Malta Electronic Certification Services (MECS) Ltd

Government of Malta Certificate Policy for Citizen Authentication Certificates and Citizen Qualified Electronic Signature Certificates

Date of Issue: 17/04/2020

Version Number: 2.3

This document is the Government of Malta Certificate Policy (CP) for Citizen Authentication Certificates for Citizen Identification and Citizen Qualified Electronic Signature Certificates for the verification of Qualified Electronic Signatures.

Change Record

Date	Author	Version	QA	Description of Change
13/09/2018	DLR	1.5	MECS	Initial version for takeover by IMA, based on MITA v1.4
11/01/2019	DLR	1.6	MECS	Further updates.
23/01/2019	IMA	1.7	MECS	Review edits and commit
14/03/2019	IMA	2.0	MECS	Revised for consistent versioning
03/09/2019	IMA	2.1	MECS	General Errata
07/02/2020	IMA	2.2	MECS	Update service provider information
17/04/2020	IMA	2.3	MECS	Consolidation and Clarification of Documents

Document Details

Detail	
Title	Government of Malta Certificate Policy for Citizen Authentication Certificates and Citizen Qualified Electronic Signature Certificates
Filing Reference	GOM_Citizen_eID_CP_V2.3_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

1 INTRODUCTION

1.1 Overview

The Government of Malta (GOM) operates a national electronic Identity Card scheme (eID) for Citizens as defined within the Identity Card Act, Chapter 258 Laws of Malta [1]. The national Identity Card contains a Citizen Authentication Certificate and a Citizen Qualified Certificate for Qualified Electronic Signatures.

This document is the Government of Malta Certificate Policy (CP) for Citizen Authentication Certificates for Citizen Identification and Citizen Qualified Electronic Signature Certificates for Verification of Qualified Electronic Signatures as defined in eIDAS Regulation No 910/2014 [2].

A Certificate Policy is a named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements. The Certificate Policy is further supported by a Certification Practice Statement (CPS) which is a statement of the practices that a Trust Service Provider[1] (TSP) employs in issuing, managing, revoking, and renewing or re-keying certificates. Malta Electronic Certification Services Ltd (MECS) is the TSP for the GOM Public Key Infrastructure.

This Certificate Policy is structured according to the guidelines provided by IETF RFC 3647 [3] and responsibility for the Certificate Policy lies with a body known as the Policy Management Authority. Any queries regarding the content of this Certificate Policy should be directed to the Policy Management Authority. MECS is the Policy Management Authority for the Public Key Infrastructure (see section 1.3.5.1).

The TSP which issues Certificates in accordance with this Certificate Policy has made its own stipulations regarding Participants, restrictions on usage of Certificates, additional liability provisions, etc. These stipulations are published by the TSP in a document termed a PKI Disclosure Statement (PDS), which serves as the highest-level vehicle by which provisions affecting Subscribers and Relying Parties are defined. Subscriber and Relying Party provisions are further defined in the Subscriber Agreement and Relying Party Agreement. A PKI Disclosure Statement supporting this Certificate Policy incorporates this Certificate Policy by reference. All Certificates Issued under this policy shall contain a reference to where the PKI Disclosure Statement published by the TSP that issued the Certificate, may be found. This Certificate Policy, in conjunction with the PDS, Subscriber Agreement and Relying Party Agreement specifies:

- Those who can participate in the Government of Malta Citizen eID Public Key Infrastructure.
- The primary rights, obligations and liabilities of the Participants governed by this Certificate Policy.
- The purposes for which Certificates issued under this Certificate Policy may be used.
- Minimum requirements to be observed in the issuance, management, usage and reliance upon Certificates.

[1] Also known as the Certification Authority (CA). These terms are used interchangeable throughout this document.

The Government of Malta has commissioned MECS as the Trust Service Provider[2] (TSP) for the Government of Malta Citizen eID Public Key Infrastructure.

MECS has nominated Identity Malta Agency (IMA) as the primary Participant for management of the Government of Malta Citizen eID Public Key Infrastructure and provision of the Public Key Infrastructure's operational services.

The various terms used throughout this document are explained in the Glossary, the location of which is defined in section 2.

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 [3].

1.2 Document name and identification

This Certificate Policy is named "Government of Malta Certificate Policy for Citizen Authentication Certificates and Citizen Qualified Electronic Signature Certificates".

The Citizen Authentication Certificates and Citizen Qualified Electronic Signature Certificates are linked to this Certificate Policy through an Object Identifier (OID) contained within each Certificate. The Object Identifiers associated with this Certificate Policy and assigned to the respective Certificates are defined in section 7.1.6.

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.

For the Government of Malta Citizen eID Public Key Infrastructure the Participant roles are:

- TSP (MECS).
- Policy Management Authority (MECS).
- Certification Services providers - Registration Service (IMA), Certificate Generation Service (HID[3]), Dissemination Service (HID), Revocation Management Service (IMA), Revocation Status Service (HID), Subject Device Provision Service (IMA).
- Subscribers.
- Relying Parties.

Under this scheme Subscribers and Relying Parties only have a contractual relationship with MECS. These relationships are defined by the Government of Malta Citizen eID Public Key Infrastructure Subscriber Agreements and Relying Party Agreements.

The requirements placed upon Participants providing Certification Services which support the TSP are controlled by the provisions of this Certificate Policy and the contractual arrangements between them and the TSP.

[2] Entities providing a Trust Service as defined in the eIDAS Regulation [2]

[3] HID Global Corporation

In any case of non-compliance with this Certificate Policy, the TSP will determine the steps to be taken. It may refer matters to the Policy Management Authority which has overall and final control over the content of the Certificate Policy and related documentation.

1.3.1 Certification authorities

The term Certification Authority refers to the TSP that creates and assigns certificates.

MECS is the TSP for the Government of Malta Citizen eID Public Key Infrastructure (see section 1.1)

1.3.2 Registration authorities

The Registration Authorities are responsible for a number of activities including the identification and authentication of Certificate applicants, ensuring their eligibility to be issued with Certificates, checking the accuracy and integrity of the information presented by applicants, Certificate revocation and suspension, and device provision.

The Registration Authorities approve requests from applicants for the issue of Certificates and for their revocation and suspension as detailed in this Certificate Policy.

The Certification Services provided by the Registration Authorities are the Registration Service, Revocation Management Service and Subject Device Provision Certification Service (see 1.3.5.2).

The TSP has approved these Registration Authorities to register Subscribers under this Certificate Policy:

- GOM PKI IMA Registration Authority.

1.3.3 Subscribers

A Subscriber is an applicant that has applied for and received a Certificate and who bears responsibility for the use of the private key associated with the Certificate.

The following types of Subscribers are eligible to be issued with Certificates under this Certificate Policy:

- Maltese Citizens in accordance the Malta Identity Card Act, Chapter 258 Laws of Malta [1].

1.3.4 Relying parties

A Relying Party is an End Entity that does not necessarily hold a Certificate but even so, may rely on a Certificate and/or Electronic Signature created using a Certificate.

Eligible Relying Parties for Certificates issued under this Certificate Policy include notably:

- Government of Malta: MFSA
- Exclusively in relation to any Citizen Qualified Electronic Signature Certificate: any relying party as defined in the eIDAS Regulation [2]
- Any other party, whether natural or legal person, who has concluded an agreement with MECS to abide by the Relying Party Agreement and the corresponding Certificate Policy.

To contact the TSP regarding becoming an eligible relying party, one may send an email to info.mecs@gov.mt.

1.3.5 Other participants

1.3.5.1 Policy Management Authority

The Policy Management Authority defines, supervises and maintains the overall framework for this PKI including the definition of the policies under which it operates. The Policy Management Authority's responsibilities include, and are not limited to:

- Defining this Certificate Policy.
- Validation of associated CPS and supporting documents.
- Supervising the correct implementation of the CPS in conformance with this Certificate Policy.
- The Conformity of the CPS with this Certificate Policy.
- Audit and compliance management.

1.3.5.2 Certification Services Providers

These services are:

- Certificate Generation Service: creates and signs Certificates based on the identity and other attributes verified by the Registration Service. This can include key generation.
- Dissemination Service: disseminates Certificates to subjects, and if the Subject consents, makes them available to Relying Parties. This service also makes available the TSP's terms and conditions, and any published policy and practice information, to Subscribers and Relying Parties.
- Revocation Status Service: provides Certificate revocation status information to Relying Parties.
- Registration Service: verifies the identity and if applicable, any specific attributes of a Subject. The results of this service are passed to the Certificate Generation Service.
- Revocation Management Service: processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the Revocation Status Service.
- Subject Device Provision Service: prepares, and provides or makes available secure cryptographic devices, or other secure devices, to Subjects.

