Government of Malta Electronic Identity Scheme Certification Practice Statement

Date of Issue: 17/04/2020

Version Number: 2.2

This document is the Government of Malta (GOM) Certification Practice Statement for the national electronic Identity Card scheme (eID) for Citizens and Residents as defined within the Identity Card Act, Chapter 258 Laws of Malta.

Change Record

Date	Author	Version	QA	Description of Change
14/09/2018	DLR	1.5	MECS	Initial draft based on existing CP & CPS
23/01/2019	IMA	1.6	MECS	Reviewed and updated for publishing
18/02/2019	IMA	1.7	MECS	Incorporated DLR changes for publishing
22/02/2019	DLR/IMA	1.8	MECS	Profile changes for updated PKI
26/02/2019	IMA	1.9	MECS	Revised for consistent versioning
12/03/2019	IMA	2.0	MECS	Consistent language update
03/09/2019	IMA	2.1	MECS	Clarifications incorporated from feedback.
17/04/2020	IMA	2.2	MECS	Adjustments for Regulatory Body

Document Details

Detail	
Title	Government of Malta Electronic Identity Scheme Certification Practice Statement
Filing Reference	GOM_eID_CPS_V2.2_PUB
Owner	MECS, Policy Management Authority (PMA)
Change Authority / Approver	PMA
Distributor	PMA

Reviewers

Name	Position
Name: Greg Smith	Sr. Manager ICT
Name	
Name	

Table of Contents

CONFIDENTIAL

CONFIDENTIAL

CONFIDENTIAL

1 INTRODUCTION

1.1 Overview

This document is the Certification Practice Statement (CPS) for the Government of Malta (GOM) national electronic Identity Card scheme (eID) for Citizens and Residents as defined within the Identity Card Act, Chapter 258 Laws of Malta [1].

A CPS is a statement of the practices that a Certification Authority Trust Service Provider (TSP) employs in issuing managing, revoking, and renewing or re-keying Certificates to satisfy the requirements specified in the governing Certificate Policy (CP).

This CPS is structured according to the guidelines provided by IETF RFC 3647 [2] and applies to authorised Participants of the GOM eID Public Key Infrastructure (PKI) whereby compliance with this CPS is prescribed via the governing Certificate Policies, agreement or contractual requirement. This includes but is not limited to all Participants whose organisations provide one of more of the following services: Registration Service; Certificate Generation Service; Dissemination Service; Subject Device Provision Service; Revocation Management Service; Certificate Revocation Status Service.

The GOM has commissioned Malta Electronic Certification Services Ltd., hereafter referred to as MECS, as the TSP for the GOM Citizen and Resident eID PKI. MECS is the legal entity issuing certificates under this CPS. MECS is also the Policy Management Authority for the Public Key Infrastructure (see section 1.3.5.1).

MECS has nominated IMA as the primary Participant for management of the GOM eID Public Key Infrastructure and provision of the Public Key Infrastructure's operational services.

The electronic Identity Card scheme issues the following cards which contain Subscriber Certificates issued from the GOM eID PKI (comprising the GOM Citizen and Resident eID PKI):

- National electronic Identity Card, for use by Citizens of Malta.
- National electronic Resident Card for use by Residents of Malta.
- Administrator Card for use by the Registration Service and Revocation Management Service (National Identity Management System) administrators.

Other Certificates are issued internally to support the GOM eID PKI.

The Public Key Infrastructure which underpins the national electronic Identity Card scheme comprises a Certificate hierarchy containing a Root CA Certificate, Sub-CA Certificates, and End Entity Certificates. Each CA Certificate and associated CA private key is managed by a Certificate Authority application that provides PKI services such as Certificate and CRL issuance, Certificate lifecycle management. The End Entity Certificates are issued to users and Certificate using systems and devices. The names for, and the relationship between these Certificates are shown in Figure 1 and described below.

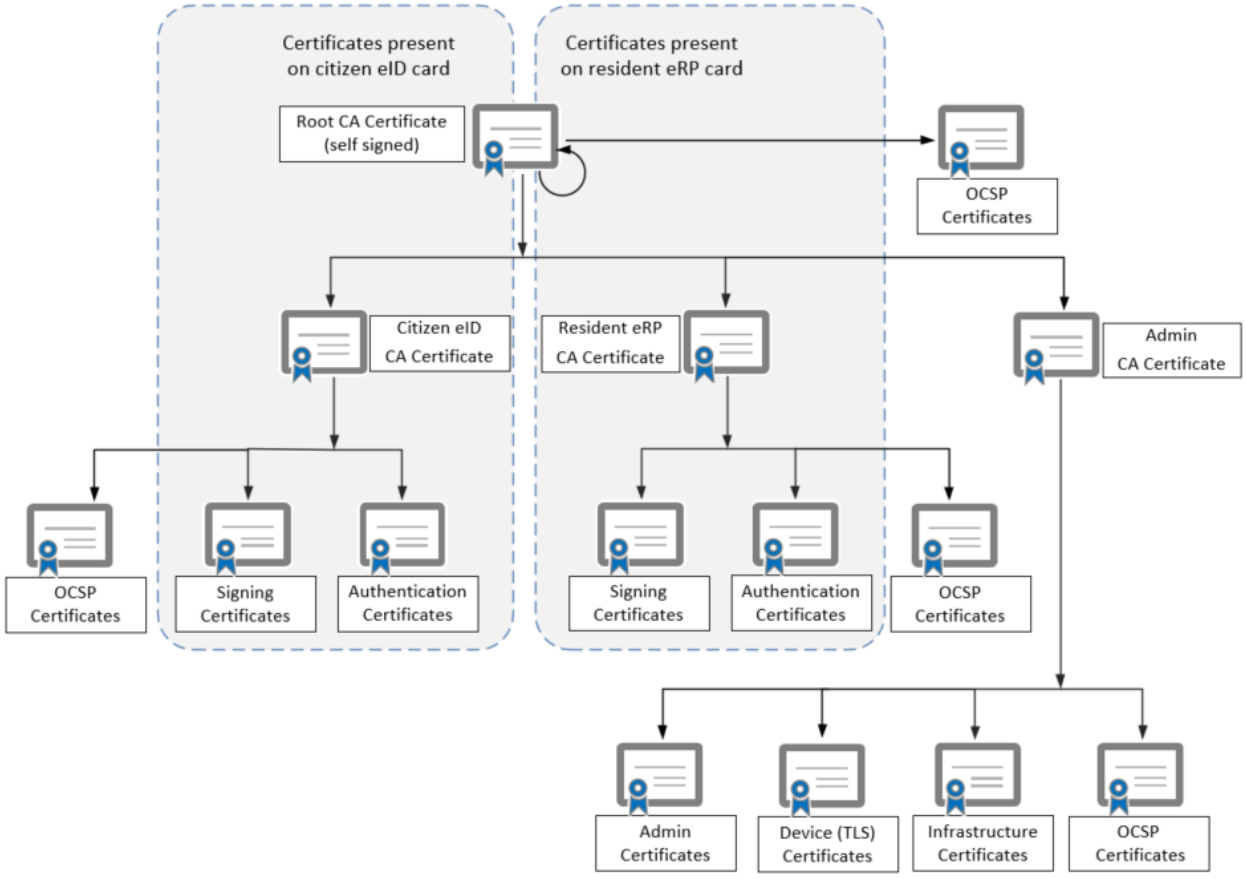

Figure 1: GOM eID PKI Certificate Hierarchy

1. GOM Root CA Certificate: The GOM Root CA Certificate is the trust anchor point within the GOM eID PKI and issues the following Certificates:

- Citizen eID CA Certificate.
- Resident eRP CA Certificate.
- Administrator CA Certificate.
- OCSP Response Signing Certificates.

2. Citizen eID CA Certificate. The Citizen eID CA issues:

- Citizen Qualified Electronic Signature Certificates.
- Citizen Authentication Certificates.
- OCSP Response Signing Certificates.

The Citizen Qualified Electronic Signature Certificate and Authentication Certificates are used for the purposes defined in the associated CP [3].

3. Resident eRP CA Certificate. The Resident eID CA issues:

- Resident Qualified Electronic Signature Certificates
- Resident Authentication Certificates
- OCSP Response Signing Certificates.

CONFIDENTIAL

The Resident Qualified Electronic Signature Certificate and Authentication Certificates are used for the purposes defined in the associated CP [4].

4. Administrator CA Certificate. The Administrator CA issues:

- Administrator (LRAA, RMAA, LRAO, RMAO, RMIO, CRAO, etc.) Authentication Certificates.
- OCSP Response Signing Certificate.
- Infrastructure and device Certificates e.g. internal signing Certificates, SSL Certificates.

The Administrator Authentication Certificates are used for the purposes defined in the associated CP [5].

MECS Ltd. is a Qualified Trust Service Provider (QTSP), issuing the qualified certificates noted above, as documented in the Maltese national trusted list at https://www.mca.org.mt/tsl/MT_TSL.xml under the supervision of the Malta Communications Authority.

