.

Where the Subscriber are Residents of Malta applying for an Electronic Resident Card, the Certificates will be provided to them embedded inside their Electronic Resident Card when collected from the RMA office and accepted by the Resident in accordance with the terms of the Subscriber Agreement.

Where the Subscriber is an individual suitably authorised by Government applying for an Administrator Card, the Certificate will be provided to them embedded inside their

Administrator Card when collected from their Registration Officer and accepted by the Administrator in accordance with the terms stipulated in the enrolment form.

4.4. *Certificate Acceptance*

Where the Subscriber is a Citizen applying for an Electronic Identity Card, they will be required to sign a number of forms (e.g an application form, the Subscriber Agreement and electoral register forms), accepting delivery of the Electronic Identity Card and any Certificates embedded within the card. The Citizen is responsible for checking the visible details associated with their card (for example the name) and asking for revocation of the card if these details are not correct. Usage of the card is considered as acceptance of the associated embedded Certificates.

Where the Subscriber is a Resident of Malta applying for an Electronic Resident Card, they will also be required to sign a number of forms accepting delivery of the Electronic Resident Card and any Certificates embedded within the card. The Resident is responsible for checking the visible details associated with their card (for example the name) and asking for revocation of the card if these details are not correct. Usage of the card is considered as acceptance of the associated embedded Certificates.

Where the Subscriber is a natural person applying for an Administrator Card, they will also be required to sign a number of forms accepting delivery of the Administrator Card and any Certificate embedded within the card. The Administrator is responsible for checking the visible details associated with their card (for example the name) and asking for revocation of the card if these details are not correct. Usage of the card is considered as acceptance of the associated embedded Certificate.

4.5. *Key pair and Certificate usage*

Subscribers shall only use key pairs and their associated Certificates for purposes defined within the respective Certificate Policy.

Relying Parties shall check the key usage of a Certificate and any Certificate usage restriction every time before relying upon an associated Electronic Signature and authentication Certificate.

Certificates issued for key pairs embedded within the National Identity or Resident or Administrator Card shall only be used in conjunction with that card. The Private Keys will never leave the card.

The National Identity Card has been certified against the appropriate protection profile as a Secure Signature creation Device (SSCD) [13] as also defined within the Electronic Commerce Act [10].

4.6. *Certificate Renewal*

Certificate renewal is not allowed by the GOM eID PKI.

All applications for Certificate renewal from a Citizen shall be treated as applications for a new Electronic Identity Card with new embedded authentication and signing Certificates.

All applications for Certificate renewal from a Resident of Malta shall be treated as applications for a new Electronic Residence Card with new embedded authentication and signing Certificates.

All applications for Certificate renewal from an existing Administrator shall be treated as applications for a new Administrator Card with a new embedded authentication Certificate.

4.7. *Certificate Re-Keying*

The GOM Root CA shall support Certificate re-key. This self-signed Certificate shall be embedded within each National Identity Card as part of a full Certificate chain. Following Root CA re-key, the new self-signed Public Key Certificate shall be embedded into all new cards, but the existing cards shall retain the previous version.

The Malta Citizen eID CA shall support Certificate re-key. This Certificate shall be embedded within each National Identity Card as part of a full Certificate chain. Following Malta Citizen eID CA re-key, the new Public Key Certificate shall be embedded into all new National Identity Cards, but the existing cards shall retain the previous version.

The Malta Resident eID CA shall support Certificate re-key. This Certificate shall be embedded within each National Electronic Resident Card as part of a full Certificate chain. Following Malta Resident eID CA re-key, the new Public Key Certificate shall be embedded into all new National Electronic Resident Cards, but the existing cards shall retain the previous version.

The GOM Administrator CA shall support Certificate re-key. This Certificate shall be embedded within each Administrator card as part of a full Certificate chain. Following GOM Administrator CA re-key, the new Public Key Certificate shall be embedded into all new Administrator Cards, but the existing cards shall retain the previous version.

All applications for a Certificate re-key from a Citizen shall be treated as applications for a new Electronic Identity Card with new embedded authentication and signing Certificates.

All applications for a Certificate re-key from a Resident of Malta shall be treated as applications for a new Electronic Resident Card with new embedded authentication and signing Certificates.

All applications for a Certificate re-key from an existing Administrator shall be treated as applications for a new Administrator Card with a new embedded authentication Certificate.

4.8. *Certificate Modification*

Certificate modification is not allowed by the GOM eID PKI.

4.9. *Certificate Revocation and Suspension*

4.9.1. *Circumstances for revocation*

If the CA or RA (through a NIDMS Office) is notified of at least one of the following circumstances then the Certificate must be revoked.

Possible reasons for the revocation of a Certificate will include:

- The Certificate contains invalid information;
- The National Identity Card of the Subscriber was reported factually lost, stolen, disclosed or otherwise compromised/misused;
- The Subscriber is no longer authorized to use the certificate (see Section 1.4).
- The Subscriber does not comply with the GOM eID CPS;
- The Subscriber requests that the Certificate is revoked through a Local Registration Authority Office;
- The CA or RA responsible does not comply with the associated CP or the present GOM eID CPS, or;
- The CA terminates its operation.

4.9.2. *Revocation checking requirement for Relying Parties*

Before a Certificate is used, Relying Parties should check its validity and then use the Certificate solely in compliance with this CPS and the associated Certificate Policy.

When using a CRL to check the validity of any End Entity Certificate issued by the Malta Citizen eID CA or the Malta Resident eID CA, the Relying Party must consult the CRL indicated in the CRL Distribution Point of that End Entity Certificate.

4.9.3. *Circumstances for suspension*

The GOM eID PKI allows Certificate suspension during the initial quality checking processes associated with the issuance of a new Electronic Identity Card prior to the card being received by the Subscriber.

The GOM eID PKI shall also initially suspend a Certificate when notified of a potential problem by the Subscriber through the help desk or at a NIDMS office, in order that an internal investigation may be conducted.

A Certificate that has been suspended for more than 14 days will be revoked.

4.9.4. *Suspension checking requirement for Relying Parties*

Before a Certificate is used, Relying Parties should check its validity and then use the Certificate solely in compliance with this CPS and the associated Certificate Policy.

4.9.5. *Subscriber Revocation Process*

The Subscriber Revocation Process for the Malta Citizen eID CA is described within this document in section 1.3.6.

4.10. *Certificate Status Services*

The obligation of each CA within the GOM eID PKI, is to provide an associated corresponding CRL that describes a change in Certificate status from “active” to either “revoked” or “suspended”. Further details are provided in Section 2.

Certificate Status information will be published to OCSP by each CA within the GOM eID PKI. Details on where a Relying Party shall check the status of a Certificate will be found in the CRL distribution points of the Certificate.