Participants providing operational Certification Services for the TSP are:

- Identity Malta Agency (IMA): provides the Registration Service, Revocation Management Service, and Subject Device Provision Services (see 1.3).
- HID Global Corporation (HID): provides the Certificate Generation Service, Dissemination Service, and Revocations Status Service. (See section 1.3).

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

The categories of transactions, applications, or purposes for which Certificates Issued under this policy may be used are:

- Citizen Authentication Certificate: This shall be used for the Identification and Authentication of Maltese Citizens to applications or systems approved by the Government of Malta for use with the Authentication Certificate.

- Citizen Qualified Electronic Signature Certificate: This shall be used for the verification of Qualified Electronic Signatures associated with applications or systems approved by the Government of Malta.

1.4.2 Prohibited certificate uses

All application use and any usage categories for Certificates Issued under this Certificate Policy that are not described in section 1.4.1 are prohibited.

1.5 Policy administration

1.5.1 Organization administering the document

The Policy Management Authority administers this document. In the first instance, all questions and comments regarding this Certificate Policy should be addressed to the TSP (see section 1.5.2).

1.5.2 Contact person

Contact details for the TSP are:

MECS Ltd.
Castagna Building
Valley Road
Msida, MSD9020
Malta
Telephone: +356 25904900
E-mail: info.mecs@gov.mt

1.5.3 Person determining CPS suitability for the policy

The Policy Management Authority determines the suitability of any Certification Practice Statement operating under this Certificate Policy.

1.5.4 CPS approval procedures

The Policy Management Authority determines the suitability and approves the use of any Certification Practice Statement which is used to support this Certificate Policy.

1.6 Definitions and acronyms

Refer to the Glossary for a description of the applicable definitions and acronyms. The Glossary location is in the repository as defined in section 2 below.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

An information Repository shall be made available under the terms of this Certificate Policy. It shall be located at:

https://repository.qca.gov.mt

The TSP is the entity with overall responsibility for the operation of the Repository which it may delegate to Participants providing Certification Services.

2.2 Publication of certification information

The TSP shall ensure the following items are published and made continuously available for all PKI Participants:

- This Certificate Policy with its associated PKI Disclosure Statement.
- Subscriber Agreement and Relying Party Agreement.
- All CA Certificates issued by the TSP.
- Certificate status information for all Certificates Issued under this Certificate Policy.

The location of or mechanism to obtain access to this Certificate Policy shall be provided in Certificates issued under this Certificate Policy.

When superseded, the documents listed above shall be archived at location

https://repository.qca.gov.mt/Archive/ and made continuously available for all PKI Participants.

2.3 Time or frequency of publication

Information as listed in 2.2 shall be published promptly upon its creation, with the exception that if Certificate Revocation Lists (CRLs) are used to provide Revocation information, they shall be published according to section 4.9.7 and 4.9.8 of this Certificate Policy.

2.4 Access controls on repositories

The Repository shall make available the information specified in section 2.2. The Repository may control access to this information.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Each Subject shall have an unambiguous, clearly distinguishable and unique X.500 Distinguished Name (DN) in the Certificate Subject name field in accordance with RFC 5280 [7], as updated by RFC 6818 [8].

3.1.2 Need for names to be meaningful

The contents of each Certificate Subject name field shall have a direct association with the authenticated name of the Subject.

3.1.3 Anonymity or pseudonymity of subscribers

Shall only be permitted if the authorised officer is satisfied that there are sufficient grounds to merit the inclusion of pseudonyms, as per our national law [1].

3.1.4 Rules for interpreting various name forms

Citizen Authentication and Qualified Electronic Signature Certificates name field contents and their interpretation is shown in table 1 below.

Field	Contents
CN	[First name(s) Known as Name (if available) Surname Known as Surname (if available) (Authentication or Signature)]
Surname	Family name
Given Name	First name(s)
Title	GOM approved legal, religious or government assigned titles may be used during registration
Serial number	MBUN (meaningless but unique number)
C	MT

Table 1: Subject name field contents

CA Certificate name field contents are static and defined in Appendix 2.

3.1.5 Uniqueness of names

Certificate Subject Distinguished Names are unique.

3.1.6 Recognition, authentication and role of trademarks

Trademarks, logos or otherwise copyrighted graphic or text material are not permitted in Certificates.

It is solely the Subscriber's responsibility that their choice of name does not violate any trademark and copyright or Intellectual Property infringement of any person or entity, whether fraudulently, negligently, innocently or otherwise. The TSP or Participants providing Certification Services are not obligated to check such rights. If the TSP is notified of a violation of such rights, it has the right to revoke the Certificate.

Subscribers are required to declare legitimacy of their registration details as part of the Registration Process.

Name claim disputes are resolved in conformance with this Certificate Policy.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

For Citizen Authentication and Citizen Qualified Electronic Signature Certificates, the issuance process shall involve a stage in which the Registration Authority acting on behalf of the Subscriber generates and demonstrates possession of the Private Key.

For all Certificate types, technical means employed to ensure possession of Private Keys will be PKCS#10 or other equivalent cryptographic mechanism approved by the Policy Management Authority.

3.2.2 Authentication of organization identity

Not applicable.

3.2.3 Authentication of individual identity

The identity of the Subscriber and, if applicable, any specific attributes of the Subscriber, shall be verified during a process that requires the physical presence of the applicant.

At a minimum, evidence of the Subscriber particulars defined in the Identity Card Act, Chapter 258 Laws of Malta [1] shall be presented and verified.

For CA Certificates, the Identity of the Subscriber and its authorised representative(s) shall be carried out using a procedure approved by the Policy Management Authority.

3.2.4 Non-verified subscriber information

Use of non-verified information is not permitted by this Certificate Policy.

3.2.5 Validation of authority

For CA Certificates, validation of authority shall be carried out using a procedure approved by the Policy Management Authority.

3.2.6 Criteria for interoperation

The criteria by which another TSP wishing to operate within or interoperate with the PKI governed by this Certificate Policy, will be defined by the Policy Management Authority. The Policy Management Authority shall also determine whether any specific TSP is approved for interoperation.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

All Citizen Authentication and Citizen Qualified Electronic Signature Certificates issued under this policy shall follow the procedure used for initial Certificate issuance and conform to the policy requirements defined in section 3.2.

For CA Certificates, identification and authentication for routine re-key shall be carried out using a procedure approved by the Policy Management Authority.

3.3.2 Identification and authentication for re-key after revocation

After revocation, all Certificates issued under this policy shall follow the procedure used for initial Certificate issuance and conform to the policy requirements defined in section 3.2.

3.4 Identification and authentication for revocation request

Revocation requests shall at a minimum identify and authenticate the requestor, contain sufficient information to uniquely identify the Certificate to be revoked, and ensure the requestor is authorised to revoke the Certificate to which the revocation request pertains.

Subscriber requested revocation shall be verified during a process that requires the physical presence of the Subscriber.

For CA Certificates, revocation requests shall be made directly to the TSP who will perform identification and authentication using a procedure approved by the Policy Management Authority.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

The policy requirements in this section apply to Citizen Authentication and Citizen Qualified Electronic Signature Certificates unless indicated otherwise.

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Certificate applications shall only be accepted from Maltese Citizens in accordance with the Identity Card Act, Chapter 258 Laws of Malta [1].

Applications for CA Certificates shall only be accepted from the TSP.

4.1.2 Enrolment process and responsibilities

At a minimum, enrolment processes shall include:

- Provision of accurate information in support of identification and authentication of the applicant.
- Acceptance of the Subscriber Agreement by the applicant.
- Compliance with this Certificate Policy.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Only approved Registration Authorities acting on behalf of the TSP are permitted to conduct identification and authentication of Subscribers.

4.2.2 Approval or rejection of certificate applications

It shall not be possible for a single individual acting in a Registration Service trusted role to process and approve a certificate application resulting in the issuance of a Certificate. Authorisation from a minimum of two persons is required before any Certificate is issued.

The Registration Service will either approve or reject a Certificate application.

Where an application fails to achieve the specified authentication requirements or the level of assurance of authentication as required under this Certificate Policy cannot be met a Certificate application will be rejected.

Where approved, the Certificate application will be digitally signed for processing by the Certificate Generation Service.

4.2.3 Time to process certificate applications

Applicants will be notified at the time of application by the Registration Service of the timescales within which their Identity Card will be ready for collection.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Certificates shall be issued automatically by the Certificate Generation Service only in response to a properly constructed, signed and validated Certificate request from an authorised Registration Service.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Notification of Certificate issuance is provided via receipt of the Identity Card & PIN via post when the Subscriber requests the Identity Card to be sent to them directly, or by receipt of the Identity Card PIN via post when the Subscriber elects to collect the Identity Card in person from the Registration Service.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Before entering into a contractual relationship with an applicant, the TSP shall inform the applicant of the terms and conditions regarding use of the certificate, as expressed through the Subscriber Agreement and Certificate Policy, and record their explicit acceptance of these terms and conditions.