All Certificates other than those present on Citizen and Resident Identity Cards and Administrator Cards are used internally by GOM eID PKI Participant organisations for the management and operation of the PKI. These Certificates are referred to as internal Certificates within this document[1]. This includes Certificates for management of the CA systems e.g. CAO Certificates, and Certificates for Registration Authority infrastructure components e.g. NIDMS, Smartcard Management System.

The various terms used throughout this document are explained in the Glossary located at https://repository.qca.gov.mt/.

Capitalisation is used throughout this document for referencing defined terms with the exception of section headings which have been retained in the format compliant with RFC 3647.

1.2 Document name and identification

This Certification Practice Statement is named “Government of Malta Electronic Identity Scheme Certification Practice Statement” and has been assigned an OID of 2.16.470.4.1.1.1.

This Certification Practice Statement specifies the practices implemented by GOM eID PKI Participants in meeting the policy requirements specified in the following Certificate Policies:

- Government of Malta Certificate Policy for Citizen Authentication Certificates and Citizen Qualified Electronic Signature Certificates [3].
- Government of Malta Certificate Policy for Resident Authentication Certificates and Resident Qualified Electronic Signature Certificates [4]
- Government of Malta Certificate Policy for Administration Certificates [5]

1.3 PKI participants

As a TSP, MECS has an obligation to operate a Public Key Infrastructure in accordance with the defined Certificate Policy. MECS does not however have to conduct all aspects of Public Key Infrastructure operations itself. There are sets of services that are logically and conveniently grouped and delegated.

[1] Only the OCSP, infrastructure and device internal certificates are shown in figure 1.

1.3.1 Certification authorities

Refer to the governing Certificate Polices (listed in section 1.2 of the current document) for a description of Certification Authorities.

1.3.2 Registration authorities

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for a description of Registration Authorities.

1.3.3 Subscribers

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for a description of Subscribers.

1.3.4 Relying parties

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for a description of Relying Parties.

1.3.5 Other participants

1.3.5.1 Policy Management Authority

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for a description of the PMA.

1.3.5.2 Certification Services Providers

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for a description of Certification Services Providers.

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for a description of appropriate Certificate uses.

1.4.2 Prohibited certificate uses

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for a description of prohibited Certificate uses.

1.5 Policy administration

1.5.1 Organization administering the document

MECS is responsible for this CPS, its management and change control, and can be contacted as follows:

Contact Person: CA Manager

Postal Address: MECS Ltd., ONDA Building, Aldo Moro Street, Marsa, MRS9065, Malta

Telephone: +356 25904900

E-mail: info.mecs@gov.mt

1.5.2 Contact person

In the first instance, MECS should be contacted regarding the contents of this CPS. Refer to section 1.5.1 for the contact details.

1.5.3 Person determining CPS suitability for the policy

MECS determines the suitability of any CPS operating under the governing Certificate Policies (listed in section 1.2 of the current document).

1.5.4 CPS approval procedures

1.6 The Policy Management Authority determines the suitability and approves the use of any Certification Practice Statement. Definitions and acronyms

Refer to the Glossary at https://repository.qca.gov.mt/ for a description of the applicable definitions and acronyms.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The Repository publishes the information defined in section 2.2 of the governing Certificate Policies (listed in section 1.2 of the current document) as part of the Dissemination Service and Certificate Status Service. The Repository comprises the following components:

- Website and eID Directory hosting the information defined in the governing Certificate Policies (including CRL information).
- An OCSP system providing Certificate status information for all Certificates issued under the governing Certificate Policies.

The provision of Certificate status information via the CRLs and the OCSP services together comprises the Certificate Status Service.

Publication of certification information

The repository locations and publishing systems for the CA Certificates and CRLs are shown below.

Artefact	Published By	Location	Access URL
Root CA Certificate	Root CA	Website Directory	https://crt.qca.gov.mt/RootCA_rs.crt
Root CA ARL	Root CA	Website Directory	https://crl.qca.gov.mt/RootCA.crl URI=ldap://ldap.qca.gov.mt/cn=CitizenCA,o=Government of Malta,c=MT?certificateRevocationList?base
Citizen eID CA Cert	Citizen eID CA	Website Directory	https://crt.qca.gov.mt/CitizenCA.crt
Citizen eID CA CRL (master)	Citizen eID CA	Website Directory	https://crl.qca.gov.mt/Master_CitizenCA.crl

CONFIDENTIAL

Artefact	Published By	Location	Access URL
Citizen eID CA CRL	Citizen eID CA	Website Directory	https://crl.qca.gov.mt/CitizenCA.crl URI=ldap://ldap.qca.gov.mt/cn=CitizenCA,o=Government of Malta,c=MT?certificateRevocationList?base
Citizen eID CA Partitioned CRL	Citizen eID CA	Website Directory	https://crl.qca.gov.mt/CitizenCA_YYYY_NNN.crl[2] URI=ldap://ldap.qca.gov.mt/cn=CitizenCA_YYYY_NNN,o=Government of Malta,c=MT?certificateRevocationList?base
Resident eRP CA Cert	Resident eID CA	Website Directory	https://crt.qca.gov.mt/ResidentCA.crt
Resident eRP CA CRL	Resident eID CA	Website Directory	https://crl.qca.gov.mt/ResidentCA.crl

Table 1: CA Certificate and CRL locations

Citizen eID CA CRL (master) contains revocation information for all certificates issued from the Citizen CA.

Citizen eID CA CRL contains revocation information for all certificates issued from the Citizen CA prior to production of the first partitioned CRL.

Resident eID CA CRL (master) contains revocation information for all certificates issued from the Resident CA.

Resident eID CA CRL contains revocation information for all certificates issued from the Resident CA prior to production of the first partitioned CRL.

Certificate status information for all Certificates is available at http://ocsp.qca.gov.mt/.

The following policy and practice documents are published to the website https://crt.qca.gov.mt/ under control of the MECS:

- Government of Malta Certificate Policy for Citizen Authentication Certificates and Citizen Qualified Electronic Signature Certificates.
- Government of Malta PKI Disclosure Statement for Citizen Authentication Certificates and Citizen Qualified Electronic Signature Certificates.
- Government of Malta Certificate Policy for Resident Authentication Certificates and Resident Qualified Electronic Signature Certificates.

[2] The Citizen CA partitions CRLs to manage their size and increase performance. This means periodically changing the CRL location after a defined number of certificates has been issued. YYYY represents the year and NNN represents the CRL number in that year e.g. 2015_004.

CONFIDENTIAL

- Government of Malta Resident PKI Disclosure Statement for Resident Authentication Certificates and Resident Qualified Electronic Signature Certificates.
- Government of Malta Electronic Identity Scheme Certification Practice Statement (this document).
- Citizen eID Card Subscriber Agreement.
- Resident eRP Card Subscriber Agreement.
- Relying Party Agreement.

Archive information for the artefacts shown in the table above and the policy and practice documents listed above is held at https://repository.qca.gov.mt/Archive/.

Certificate Policies, related documents and CA Certificates are republished as required by the change control process for the repository and in accordance with the certification services procedures.

2.2 Time or frequency of publication

CA Certificates are published once they are manufactured and introduced into production operations. Certificate Status Information is published in accordance with the governing Certificate Policies (listed in section 1.2 of the current document). Subscriber CRLs are published at least hourly. CA CRLs are published at least every 92 days.

2.3 Access controls on repositories

Only Trusted Role holders, as specified in section 5 of this CPS have write and change access to the Repository. The TSP has ensured that appropriate security measures have been implemented to protect the Repository and to monitor access and maintenance.

Repository access control and management is undertaken in accordance with the certification services procedures.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Naming conventions are operated in conformance with the governing Certificate Policies (listed in section 1.2 of the current document).

3.1.2 Need for names to be meaningful

Naming conventions are operated in conformance with the governing Certificate Policies (listed in section 1.2 of the current document).

3.1.3 Anonymity or pseudonymity of subscribers

Anonymity or pseudonymity of Subscribers is operated in conformance with the governing Certificate Policies (listed in section 1.2 of the current document).

3.1.4 Rules for interpreting various name forms

Rules are interpreted in conformance with the governing Certificate Policies (listed in section 1.2 of the current document).

3.1.5 Uniqueness of names

Name uniqueness is interpreted in conformance with the governing Certificate Policies (listed in section 1.2 of the current document).

3.1.6 Recognition, authentication, and role of trademarks

Recognition, authentication and role of trademarks are operated in conformance with the governing Certificate Policies (listed in section 1.2 of the current document).

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

Identity Card and Administrator Card key pairs are generated on the Subscriber card by the Card Management System as part of the Subject Device Provision Service. Certificate requests are created in PKCS#10 format and submitted to the appropriate Certificate Generation Service Certificate Authority by the Card Management System. The PKCS#10 format permits the Certificate Authority to prove the key generating entity (Subscriber card) has possession of the private key.