4.11. *End of Subscription*

Certificate usage may be terminated by the Subscriber by means of revocation of their Certificates.

4.12. *Key Escrow and Recovery*

Key Escrow or Key Recovery are not supported by the GOM eID PKI.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The GOM has implemented a wide range of physical, procedural and personnel controls to maintain the confidentiality, integrity and availability of the GOM eID PKI in line with applicable industry best practice.

5.1. *Physical controls*

The GOM eID PKI implements physical controls on its premises including the following:

- The GOM eID PKI uses premises that are located in an area appropriate for high-security operations. There are numbered zones and locked rooms, cages, safes and cabinets;

- Physical access is restricted by implementing mechanisms to control access from one area of the facility to another or access into high-security zones, such as locating CA operations in a secure computer room, physically monitored and supported by security alarms, and requiring movement from zone to zone to be accomplished using a token and access control lists;
- Visitor access must be approved in advance by the GOM eID PKI and visitors shall be required to provide a recognised form of photographic identity. All visitors shall be accompanied at all times by a member of the GOM eID PKI;
- Power and air conditioning operate with a high rate redundancy;
- The premises are protected from any water exposure;
- Prevention and protection measures against fire exposure are implemented;
- All media is stored securely, with backup media being stored in a separate location that is physically secure and protected from accident, fire and water damage, and;
- Waste disposal is controlled with secure destruction mechanisms being implemented for all media containing sensitive or confidential information.

Physical controls are further described in a confidential and internal document [int.doc reference 2].

5.2. *Procedural controls*

The GOM eID PKI follows personnel and management practices that provide reasonable assurance and trustworthiness and competence of the members of staff and of the satisfactory performance of their duties in the fields of Electronic Signature related technologies.

Each staff member of the GOM eID PKI executes a statement on abiding by confidential and personal data protection legislation, having met confidentiality requirements associated with their role, such as described in their job description / or employment contract.

All GOM eID PKI personnel, or personnel of an authorised outsourced agent for the GOM eID PKI are considered as serving in a trusted position by all parties.

The GOM eID PKI conducts an initial investigation of all trusted staff who are candidates to serve in trusted roles to make a reasonable attempt to determine their trustworthiness and competence.

Where dual control is required, at least two trusted staff members of the GOM eID PKI need to bring their respective and split knowledge in order to be able to proceed with the ongoing operation.

Procedural controls are further described in a confidential and internal document [int.doc reference 3].

5.3. *Personnel controls*

5.3.1. *Qualifications, experience and clearance requirements*

The GOM eID PKI and its outsourced partner organisations perform checks to establish the background, qualifications and experience of candidates to perform the specific roles under consideration.

Such background checks are intended to determine whether the subject is:

- of unquestioned loyalty;
- of such character and discretion as to cast no doubt upon his/her integrity; or may be vulnerable to pressure from foreign or other sources (e.g. due to former residence or past associations) which might constitute a risk to security.

5.3.2. *Background check procedures*

The GOM eID PKI will follow the GOM background check procedures.

5.3.3. *Training requirements*

The GOM eID PKI makes available to their personnel appropriate technical and security training related to the role they execute.

Training plans are further described in a confidential and internal document.

5.3.4. *Retraining frequency and requirements*

Where appropriate, the GOM eID PKI provides appropriate retraining and training updates for personnel.

5.3.5. *Sanctions for unauthorized actions*

The GOM eID PKI will follow the GOM procedures for imposing sanctions for unauthorized actions.

5.3.6. *Independent contractor requirements*

All independent contractors are subject to equivalent data security, privacy protection and confidentiality conditions as GOM eID PKI personnel.

5.3.7. *Documentation supplied to personnel*

The GOM makes available appropriate documentation to eID PKI personnel during training, retraining or under other circumstances.

The documentation supplied to the holder of each trusted role is described in confidential and internal documents.

5.4. *Audit logging procedures*

The GOM eID PKI implements audit logging procedures that include event logging and audit systems implemented for the purpose of maintaining a secure environment.

The GOM eID PKI implements the following controls:

- The recording of events that include but are not limited to certificate lifecycle operations, attempts to access the system, and requests made to the system;
- The storage of real-time audit logs, which are subsequently processed and retained on a weekly basis;
- The audit logs can only be viewed by authorised personnel, including the CA Auditor, and
- The audit logs are backed up and securely stored for a period of up to 40 years for evidential and audit purposes and in order to protect against loss or modification.

The GOM eID PKI will not routinely notify a subject that their actions have triggered an audit event.

5.5. *Records archival and retention*

5.5.1. *Types of records archived*

The records retention and archival process for the GOM eID PKI is stipulated in an internal document. The retained records are sufficiently detailed to determine the proper operation of the CA, and the validity of any Certificate (including those revoked or expired) issued by the CA.

5.5.2. *Retention period for archive*

The GOM eID PKI keeps internal records or ensures the archival, in a trustworthy manner, of the following items for a period of up to 40 years:

- All Certificates;
- Audit trails on the issuance of Certificates;
- Audit trail of the revocation of a Certificate, and;
- CRLs.

The above information shall be retained and processed so as to enable the CA to meet legal and evidential requirements under the Maltese Electronic Commerce and other legislation. In accordance with the Data Protection Act, the CA may access and/or disclose personal information if such action is necessary to:

(a) Comply with the laws of Malta;
(b) Protect and defend the rights or property of the Government of Malta;
(c) Act in urgent circumstances to protect the personal safety of Subscribers or members of the public.

The GOM eID PKI keeps records in a retrievable format.

Records are accessible to the authorized personnel of the GOM eID PKI, of the RA and designated auditors as described in internal documents.

Additional event record information may be retained directly by the GOM eID PKI and are documented within the GOM eID PKI policies and procedures [int.doc reference 4].

5.5.3. *Protection of archive*

The GOM eID PKI ensures:

- Implementation of proper copying mechanisms to prevent data loss or data access loss over time during their retention period and;
- That the confidentiality and integrity of the archive and its physical storage media shall be maintained during its retention period, and;
- That records concerning Certificates shall be completely and confidentially archived in accordance with this CPS.

Archives are accessible to the authorized personnel of the GOM eID PKI and designated auditors as described in internal documents.

5.5.4. *Requirements for time-stamping of records*

The GOM eID PKI ensures that the precise time of archiving all events, records and documents listed in section 5.4 and 5.5 shall be recorded with support of appropriate references to timing of such events.

The GOM eID PKI synchronises its time with a predictable and trusted time source to UTC.

5.5.5. *Procedures to obtain and verify archive information*

Archives are accessible to the authorized personnel of the GOM eID PKI, of the RAs and designated auditors as described in internal documents available on request.

Records are retained in electronic or in paper-based format.

Requests for information shall be sent to the Malta Certification Authority for review.