A Subscriber shall acknowledge that it agrees to the terms and conditions stipulated in the Certificate Policy and associated Subscriber Agreement and any other applicable contractual commitments prior to first use of the Certificate.

A Subscriber shall check the visible details (e.g. their name) on the Identity Card containing their Certificate(s) upon receipt.

A Subscriber shall explicitly indicate acceptance of a Certificate to the Registration Service. This may be via technical or procedural processes.

Use of a Private Key for an activity or transaction approved under this Certificate Policy shall constitute acceptance of the associated Certificate.

For CA Certificates, acceptance shall be carried out by a person authorised by the TSP.

4.4.2 Publication of the certificate by the CA

CA Certificates shall be published to the Repository. Subscriber Certificates shall not be published.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

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

Subscribers shall ensure that use of the Private Key associated with the Certificate is consistent with the usage restrictions in the Certificate as stipulated and published by the TSP.

CAs shall only use CA key pairs and associated Certificates for purposes defined in the CA Certificate key usage extension.

4.5.2 Relying party public key and certificate usage

A Relying Party may only rely on a Subscriber's Public Key and Certificate for the specific functions stipulated within this Certificate Policy.

Relying Parties must comply with the requirements defined in the Relying Party Agreement located at https://repository.qca.gov.mt/. Relying Parties' eligibility is defined by section 1.3.4 of this CP. The TSP makes no stipulation on limiting that reliance.

The Relying Party shall also check the validity of a Certificate on which they may wish to rely and all Certificates in the Certificate Chain. The location of revocation and status information for (Q)TSP issued certificate can be found through the CPS section 2.1. Additionally, the suspension and revocation status of a Certificate on which the Relying Party may wish to rely and all the Certificates in the Certificate Chain up to but not including the Root CA Certificate shall be checked. If any of the Certificates has expired or has been suspended or revoked, any reliance on the Certificate for the validation of Electronic Signatures is solely at the Relying Party's own risk. To this end the Relying Party shall on the occasion of each reliance refer to CRL or OCSP status information in accordance with this policy.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

Certificate renewal is not allowed by the GOM eID PKI. All applications for Certificate renewal from a Citizen shall be treated as applications for a new Authentication Certificate and if required Qualified Electronic Signature Certificate.

CA Certificate renewal is not supported.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing certificate renewal requests

Not applicable.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

All applications for a Certificate re-key from a Citizen shall be treated as applications for a new Electronic Identity Card with new embedded Authentication Certificate and if required Qualified Electronic Signature Certificate.

For CA Certificates, re-key is supported.

4.7.2 Who may request certification of a new public key

CA Certificate re-key requests shall only be accepted from the TSP.

4.7.3 Processing certificate re-keying requests

Re-key of CA Certificates is supported provided that:

- The keys and certificate for the CA are still valid (e.g. not expired) at the time when routine re-key falls due.
- The identification details of the concerned CA have not changed.
- The CA has not been listed as compromised.
- The CA remains listed at the time of re-keying as a qualified TSP as defined in the eIDAS Regulation [2] on the trusted list held by the Malta Communications Authority in accordance with the requirements of the Electronic Commerce Act [10].
- The GOM Root CA Certificate has not expired.

4.7.4 Notification of new certificate issuance to subscriber

Notification of new certificate issuance to a subscriber shall follow the procedure used for initial Certificate issuance (see 4.3.2).

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Conduct constituting acceptance of a re-key Certificate shall follow the procedure used for initial Certificate acceptance (see 4.4.1).

4.7.6 Publication of the re-keyed certificate by the CA

Re-keyed CA Certificates shall be published to the repository.

4.7.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

Certificate modification is not allowed by the GOM eID PKI.

4.8.2 Who may request certificate modification

Not applicable.

4.8.3 Processing certificate modification requests

Not applicable.

4.8.4 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 CA

Not applicable.

4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A Certificate shall be revoked when:

- The Certificate contains invalid information.
- The electronic Identity Card of the Subscriber which contains the Certificate(s) has been reported lost/stolen, disclosed or otherwise compromised/misused/defaced.
- The Subscriber is deceased or no longer authorized to use the Certificate.
- The Subscriber does not comply with this Certificate Policy, Subscriber Agreement or any other applicable terms and conditions specified by the TSP.
- Any Certification Services provider associated with Certificate issuance does not comply with the GOM eID CPS.
- The TSP terminates its operation.
- A Subscriber requests that the Certificate is revoked, and the request is properly authorised in accordance with section 3.4.
- A request is received and authenticated from a person who has power of attorney, or any reliable third-party, as defined in section 4.9.2.
- A suspended Certificate has exceeded the permitted Certificate suspension period (see 4.9.16).
- In relation to the Qualified Electronic Signature Certificate: when the Qualified Electronic Signature Certificate no longer complies with the requirements of the eIDAS Regulation [2] in relation to qualified certificates for electronic signatures; or when the TSP issuing the Qualified Electronic Signature Certificate no longer complies with the requirements of the eIDAS Regulation [2] in relation to qualified trust service providers; or when the TSP issuing the Qualified Electronic Signature Certificate is no longer listed as a supervised qualified TSP on the trusted list held by the Malta Communications Authority in accordance with the requirements of the Electronic Commerce Act [10].

A CA Certificate shall be revoked if it is no longer trusted by the Policy Management Authority.

4.9.2 Who can request revocation

Requests for revocation 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 recognised 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.

The Policy Management Authority shall also have authority to request Certificate Revocation with reasonable discretion.

Revocation requests for CA Certificates shall be made by the TSP.

4.9.3 Procedure for revocation request

An approved Certificate revocation request shall result in the revocation of all Certificates held by the Subscriber under this Certificate Policy.

Subscriber requested Certificate revocation shall only be undertaken as part of a process that requires the physical presence of the Subscriber and verifies their identity. Where a Subscriber is authenticated but is not physically present, the Certificate that is the subject of the revocation request and all other Certificates held by the Subscriber under this Certificate Policy shall be suspended.

Certificate Revocation requests shall include sufficient information to uniquely identify the Certificate which is the subject of the request.

Revocation shall be requested promptly upon any circumstance for revocation arising.

Revocation requests shall be made to the Revocation Management Service which shall:

- Conduct authentication of the requestor.
- Validate the reason for the request.
- Ensure sufficient information is available to uniquely identify the Certificate(s) which is/are the subject of the request.

Where reliable authentication of the revocation request is not possible or even omitted, the Revocation Management Service is authorised to conduct revocation after seeking confirmation of the request to the greatest extent possible. Processes may involve additional checking and information gathering to allow the Revocation Management Service to achieve a satisfactory level of assurance in the validity of the request.

For CA Certificates, revocation shall be carried out the by the Certificate Generation Service.

4.9.4 Revocation request grace period

If a revocation request is approved, it shall be reflected in the next scheduled publication of a CRL and in the next update of the Certificate status services (see 4.10).

Revocation of a CA Certificate shall result in a new CRL being issued promptly. This action shall be carried out in accordance with a timescale defined by the TSP and agreed with the Policy Management Authority.

4.9.5 Time within which CA must process the revocation request

The time to process a Certificate Revocation request is made up of two elements:

- The time for the request to be validated, approved and action taken by the Revocation Management Service.
- The time taken for the Certificate Generation Service to respond to the authorised Certificate revocation request and for updated Certificate status information to be published.

The overall time for completion of the two elements stated above shall not exceed 24 hours.

4.9.6 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 of the CPS [13].

4.9.7 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 of the CPS [13].

4.9.8 Maximum latency for CRLs (if applicable)

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

4.9.9 On-line revocation/status checking 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 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..

4.9.10 On-line revocation checking requirements

See section 4.9.6.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 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.

4.9.13 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.

4.9.14 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).

4.9.15 Procedure for suspension request

An approved request for Certificate suspension shall result in the suspension of all Certificates held by the Subscriber under this Certificate Policy.

Certificate suspension requests shall include sufficient information to uniquely identify the Certificate which is the subject of the request.

Suspension requests shall be made to the Revocation Management Service which shall:

- Conduct authentication of the requestor.
- Validate the reason for the request.
- Ensure sufficient information is available to uniquely identify the Certificate(s) which is/are the subject of the request.

Where reliable authentication of the suspension request is not possible or even omitted, the Revocation Management Service is authorised to conduct suspension after seeking confirmation of the request to the greatest extent possible. Processes may involve additional checking and information gathering to allow the Revocation Management Service to achieve a satisfactory level of assurance in the validity of the request.