For internal Certificates the key pair generation and request procedures also involves PKCS#10 to prove possession of the private key.

3.2.2 Authentication of organization identity

Certificates issued for purposes other than inclusion in Identity Cards and Administrator Cards are internal Certificates issued to Participants supporting the operation of the GOM eID PKI. In all cases, the Certificate request is made using a request and procedure authorised and approved by the PMA. The request is signed by an authorised Participant member of staff who has been validated as belonging to and authorised to act on behalf of the Participant organisation. All activities are undertaken in accordance with the MECS internal certificate management procedures.

3.2.3 Authentication of individual identity

Identity Card Subscriber identity is established during a registration process involving the physical presence of the Subscriber and the collection and verification of Subscriber information. At a minimum this includes the Subscriber details defined in the Identity Card Act, Chapter 258 Laws of Malta [1]. All activities are undertaken in accordance with the MECS certification services procedures.

Administrator Card Subscriber Identity is established using an IMA internal process similar to that described above involving the physical presence of the Subscriber and the collection and verification of Subscriber information. All activities are undertaken in accordance with the MECS certification services procedures.

See section 3.2.2 for internal Certificates.

3.2.4 Non-verified subscriber information

The use of non-verified Subscriber information is in accordance with the governing Certificate Policies (listed in section 1.2 of the current document). Using information for non-verified subscribers is not applicable. The only subscribers allowed are verified subscribers.

3.2.5 Validation of authority

See section 3.2.2.

3.2.6 Criteria for interoperation

Criteria for interoperation is defined in the governing Certificate Policy (listed in section 1.2 of the current document).

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

All Certificates issued under the governing Certificate Policies (listed in section 1.2 of the current document) follow the procedure used for initial Certificate issuance. See section 3.2.3.

3.3.2 Identification and authentication for re-key after revocation

All Certificates issued under the governing Certificate Policies (listed in section 1.2 of the current document) follow the procedure used for initial Certificate issuance. See section 3.2.3.

3.4 Identification and authentication for revocation request

Identity Card Certificate Revocation is carried out by the Certificate Revocation Management Service. Prior to a revocation being carried out, the Certificate Revocation Management Service validates the requestor's identity during a face-to-face engagement and identifies the Certificate(s) to be revoked. The procedures for identification and authentication of a revocation request are undertaken in accordance with the MECS certification services procedures.

Administrator Card Certificate Revocation is carried out using a similar process to that described above. All activities are undertaken in accordance with the MECS certification services procedures.

For internal Certificates, the revocation request is made using a request and procedure authorised and approved by the PMA. The request is signed by an authorised Participant member of staff who has been validated as belonging to and authorised to act on behalf of the Participant organisation. All activities are undertaken in accordance with the MECS internal certificate management procedures.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Subscribers eligible to submit Certificate applications are defined in the governing Certificate Policies (listed in section 1.2 of the current document).

The Registration Service procedures ensure Certificate applications are only accepted from eligible Subscribers. Activities are undertaken in accordance with the MECS certification services and internal certificate management procedures.

4.1.2 Enrolment process and responsibilities

Identity Card Subscribers enrol by completing an initial registration process at a local Registration Authority office where their credentials, including biometric data, are captured and validated, their eligibility to hold an Identity Card validated and approved, and the application reviewed and authorised.

Credentials capture and validation is carried out by the Local Registration Authority Officer (LRAO) for Citizen Certificates and the Residence Card Management Authority Officer (RMAO) for Resident Certificates). Further validation and approval is carried out by the Local Registration Authority

Administrator (LRAA) for Citizen Certificates and the Residence Card Management Authority Administrator (RMAA) for Resident Certificates. Final review and authorisation are carried out by the Central Registration Authority Officer (CRAO). The application is then passed for production processing.

The enrolment process and associated responsibilities for Citizen and Resident Subscribers obtaining Identity Cards are undertaken in accordance with the MECS certification services procedures and published online by MECS.

Administrator card Subscriber enrolment follows a similar process to that described above. All activities are undertaken in accordance with the MECS certification services procedures.

For internal Certificates, the Certificate Authorities support a direct Registration Authority interface for use solely for the enrolment, issuance and maintenance of internal certificates. For this purpose, the Certificate Authority Officer (CAO) is permitted to perform manual registration for internal Certificates using procedures approved by the MECS. All activities are undertaken in accordance with internal certificate management procedures.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Identification and authentication of Subscribers is described in section 3.2. The TSP approves all Registration Service Participants acting on its behalf that are permitted to conduct identification and authentication of Subscribers.

4.2.2 Approval or rejection of certificate applications

Upon successful completion of the dual approval registration process referred to in section 4.1.2, the Central Registration Authority Officer (CRAO) authorises via NIDMS the creation of the required Identity Card or Administrator Card as appropriate, including the associated Subscriber Certificate(s). All procedures are undertaken in accordance with the MECS certification services procedures.

Internal PKI Certificates are approved manually by the Certificate Authority Operator in accordance with internal certificate management procedures.

4.2.3 Time to process certificate applications

For the time to process applications, refer to the governing Certificate Policies (listed in section 1.2 of the current document).

4.3 Certificate issuance

4.3.1 TSP actions during certificate issuance

For Identity Cards and Administrator Cards, the authorisation provided by the CRAO (see section 4.2.2) instructs NIDMS to generate the appropriate card request message which is sent to the card Subject Device Provision Service for processing. The Card Management System (part of the Subject Device Provision Service) initiates the generation of Subscriber private keys on the allocated Subscriber smart card and submits the associated Certificate request(s) to the appropriate Certificate Generation Service Certificate Authority. Issued Certificates are returned to the Subject Device Provision Service for import into the Subscriber smart card. All activities are undertaken in accordance with the MECS certification services procedures.

For internal Certificates, Certificate requests are submitted and approved manually by the Certificate Authority Operator. Certificates are generated by the Certificate Generation Service in response to the Certificate Authority Operator approval. All activities are undertaken in accordance with the internal certificate management procedures.

For Identity Cards and Administrator Cards, Certificates are automatically issued by the Certificate Generation Service in response to a properly constructed and signed request from the Subject Device Provision Service. All activities are undertaken in accordance with the MECS certification services procedures.

For internal Certificates, Certificates are issued directly after Certificate Authority Operator approval, in accordance with internal certificate management procedures.

Only approved Registration Services and Subject Device Provision Services can communicate with the Certificate Generation Service to submit a certificate request.

4.3.2 Notification to subscriber by the TSP of issuance of certificate

For Identity Cards, Subscribers either receive their Identity Card via post, or receive their card PIN via post. Receipt of a card PIN via the post is taken as notification that the Identity Card containing the Subscriber Certificate(s) is ready for collection. All activities are undertaken in accordance with the MECS certification services procedures.

For internal Certificates, the Certificate Authority Operator manages the full Certificate lifecycle and notifies the Subscriber as required, in accordance with internal certificate management procedures.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

For Identity Cards and Administrator Cards, the Subscriber is required to sign a Subscriber Agreement accepting delivery of the card and any Certificates embedded within the card. All activities are undertaken in accordance with the MECS certification services procedures.

The Subscriber's acceptance of the agreement is recorded and retained in accordance with section 5.4.

The Subscriber is responsible for checking the visible details associated with their card upon receipt of the card (for example the name) and asking for revocation of the card (and hence Certificates contained within the card) if these details are not correct.

For internal Certificates, the applicant accepts and uses the Certificate in accordance with their Trusted Role status. All activities are undertaken in accordance with the internal certificate management procedures.

4.4.2 Publication of certificates by the TSP

Subscriber Certificates are not published. CA certificates are published to the repository in accordance with the certification services procedures.

4.4.3 Notification of certificate issuance by the TSP to other entities

The Certificate Generation Service does not directly inform any other Participants of the issuance of a Certificate.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for a description of Subscriber private key and Certificate usage.

4.5.2 Relying party public key and certificate usage

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for a description of Relying party public key and Certificate usage.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details of Certificate renewal. Certificate renewals are not applicable under current policy.

4.6.2 Who may request renewal

See section 4.6.1.

4.6.3 Processing certificate renewal requests

See section 4.6.1.

4.6.4 Notification of new certificate issuance to subscriber

See section 4.6.1.

4.6.5 Conduct constituting acceptance of a renewal certificate

See section 4.6.1.

4.6.6 Publication of the renewal certificate by the CA

See section 4.4.2.

4.6.7 Notification of certificate issuance by the TSP to other entities

See section 4.4.3..

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details of Certificate re-key. Participating parties follow sections 4.1 to 4.4 for certificate re-keys as new applications. Certificate Authorities requesting re-keys will follow MECS certification services procedures.

4.7.2 Who may request certification of a new public key

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

4.7.3 Processing certificate re-keying requests

Refer to the governing Certificate Policies (listed in section 1.2 of the current document). Processing certificate re-keying requests follow MECS certification services procedures.