Records concerning Certificates shall be made available if required for the purposes of providing evidence of certification for the purpose of legal proceedings and audit or for the purpose of investigating potential offences.

5.6. *Key Changeover*

The details of Key Changeover following a re-key by the Root CA or an issuing CA are covered within the internal operating procedures.

Key Changeover will not affect existing cards and their associated Certificates as the issuing CA Public Key Certificate and Root CA Public Key Certificate are stored within the card during the initial generation and issuance process.

Following Key Changeover at an issuing CA all new cards issued after that point will include a copy of the new Certificates.

5.7. *Compromise and Disaster Recovery*

The GOM eID PKI incorporates a number of high-availability options in the technical and operational design of the system in order to ensure continuity of service in the event of a disaster.

The system will be based across two locations, with automatic replication of data between the primary and secondary sites as well as regular media backups to secure off-site locations.

The design of the computer facilities includes the provision of controls to protect against potential environmental disasters such as fire, flood and earthquake. Provision is also made to protect against loss or disruption to essential services including power, air conditioning and communications links.

The GOM eID PKI has implemented a business continuity plan to ensure business continuity following a natural or other disaster. The applicable incident, compromise reporting and handling procedures are documented within internal documentation.

5.8. *CA or RA termination*

In the event of the termination of the CA or RA, the CA or RA shall take all the necessary measures to ensure that all the information, data, documents, repositories, archives and audit trails concerning the qualified certificate are preserved for the purpose of providing evidence of certification in legal proceedings.

Before the CA terminates its services the following procedures have to be completed as a minimum:

- Inform all Subscribers, cross-certifying CA's and Relying Parties with which the CA has agreements or other form of established relations;
- Inform the Malta Communications Authority and the Government of Malta of the termination and its possible consequences;
- Hand over its activities to another CA of the same quality and security level; if this is not possible, revoke the Certificates two (2) months after having informed the Subscribers and archive all relevant Certificate information;

- If possible, make publicly available information of its termination at least 3 month prior to termination;
- Terminate the revocation checking service for all Certificates issued under the terminated issuing keys. This will stop any of these Certificates from being accepted by any relying party who follows proper revocation checking procedures according to this CPS.

6. TECHNICAL SECURITY CONTROLS

6.1. *Key Pair Generation and Installation*

6.1.1. *Key Pair Generation*

All key pairs are generated within hardware devices.

The GOM Root CA will generate and store its Private Keys within a dedicated Hardware Security Module that has been validated at FIPS 140-2 Level 3.

The Malta Citizens eID CA, Malta Residence eID CA and GOM Administrator CA as well as the GOM eID Time Stamp server and GOM OCSP responder will generate and store their Private Keys within a networked Hardware Security Module that has been validated at FIPS 140-2 Level 3.

The CAO keys will be generated and stored within a physical token that has been validated at FIPS 140-2 level 2, with the passphrase being a random 15 character value that includes upper and lower case, characters and numbers.

The key pairs associated with the Malta National Identity Card will be generated and stored upon the card itself, within a secure module that has been validated against the appropriate Protection Profile for a Secure Signature Creation Device as defined within Annex III of the eSignature Directive 1999/93/EC [12].

The key pairs associated with the Malta national Electronic Resident Card will be generated and stored upon the card itself, within a secure module that has been validated against the appropriate Protection Profiles for a Secure Signature Creation Device as defined within Annex III of the eSignature Directive 1999/93/ EC [12].

The key pair associated with the GOM Administrator Card will be generated and stored upon the card itself, within a secure module that has been validated against the appropriate Protection Profile for a Secure Signature Creation Device as defined within Annex III of the eSignature Directive 1999/93/ EC [12].

6.1.2. *Private Key Delivery to Card applicant Subscriber*

Private Keys are created securely on the card, so no Private Key delivery is required.

The sole control on the key by the subscriber is insured during the issuance process by generating and storing the private key upon the card and then distributing the PIN via a separate channel. As such only the subscriber has access to both the card and the associated PIN.

6.1.3. *Public Key Delivery to Certificate Issuer*

For Card applicant Subscriber the Card Management System component of NIDMS will generate the Certificate Service Request and deliver this to the appropriate Certification Authority.

The Certificate will be returned to NIDMS from the Certification Authority using the PKCS#7 format and will then be embedded onto the National Identity Card containing the associated key pair.

6.1.4. *CA Public Key Delivery to Relying Parties*

The Root CA Public Key and associated issuing CA Public Key will be embedded into the National Identity Card prior to the card being handed over to the applicant.

The following CA Public Key Certificates will be published in the GOM eID Directory:

- GOM Root CA;
- Malta Citizen eID CA;
- Malta Residence eID CA, and;
- GOM Administrator CA.

6.1.5. *Key Sizes*

The GOM Root CA will have a key size of 4096 bits.
The Malta Citizen eID CA will have a key size of 2048 bits.
The Malta Resident eID CA will have a key size of 2048 bits.
The GOM Administrator CA will have a key size of 2048 bits.

All other Subscriber key sizes will be 2048 bits.

6.1.6. *Public Key Parameters Generation and Quality Checking*

The quality of the Public Key parameters will be checked during the key generation process and weak key values will be discarded.

6.1.7. *Key Usage Purposes (as per X.509 v3 key usage field)*

The following values are defined within the key usage field for the supported End Entity Certificates:

Certificate	Key Usage
Identity card Authentication Certificate	Electronic Signature

Certificate	Key Usage
Identity card Digital Signing Qualified Certificate	Non repudiation
Residence card Authentication Certificate	Electronic Signature
Residence card Digital Signing Qualified Certificate	Non repudiation
Administrator Authentication Certificate	Electronic Signature
SSL Client Certificate (for NIDMS)	Electronic Signature (client authentication)
SSL Server Certificate (for NIDMS)	Electronic Signature, Key encipherment (server authentication)

Refer to the appropriate Certificate Policy for further details.

6.2. *Private Key Protection and Cryptographic Module Engineering Control*

6.2.1. *Cryptographic Module Standards and Controls*

For the GOM Root CA, a dedicated hardware security module is used that is certified to FIPS 140-2 level 3.

For the following Certification Authorities and GOM eID PKI components a networked Hardware Security Module is implemented that has been certified to FIPS 140-2 level 3:

- GOM Root CA;
- Malta Citizen eID CA;
- Malta Resident eID CA;
- GOM Administrator CA:
- GOM Time Stamp Server, and;
- GOM OCSP Responder.

6.2.2. *Private Key n out of m Multi-Person Control*

Certain tasks such as those associated with the handling of the Private Keys of certificate authorities are performed under multi-person control using an “n out of m” approach. This is configured to ensure that a minimum of “n” separate individuals amongst “m” potential individuals must participate in creating, recovering or renewing these keys.