Subscriber requested Certificate un-suspension shall only be undertaken as part of a process that requires the physical presence of the Subscriber and verifies their identity and shall result in the unsuspension of all Certificates held by the Subscriber under this Certificate Policy.

4.9.16 Limits on suspension period

There is no limit on a period of suspension.

4.10 Certificate status services

4.10.1 Operational characteristics

The types of Certificate status checking services made available to the Relying Party by the Certificate Status Service are defined in Section 4.10 of the CPS [13] and shall include as a minimum CRL and OCSP.

4.10.2 Service availability

The availability of any Certificate status checking services that are available to Relying Parties is, if applicable, published in Section 4.10 of the CPS [13].

4.10.3 Optional features

The optional features of any Certificate status checking services that are available to the Relying Parties, if applicable, are published in Section 4.10 of the CPS [13].

4.11 End of subscription

Citizen Authentication Certificate and Citizen Qualified Electronic Signature Certificate usage may be terminated by the Subscriber by means of revocation of their Certificates.

The PMA may terminate any certificate subscription at its discretion at any time. This will result in Certificate revocation.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Key escrow or key recovery is not supported or permitted under this Certificate Policy.

For CA keys, escrow and recovery procedures shall be defined in the CPS.

4.12.2 Session key encapsulation and recovery policy and practices

The TSP does not offer or support any form of session key encapsulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

The TSP and all Participants providing Certification Services shall minimize risks related to physical security and control physical access by authorized individuals to those components of their systems whose security is critical to the provision of its services.

Components that are critical for the secure operation of Certification Services e.g. Certificate generation and revocation management systems, shall be located within a protected security perimeter with physical protection against intrusion, controls on access through the security perimeter and alarms to detect intrusion.

Physical and environmental security controls shall be implemented to protect the facilities housing system resources, the system resources themselves, and the facilities used to support their operation.

Controls shall be implemented to avoid loss, damage, compromise and interruption to business activities or assets, information and information processing facilities.

Sites where Certificate Generation Services and Subject Device Provision Services are carried out shall:

- Satisfy at least the requirements specified by ISO 27001: 2013 or a recognised equivalent.
- Use ISO 27002: 2013 as guidance.
- Be manually or electronically monitored for unauthorised intrusion at all times.
- Apply controls such that unescorted access is limited to authorised personnel.
- Ensure unauthorised personnel are properly escorted and supervised.
- Ensure a site access log is maintained and inspected periodically.
- Ensure all removable media and paper containing sensitive plain text information is stored in secure containers.

Registration Service and Revocation Management Service sites shall be located in areas that at least satisfy the controls applicable for the assurance levels for the level of registration and/or identity management activities conducted; and at a minimum be compliant with ISO 27001:2013.

If a Registration Service is permitted to initiate requests for Certificate issuance, the Certificate Generation Service shall ensure the operation of the Registration Service site provides appropriate security protection for any cryptographic module and/or Registration Service Administrator's Private Key used in the process.

All Dissemination Service and Certificate Status Service sites shall be located in areas that at a minimum satisfy the requirements for ISO 27001:2013 and in addition, shall:

- Ensure unescorted access to the repository server(s) is limited to authorised personnel.
- Ensure unauthorised personnel are properly escorted and supervised
- Ensure a site access log is maintained and inspected periodically.

Where PINs, pass-phrases or passwords are recorded, they shall be stored in a security container accessible only to authorised personnel.

5.1.2 Physical access
See section 5.1.1.

5.1.3 Power and air conditioning
See section 5.1.

5.1.4 Water exposures
See section 5.1.

5.1.5 Fire prevention and protection
See section 5.1.

5.1.6 Media storage
Controls shall be placed on all media used for the storage of information such as keys, activation data, confidential Subscriber information or TSP information.

5.1.7 Waste disposal
All media used for the storage of information such as keys, activation data, confidential Subscriber information or system files shall be sanitised or destroyed using controlled mechanisms before being released for disposal. The CPS shall detail the mechanism used. See also 5.1.6.

5.1.8 Off-site backup
Off-site backup arrangements shall be in place as required by the business continuity arrangements outlined in Section 5.7

Where data and facilities are removed from primary locations or in support of business continuity activities, controls shall be applied which are at least comparable with those of the primary location.

5.2 Procedural controls

5.2.1 Trusted roles
All Participants providing Certification Services shall ensure a separation of duties for critical functions to prevent a single person from compromising, maliciously using or modifying a PKI or supporting system without detection.

The Certificate Generation Service shall provide for the separation of distinct PKI personnel roles by named personnel, distinguishing between day-to-day operation of the PKI systems and the management and audit of those operations. To the greatest extent possible, differing levels of physical and systems access control based on roles and responsibilities shall be employed to reflect the requirements of those roles and responsibilities. Controls shall be detailed in the CPS [13] and/or supporting documentation.

Registration Authorities shall ensure that all Registration Authority personnel are adequately trained and understand their responsibility for the identification and authentication of prospective Subscribers and related Certificate management tasks. Registration Authorities shall document arrangements for trusted roles in their documentation that supports the CPS.

5.2.2 Number of persons required per task

Multi-person control is required for all operations on CA keys.

Multi-person controls shall be established for the performance of critical functions associated with the build and management of Participant systems, including the software controlling Certificate Generation operations.

Certificate issuance by the root CA shall be under at least multi-person control by authorized, trusted personnel such that one person cannot sign subordinate certificates on his/her own.

5.2.3 Identification and authentication for each role

All Participants providing Certification Services shall ensure personnel in trusted roles are formally appointed and approved to hold the position.

5.2.4 Roles requiring separation of duties

For the Certificate Generation Service, roles requiring the separation of duties are not specifically prescribed. The assignment of duties among personnel shall maintain appropriate separation of duties so as not to compromise the security arrangements for the Certificate generation and other critical processes. The Certificate Generation Service shall provide and maintain records of role allocation.

Other Participants providing Certification Services shall maintain appropriate separation of duties so as not to compromise the security arrangements for critical processes.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Participants shall ensure all personnel (internal and outsourced Participant) who serve in trusted roles shall have their qualifications, competence, experience and trustworthiness assessed and that all personnel performing duties with respect to its operations shall:

- Be appointed in writing.
- Be bound by contract or statute to the terms and conditions of the position they are to fill.
- Have received training with respect to the duties they are to perform.
- Be bound by statute or contract not to disclose sensitive security-relevant information or Subscriber information and maintain required protection of personal information.
- Not be assigned duties that may cause a conflict of interest with their service provision duties.
- Not have been, as far as known, previously relieved of a past assignment for reasons of negligence or non-performance of duties.

Participants providing Certification Services may also specify additional criteria for security clearance of personnel, such as requirements for citizenship, rank, qualifications, satisfactory credit check, and absence of a criminal record. Any such additional requirements or stipulations for this and sections of 5.3.2 to 5.3.6 inclusive shall be described in the CPS [13] and/or supporting documentation.

5.3.2 Background check procedures.

See 5.3.1.

5.3.3 Training requirements
See 5.3.1.

5.3.4 Retraining frequency and requirements
No stipulation.

5.3.5 Job rotation frequency and sequence
No stipulation.

5.3.6 Sanctions for unauthorized actions
The GOM eID PKI shall follow the GOM procedures for imposing sanctions for deliberate or repeated wrong behaviour or unauthorised actions.

5.3.7 Independent contractor requirements
Independent contractors holding Trusted Roles shall be subject to the same background, trustworthiness and competence check as other GOM eID PKI staff. See section 5.3.1

Participants providing Certification Services shall ensure that contractor access to its facilities is in accordance with this Certificate Policy.

The actions of contracting staff are subject to the same audit arrangements and requirements as those of the personnel of the Participant providing Certification Services.

5.3.8 Documentation supplied to personnel
All personnel associated with Certification Services provision shall be provided access to all documentation relevant to their position. This will include the Certificate Policies and associated Certification Practice Statements relevant to the service, together with any specific supporting documentation, statutes, policies or contracts relevant to the position and role of the personnel.

5.4 Audit logging procedures

5.4.1 Types of events recorded
Participants providing Certification Services shall record and keep accessible for the period of time specified in section 5.4.3, including after the activities of the Participant have ceased, all relevant information concerning data issued and received by the Participant, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service.

The events shall be logged in a way that they cannot be modified deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held.

Security events shall be logged. Logging shall reflect the risks applicable for the aspects of the service for which logging is conducted. All events relating to the life-cycle of CA keys, issued Certificates, keys managed by the CA and Subscriber keys provided by the Certificate Generation Service shall be logged.