4.7.4 Notification of new certificate issuance to subscriber

4.7.5 Subscribers refer to section 4.7.1 for re-key circumstances. Conduct constituting acceptance of a re-keyed certificate

Subscribers refer to section 4.7.1 for re-key circumstances.

4.7.6 Publication of the re-keyed certificate by the TSP

Publications of re-keyed certificates will be done according to MECS certification services procedures to the repository.

4.7.7 Notification of certificate issuance by the TSP to other entities

Not applicable.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details of Certificate modification.

4.8.2 Who may request certificate modification

Not applicable.

4.8.3 Processing certificate modification requests

4.8.4 Not applicable. Notification of new certificate issuance to subscriber

Not applicable.

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable.

4.8.6 Publication of the modified certificate by the TSP

Not applicable.

4.8.7 Notification of certificate issuance by the TSP to other entities

4.9 Not applicable. Certificate revocation and suspension

4.9.1 Circumstances for revocation

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for circumstances for revocation.

4.9.2 Who can request revocation

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details on who can request revocation.

4.9.3 Procedure for revocation request

Certificate revocation requests for Identity Cards and Administrator Cards will be received by the Revocation Management Service which will authenticate the requestor, validate the reason for the request, determine the Certificate(s) to be revoked, and make an assessment based on the circumstances, information provided and the identity of the submitting party as to whether the Certificate(s) should be revoked.

Applicants can submit a revocation request using one of the methods described below:

- Online (through e-mail or web portal).
- Phoning the Revocation Management Service (IMA - Identity Cards) helpdesk.
- Calling personally at the Revocation Management Service office.

In all cases, such requests are processed by the Revocation Management Service helpdesk. Authentication of persons submitting requests online or by phone is done by the helpdesk through phone contact with the requestor to verify their identity through confirmation of any of their personal data.

In order for a revocation of Certificates to be carried out, the applicant has to personally call at the Revocation Management Service Office and present his/her identification (or alternative) document (except in cases where the request is made by a reliable third-party established by the PMA).

In all other cases the Revocation Management Service limits itself to temporarily suspending the Certificates – the Subscriber would be asked to call personally at the Revocation Management Service office so that revocation could then be completed.

If, subsequent to submitting a revocation/suspension request, the applicant informs the Revocation Management Service that he/she would wish to lift the suspension (i.e. to rescind a suspension) he/she would be required to call personally at the Revocation Management Service to confirm this. In those cases where a person requests the issuance of a Certificate after this has been revoked, the person is required to apply for a new identification document.

Once approved by the Revocation Management Service, the revocation request will be processed automatically, and the new Certificate status published with the next CRL.

All activities are undertaken in accordance with the MECS certification services procedures.

Internal Certificate revocation requests are processed according to the internal certificate management procedures which are approved by the TSP.

4.9.4 Revocation request grace period

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details of revocation request grace period. All activities are undertaken in accordance with the MECS certification services procedures.

Time within which Certification Authority must process the revocation request:

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details on revocation request processing times.

The cumulative time incorporates the time for the revocation request to be received and acknowledged until the time the PMA has authorised the revocation, and the time from the authorisation to the time the revocation is entered into the CRL.

4.9.5 Revocation checking requirement for relying parties

Certificate status checking requirements for Relying Parties are defined in section 4.5.2.

Specific status checking mechanisms are defined in Section 2. Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details of revocation checking requirements for Relying Parties.

4.9.6 CRL issuance frequency (if applicable)

Subscriber CRLs are published at least hourly. CA CRLs are published at least every 92 days. See Section 2.2.

4.9.7 Maximum latency for CRLs (if applicable)

The maximum latency of CRL issuance after a status change shall be 24 hours.

4.9.8 On-line revocation/status checking availability

The availability of on-line Certificate Status checking shall be published by the TSP in accordance with Section 4.10.

4.9.9 On-line revocation checking requirements

See section 4.9.5.

4.9.10 Other forms of revocation advertisements available

No stipulation.

4.9.11 Special requirements regarding key compromise

In the event of the compromise, or suspected compromise, of a Subscriber's Private Key, the Subscriber shall notify the Revocation Management Service immediately and shall indicate the nature and circumstances of the compromise, to the fullest extent known.

CA key compromise is discussed in section 5.7.1.

4.9.12 Circumstances for suspension

Certificates shall be suspended in the following circumstances:

- When a Subscriber requests a Certificate revocation and the Subscriber is authenticated but is not physically present.
- When a Subscriber requests a Certificate suspension.

When a request is received with appropriate authentication from a person who has power of attorney, or any reliable third-party, as defined in section 4.9.14.

4.9.13 Who can request suspension

Requests for suspension of Certificates shall only be accepted from:

- Certificate Subscribers.
- Any person who has a power of attorney to manage Identification Documents on behalf of an electronic Identity Card holder.

Any reliable third-party which shall be established as such by the Policy Management Authority. 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).

4.9.14 Procedure for suspension request

The procedure for suspension request follows that presented in in section 4.9.3 with the following differences:

- The request is for Certificate suspension rather than Certificate revocation.

- A face-to-face meeting is not required.

4.9.15 Limits on suspension period

Currently there are no limits on the suspension period.

4.10 Certificate status services

4.10.1 Operational characteristics

Operational characteristics are covered in the certification services procedures. Methods of publication of certificate information are outlined in section 2.

4.10.2 Service availability

Certificate status information shall be made available via CRLs and the OCSP protocol. CRL Certificate status information shall include status information on expired Certificates. The specifics are listed in section 2 of this document.

To support Subscribers and Relying Parties and provide flexibility to users, the GOM PKI is in multiple locations and formats.

The definitive status of a certificate is provided via the OCSP method. It is recommended this mechanism is used. One may also check certificate revocation lists, these however, are provided for assistance and convenience only.

4.10.3 Optional features

Any optional features are covered in the certification services procedures.

4.11 End of subscription

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details of end of subscription.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Not applicable. Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details of key escrow and recovery policy and practices. Refer to section 6.2 to see information on key escrow and recovery practices for CA keys.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable..

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

All Certification Services facilities are located at sites offering appropriate physical and environmental protection in accordance with the governing Certificate Policies (listed in section 1.2 of the current document)

Back-end systems providing the Certificate Generation Service, Dissemination Service, Revocation Status Service, and other systems e.g. NIDMS, Smartcard Management System, that support these core systems plus other Certification Services are located at MITA data centres.

Front-end systems that provide PKI services and interface to back-end systems e.g. Registration Service systems and Revocation Management Service systems are located at facilities subject to MECS approval.

Facilities for back-end services are described in MECS certification services physical descriptions.

5.1.2 Physical access

Physical access to Certification Services systems is restricted to authorised persons who are members of staff. Unauthorised personnel e.g. technical support personnel, are admitted only when approved and accompanied by an authorised person. These controls are described in the MECS certification services procedures.

5.1.3 Power and air conditioning

Certification Services facilities have power and air conditioning facilities as described in the MECS certification services physical descriptions.

5.1.4 Water exposures

Certification Services facilities have protection against water exposure as described in the MECS certification services physical descriptions.

5.1.5 Fire prevention and protection

Certification Services facilities have fire prevention and protection facilities as described in the MECS certification services physical descriptions.

5.1.6 Media storage

All media related to Certification Services activity is stored within Certification Services facilities as described in the MECS certification services physical descriptions.

Access to this media is controlled as described in the MECS certification services procedures.

5.1.7 Waste disposal

All sensitive waste material is disposed of as described in the MECS certification services procedures.

5.1.8 Off-site backup

All material which is moved off-site from any Certification Services facility is protected both while in transit and while stored at the off-site location as described in the MECS certification services procedures.

5.2 Procedural controls

5.2.1 Trusted roles

All activities that may impact PKI facilities, support services, authentication or validity of Certificates require pre-vetted, authorised and approved staff. Such staff are allocated trusted roles to ensure conformance with the governing Certificate Policies (listed in section 1.2 of the current document).

The definitions of and the associated requirements and management procedures for the trusted roles associated with the secure operation of Certification Services are provided in the trusted role procedures.

5.2.2 Number of persons required per task

Service critical functions are performed under multi-person control. These functions and the associated authorised persons are described in the MECS certification services procedures. Procedural and physical mechanisms are used to enforce multi person control.

Operational CA keys are always managed under multi person control.

5.2.3 Identification and authentication for each role

Identification and authentication of staff for the various roles and in particular, trusted roles, is undertaken in accordance with the trusted role procedures.

All persons who perform a Certification Services trusted role have both their identity and their current authority to perform that role verified in accordance with the trusted role procedures.

5.2.4 Roles requiring separation of duties

Certification Services duties that cannot be performed by single individuals are described in the trusted role procedures.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Background, qualifications, experience, security clearance and other personnel criteria are prescribed and checked via formal mechanisms to ensure support for the governing Certificate Policies (listed in section 1.2 of the current document). In addition, local requirements may be imposed as a result of local policies and risk management activities.