The details on the usage and management of these Private keys and associated tokens is documented in internal operating procedures [int.doc reference 1].

6.2.3. *Private Key Backup*

The GOM eID PKI shall not archive the Subscriber Private Key.

6.3. *Other Aspects of Key Pair Management*

6.3.1. *Certificate Operational Periods and Key Pair Usage Periods*

The following Certificate validity periods are defined:

GOM Root CA:	30 years from time of issue
Malta Citizen eID CA:	20 years from time of issue
Malta Resident eID CA:	20 years from time of issue
GOM Administrator CA:	20 years from time of issue
Malta Citizen eID digital signing	maximum of 10 years
Malta Citizen eID authentication	maximum of 10 years
Malta Resident eID digital signing	maximum of 10 years
Malta Resident eID authentication	maximum of 10 years
GOM Administrator authentication	3 years
GOM OCSP Responder	1 year from time of issue
GOM Timestamp Authority	10 years from time of issue
GOM Timestamp Administrator	10 years from time of issue
GOM Timestamp Auditor	10 years from time of issue
GOM SSL Server Certificates	3 years from time of issue
GOM SSL Client Certificates	1 year from time of issue

6.4. *Activation Data Generation and Installation*

6.4.1. *Activation Data Protection*

The activation of the Subscriber Citizens or Residents Certificates shall be through two PIN code(s), one for each Certificate. The PIN code(s) shall be communicated to the Subscriber through normal post to his/her address on the Electronic Identity Card or Residence Permit Card.

A passphrase shall be used to activate all Certification Authority keys.

6.5. *Computer Security Controls*

The GOM eID PKI shall implement computer security controls as defined within the PKI eID security implementation document, which is required to avoid unauthorised access. [int.doc reference 5].

6.6. *Life cycle technical controls*

The GOM eID PKI shall implement life-cycle technical controls including the execution of tools and procedures to ensure that operational systems and networks adhere to their configured security.

6.7. *Network security controls*

The GOM eID PKI shall implement network security controls as defined within the NIDMS infrastructure document [int.doc reference 6].

6.8. *Time-stamping*

The GOM eID PKI will obtain time from a consistent and predictable source that is linked to an external trusted source.

7. CERTIFICATE AND CRL PROFILES

This section is used to specify the Certificate and CRL formats. This includes information on profiles, versions, and extensions used.

7.1. *Certificate profile*

Details of End Entity Certificates are provided in the applicable Certificate Policy.

Details of other Certificates issued by the GOM eID PKI are provided in this CPS in Section 11. Appendix 2. Certificate Profiles.

Details of the Certificate Revocation Lists issued by the GOM eID PKI are provided in this CPS in Section 11. Appendix 2. Certificate Profiles.

Details of the Online Certificate Status Protocol certificate issued by the GOM eID PKI are provided in this CPS in Section 11. Appendix 2. Certificate Profiles.

8. COMPLIANCE AUDIT AND RISK ASSESSMENTS

8.1. *Assessment topic*

Malta Certification Authority shall conduct an assessment for compliance of its PKI for the issuance of qualified certificates with ETSI TS 101 862 [6] and ETSI TS 101 456 [5]. Periodic compliance inspections will also be conducted to ensure that the Malta eID PKI follows the processes stated in this CP and its associated CPS.

The Malta Certification Authority may additionally be subject to assessment by the Malta Communications Authority.

8.2. *Frequency or circumstances of risk assessment*

The GOM eID PKI shall be audited on a periodic basis not exceeding 12 months on its policies, including this CPS.

This CPS shall be assessed in recognition of the role of the GOM eID PKI as the Certified Service Provider (CSP) for the provision of Qualified Certificates for use as described within the ETSI standard [5], the Laws of Malta [10] and Article 3.3 of the eSignature Directive 1999/93/EC [12].

8.3. *Identity/qualifications of assessor*

For the assessment conducted by the Malta Certification Authority, the identity and relevant qualifications for an approved assessor is at the sole discretion of the Malta Certification Authority.

8.4. *Auditor's relationship to assessed entity*

To carry out the audits there will be an independent auditor appointed by the Malta Certification Authority.

Aside from the audit function, the auditor and audited party shall not have any current or planned financial, legal or other relationship that could result in a conflict of interest.

8.5. *Topics covered by assessment*

The compliance audit will include the control requirements defined within the ETSI standards:

ETSI TS 101 456 v1.4.3 (2007-05): Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Authorities Issuing Qualified Certificates [5]

ETSI TS 101 862 v1.3.3 (2006-01): Qualified Certificate profile [6].

8.6. *Actions taken as a result of deficiency*

At the sole discretion of the Malta Certification Authority, the actions resulting from any identified actual or possible deficiency may include:

- Temporary suspension of service until the deficiencies have been corrected;
- Revocation of Certificates issued to the assessed entity;
- Changes in personnel;
- Further investigations;
- Claims for damages against the assessed entity.

8.7. *Communication of results*

Among the deliverables of the compliance audit, the auditor will provide an audit assessment document that contains:

- A definition of the purpose and scope of work that was performed, and the identification of the timeframe in which the work was performed;
- A high-level summary of the primary findings, and;
- An overall conclusion expressing the auditor's audit opinion of adequacy and compliance to the CPS.

The distribution of any deliverables resulting from the audit and the communication of results is at the discretion of the Malta Certification Authority.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. *Fees*

The Malta Certification Authority shall not charge fees for the provision of services described within this CPS.

9.2. *Financial responsibility*

The Malta Certification Authority shall either itself or in conjunction with its contractors, maintain appropriate human resource and IT management capabilities to meet its obligations under this CPS. However, the Malta Certification Authority is a limited liability company whose liability is excluded and limited in the manner set out in the Agreements and in this paragraph 9.

9.3. *Confidentiality of business information*

The Malta Certification Authority observes confidentiality rules as described in this CPS for information that is marked as business information by the supplier to the GOM eID PKI in accordance with EU law [12].

9.4. *Privacy of personal information*

The GOM eID will comply with the Malta Data Protection Law. Information collected by the GOM eID PKI as part of the NIDMS registration process will only be used for the purposes of generation and maintenance of the National Identity Cards and associated Public Key Certificates.

9.5. *Intellectual property rights*

The GOM owns and reserves all intellectual property rights associated with its databases, web sites, Certificates and any other publication whatsoever originating from the GOM, including this CPS.

9.6. *Representations and warranties*

The respective obligations and liabilities of the Malta Certification Authority (as Certification Service Provider), Subscribers and Relying Parties are as expressly set out in this CPS, the CP, the Subscriber Agreement and the Relying Party Agreement. The Malta Certification Authority does not warrant that the GOM eID will be uninterrupted or error free and all other statements, representations, warranties or conditions are excluded to the fullest extent permitted by law. Nothing in this paragraph 9.6 shall exclude the liability of a party for death or personal injury caused by its negligence nor shall this paragraph operate to exclude the liability of a party caused by any fraud or fraudulent misrepresentation perpetrated by any party.