All events related to Subscriber registration including requests shall be logged, and logs shall include the following:

- Type of document(s) presented by the applicant to support registration.
- Record of unique identification data, numbers, or a combination thereof (e.g. applicant's identity card or passport) of identification documents, if applicable.

- Storage location of copies of applications and identification documents, including the subscriber agreement.
- Any specific choices in the subscriber agreement (e.g. consent to publication of certificate).
- Identity of entity accepting the application.
- Method used to validate identification documents, if any.
- Name of receiving TSP and/or submitting Registration Authority, if applicable.

All key ceremony records and information used to verify key ceremony attendee identity shall also be retained.

Participants providing Revocation Management Services shall log all requests and reports relating to revocation, as well as the resulting action.

5.4.2 Frequency of processing log

Participants providing Certification Services shall review audit logs as appropriate to the items being recorded and shall provide details of audit log processing in their records of role allocation in the Certification Practice Statement and/or supporting documentation.

5.4.3 Retention period for audit log

Audit logs shall be retained for a period of no less than 40 years.

5.4.4 Protection of audit log

Any electronic audit log system shall include mechanisms to protect the log files from unauthorised viewing, modification, and deletion. Manual audit information shall be protected from unauthorised viewing, modification and destruction.

5.4.5 Audit log backup procedures

Audit logs and audit summaries shall be backed up or if in manual form, shall be copied and stored in independent locations.

All backups shall be provided with the same level of security as the originals and shall be commensurate with the data contained within them.

5.4.6 Audit collection system (internal vs. external)

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

No stipulation.

5.5 Records archival

5.5.1 Types of records archived

The event records and any accompanying data as described in section 5.4.1 of this Certificate Policy are to be archived.

Participants providing Certification Services may also be required to retain additional information to ensure compliance with this Certificate Policy and/or legal requirements.

The Registration Service and Revocation Management Service shall retain records of information provided in support of Certificate application and revocation requests.

5.5.2 Retention period for archive

Archived information is to be retained for a period of no less than 40 years.

5.5.3 Protection of archive

Archives are to be protected from unauthorised viewing, modification, and deletion. Archives are to be adequately protected from environmental threats such as temperature, humidity and magnetism.

Details of protection shall be described in the Certification Practice Statement and/or supporting documentation.

Multiple copies of information may be archived.

5.5.4 Archive backup procedures

No stipulation.

5.5.5 Requirements for time-stamping of records

No stipulation.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

Participants providing Certification Services shall ensure availability of their archives and that archived information is stored in a readable format during its retention period, even if the TSP's operations are interrupted, suspended or terminated.

In the event that the services of a Participant providing Certification Services for or on behalf of the TSP are to be interrupted, suspended or terminated, the TSP shall ensure the continued availability of the archive.

All requests for access to archived information shall be sent to the TSP or to the entity identified by the PMA prior to terminating its service.

5.6 Key changeover

CA key changeover shall be conducted only at the specific direction of the PMA.

All new CA keys shall be generated and a new CA Certificate corresponding to the new keys issued sufficiently in advance of expiry of the existing CA Certificate to maintain continuity of service.

Following CA key changeover, the new CA Certificate shall be made available in the repository (see section 2.2) and as required to meet Certificate chaining requirements.

All copies of old CA private keys shall be destroyed.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

A business continuity plan shall be in place to protect critical Public Key infrastructure processes from the effect of major compromises, failures or disasters. These shall enable the recovery of all

TSP services. Business continuity plans for Participants providing Certification Services shall be detailed in the Certification Practice Statement and/or supporting documentation.

Participants providing Certification Services shall provide evidence that such plans have been exercised.

In the case of compromise of a CA or CA keys, the TSP shall as a minimum require the following:

- Immediately cause the suspension of the Certificate Status checking service for all Issued Certificates affected by a compromise, failure or disaster. This will stop any of these Certificates from being accepted by any Relying Party who follows proper Revocation checking procedures according to section 4.5.2 of this document.
- Suspension of any further Certificate Issuance from the affected CA.

The Policy Management Authority and/or TSP shall make any determination relating to Revocation of CA Certificates.

The TSP shall, in accordance with eIDAS Regulation No 910/2014 [2], notify the relevant parties of any breach of security or loss of integrity that has a significant impact on the Trust Service provided or on the personal data maintained therein.

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

Participants providing Certification Services shall establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data.

Business continuity plans for Participants providing Certification Services shall be detailed in the Certification Practice Statement and/or supporting documentation. Plans shall be approved by the TSP.

5.7.3 Entity private key compromise procedures

See section 5.7.1. and section 4.9.12.

5.7.4 Business continuity capabilities after a disaster

The business continuity plan for the TSP shall be designed to deal with any disruption to services and shall ensure managed, progressive recovery of components used to provide the service. A geographically separate alternative backup facility to maintain, at a minimum, Certificate Status information shall be made available.

Any backup facility used for relocation following a disaster shall maintain compliance with this Certificate Policy. The provisions of this Certificate Policy shall be maintained during any relocation/transition procedures.

Registration Authority business continuity arrangements shall be approved by PMA.

5.8 CA or RA termination

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

The PMA shall be responsible for the execution of the termination plan.

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

- Inform all Subscribers, cross-certifying CAs, Relying Parties and Subcontractors 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.
- Inform all relevant trusted personnel
- Hand over its activities to another TSP of the same quality and which holds applicable certifications of compliance; if this is not possible, revoke the Certificates two (2) months after having informed all Subscribers and archive all relevant Certificate information.
- Where practicable, make publicly available details of termination arrangements at least 3 months prior to termination.
- Publish the last CRL issued after the revocation of the last unexpired and unrevoked Certificate in the repository.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

CA key pairs shall be generated during a witnessed key signing ceremony in a physically secured environment under a minimum of dual control by persons holding trusted roles. All private keys used by the TSP or other Participants providing Certification Services that affect the status of issued Certificates or Certificate status information shall be generated securely under controlled procedures. Participants conducting such key generation shall provide details of the procedure in the CPS [13] and/or supporting documentation.

Subscriber keys for use with secure subject devices (Identity Cards) shall be generated and stored on the device under control of the Registration Authority. It shall not be possible to export any Private Key from the device and the device shall be appropriately secured during preparation, storage and distribution.

6.1.2 Private Key delivery to subscriber

Private Key delivery to Subscribers shall satisfy the following:

- The secure subject device (Identity Card) containing the Private Key, protected with its initial activation data, shall be distributed to the Subscriber using a sufficient strength of mechanism that prevents it from being found together with the activation data, until it has been delivered to the Subscriber.
- Delivery of a secure subject device containing a Private Key that is (or will be) associated with a Certificate according to this Certificate Policy, is only allowed to be effected to the Subscriber through a registered postal delivery service or in person through a face to face meeting with the Registration Service.

- To obtain the secure subject device, the Subscriber shall present valid identification that at least meets the requirements for initial registration see Section 3.2. The means of identification shall be recorded.
- Subscribers shall acknowledge receipt of the secure subject device in writing which is retained by the TSP.
- Controls shall be in place to ensure the Subscriber replaces initial activation data for the secure subject device with personally chosen activation data.

6.1.3 Public key delivery to certificate issuer

All Subscriber Public Keys from Registration Authorities shall be delivered to the Certificate Generation Service in a secure manner using a standard, recognised protocol; (e.g. PKCS#10).

For CA Certificates, the public key shall be delivered to the Certificate issuer in the form of a Certificate request. Proof of possession is achieved using the mechanism defined in section 3.2.1.

6.1.4 CA public key delivery to relying parties

CA Certificates for Relying Party use shall be distributed via the repository. See section 2.2.

6.1.5 Key sizes

Root CA Key Pairs shall be 4096 bits RSA.

Citizen eID CA Key Pairs shall be 2048 bits RSA.

Subscriber Key Pairs shall be 2048 bits RSA.

6.1.6 Public key parameters generation and quality checking

Public Key exponents shall be of values and lengths that make known attacks (e.g. low exponent attacks) infeasible.

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

CA Certificates shall be used for the following key usages purposes: Certificate Signature, CRL Signature.

Qualified Electronic Signatures Certificates shall be used for the following key usages purposes: Non-repudiation.

Authentication Certificates shall be used for the following key usages purposes: Digital Signature.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

CA keys shall be protected by high assurance physical and logical security controls. They shall be stored in and operated from inside a specific tamper resistant hardware-based security module that complies with FIPS140-2 level 3, its equivalents and successors.

Private Keys used in any Certification Service and/or Registration Authority process that affects the outcome of issued Certificates and Certificate status information services (such as signing Certificate Revocation Lists), shall be protected by, maintained in, and restricted to, a cryptographic module designed to meet the level of requirements as specified in FIPS 140-2 level 2, or its equivalents and successors.