Prior to being allocated a trusted role, staff must undertake appropriate induction procedures and be approved prior to commencing trusted role duties in accordance with the trusted role procedures.

5.3.2 Background check procedures

For some trusted roles, where applicable, the GOM and/or other Participants conduct background checks on staff. Background checking requirements for those serving in trusted roles are described in in the trusted role procedures.

5.3.3 Training requirements

Appropriate training is provided to all trusted role staff. This is tailored to each trusted role. All activities are undertaken in accordance with the trusted role procedures.

5.3.4 Retraining frequency and requirements

Appropriate update training is provided to all trusted role staff in accordance with the trusted role procedures.

5.3.5 Job rotation frequency and sequence

Job rotation requirements are undertaken by Participants providing Certification Services provided that the provisions of the governing Certificate Policies (listed in section 1.2 of the current document) are maintained.

5.3.6 Sanctions for unauthorized actions

Unauthorised actions by members of staff are subject to formal personnel and Information System Security Management procedures. Details of the processes and sanctions are described in the trusted role procedures.

Irrespective of sanctions for particular events, authorisation to operate in an operational or trusted role may be withdrawn.

5.3.7 Independent contractor requirements

Background checks may be applied as described in section 5.3.2. Where risk management prescribes, in addition to the checking and approval requirements, contractors are escorted as described in the MECS certification services procedures.

5.3.8 Documentation supplied to personnel

Documentation is supplied in conformance with the governing Certificate Policies (listed in section 1.2 of the current document). This includes the appropriate Certificate Policies and the CPS (this document).

All members of staff associated with Certification Services are provided with documentation relevant to their position as described in the MECS certification services procedures.

5.4 Audit logging procedures

5.4.1 Types of events recorded

A range of specific events relating to the operation of the PKI are recorded to align with the governing Certificate Policies (listed in section 1.2 of the current document). The determination of events recorded is controlled by the governing Certificate Policy, the applicable best practice, and the risk profile for the system for which logging is being conducted.

The resultant logging activities and their operational practices are undertaken in accordance with the MECS certification services procedures.

5.4.2 Frequency of processing log

Processing of Audit Logs is controlled by the risk profile of the system being logged and any specific requirements of the governing Certificate Policy

Audit Log processing (and / or archived) is undertaken in accordance with the MECS certification services procedures.

5.4.3 Retention period for audit log

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details of retention period of audit log.

5.4.4 Protection of audit log

The procedures for the protection of Certification Services audit logs are undertaken in accordance with the MECS certification services procedures.

5.4.5 Audit log backup procedures

The procedures for the backup of Certification Services audit logs are undertaken in accordance with the MECS certification services procedures.

5.4.6 Audit collection system (internal vs. external)

Audit log collection systems are described in the MECS certification services procedures.

5.4.7 Notification to event-causing subject

Where significant events are considered security or policy relevant, the Certification Service informs the TSP in accordance with the MECS certification services procedures.

5.4.8 Vulnerability assessments

Regular risk and vulnerability assessments will be carried out on both the physical and logical infrastructure under the control of the Certification Services. These will take place at regular intervals to support compliance audit and undertaken in accordance with MECS certification services procedures and risk management procedures.

5.5 Records archival

5.5.1 Types of records archived

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details of the types of records archived.

5.5.2 Retention period for archive

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for the retention period of archived records.

5.5.3 Protection of archive

Archive records are protected and controlled to the same standards as the original data.

The procedures for the protection or archive records are undertaken in accordance with the MECS certification services procedures.

5.5.4 Archive backup procedures

The procedures for the backup or archived records are undertaken in accordance with the MECS certification services procedures.

5.5.5 Requirements for time-stamping of records

Certification Services obtain the current time for record time-stamping from a global verifiable source. Synchronisation and control of time used is undertaken in accordance with the MECS certification services procedures.

5.5.6 Archive collection system (internal or external)

Archive collection systems are undertaken in accordance with the MECS certification services procedures.

5.5.7 Procedures to obtain and verify archive information

The procedures to obtain and verify archive information are undertaken in accordance with the MECS certification services procedures.

5.6 Key changeover

All key changeover procedures strictly enforce the defined trust model for the PKI.

The procedures relating to key changeover are undertaken in accordance with the MECS certification services procedures.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Participants providing Certification Services deal with incidents or the compromise of information in accordance with MECS certification services procedures.

Where significant actions are required as part of incident management procedures, approval of the PMA is sought.

The procedure by which the TSP notifies relevant parties of any significant breach of security, loss of integrity or impact on personal data is described in the MECS security breach notification plan.

The TSP is responsible for authorising all incident and compromise handling procedures.

5.7.2 Computing resources, software, and/or data are corrupted

Participants providing Certification Services deal with any disruption to services in accordance with MECS certification services procedures.

5.7.3 Entity private key compromise procedures

The obligation of Subscribers and the actions to be taken in such circumstances is established by the TSP and published in the Subscriber Agreement associated with the governing Certificate Policies (listed in section 1.2 of the current document). Where procedures for End Entity private key compromise involve action by the Revocation Management Service, processes are undertaken in accordance with the MECS certification services procedures.

5.7.4 Business continuity capabilities after a disaster

The PKI business continuity strategy for the Generation, Dissemination, Subject Device Provision and Revocation Status services accommodates all circumstances up to and including a major disaster at the primary service provision location. The contingency plan incorporates transition to a backup facility located geographically separate from the main operational site.

Business continuity for the Registration Service and Revocation Management Services is the responsibility of the TSP and is undertaken in accordance with the PKI contingency plan.

5.8 Certification Authority or Registration Authority termination

Termination procedures are designed to maintain conformance with the governing Certificate Policy.

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

- Inform all Subscribers (via email), and Relying Parties (via repository) with which the TSP 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 Certification Authority 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 months prior to termination;

- Publish the last CRL issued after the revocation of the last unexpired and unrevoked Certificate on the GOM Qualified Certificate Authority Information URI.

This process is documented in the Government of Malta PKI Trust Service Provider – PKI Termination Plan [6].

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

Private Keys are managed by a variety of mechanisms designed to achieve security and integrity in order to ensure conformance with the governing Certificate Policy.

6.1.1 Key pair generation

CA keys, Subscriber keys, and keys supporting infrastructure components that affect the status of issued Certificates or Certificate status information are generated in accordance with the certification services procedures.

The TSP defines and communicates requirements for Subscriber key pair generation and management via the governing Certificate Policies (listed in section 1.2 of the current document) and Subscriber Agreement.

6.1.2 Private Key delivery to subscriber

The mechanisms for delivery of key pairs to Subscribers are undertaken in accordance with the MECS certification services procedures.

6.1.3 Public key delivery to certificate issuer

The delivery of public keys to the Certificate Generation Service uses PKCS#10 across a secure and authenticated channel. See 4.3.1 for further details.

6.1.4 CA public key delivery to relying parties

The Dissemination Service ensures all CA public keys are made available to Participants via the repository as described in section 2.2 and the certification services procedures

6.1.5 Key sizes

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding key sizes.

Subscriber's key lengths are defined by the TSP and controlled by formal procedures for the management of Certificate Profiles. Only the Certificate Generation Service may implement or modify Certificate profiles on behalf of the TSP through formal control procedures for Certificate profile management in accordance with the certification services procedures.

6.1.6 Public key parameters generation and quality checking

Keys created and managed by the Certificate Generation Service, public key parameter generation and checking is undertaken in accordance with the certification services procedures.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding key usage purposes.

The Certificate Generation Service implements the TSP requirements through formal control procedures for Certificate profile management in accordance with the certification services procedures.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding cryptographic module standards and controls.

The controls applied to Cryptographic Modules are undertaken in accordance with the MECS certification services procedures

6.2.2 Private Key (n out of m) multi-person control

Certain tasks such as those associated with the Certificate Generation Service handling of private keys are performed under multi-person control using an “n out of m” approach. The level of control for specific private keys is determined via a risk management process and described in the applicable procedures.

All activities are undertaken in accordance with the MECS certification services procedures.

6.2.3 Private Key escrow

Private Key escrow is not supported/permitted.

6.2.4 Private Key backup

CA private keys are never available outside the cryptographic module in clear text form including if backed up and are protected by the “n out of m” control mechanism.

Certificate Generation Service CA private keys are securely backed up in accordance with the certification services procedures

The backup of private keys relating to other Certification Services is undertaken in accordance with the MECS certification services procedures.

6.2.5 Private Key archival

CA private keys are never available outside the cryptographic module in clear text form including if archived and are protected by the “n out of m” control mechanism.

Certificate Generation Service CA private keys are archived in accordance with certification services procedures.

The archival of private keys relating to other Certification Services is undertaken in accordance with the MECS certification services procedures.