All parties of the GOM eID PKI, including the Certification Authorities and Subscribers warrant the integrity of their respective Private Key(s). If any such party suspects that a Private Key has been compromised they will immediately notify the appropriate Malta Certification Authority.

9.6.1. *Subscriber Obligations*

The Subscriber warrants, represents and undertakes to the CA that s/he will comply with his/her obligations under the Subscriber Agreement.

9.6.2. *Relying Party Obligations*

Each Relying Party warrants, represents and undertakes to the CA that s/he will comply with his/her obligations under the Relying Party Agreement.

9.6.3. *Subscriber Liability towards Relying Parties*

The reliance placed upon any Electronic Signature created using the authentication Certificate and associated Private Key embedded within the National Identity Card shall be limited to proof-of-possession of the card and knowledge of the associated activation data. The Certification Authority does not authenticate the content of any message signed using an Electronic Signature and accordingly does not entertain any liability or risk in relation thereto.

Without limiting other Subscriber obligations stated elsewhere in this CPS, Subscribers are liable for any misrepresentations they make in Certificates to third parties that, reasonably rely on the representations contained therein.

9.6.4. *GOM eID Directory*

Parties (including Subscribers and Relying Parties) accessing the GOM eID Directory agree with the provisions of this CPS and any other conditions of usage that the Malta Certification Authority may make available. Parties demonstrate acceptance of the conditions of usage of the CPS by submitting a query with regard to the status of a Certificate or by anyway using or relying upon any such information or services provided. The GOM eID Directory includes or contains:

- Information to verify the status of Electronic Signatures created with a Private Key corresponding to a Public Key listed in a Certificate.
- Information published on the Malta Certification Authority web site.
- Any other services that the Malta Certification Authority might advertise or provide through its web site.

It is the sole responsibility of the parties accessing information featured in the GOM eID Directory to assess and rely on information featured therein. Parties acknowledge that they have received adequate information to decide whether to rely upon any information provided in a Certificate. The Malta Certification Authority takes steps necessary to update its records and directories concerning the status of the certificates.

The Malta Certification Authority makes every effort to ensure that parties accessing its directory receive accurate, updated and correct information. The Malta Certification Authority, however, cannot accept any liability beyond the limits set in this CPS and in the Agreements.

9.6.5. *GOM CA Obligations*

To the extent specified in the relevant sections of the CPS each of the following Certification Authorities are operating within the GOM eID PKI and are owned by the Malta Certification Authority:

GOM Root CA;
Malta Citizen eID CA;
Malta Resident eID CA, and;
GOM Administrator CA

Subject to the limitations and exclusions set out in paragraphs 9.7, 9.8 and 9.16.5, the Malta Certification Authority warrants that it will:

- Comply with this CPS and its amendments as published under http://repository.qca.gov.mt/cps.html
- Provide infrastructure and certification services, including the establishment and operation of the GOM eID Directory for the operation of public Certificate management services.
- Provide Trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its own Private Key(s).
- Provide and validate application procedures for the various types of Certificates that it makes publicly available.
- Issue electronic Certificates in accordance with this CPS and fulfil its obligations presented herein.
- Revoke Certificates issued according to this CPS upon receipt of a valid and authenticated request to revoke a certificate from a NIDMS Administrator.
- Publish accepted Certificates in accordance with this CPS.

- Provide for the expiration and renewal of Certificates according to this CPS.
- Publish CRLs and/or OCSP responses of all revoked certificates on a regular basis in accordance with this CPS.
- Notify Relying Parties of Certificate revocation by publishing CRLs on the GOM eID Directory.

To the extent permitted by law and save to the extent arising from its own fraud or wilful misconduct, the Malta Certification Authority shall not be liable for:

- Any use of Certificates, other than as specified in this CPS and in the Agreements.
- Falsification of transactions.
- Improper use or configuration of equipment, not operated under the responsibility of the associated GOM eID PKI CA, used in a transaction involving Certificates.
- Compromise of private keys associated with the Certificates.
- Loss, exposure or misuse of PIN code(s) etc. protecting Private Keys associated with the Certificates.
- Any liability which has been excluded in the Agreements or any liability in excess of the liability limits set out in the Agreements.

9.7. *Disclaimers of Warranties*

This section includes disclaimers of express warranties.

9.7.1. *Limitation for Other Warranties*

See paragraph 9.6 above.

9.7.2. *Exclusion of Certain Elements of Damages*

In no event (save to the extent arising from the fraud or wilful misconduct of the Malta Certification Authority) shall the Malta Certification Authority be liable for:

- Any loss of profits.
- Any loss of data.
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of Certificates or Electronic Signatures.
- Any liability incurred in any case if the error in such verified information is the result of fraud or wilful misconduct of the Subscriber or a Relying Party.

9.8. *Limitations of liability*

The GOM eID PKI accepts financial liability as a Certification Authority, also known as a Signature Certification Service Provider, as defined within Chapter 426, Laws of Malta also known as the Electronic Commerce Act III of 2001 (amended 2002, 2004, 2005 and twice in 2007) for Qualified Certificates that it has issued subject to the following:

(i) the CA shall not be under any liability in respect of any loss or damage (including, without limitation, consequential loss or damage) which may be suffered or incurred or which may arise directly or indirectly in relation to the use or reliance upon Certificates or associated public/private key pairs for any use other than in accordance with this CA and the Subscriber Agreement.

(ii) In any case, the CA's total liability for damages sustained by the Subscriber and any Third Party for any use or reliance on a Certificate shall be limited, in total, to two thousand five hundred Euro (€2,500) per transaction. This limitation shall be the same regardless of the number of Electronic Signatures, transactions or claims relating to such Certificate.

(iii) The CA shall not be under any liability for failure to perform any of its obligations herein where such failure arises from a force majeure event that is an event beyond the CA's reasonable direct control, including, but not limited to, Acts of God (including weather of exceptional severity, floods, lightning or fire), general or local strikes, national emergency, acts or omission of Government or other competent authorities, fire or destruction of the CA's works or materials, insurrection or other civil disorder, war or military operations, or explosions.

The financial limitation of liability is defined within the issued Qualified Certificates and is defined as two thousand five hundred Euro (€2,500) per transaction.

9.9. *Indemnities*

To the extent permitted by law the Subscriber agrees to indemnify and hold the GOM eID PKI harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees that the GOM eID PKI may incur as a result of the Subscriber's negligence or its failure to comply with the Subscriber Agreement or with the terms of this CPS.