CA keys shall not be available in unprotected form (complete or unencrypted) except in approved cryptographic modules.

Subscriber secure subject devices (Identity Cards) shall be Qualified Electronic Signature Creation Devices (QSCD) as defined in eIDAS Regulation No 910/2014 [2].

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

For any CA keys, and keys that affect the outcome of issued Certificates and Certificate status information services, at a minimum two-person control is required for management of the Private Keys.

6.2.3 Private Key escrow

Key escrow by Participants is not permitted.

6.2.4 Private Key backup

Participants providing Certification Services may backup and archive Private Keys, including CA keys. In all cases key backups shall at a minimum be protected to the standards stipulated for the primary version of the key.

6.2.5 Private Key archival

No stipulation.

6.2.6 Private Key transfer into or from a cryptographic module

Subscriber keys are generated and stored on the Subscriber secure subject device and are never transferred to or exported from the device.

Any CA Private Key transfer shall be done such that the Private Key is protected cryptographically in accordance with FIPS140-2 level 3, its equivalents and successors.

6.2.7 Private Key storage on cryptographic module

For any CA keys and keys that affect the outcome of issued Certificates and Certificate status information services and other business processes prescribed standards are required for the cryptographic protection of Private Keys. See Section 6.2.1.

6.2.8 Method of activating private key

Subscribers shall be authenticated to their secure subject device before the activation of the Private Key. This authentication may be in the form of a PIN, pass-phrase password or other activation data, as detailed in the Subscriber Agreement.

6.2.9 Method of deactivating private key

Strict controls over destruction of CA keys and keys that affect the outcome of issued Certificates and Certificate status information services, shall be exercised.

Whether active, expired or archived, the PMA shall approve the destruction of CA keys and supporting keys.

6.2.10 Method of destroying private key

Strict controls over destruction of CA keys and keys that affect the outcome of issued Certificates and Certificate status information services, shall be exercised. Whether active, expired or archived, the PMA shall approve the destruction of CA keys and supporting keys.

6.2.11 Cryptographic Module Rating
See section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival
Public keys shall be archived in accordance with Section 5.5 of this Certificate Policy.

6.3.2 Certificate operational periods and key pair usage periods
Usage periods for key pairs shall be governed by validity periods set in Issued Certificates. These shall have the following maximum values:

- Citizen eID Qualified Electronic Signature Certificate - maximum of ten years.
- Citizen eID Authentication Certificate - maximum of ten years.
- Citizen eID CA Certificate - twenty years.
- GOM Root CA Certificate - thirty years.

Private Keys shall not be extended beyond the initial lifetime of the Certificate Issued to verify them.

6.4 Activation data

6.4.1 Activation data generation and installation
All TSP CA keys and keys that affect the outcome of issued Certificates and Certificate status information services shall have activation data that is unique and unpredictable. The activation data, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected.

Activation data for CA Private Keys shall be compliant with FIPS 140-2 Level 3, its equivalents and successors.

Activation data for Subscriber Private Keys shall be managed in accordance with the requirements for Qualified Electronic Signature Creation Devices (QSCD) as defined in eIDAS Regulation No 910/2014 [2].

Where PINs, passwords or pass-phrases are used, an entity shall have the capability to change these at any time.

If applicable, unblocking code for a cryptographic module (if available) shall only be delivered to the legitimate holder of the module after an express request from the holder. Delivery of the unblocking code requires strong identification of the holder. See Section 6.2.8.

6.4.2 Activation data protection
All CA keys and keys that affect the outcome of issued Certificates and Certificate status information services shall have mechanisms for the protection of activation data which is appropriate to the Keys being protected.

Details of protection shall be provided in the CPS [13[and/or supporting documentation.

6.4.3 Other aspects of activation data
No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Participants providing Certification Services shall implement security measures that have been identified through a threat assessment exercise and shall cover the following functionality where appropriate:

- Access control to Certification Services and PKI roles.
- Enforced separation of duties for PKI roles.
- Identification and authentication of PKI roles and associated identities.
- Use of cryptography for session communication and database security.
- Archival of Participant history and audit data.
- Audit of security related events.
- Trusted path for identification of PKI roles and associated identities.
- Recovery mechanisms for keys of Participants providing Certification Services.

This functionality may be provided by the operating system, or through a combination of operating system, PKI application software, and/or physical safeguards.

Procedures shall at a minimum include logging and audit requirements for processes related to initialisation, resetting, shutdown or reconfiguration of CAs and any services that affect the outcome of issued Certificates and Certificate status information.

Participants providing Certification Services shall document procedures in the Certification Practice Statement and/or supporting documentation.

6.5.2 Computer security rating

The TSP shall use Trustworthy Systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

Any hardware security module or device holding CA Keys shall comply with the requirements of 6.2.1 of this Certificate Policy.

Where specific computer security rating requirements are specified in this Certificate Policy, the Participant providing Certification Services shall provide details in the CPS [13] and/or supporting documentation of relevant components and how they satisfy the requirements.

6.6 Life cycle technical controls

6.6.1 System development controls

The development of software, that implements Certification Services functionality shall as a minimum be performed in a controlled environment that, together with at least one of the following approaches, shall protect against the insertion of malicious logic.

- The system developer shall have a quality system certified as compliant with international standards or;
- The system developer shall have a quality system available for inspection and approval by the TSP.

6.6.2 Security management controls

The configuration of systems operated by Participants providing Certification Services as well as any modifications, upgrades and enhancements shall be documented and controlled. There shall be a method of detecting unauthorised modification or configuration of the software supporting Certification Services. Participants providing Certification Services shall ensure that it has a configuration management process in place to support the evolution of the systems under its control.

Details of security management systems shall be provided in the CPS [13] and/or supporting documentation.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

Participants systems providing Certification Services shall be protected from attack through any open or general-purpose network with which they are connected. Such protection shall be provided and configured to allow only the minimal set of functions, protocols and commands required for the operation of the Certification Services.

Participants providing Certification Services shall detail the standards procedures and controls for network security in the CPS [13] and/or supporting documentation.

6.8 Time-stamping

Time recording shall be implemented for all Certificate and other related activities that require recorded time. A synchronised and controlled time source shall be used.

Participants providing Certification Services shall detail the time source used and mechanisms for its control in the CPS [13] and/or supporting documentation which shall be approved by the Certification Authority or Auditors acting on its behalf.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

Certificate Profiles are under the direct control of the PMA and are shown in Appendix 2.

Procedures for development of Certificate Profiles shall incorporate approval by the PMA prior to implementation.

Certificates governed by this Certificate Policy shall conform to the profiles given in Appendix 2: Certificate Profiles.

7.1.1 Version number(s)

Only Certificates conformant to X.509 Version 3 and IETF RFC 5280 [7] may be issued.

7.1.2 Certificate extensions

Key Usage: Key usage shall be consistent with Section 6.1.7 of this Certificate Policy.

CRL Distribution Point: This field shall contain the location of http and directory hosted CRL information.

Basic Constraints: The Subject Type value shall be set to “end entity”, with Path Length constraint not asserted. This field shall not be marked critical.

Authority Key Identifier: This field shall not be marked critical.

Subject Key Identifier: This field shall not be marked critical.

Certificate Policies: See section 1.2.

OID: See section 7.1.6.

IssuerAltName: This extension is used to associate Internet style identities with the certificate issuer, as follows:

Field	Contents
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

Table 2: Issuer Alternative Name field contents

7.1.3 Algorithm object identifiers

The signature algorithm that shall be used to sign Qualified Electronic Signature Certificates, Authentication Certificates and CA Certificates is RSA with SHA2 (256). Its Object Identifier is {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}.

7.1.4 Name forms

See section 7.1 and section 3.1.

7.1.5 Name constraints

See section 7.1.

7.1.6 Certificate policy object identifier

This Certificate Policy has been assigned the following Object Identifiers (OIDs).

Class of certificate	Object Identifier

GOM PKI Citizen Qualified Electronic Signature Certificate	2.16.470.4.2.2
GOM PKI Citizen Authentication Certificate	2.16.470.4.2.3

The OIDs are assigned within the range registered to MECS and assigned to the GOM PKI.

The appropriate OID shall be included in the certificate Policies extension of all Certificates Issued under this Certificate Policy.

7.1.7 Usage of Policy Constraints extension
See section 7.1.

7.1.8 Policy qualifiers syntax and semantics
See section 7.1.

7.1.9 Processing semantics for the critical Certificate Policies extension
No stipulation.

7.2 CRL profile

7.2.1 Version number(s)
Only CRL conformant to X.509 Version 2 and IETF RFC 5280 [7] and RFC 6818 [8] may be issued.

7.2.2 CRL and CRL entry extensions
Authority Key ID.

CRL Number.