6.2.6 Private Key transfer into or from a cryptographic module

The transfer in to and from cryptographic modules of the Certificate Generation Service CA private keys is undertaken in accordance with the certification services procedures. CA private keys are never available outside the cryptographic module in clear text form and are protected by the “n out of m” control mechanism (see Section 6.2.2).

The transfer into and from cryptographic modules of the private keys relating to other Certification Services is undertaken in accordance with the certification services procedures

6.2.7 Private Key storage on cryptographic module

The storage of private keys in cryptographic modules of the Certificate Generation Service is undertaken in accordance with the certification services procedures. CA Private Keys are never available outside the cryptographic module in clear text form and recovery is protected by the “n out of m” control mechanism (ref. Section 6.2.2)

The storage of keys used by other Certification Services is undertaken in accordance with the certification services procedures.

6.2.8 Method of activating private key

A number of mechanisms for activation of private keys are used to ensure compliance with governing Certificate Policies (listed in section 1.2 of the current document).

The activation of the keys in the cryptographic modules used by the Certificate Generation Service is undertaken in accordance with the certification services procedures

The activation of Keys used by other Certification Services is undertaken in accordance with the certification services procedures

6.2.9 Method of deactivating private key

A number of mechanisms for deactivation of private keys are used to ensure compliance with governing Certificate Policies (listed in section 1.2 of the current document).

The deactivation of the keys used by the Certificate Generation Service is undertaken in accordance with the certification services procedures.

The deactivation of keys used by other Certification Services is undertaken in accordance with the certification services procedures.

6.2.10 Method of destroying private key

Strict controls are implemented over private key destruction to ensure compliance with the governing Certificate Policy.

The destruction of the keys in the cryptographic modules used by the Certificate Generation Service is undertaken in accordance with the certification services procedures.

The destruction of keys used by other Certification Services is undertaken in accordance with the certification services procedures.

In all cases, destruction of private keys follows a procedure authorised and approved by the PMA.

6.2.11 Cryptographic Module Rating

Cryptographic modules are in conformance with the governing Certificate Policy. Only cryptographic modules which are assessed, rated and certified to accepted international standards are employed.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The archiving of Public Keys, and other backup related activities, by the Certificate Generation Service and Subject Device Provision Service are undertaken in accordance with the certification services procedures.

6.3.2 Certificate operational periods and key pair usage periods

Certificate operational periods and key pair usage periods are specified in the governing Certificate Policy.

The Certificate Generation Service implements the TSP requirements through formal control procedures for Certificate Profile management in accordance with the certification services procedures.

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data relating to Certificate Generation Service private keys and cryptographic modules is securely generated and installed in accordance with the certification services procedures.

Activation data generation and installation for other Certification Services private keys is undertaken in accordance with the certification services procedures.

The activation of the Subscriber Identity Card Certificates is through PIN code(s), one for each Certificate on the card. The PIN code(s) are communicated to the Subscriber through normal post to his/her address on the Identity Card. All activities are undertaken in accordance with the MECS certification services procedures.

6.4.2 Activation data protection

Activation data relating to Certificate Generation Service CA keys and associated cryptographic modules is protected as described in the certification services procedures. The PMA defines Certification Services Participants authorised to hold Key shares.

Activation data protection for other Certification Services private keys is undertaken in accordance with the MECS certification services procedures.

In the case of Subscriber Identity Card Certificates, activation data protection is undertaken in accordance with MECS certification services procedures.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Computer security technical measures are in conformance with the governing Certificate Policies (listed in section 1.2 of the current document) and include measures derived through risk assessment methods.

All activities are undertaken in accordance with the MECS certification services procedures.

6.5.2 Computer security rating

Computer security ratings are in conformance with the governing Certificate Policies (listed in section 1.2 of the current document) and undertaken in accordance with the MECS certification services procedures.

6.6 Life cycle technical controls

6.6.1 System development controls

The Certificate Generation Service does not conduct software development of security enforcing CA Systems. The Certificate Generation Service uses a number of established products from a range of suppliers. Such products, where appropriate, carry accreditations and certifications applicable to their role and required assurance levels.

The configuration of the operational systems built from these standard products is managed in compliance with eIDAS and in accordance with applicable risk management requirements.

External audit and approval for all Certification Services undertaken in accordance with the MECS certification services procedures.

6.6.2 Security management controls

The PMA has responsibility and controls all security management activities.

For Certificate Generation, Dissemination, Subject Device Provision, and Revocation Status services, security and its management are conducted in compliance with ISO 27001:2013 and is subject to external audit and approval.

The Security Management controls associated with the Registration, and Revocation Management services are conducted in accordance with the requirements of PMA.

In both cases, details of security management controls are described in the certification services procedures.

6.6.3 Life cycle security controls

Life cycle security controls are enforced in accordance with the MECS certification services procedures

6.7 Network security controls

The network security controls in use within the Certification Services facilities consist of a combination of security products and appropriate network monitoring, control and operating procedures, in accordance with the MECS certification services procedures.

6.8 Time-stamping

Time Stamping is conducted as an integral component of Certification Services operations for all Certificate and other related activities that require recorded time. A global verifiable time source is used. Synchronisation and control of time used by the Certification Services is undertaken in accordance with the MECS certification services procedures.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

Certificate Profiles are used to define and control parameters in Certificates issued.

All aspects of Certificate Profile development, implementation and management are conducted by the Certificate Generation Service on behalf of the TSP which defines the profiles for Certificates and Certificate status information as part of the Certificate Policy. This is undertaken in accordance with the MECS certification services procedures.

The Certificate Profiles for the GOM PKI Root, Sub-CA, Citizen authentication, Citizen qualified electronic signing, Resident authentication, Resident qualified electronic signing and OCSP response signing Certificates are provided in section 11.

7.1.1 Version number(s)

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding version number(s).

7.1.2 Certificate extensions

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding Certificate extensions.

7.1.3 Algorithm object identifiers

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding algorithm object identifiers.

7.1.4 Name forms

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding name forms.

7.1.5 Name constraints

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding name constraints.

7.1.6 Certificate policy object identifier

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding Certificate Policy object identifiers.

7.1.7 Usage of Policy Constraints extension

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding usage of the policy constraints extension.

7.1.8 Policy qualifiers syntax and semantics

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding policy qualifiers syntax and semantics.

7.1.9 Processing semantics for the critical Certificate Policies extension

Not defined. Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding processing semantics for the critical Certificate Policies extension.

7.2 CRL profile

7.2.1 Version number(s)

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding CRL version numbering.

7.2.2 CRL and CRL entry extensions

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding CRL and CRL entry extensions.

7.3 OCSP profile

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding OCSP profiles.

7.3.1 Version number(s)

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding version numbers.

7.3.2 OCSP extensions

Not defined. Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding OCSP extensions.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding frequency or circumstances of assessment.

The details for assessment are specified in contractual arrangements between the TSP and the Participants providing trust services.

8.2 Identity/qualifications of assessor

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding identity/qualifications of assessor.

8.3 Assessor's relationship to assessed entity

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding assessor's relationship to assessed entity.

8.4 Topics covered by assessment

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding identity/qualifications of assessor.

8.5 Actions taken as a result of deficiency

The actions that are taken as a result of any deficiencies that are identified during any assessment will depend on the seriousness of the deficiency and its potential impact. The PMA has the overall responsibility for deciding what actions are to be taken.

Participants inform the TSP of all significant reported deficiencies, whether identified by internal or external audit.

The MECS has ultimate authority upon remedial actions taken following identification of deficiencies.

8.6 Communication of results

Refer to the governing Certificate Policies (listed in section 1.2 of the current document) for details regarding communication of results.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No fees are charged except for certain cases as required by law or for replacement cards. Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.1.2 Certificate access fees

See section 9.1.1.

9.1.3 Revocation or status information access fees

See section 9.1.1.

9.1.4 Fees for other services

See section 9.1.1.

9.1.5 Refund policy

9.2 See section 9.1.1.Financial responsibility

9.2.1 Insurance coverage

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.2.2 Other assets

Not defined. Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.2.3 Insurance or warranty coverage for end-entities

Not defined. Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.3.2 Information not within the scope of confidential information

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.3.3 Responsibility to protect confidential information

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.4 Privacy of personal information

9.4.1 Privacy plan

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.4.2 Information treated as private

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.4.3 Information not deemed private

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.4.4 Responsibility to protect private information

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.4.5 Notice and consent to use private information

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.4.6 Disclosure pursuant to judicial or administrative process

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.4.7 Other information disclosure circumstances

Not defined. Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.5 Intellectual property rights

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.6 Representations and warranties

9.6.1 TSP representations and warranties

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.6.2 RA representations and warranties

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.6.3 Subscriber representations and warranties

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.6.4 Relying party representations and warranties

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.6.5 Representations and warranties of other participants

Not defined. Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.7 Disclaimers of warranties

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.8 Limitations of liability

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.9 Indemnities

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.10 Term and termination

9.10.1 Term

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.10.2 Termination

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.10.3 Effect of termination and survival

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.11 Individual notices and communications with participants

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

MECS Ltd.
Castagna Building
Valley Road
Msida, MSD9020

9.12 Malta Amendments

9.12.1 Procedure for amendment

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.12.2 Notification mechanism and period

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.12.3 Circumstances under which OID must be changed

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.13 Dispute resolution provisions

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.14 Governing law

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.15 Compliance with applicable law

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.16.2 Assignment

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.16.3 Severability

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.16.5 Force Majeure

Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

9.17 Other provisions

Not defined. Refer to the governing Certificate Policies (listed in section 1.2 of the current document).