9.10. *Term and Termination*

This CPS commences on 10th January 2013 and will continue indefinitely unless and until it is amended in accordance with paragraph 9.12 below.

This CPS may be terminated by the Malta Certification Authority by serving a notice on its web site or via the GOM eID Directory.

9.11. *Individual notices and communications with participants*

Individual communications made to the GOM eID PKI must be addressed to:

Malta Certification Authority
Gattard House

National Road
Blata l–Bajda
Malta

9.12. *Amendments*

Minor changes to this CPS that do not materially affect this CPS are indicated by a version number that contains a decimal number e.g. version 1.1 for a version with minor changes as opposed to version 2.0 that addresses major issues.

Minor changes to this CPS do not require a change in the pointer to this version.

Amendments to this CPS are applicable from the date on which they are published.

9.13. *Dispute resolution provisions*

Any dispute, controversy or claim arising under, out of or relating to this CPS and any subsequent amendments of this CPS, including, without limitation, its formation, validity, binding effect, interpretation, performance, breach or termination, as well as non-contractual claims, shall be referred to and finally resolved by the courts of Malta.

9.14. *Governing law*

This CPS is governed, construed and interpreted in accordance with the laws of Malta.

9.15. *Compliance with applicable law*

The GOM eID PKI complies with applicable laws of Malta.

9.16. *Miscellaneous provisions*

9.16.1. *Entire agreement*

This CPS shall supersede all prior and contemporaneous written or oral understandings relating to the same subject matter. This CPS together with the Certificate Policy, the Relying Party Agreement and the Subscriber Agreement constitutes the entire agreement between the participants in the GOM eID PKI and supersedes all prior agreements, understandings, negotiations and discussions, whether oral or written, of the parties. There are no representations, warranties, covenants, conditions or other agreements, express or implied, collateral, statutory or otherwise, between the parties in connection with the subject matter of this CPS except as specifically set forth herein and none of the GOM eID PKI participants has relied or is relying on any other information, discussion or understanding in entering into and completing the transactions contemplated in this CPS. [Nothing in this paragraph 9.16.1 shall affect any party’s liability arising from its own fraud or fraudulent misrepresentation.

9.16.2. *Assignment*

No rights, obligations or liabilities defined under this CPS may be assigned by a Subscriber or Relying Party to another party without the explicit written permission of the Malta Certification Authority. The Malta Certification Authority may assign its rights and obligations under this CPS to another party.

9.16.3. *Severability*

If any provision of this CPS, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of this CPS shall be interpreted in such manner as to effect the original intention of the parties.

9.16.4. *Enforcement (attorneys' fees and waiver of rights)*

Within the provisions of this CPS a party's waiver of one breach of contract does not constitute a continuing waiver or a future waiver of other breaches of contract.

9.16.5. *Force Majeure*

THE MALTA CERTIFICATION AUTHORITY ON BEHALF OF THE GOVERNMENT OF MALTA ELECTRONIC IDENTITY PUBLIC KEY INFRASTRUCTURE (GOM EID PKI) ACCEPTS NO LIABILITY FOR ANY BREACH OF WARRANTY, DELAY, OR FAILURE IN PERFORMANCE THAT RESULTS FROM EVENTS BEYOND ITS CONTROL SUCH AS ACTS OF GOD, ACTS OF WAR, ACTS OF TERRORISM, EPIDEMICS, POWER OR TELECOMMUNICATION SERVICES FAILURE, FIRE, AND OTHER NATURAL DISASTERS.

9.16.6. *Conflict*

In the event of any conflict between the terms of this CPS and the Agreements, the term of the relevant Agreement shall take precedence to the extent necessary to resolve the conflict.

9.17. *Other provisions*

No stipulation.

10. Appendix 1. References

[1]. RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework (obsoletes RFC 2527)

[2]. RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.

[3]. RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile.

[4]. ISO/IEC 27001:2005 and related standards on information security and infrastructure

[5]. ETSI TS 101 456 v1.4.3 (2007-05): Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Authorities issuing Qualified Certificates

[6]. ETSI TS 101 862 v1.3.3 (2006-01): Qualified Certificate profile

[7]. IDENTITY CARD ACT (CAP. 258) Identity Cards (Issue and Validity) (Amendment) Regulations, 2008 Government Gazette of Malta No. 18,170 - 04.01.2008

[8]. RFC 2560: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP

[9]. RFC 6277: Online Certificate Status Protocol Algorithm Agility. (Updates RFC 2560)

[10]. Chapter 426, Laws of Malta also known as the Electronic Commerce Act III of 2001 (amended 2002, 2004, 2005 and twice in 2007)

[11]. eID PKI Network Architecture V1.7, 2012

[12]. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[13]. CEN/ISSS PPSSCD-Type3-v105 25th July 2001: Secure Signature creation Device Type 3 – Protection Profile.

[14]. NIDMS_Functional_Specification Issue 1.0 Final

11. Appendix 2. Certificate Profiles

This Appendix provides details on the Certificate Profiles and supported extensions for infrastructure Certificates issued by the GOM Root CA.

Details of End Entity Certificates issued by the GOM eID PKI may be found in their respective Certificate Policy documents.

11.1. *GOM Root CA*

The following table gives the GOM Root CA Certificate profile and extension.

GOM Root CA Certificate Profile		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	Sha-2/RSA	
Issuer	CN	Government of Malta Root CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Validity	From:	[Time of issue]
	To:	Time of issue + 30 years
Subject	CN	The same as the issuer
	OU	
	O	
	C	
Public Key Length/Type	4096 bits	
Extensions		
Subject Key Identifier	(sha1 of the Public key of PKCS10)	
Basic Constraints (critical)	Subject Type= CA Path Length Constraint = -1 (none)	
Key Usage (Critical)	KeyCertSign CRLSign	

Certificate Policy	OID= 2.5.29.32.0 [AnyPolicy]
	URL=http://repository.qca.gov.mt	

Table 1: GOM Root CA Certificate profile

11.2. *Malta Citizen eID CA*

The following table gives the Malta Citizen eID CA Certificate profile and extension.

Malta Citizen eID CA Certificate Profile		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	Sha-2/RSA	
Issuer	CN	Government of Malta Root CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Validity	From:	[Time of issue]
	To:	Time of issue + 20 years
Subject	CN	Malta Citizen Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Public Key Length/Type	2048 bits	
Extensions		
Authority Key Identifier	sha1 of the Public Key of Malta Top Root CA	
Subject Key Identifier	sha1 of the Public key of PKCS10	
Basic Constraints (critical)	Subject Type= CA Path Length Constraint = 0	
Key Usage (Critical)	KeyCertSign CRLSign	

CRL Distribution Point	URL=http://crl.qca.gov.mt/rootca.crl
	URI=ldap://ldap.qca.gov.mt/cn=RootCA,o=Government of Malta,c=MT?certificateRevocationList?base
	1.1.	