ExpiredCertsOnCRL. This extension shall be used to ensure expired Certificate information is available in the CRL.

7.3 OCSP profile

7.3.1 Version number(s)
Version 1.0, as supported by RFC 6960 [9].

7.3.2 OCSP extensions
No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment
The GOM eID PKI shall be audited in accordance with the eIDAS Regulation No 910/2014 [2] for the provision of qualified certificates.

Such audits shall be conducted by an authorised Conformity Assessment Body that complies with ETSI EN 319 403 and ISO/IEC 17065-2012.

Malta Electronic Certification Services Ltd shall submit a Conformity Assessment Report to the Supervisory Body, Malta Communications Agency (MCA), as required by the eIDAS Regulation No 910/2014 [2], in accordance with the requirements of the MCA.

The Policy Management Authority may at its discretion audit or commission a third-party audit of any Participant providing Certification Services governed by this Certificate Policy.

The GOM eID PKI shall be audited on a periodic basis not exceeding 24 months.

8.2 Identity/qualifications of assessor

See section 8.1.

For any assessment commissioned by the Policy Management Authority, the identity and relevant qualifications for an approved assessor is at its sole discretion, subject to section 8.3 of this Certificate Policy and the eIDAS Regulation No 910/2014 [2].

8.3 Assessor's relationship to assessed entity

Aside from the audit function, the auditor and audited party shall have no current or planned financial, legal or other relationship that could result in a conflict of interest.

8.4 Topics covered by assessment

The compliance audit will include the control requirements defined within the eIDAS Regulation No 910/2014 [2] and as specified by the MCA for persons intending to provide a qualified trust service.

8.5 Actions taken as a result of deficiency

Actions taken as a result of deficiency shall comply with the eIDAS Regulation No 910/2014 [2].

A remedial action plan shall be created to address the audit finding and the specific actions to be undertaken will depend on the severity of the findings. At the sole discretion of the PMA, actions resulting from any identified actual or possible deficiency may include:

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

8.6 Communication of results

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

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

The distribution of any deliverables resulting from audits and the communication of results is at the discretion of the Policy Management Authority.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

The TSP shall not charge fees for the provision of services described within this Certificate Policy. Additional Subscriber fees may apply however, in particular where an application is made for an Identity Card in substitution of an Identity Card lost, stolen, destroyed or defaced, as determined in accordance with the provisions of the Identity Card Act [1].

9.1.1 Certificate issuance or renewal fees

See section 9.1.

9.1.2 Certificate access fees

See section 9.1.

9.1.3 Revocation or status information access fees

See section 9.1.

9.1.4 Fees for other services

See section 9.1.

9.1.5 Refund policy

See section 9.1.

9.2 Financial responsibility

The TSP shall either itself or in conjunction with its contractors, maintain appropriate human resource and IT management capabilities to meet its obligations under this Certificate Policy and as required under the eIDAS Regulation [2] and the Electronic Commerce Act [10]. The TSP is responsible for maintaining its financial books and records in accordance with Maltese law and shall engage the services of an international accounting firm to provide financial services, including periodic audits.

However, the TSP is a limited liability company whose liability is excluded and limited in the manner set out in the Subscriber Agreement, the Relying Party Agreement, and the PKI Disclosure Statement, and as set out in this section 9.

9.2.1 Insurance coverage

The TSP maintains appropriate insurance coverage in relation to its obligations under the eIDAS Regulation [2] and the Electronic Commerce Act [10]. The TSP provides the Maltese Communications Authority with proof of the insurance coverages in accordance with the provisions of the eIDAS Regulation [2].

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

The TSP observes confidentiality rules as described in this Certificate Policy for any personal information as described in section 9.4, and for any other information that is explicitly marked as

business information or as confidential information by either the TSP or by the Policy Management Authority, as well as for any other information that, by reason of its content or nature, manifestly must be considered as not being suitable for public dissemination or for public knowledge.

9.3.1 Scope of confidential information

Confidential information explicitly includes:

- Any personal identifiable information on citizens, other than that contained in a certificate;
- Exact reason for the revocation or suspension of a certificate;
- Any audit trails;
- Logging information for reporting purposes, such as logs of requests by the RA;
- Correspondence regarding CA services;
- CA private key(s).

9.3.2 Information not within the scope of confidential information

Confidential information explicitly excludes:

- Certificates and their content;
- Status of any certificate as communicated via a Certificate status service

9.3.3 Responsibility to protect confidential information

Parties requesting or receiving confidential information may be granted permission on the condition that they use it for the requested purposes, secure it from compromise, and refrain from using it or disclosing it to third parties. These parties are bound to observe personal data privacy rules in accordance with the law and are responsible for complying with any Maltese law that applies to such confidential information. Where Maltese law contains any limitation on permissible use of the confidential information, such limitation shall apply to the recipient of the confidential information.

9.4 Privacy of personal information

The TSP and any processing of personal information in the context of the GOM eID will comply with the General Data Protection Regulation (No 2016/679) [11] and with the Data Protection Act [12]. Information processed within the GOM eID PKI as part of the performance and management of this Certificate Policy will comply with the Identity Card Act [1].

9.4.1 Privacy plan

The TSP maintains a privacy plan that permits it to comply with the provisions of the General Data Protection Regulation (No 2016/679) [11] and with the Data Protection Act [12]. The TSP does not release nor is it required to release any personal information except as set out in the Certificate Policy without an authenticated and justified request specifying either:

- The party to whom the TSP owes a duty to keep information confidential. The TSP owes such a duty to the Policy Management Authority and promptly responds to any such requests;
- A court order which is valid and enforceable under Maltese law, after consultation of the Policy Management Authority.

9.4.2 Information treated as private
Information shall be treated as private personal information when it constitutes personal data under the General Data Protection Regulation (No 2016/679) [11].

9.4.3 Information not deemed private
Information shall not be treated as private personal information when it does not constitute personal data under the General Data Protection Regulation (No 2016/679) [11].

9.4.4 Responsibility to protect private information
The TSP properly manages the disclosure of personal information to the TSP personnel or other persons involved in the management and operation of the GOM eID PKI. Other disclosures of private information are only permitted in accordance with the terms of this Certificate Policy, the Identity Card Act [1], or other applicable Maltese law, and shall at all times comply with the General Data Protection Regulation (No 2016/679) [11].

9.4.5 Notice and consent to use private information
The TSP operates within the boundaries of the General Data Protection Regulation (No 2016/679) [11] and with the Data Protection Act [12]. Where necessary, notice and consent of Subscribers is obtained through the Subscriber Agreement, complementary to the publication of Maltese law, and through publications made in coordination with the Policy Management Authority.

9.4.6 Disclosure pursuant to judicial or administrative process
See section 9.4.1.

9.4.7 Other information disclosure circumstances
No stipulation.

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

9.6 Representations and warranties
The respective obligations and liabilities of the TSP, Subscribers and Relying Parties are as expressly set out in the CPS, this Certificate Policy, the Subscriber Agreement and the Relying Party Agreement.

All parties within the domain of the TSP, including the TSP itself, the Policy Management Authority, the Registration Authorities and the Subscribers warrant the integrity of their respective private key(s). If any such party suspects that a private key has been compromised, they will immediately notify their Registration Authority, the TSP or the police.

9.6.1 TSP representations and warranties
To the extent specified in the relevant sections of the Certificate Policy each of the following Certification Authorities are operating within the GOM eID PKI and are owned by the TSP:

- GOM Root CA;
- Malta Citizen eID CA.

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

- Comply with this Certificate Policy and its amendments as published at https://repository.qca.gov.mt/.
- Provide infrastructure and certification services, including the establishment and operation of the GOM eID Directory for the operation of public Certificate management services.
- Provide Trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its own Private Key(s).
- Provide and validate application procedures for the various types of Certificates that it makes publicly available.
- Issue electronic Certificates in accordance with this Certificate Policy and fulfil its obligations presented herein.
- Revoke Certificates issued according to this Certificate Policy upon receipt of a valid and authenticated request to revoke a certificate from a NIDMS Administrator.
- Provide for the expiration and renewal of Certificates according to this Certificate Policy.
- Publish CRLs and/or OCSP responses of all revoked certificates on a regular basis in accordance with this Certificate Policy.
- Notify Relying Parties of Certificate revocation by publishing CRLs on the GOM eID Directory.
- Operate in compliance with the laws of Malta. In particular the TSP meets all legal requirements associated with qualified electronic signature certificates and qualified trust services (where applicable) emanating from the eIDAS Regulation [2] and the Electronic Commerce Act [10].

When using third party agents the TSP will make best efforts to ensure the proper financial responsibility and liability of such contractors.