Appendix 1: References

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

[2] RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework [link]

[3] Certificate Policy for Government of Malta Citizen Authentication Certificates and Qualified Electronic Signature Certificates [link]

[4] Certificate Policy for Government of Malta Resident Authentication Certificates and Qualified Electronic Signature Certificates [link]

[5] Certificate Policy for Government of Malta Administration Certificates [link]

[6] Government of Malta PKI Trust Service Provider – PKI Termination Plan

Appendix 2: Certificate and CRL Profiles

In this Appendix, text enclosed in parentheses {} is comment text inserted to facilitate understanding of the profiles. Text in square brackets [ ] represents variable values.

A2.1 CA Certificate Profiles

A2.1.1 Root CA Certificate

The following table gives the Root CA Certificate profile and extensions.

Root CA Certificate Profile		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	SHA256/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 Size/Algorithm	4096 bits/RSA
Extensions	
Subject Key Identifier	[sha1 of the Public key of PKCS10]
Basic Constraints (critical)	Subject Type= CA Path Length Constraint = [none]
Key Usage (Critical)	KeyCertSign CRLSign
Certificate Policy	2.5.29.32.0 {AnyPolicy} URL = http://repository.qca.gov.mt

A2.1.2 Citizen eID CA Certificate

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

Citizen eID CA Certificate Profile		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	SHA256/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 Size/Algorithm	2048 bits/RSA	
Extensions		
Authority Key Identifier	[sha1 of the Public Key of Malta Root CA Certificate]	
Subject Key Identifier	[sha1 of the Public key of PKCS10]	

CONFIDENTIAL

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

A2.1.3 Resident eID CA Certificate

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

Resident eID CA Certificate Profile		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	SHA256/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 Size/Algorithm	2048 bits/RSA	
Extensions		
Authority Key Identifier	[sha1 of the Public Key of Malta Root CA Certificate]	
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_rs.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	2.5.29.32.0 {AnyPolicy} 2.16.470.4.3.1 {OID for Malta Resident Electronic Identity CA Certificate Policy} URL= http://repository.qca.gov.mt	

A2.1.4 Administrator eID CA Certificate

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

Administrator eID CA Certificate Profile		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	SHA256/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 Size/Algorithm	2048 bits/RSA	
Extensions		
Authority Key Identifier	[sha1 of the Public Key of Malta Root CA Certificate]	
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_rs.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	2.5.29.32.0 {AnyPolicy} 2.16.470.4.4.1 {OID for Government of Malta Administrator CA Certificate Policy} URL= http://repository.qca.gov.mt

A2.2 Subscriber Certificate Profiles

A2.2.1 Citizen eID Authentication Certificate Profile

The following table gives the Citizen eID Authentication Certificate profile and extensions.

Citizen eID Authentication Certificate Profile		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	SHA256/RSA	
Issuer	CN	Malta Citizen Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
IssuerAltName	CN	Malta Citizen Electronic Identity CA
	OU	Class Qualified
	OU	Government of Malta
	OU	NTRMT-C43419
	O	Malta Electronic Certification Services Ltd (MECS Ltd)
	C	MT

CONFIDENTIAL

Validity	Variable validity, expressed in registration request, with maximum 10 years	
Subject	CN	[First name(s) Known as Name (if available) Surname Known as Surname (if available) (Authentication)]
	C	MT
	Surname	[Surname]
	Given Name	[Given name]
	Serial	[MBUN] {meaningless but unique number}
Public Key Size/Algorithm	2048 bits/RSA	
Extensions		
Authority Key Identifier	[sha1 of the Public Key of Malta Citizen CA Certificate]	
Subject Key Identifier	[sha1 of the Public key of registration request]	
Basic Constraints	Subject Type= end entity Path Length Constraint = [none]	
Key Usage (Critical)	Digital signature	
CRL Distribution Point	URL=https://crl.qca.gov.mt/citizenca.crl, or URL=https://crl.qca.gov.mt/CitizenCA_YYYY_NNN.crl URI=ldap://ldap.qca.gov.mt/cn=CitizenCA,o=Government of Malta,c=MT?certificateRevocationList?base, or URI=ldap://ldap.qca.gov.mt/cn=CitizenCA_YYYY_NNN,o=Government of Malta,c=MT?certificateRevocationList?base	
Certificate Policy	2.16.470.4.2.3 URL=https://repository.qca.gov.mt UserNotice = Trust Service Provider: Malta Electronic Certification Services Ltd (MECS Ltd) – NTRMT-C43419	

CONFIDENTIAL

AuthorityInfoAccess	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=https://crt.qca.gov.mt/CitizenCA.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

A2.2.2 Citizen eID Qualified Electronic Signature Certificate Profile

The following table gives the Citizen eID Qualified Electronic Signature Certificate profile and extensions.

Citizen eID Qualified Electronic Signature Certificate Profile		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	SHA256/RSA	
Issuer	CN	Malta Citizen Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
IssuerAltName	CN	Malta Citizen Electronic Identity CA
	OU	Class Qualified
	OU	Government of Malta
	OU	NTRMT-C43419
	O	Malta Electronic Certification Services Ltd (MECS Ltd)
	C	MT
Validity	[Variable validity, expressed in registration request, with maximum 10 years]	

Subject	CN	[First name(s) Known as Name (if available) Surname Known as Surname (if available) (Signature)]
	C	MT
	Surname	[Surname]
	Given Name	[Given name]
	Serial	[MBUN] {meaningless but unique number}
Public Key Size/Algorithm	2048 bits/RSA	
Extensions		
Authority Key Identifier	[sha1 of the Public Key of Malta Citizen CA Certificate]	
Subject Key Identifier	[sha1 of the Public key of registration request]	
Basic Constraints	Subject Type= end entity Path Length Constraint = [none]	
Key Usage (Critical)	Non repudiation	
CRL Distribution Point	URL=https://crl.qca.gov.mt/citizenca.crl , or URL=https://crl.qca.gov.mt/CitizenCA_YYYY_NNN.crl URI=ldap://ldap.qca.gov.mt/cn=CitizenCA,o=Government of Malta,c=MT?certificateRevocationList?base, or URI=ldap://ldap.qca.gov.mt/cn=CitizenCA_YYYY_NNN,o=Government of Malta,c=MT?certificateRevocationList?base	
Certificate Policy	2.16.470.4.2.2 URL=https://repository.qca.gov.mt UserNotice = Trust Service Provider: Malta Electronic Certification Services Ltd (MECS Ltd) – NTRMT-C43419	

qcStatement	id-etsi-qcs 1 {Certs are qualified} id-etsi-qcs 4 {Certs are installed on QSCDs} id-etsi-qcs 5 PDS URL Location = https://repository.qca.gov.mt Language = en id-etsi-qcs 6 OID = 0.4.0.1862.1.6.1 {esign}
AuthorityInfoAccess	[1]Authority Info Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=https://crt.qca.gov.mt/CitizenCA.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

A2.2.3 Resident eID Authentication Certificate Profile

The following table gives the Resident eID Authentication Certificate profile and extensions.

Resident eID Authentication Certificate Profile		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	SHA256/RSA	
Issuer	CN	Malta Resident Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
IssuerAltName	CN	Malta Resident Electronic Identity CA
	OU	Class Qualified
	OU	Government of Malta
	OU	NTRMT-C43419

CONFIDENTIAL

	O	Malta Electronic Certification Services Ltd (MECS Ltd)
	C	MT
Validity	[Variable validity, expressed in registration request, with maximum 10 years]	
Subject	CN	[First name(s) Known as Name (if available) Surname Known as Surname (if available) (Authentication)]
	C	MT
	Surname	[Surname]
	Given Name	[Given name]
	Serial	[MBUN] {meaningless but unique number}
Public Key Size/Algorithm	2048 bits/RSA	
Extensions		
Authority Key Identifier	[sha1 of the Public Key of Malta Resident CA]	
Subject Key Identifier	[sha1 of the Public key of registration request]	
Basic Constraints	Subject Type= end entity Path Length Constraint = [none]	
Key Usage (Critical)	Digital signature	
CRL Distribution Point	URL=https://crl.qca.gov.mt/residentca.crl URI=ldap://ldap.qca.gov.mt.mt/cn=ResidentCA,o=Government of Malta,c=MT?certificateRevocationList?base	
Certificate Policy	2.16.470.4.3.3 URL=https://repository.qca.gov.mt UserNotice = Trust Service Provider: Malta Electronic Certification Services Ltd (MECS Ltd) – NTRMT-C43419	

AuthorityInfoAccess	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=https://crt.qca.gov.mt/ ResidentCA.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

A2.2.4 Resident eID Qualified Electronic Signature Certificate Profile

The following table gives the Resident eID Qualified Electronic Signature Certificate profile and extensions.