AuthorityInfoAccess	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crt.qca.gov.mt/RootCA.crt 1.2. [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.qca.gov.mt	

Certificate Policy	OID=2.5.29.32.0 [AnyPolicy]
	OID= 2.16.470.4.2.1 [OID for Malta Citizen Electronic Identity CA Certificate Policy]
	URL= http://repository.qca.gov.mt	

Table 2: Malta Citizen eID CA Certificate profile

11.3. *Malta Resident eID CA*

The following table gives the Malta Resident eID CA Certificate profile and extension.

Malta Resident eID CA Certificate Profile		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	Sha-2/RSA	
Issuer	CN	Government of Malta Root CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Validity	From:	[Time of issue]
	To:	Time of issue + 20 years
Subject	CN	Malta Resident Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Public Key Length/Type	2048 bits	
	Extensions	
Authority Key Identifier	sha1 of the Public Key of Malta Top Root CA	
Subject Key Identifier	sha1 of the Public key of PKCS10	
Basic Constraints (critical)	Subject Type= CA Path Length Constraint = 0	
Key Usage (Critical)	KeyCertSign CRLSign	

CRL Distribution Point	URL=http://crl.qca.gov.mt/rootca.crl
	URI=ldap://ldap.qca.gov.mt/cn=RootCA,o=Government of Malta,c=MT?certificateRevocationList?base	

AuthorityInfoAccess	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crt.qca.gov.mt/RootCA.crt 1.2.1.1.1. [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.qca.gov.mt	

Certificate Policy	OID=2.5.29.32.0 [AnyPolicy]
	OID= 2.16.470.4.3.1 [OID for Malta Resident Electronic Identity CA Certificate Policy]
	URL= http://repository.qca.gov.mt	

Table 3: Malta Resident eID CA Certificate profile

11.4. *GOM Administrator CA*

The following table gives the GOM Administrator CA Certificate profile and extension.

GOM Administrator CA Certificate Profile		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	Sha-2/RSA	
Issuer	CN	Government of Malta Root CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Validity	From:	[Time of issue]
	To:	Time of issue + 20 years
Subject	CN	Government of Malta Administrator CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Public Key Length/Type	2048 bits	
Extensions		
Authority Key Identifier	sha1 of the Public Key of Malta Top Root CA	
Subject Key Identifier	sha1 of the Public key of PKCS10	
Basic Constraints (critical)	Subject Type= CA Path Length Constraint = 0	
Key Usage (Critical)	KeyCertSign CRLSign	

CRL Distribution Point	URL=http://crl.qca.gov.mt/rootca.crl
	URI=ldap://ldap.qca.gov.mt/cn=RootCA,o=Government of Malta,c=MT?certificateRevocationList?base	

AuthorityInfoAccess	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crt.qca.gov.mt/RootCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.qca.gov.mt	

Certificate Policy	OID=2.5.29.32.0 [AnyPolicy]
	OID= 2.16.470.4.4.1 [OID for Government of Malta Administrator CA Certificate Policy]
	URL= http://repository.qca.gov.mt	

Table 4: GOM Administrator CA Certificate profile

11.5. *OCSP profile*

The OCSP profile follows the rfc 2560 [8] and rfc 6277 [9]. No OCSP extensions are supported. The CA supports multiple Certificate status requests in one OCSP request as long as they are signed by the same CA. The description of the fields for this Certificate is contained in the table below.

11.5.1. *OCSP Certificate profile signed by the GOM Root CA*

Malta eID OCSP Certificate signed by Malta Root CA		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	Sha1	
Issuer	CN	Government of Malta Root CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Validity	From:	[Time of issue]
	To:	Time of issue + 1 year
Subject	CN	Government of Malta OCSP Responder
	OU	Class Qualified
	O	Government of Malta
	C	MT
Public Key Length/Type	2048bits	
Extensions		
Authority Key Identifier	sha1 of the Public Key of Malta Root CA	
Subject Key Identifier	sha1 of the Public key of PKCS10	
Key Usage (Critical)	Electronic Signature	
Enhanced Key usage	OCSP signing	
OCSPNoCheck	NULL	

Table 5: Malta OCSP Certificate profile signed by Malta Root CA

11.5.2. *OCSP Certificate profile signed by the Malta Citizen eID CA*

GOM OCSP Certificate signed by Malta Citizen eID CA		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	Sha1	
Issuer	CN	Malta Citizen Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Validity	From:	[Time of issue]
	To:	Time of issue + 1 year
Subject	CN	Government of Malta OCSP Responder
	OU	Class Qualified
	O	Government of Malta
	C	MT
Public Key Length/Type	2048bits	
Extensions		

Authority Key Identifier	sha1 of the Public Key of Malta Root CA
Subject Key Identifier	sha1 of the Public key of PKCS10
Key Usage (Critical)	Digital signature
Enhanced Key usage	OCSP signing
OCSPNoCheck	NULL

Table 6: GOM OCSP Certificate profile signed by Malta Citizen eID CA

11.5.3. *OCSP Certificate profile signed by Malta Resident eID CA*

GOM OCSP Certificate signed by Malta Resident eID CA		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	Sha1	
Issuer	CN	Malta Resident Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Validity	From:	[Time of issue]
	To:	Time of issue + 1 year
Subject	CN	Government of Malta OCSP Responder
	OU	Class Qualified
	O	Government of Malta
	C	MT
Public Key Length/Type	2048bits	
Extensions		
Authority Key Identifier	sha1 of the Public Key of Malta Root CA	
Subject Key Identifier	sha1 of the Public key of PKCS10	
Key Usage (Critical)	Electronic Signature	
Enhanced Key usage	OCSP signing	
OCSPNoCheck	NULL	

Table 7: GOM OCSP Certificate profile signed by Malta Resident eID CA

11.5.4. *OCSP Certificate profile signed by GOM Administrator CA*

GOM OCSP Certificate signed by GOM Administrator CA		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	Sha1	
Issuer	CN	Government of Malta Administrator CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Validity	From:	[Time of issue]
	To:	Time of issue + 1 year
Subject	CN	Government of Malta OCSP Responder
	OU	Class Qualified

	O	Government of Malta
	C	MT
Public Key Length/Type	2048bits	
Extensions		
Authority Key Identifier	sha1 of the Public Key of Malta Root CA	
Subject Key Identifier	sha1 of the Public key of PKCS10	
Key Usage (Critical)	Electronic Signature	
Enhanced Key usage	OCSP signing	
OCSPNoCheck	NULL	

Table 8: GOM OCSP Certificate profile signed by GOM Administrator CA

11.6. *Time Stamp Certificate profile*

The following table gives the Certificate profiles and extensions for the GOM Time Stamp server