The TSP is responsible towards Subscribers and Relying Parties for the following acts or omissions:

- Issuing Certificates not containing data as provided by the Registration Authority;
- Compromise of a private signing key of the CA;
- Failure to list a revoked certificate in a CRL in accordance with the requirements of this Certification Policy;
- Failure of the OCSP responder to report a certificate as revoked or suspended in accordance with the requirements of this Certification Policy;
- Unauthorised disclosure of confidential information or private data according to sections 9.3 and 9.4

The TSP does not warrant that the GOM eID will be uninterrupted or error free and all other statements, representations, warranties or conditions are excluded to the fullest extent permitted by law.

9.6.2 RA representations and warranties

The RA operating within the GOM eID PKI domain will:

- Provide correct and accurate information in their communication with the CA;
- Ensure that the public key submitted to the CA corresponds to the private key used;
- Create certificate requests in accordance with this Certificate Policy;
- Perform all verification and authenticity actions prescribed by the CA procedures, the CPS and this Certificate Policy;
- Submit to the CA the applicant's request in a signed message;
- Receive, verify and relay to the CA all requests for revocation, suspension and unsuspension of a certificate in accordance with the CA procedures, the CPS and this Certificate Policy;
- Verify the accuracy and authenticity of the information provided by the Subscriber at the time of renewal of a certificate according to the CPS and this Certificate Policy.

If the RA becomes aware of or suspects the compromise of a private key, it will immediately notify the CA. The RA is solely responsible for the accuracy of the Subscriber data as well as any other assigned data it provides to the CA.

The RA complies with Maltese laws and regulations pertaining to the GOM eID PKI, including but not limited to the Identity Card Act [1].

9.6.3 Subscriber representations and warranties

The Subscriber warrants, represents and undertakes to the TSP that s/he will comply with his/her obligations under this Certificate Policy, the Subscriber Agreement, and Maltese law.

Unless otherwise stated in this Certificate Policy, the Subscriber's obligations include:

- Refraining from tampering with a Certificate;
- Only using Certificates for legal and authorised purposes in accordance with the Certificate Policy and Subscriber Agreement;
- Applying for a new Identity Card (and thus new Certificates) in case of any changes in the information published in the certificate;
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private keys;
- Notify the police, the Registration Authority or the TSP to request the revocation of a Certificate in case of the suspicion of an occurrence that materially affects the integrity of a Certificate. Such occurrences include indications of loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of the Certificates, or in case control over private keys has been lost due to compromise of activation data (e.g. PIN code);
- An obligation to exercise reasonable care to avoid unauthorised use of the Subscriber's private key;

Following compromise, the obligation to immediately and permanently discontinue the use of the Subscriber's private key.

9.6.4 Relying party representations and warranties

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

The reliance placed upon any digital signature created using the Certificates and associated Private Key embedded within the National Identity Card shall be limited to proof-of-possession of the card and knowledge of the associated activation data. The TSP does not authenticate the content of any message signed using a digital signature and accordingly does not entertain any liability or risk in relation thereto.

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

- Information to verify the status of Certificates where the corresponding Private Keys were used to create digital signatures.
- Information published on the Malta TSP web site.
- Any other services that the Malta TSP might advertise or provide through its web site.

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

The TSP makes every effort to ensure that parties accessing its directory receive accurate, updated and correct information. The Malta TSP, however, cannot accept any liability beyond the limits set in this Certificate Policy and in the Subscriber Agreement, the Relying Party Agreement, and the PKI Disclosure Statement.

9.6.5 Representations and warranties of other participants

No stipulation

9.7 Disclaimers of warranties

This section includes disclaimers of express warranties.

Limitation for Other Warranties

See paragraph 9.6 above.

Exclusion of Certain Elements of Damages

In no event (save to the extent arising from the fraud or wilful misconduct of the TSP or as otherwise stipulated by Maltese law) shall the TSP be liable for:

- Any loss of profits.
- Any loss of data.
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of Certificates or electronic signatures.

- Any liability incurred in any case if the error in such verified information is the result of fraud or wilful misconduct of the Subscriber or a Relying Party.

9.8 Limitations of liability

Limitation of liability in general

The liability of the TSP towards any Subscriber or any Relying Party is at any rate limited to paying damages amounting to a maximum of two thousand five hundred Euro (2.500 €) per transaction, affected by the events listed in this section here below.

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

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

Nothing in this Certificate Policy shall exclude the liability of a party for death or personal injury caused by its negligence nor shall this paragraph operate to exclude the liability of a party caused by any fraud or fraudulent misrepresentation perpetrated by any party.

Liability in relation to qualified certificates

The TSP accepts financial liability as required within the eIDAS Regulation No 910/2014 [2] for Qualified Certificates that it has issued subject to the following:

1. the TSP shall have no liability in respect of any loss or damage (including, without limitation, consequential loss or damage) which may be suffered or incurred or which may arise directly or indirectly in relation to the use or reliance upon Certificates or associated Public/Private Key pairs for any use other than in accordance with this Certificate Policy and the Subscriber Agreement and / or which exceeds the indicated limitations of any such use or reliance.
2. In any case, and to the extent permitted by law, the TSP's total liability for damage caused to the Subscriber and any Third Party for any use or reliance on a Certificate shall be limited, in total, to two thousand five hundred Euro (€2,500) per transaction. This limitation shall be the same regardless of the number of digital signatures, transactions or claims relating to such Certificate.
3. The TSP shall not be under any liability for failure to perform any of its obligations herein where such failure arises from a force majeure event that is an event beyond the TSP's reasonable direct control, including, but not limited to, Acts of God (including weather of exceptional severity, floods, lightning or fire), general or local strikes, national emergency, acts or omission of Government or other competent authorities, fire or destruction of the TSP's works or materials, insurrection or other civil disorder, war or military operations, or explosions.

Liability in relation to other certificates

The general Maltese rules on liability apply with regard to any damage caused to any entity or legal or natural person who reasonably relies on a Certificate issued by the TSP. The TSP explicitly declines all liability towards relying parties in all cases where the Authentication Certificate is used in the context of applications allowing the use of the Authentication Certificate for the generation of electronic signatures.

9.9 Indemnities

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

9.10 Term and termination

9.10.1 Term

This Certificate Policy commences on 23rd January 2019 and will continue indefinitely unless and until it is amended in accordance with paragraph 9.12 below.

9.10.2 Termination

This Certificate Policy may be terminated by the TSP, subject to prior approval of the Policy Management Authority, by serving a notice on its web site or via the GOM eID Directory.

9.10.3 Effect of termination and survival

The provisions of this Certificate Policy shall survive the termination or withdrawal of a Subscriber, Registration Authority or Relying Party from the GOM eID PKI with respect to all actions based upon the use of or reliance upon a Certificate or other participation within the GOM eID PKI. Any such termination or withdrawal shall not act so as to prejudice or affect any right of action or remedy

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
Malta

9.12 Amendments

9.12.1 Procedure for amendment

Changes to this Certificate Policy are managed by the Policy Management Authority of the GOM eID PKI. All proposed changes to the Certificate Policy need to be approved by the Policy Management Authority.

9.12.2 Notification mechanism and period

After approval, a new version of the Certificate Policy is created and published beside the former version on the Repository website.

9.12.3 Circumstances under which OID must be changed

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

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

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

9.13 Dispute resolution provisions

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

9.14 Governing law

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

9.15 Compliance with applicable law

The GOM eID PKI complies with applicable laws of Malta.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

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

9.16.2 Assignment

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

9.16.3 Severability

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

9.16.4 Enforcement (attorneys' fees and waiver of rights)

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

9.16.5 Force Majeure

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

Conflict

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

9.17 Other provisions

No stipulation.

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

[2] eIDAS Regulation No 910/2014

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

[4] ETSI EN 319 411-1, Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

[5] ETSI EN 319 411-2, Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

[6] Government of Malta PKI Disclosure Statement for Citizen Authentication Certificates and Citizen Qualified Electronic Signature Certificates

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

[8] RFC 6818: Updates to the Internet X.59 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[9] RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP

[10] ELECTRONIC COMMERCE ACT (CAP. 426), ACT III of 2001, as amended by Acts XXVII of 2002, VII of 2004 and XIII of 2005; Legal Notice 426 of 2007; and Acts XXX of 2007,XII of 2010 and XXXV of 2016

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88

[12] DATA PROTECTION ACT (CAP. 586), ACT XX of 2018

[13] Government of Malta Electronic Identity System Certification Practice Statement.

Appendix 2: Certificate 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]	
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

A2.1.4 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
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
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

A2.2.5 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		
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
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 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	

A2.3.4 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

A2.4.5 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	