Resident eID Qualified Electronic Signature Certificate Profile		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	SHA256/RSA	
Issuer	CN	Malta Resident Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
IssuerAltName	CN	Malta Resident Electronic Identity CA
	OU	Class Qualified
	OU	Government of Malta
	OU	NTRMT-C43419
	O	Malta Electronic Certification Services Ltd (MECS Ltd)
	C	MT
Validity	[Variable validity, expressed in registration request, with maximum 10 years]	

CONFIDENTIAL

Subject	CN	[First name(s) Known as Name (if available) Surname Known as Surname (if available) (Signature)]
	C	MT
	Surname	[Surname]
	Given Name	[Given name]
	Serial	[MBUN] {meaningless but unique number}
Public Key Size/Algorithm	2048 bits/RSA	
Extensions		
Authority Key Identifier	[sha1 of the Public Key of Malta Resident CA]	
Subject Key Identifier	[sha1 of the Public key of registration request]	
Basic Constraints	Subject Type= end entity Path Length Constraint = [none]	
Key Usage (Critical)	Non repudiation	
CRL Distribution Point	URL=https://crl.qca.gov.mt/residentca.crl URI=ldap://ldap.qca.gov.mt/cn=ResidentCA,o=Government of Malta,c=MT?certificateRevocationList?base	
Certificate Policy	2.16.470.4.3.2 URL=https://repository.qca.gov.mt UserNotice = Trust Service Provider: Malta Electronic Certification Services Ltd (MECS Ltd) – NTRMT-C43419	
qcStatement	id-etsi-qcs 1 {Certs are qualified} id-etsi-qcs 4 {Certs are installed on QSCDs} id-etsi-qcs 5 PDS URL Location = https://repository.qca.gov.mt Language = en id-etsi-qcs 6 OID = 0.4.0.1862.1.6.1 {esign}	

AuthorityInfoAccess	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=https://crt.qca.gov.mt/ResidentCA.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

A2.2.5 Administrator eID Authentication Certificate Profile

The following table gives the Authentication Certificate profile and extensions.

Administrator eID Authentication Certificate Profile		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	SHA256/RSA	
Issuer	CN	Government of Malta Administrator CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
IssuerAltName	CN	Malta Citizen Electronic Identity CA
	OU	Class Qualified
	OU	Government of Malta
	OU	NTRMT-C43419
	O	Malta Electronic Certification Services Ltd (MECS Ltd)
	C	MT
Validity	[Variable validity, expressed in registration request, with maximum 3 years]	
Subject	CN	[First Name, Surname]
	OU	[Role Type]
	C	MT
	Serial	[MBUN] {meaningless but unique number}
Public Key Size/Algorithm	2048 bits/RSA	
Extensions		

CONFIDENTIAL

Authority Key Identifier	{sha1 of the Public Key of Malta Admin CA}
Subject Key Identifier	[sha1 of the Public key of registration request]
Basic Constraints	Subject Type= end entity Path Length Constraint = none
Key Usage (Critical)	Digital signature
CRL Distribution Point	URL=https://crl.qca.gov.mt/adminca.crl URI=ldap://ldap.qca.gov.mt/cn=AdminCA,o=Government of Malta,c=MT?certificateRevocationList?base
Certificate Policy	2.16.470.4.4.1.1 URL=https://repository.qca.gov.mt UserNotice = Trust Service Provider: Malta Electronic Certification Services Ltd (MECS Ltd) – NTRMT-C43419
AuthorityInfoAccess	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=https://crt.qca.gov.mt/AdminCA.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

A2.3 OCSP Profiles

A2.3.1 Root CA OCSP Response Signing Certificate

Root CA OCSP Response Signing Certificate		
Version	3	
Serial number	[Allocated automatically]	
Signature Algorithm	SHA256/RSA	
Issuer	CN	Government of Malta Root CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
	From:	[Time of issue]

CONFIDENTIAL

Validity	To:	[Time of issue] + 1 year
Subject	CN	Government of Malta OCSP Responder
	OU	Class Qualified
	O	Government of Malta
	C	MT
Public Key Size/Algorithm	2048 bits/RSA	
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	

A2.3.2 Citizen eID CA OCSP Response Signing Certificate

Citizen eID CA OCSP Response Signing Certificate		
Version	3	
Serial number	[Allocated automatically]	
Signature Algorithm	SHA256/RSA	
Issuer	CN	Malta Citizen Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
IssuerAltName	CN	Malta Citizen Electronic Identity CA
	OU	Class Qualified
	OU	Government of Malta
	OU	NTRMT-C43419
	O	Malta Electronic Certification Services Ltd (MECS Ltd)
	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 Size/Algorithm	2048 bits/RSA	
Extensions		

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

A2.3.3 Resident eID CA OCSP Response Signing Certificate

Resident eID CA OCSP Response Signing Certificate		
Version	3	
Serial number	[Allocated automatically]	
Signature Algorithm	SHA256/RSA	
Issuer	CN	Malta Resident Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
IssuerAltName	CN	Malta Resident Electronic Identity CA
	OU	Class Qualified
	OU	Government of Malta
	OU	NTRMT-C43419
	O	Malta Electronic Certification Services Ltd (MECS Ltd)
	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 Size/Algorithm	2048 bits/RSA	
Extensions		
Authority Key Identifier	[sha1 of the Public Key of Malta Resident CA Certificate]	
Subject Key Identifier	[sha1 of the Public key of PKCS10]	
Key Usage (Critical)	Digital Signature	
Enhanced Key usage	OCSP signing	
OCSPNoCheck	NULL	

A2.3.4 Administrator eID CA OCSP Response Signing Certificate

Administrator eID CA OCSP Response Signing Certificate		
Version	3	
Serial number	[Allocated automatically]	
Signature Algorithm	SHA256/RSA	
Issuer	CN	Government of Malta Administrator CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
IssuerAltName	CN	Government of Malta Administrator CA
	OU	Class Qualified
	OU	Government of Malta
	OU	NTRMT-C43419
	O	Malta Electronic Certification Services Ltd (MECS Ltd)
	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 Size/Algorithm	2048 bits/RSA	
Extensions		
Authority Key Identifier	[sha1 of the Public Key of Malta Administrator CA Certificate]	
Subject Key Identifier	[sha1 of the Public key of PKCS10]	
Key Usage (Critical)	Digital Signature	
Enhanced Key usage	OCSP signing	
OCSPNoCheck	NULL	

A2.4 CRL Profiles

A2.4.1 Root CRL profile

CRL signed by Root CA		
Version	2	
Signature Algorithm	SHA256/RSA	
Issuer	CN	Government of Malta Root CA

	OU	Class Qualified
	O	Government of Malta
	C	MT
ThisUpdate	[Time of issue]	
NextUpdate	[Time of issue] + 92 days	
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]	
ExpiredCertsOnCRL	Indicates CRL includes expired certificates {OID 2.5.29.60}	

A2.4.2 Citizen eID CA CRL Profile (Master_CitizenCA.crl)

CRL signed by Citizen eID CA		
Version	2	
Signature Algorithm	SHA256/RSA	
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]	
ExpiredCertsOnCRL	Indicates CRL includes expired certificates {OID 2.5.29.60}	

A2.4.3 Citizen eID CA CRL Profile (citizenCA.crl)

CRL signed by Citizen eID CA		
Version	2	
Signature Algorithm	SHA256/RSA	
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]	
ExpiredCertsOnCRL	Indicates CRL includes expired certificates {OID 2.5.29.60}	
IssuingDistributionPoint	Distribution Point Name: Full Name: URL= [https://crl.qca.gov.mt/citizenca.crl or URL=https://crl.qca.gov.mt/CitizenCA_YYYY_NNN.crl] Only Contains User Certs=No Only Contains CA Certs=No Indirect CRL=No	

A2.4.4 Resident eID CA CRL profile

CRL signed by Resident eID CA		
Version	2	
Signature Algorithm	SHA256/RSA	
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]	
ExpiredCertsOnCRL	Indicates CRL includes expired certificates {OID 2.5.29.60}	

A2.4.5 Administrator eID CA CRL profile

CRL signed by Administrator CA		
Version	2	
Signature Algorithm	SHA256/RSA	
Issuer	CN	Government of Malta Administrator 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 Admin CA]	
CRL Number	[CA assigned unique name]	
ExpiredCertsOnCRL	Indicates CRL includes expired certificates OID 2.5.29.60	