GOM Time Stamping Server Certificate signed by GOM Root CA		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	Sha2	
Issuer	CN	Government of Malta Root CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Validity	From:	[Time of issue]
	To:	Time of issue + 10 year
Subject	CN	Government of Malta Timestamp Server
	OU	Class Qualified
	O	Government of Malta
	C	MT
Public Key Length/Type	2048 bits	
Extensions		
Authority Key Identifier	sha1 of the Public Key of Malta Root CA	
Subject Key Identifier	sha1 of the Public key of PKCS10	
Key Usage (Critical)	Electronic Signature; non Repudiation	
Enhanced Key usage (Critical)	Timestamping	

CRL Distribution Point	URL=http://crl.qca.gov.mt/rootca.crl
	URI=ldap://ldap.qca.gov.mt/cn=RootCA,o=Government of Malta,c=MT?certificateRevocationList?base	

Certificate Policy	OID= 2.16.470.4.5.1 [OID for Government of Malta Time Stamping Authority – Unique for each TSA]
	URL=http://repository.qca.gov.mt/CPS.html [Main CPS]	

Table 9: GOM Timestamp Server Certificate Profile

The following table gives the Certificate profiles and extensions for the GOM Timestamp Administrator.

GOM Timestamp Administrator certificate		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	Sha2	
Issuer	CN	Government of Malta Administrator CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Validity	From:	[Time of issue]
	To:	Time of issue + 10 year
Subject	CN	Timestamp Administrator
	OU	Class qualified
	O	Government of Malta
	C	MT
Public Key Length/Type	2048 bits	
Extensions		
Authority Key Identifier	sha1 of the Public Key of Malta Root CA	
Subject Key Identifier	sha1 of the Public key of PKCS10	
Key Usage (Critical)	Electronic Signature; non Repudiation	

CRL Distribution Point	URL=http://crl.qca.gov.mt/adminca.crl
	URI=ldap://ldap.qca.gov.mt/cn=AdminCA,o=Government of Malta,c=MT?certificateRevocationList?base	

Certificate Policy	OID=0.4.0.2042.1.2
	OID= 2.16.470.4.4.1.2 [OID for Government of Malta Administrator CA Certificate Policy]
	URL=http://repository.qca.gov.mt/CPS.html [Main CPS]
	UserNotice=Issued in accordance with and governed by the Government of Malta Certificate Policy Statement which can be found at http://repository.qca.gov.mt/CPS.html	

Table 10: Time Stamp Administrator Certificate

The following table gives the Certificate profiles and extensions for the GOM Timestamp Auditor.

GOM Timestamp Auditor Certificate		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	Sha2	
Issuer	CN	Government of Malta Administrator CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Validity	From:	[Time of issue]
	To:	Time of issue + 10 year

Subject	CN	Timestamp Auditor
	OU	Class qualified
	O	Government of Malta
	C	MT
Public Key Length/Type	2048 bits	
Extensions		
Authority Key Identifier	sha1 of the Public Key of Malta Root CA	
Subject Key Identifier	sha1 of the Public key of PKCS10	
Key Usage (Critical)	Electronic Signature; non Repudiation	

CRL Distribution Point	URL=http://crl.qca.gov.mt/adminca .crl
	URI=ldap://ldap.qca.gov.mt/cn=AdminCA,o=Government of Malta,c=MT?certificateRevocationList?base	

Certificate Policy	OID=0.4.0.2042.1.2
	OID= 2.16.470.4.4.1.3 [OID for Government of Malta Administrator CA Certificate Policy]
	URL=http://repository.qca.gov.mt/CPS.html [Main CPS]
	UserNotice=Issued in accordance with and governed by the Government of Malta Certificate Policy Statement which can be found at http://repository.qca.gov.mt/CPS.html	

Table 11: Time Stamp Auditor Certificate

11.7. *CRL Profiles*

11.7.1. *Root CRL profile*

The GOM Root CRLs are issued in conformance with IETF PKIX RFC 2459.

GOM eID CRL signed by GOM Root CA		
Version	2	
Signature Algorithm	Sha1	
Issuer	CN	Government of Malta Root CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
ThisUpdate	[Time of issue]	
NextUpdate	Time of issue + 3 months	
Revoked Certificates	UserCertificate	Certificate serial number
	RevocationDate	revocation time
CRL Extensions		
Authority Key Identifier	Sha1 of the Public Key of Malta Root CA	
CRL Number	CA assigned unique name	

Table 12: Root CRL profile

11.7.2. *SubCA CRL profile*

Every issuing CA within the GOM eID PKI will generate its own CRL that gives the status of its Certificates.

A new CRL is generated whenever a Certificate has been revoked.

Each Certificate revoked shall have a revocation reason. The following tables provide details of the CRL profile for the Malta Citizen eID CA, Malta Resident eID CA and GOM Administrator CA.

11.7.3. *Citizen CRL profile*

GOM eID CRL signed by Malta Citizen eID CA		
Version	2	
Signature Algorithm	Sha1	
Issuer	CN	Malta Citizen Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
ThisUpdate	[Time of issue]	
NextUpdate	Time of issue + 6 days	
Revoked Certificates	UserCertificate	Certificate serial number
	RevocationDate	revocation time
CRL Extensions		
Authority Key Identifier	Sha1 of the Public Key of Malta Citizen CA	
CRL Number	CA assigned unique name	

Table 13: Citizen CRL profile

11.7.4. *GOM eID Resident CRL profile*

GOM eID CRL signed by Malta Resident eID CA		
Version	2	
Signature Algorithm	Sha1	
Issuer	CN	Malta Resident Electronic Identity CA
	OU	Class Qualified
	C	MT
ThisUpdate	[Time of issue]	
NextUpdate	Time of issue + 6 days	
Revoked Certificates	UserCertificate	Certificate serial number
	RevocationDate	revocation time
CRL Extensions		
Authority Key Identifier	Sha1 of the Public Key of Malta Resident CA	
CRL Number	CA assigned unique name	

Table 14: GOM eID Resident CRL profile

11.7.5. *Admin CRL profile*

GOM eID CRL signed by GOM Administrator CA		
Version	2	
Signature Algorithm	Sha1	
Issuer	CN	Government of Malta Administrator CA
	1.3.	Class Qualified

	O	Government of Malta
	C	MT
ThisUpdate	[Time of issue]	
NextUpdate	Time of issue + 6 days	
Revoked Certificates	UserCertificate	Certificate serial number
	RevocationDate	revocation time
CRL Extensions		
Authority Key Identifier	Sha1 of the Public Key of Malta Admin CA	
CRL Number	CA assigned unique name	

Table 15: GOM eID Admin CRL profile