Customer : Government of Malta

Project : Malta eID PKI

Title : Certificate Policy for Malta Resident Electronic Signature (Qualified) and Authentication Certificates

Date of Issue Effective 10/04/2017

Version Number 1.4

Document Control

Reviewers

Current version	Name	Date
Prepared by	De La Rue / Verizon	
Reviewed by	SEALED / Arthur Cox	
Approved by		

Change Record

Version	Date	Author	Status/Description
1.0	10/01/2013	Policy Management Authority	Issued
1.1	15/07/2015	Policy Management Authority	Updated to reflect CRL publishing frequency change
1.2	19/04/2016	Policy Management Authority	Updated to reflect legal names of sections within Identity Malta
1.3	02/06.2016	Policy Management Authority	Updated CP extension to include UserNotice re MECS Ltd
1.4	Effective 10/04/2017	Policy Management Authority	1.1 - remove reference to TS 101 456 2.3 – update time & frequency of CRL publication to hourly upon the hour 4.5 – change reference to eCommerce Act to EIDAS Regulation 5.8 – update termination plan to refer to last CRL issuance 6.1 – introduce reference to transitional measures for SSCD 7.1.5 – update certificate profile with issueraltname 7.1.12 – remove reference to TS 101 456 7.2.2 – change signingalgorithm to sha2rsa 7.2.10 – insert expiredcertsoncrl 8 – change reference to TS 101 456 to EIDAS Regulation 11.1,2,3 – update certificate and crl profiles with issueraltname, change signingalgorithm, update qcstatement, update certpolicy

Distribution list

Version	Company	Name	Action

Table of Contents

1. INTRODUCTION

1.1. Overview

1.1.1. Introduction to the Malta Government Identity System

The Government of Malta operates a national identity card for citizens and residents as defined within the Identity Card Act, Chapter 258 Laws of Malta [10]. This national identity card is currently used to facilitate interactions between Maltese citizens, residents and the Government of Malta.

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

The National Identity Management System (NIDMS) will implement strong authentication and will use a chip-embedded card that will host two Certificates: one Certificate is dedicated for the authentication purpose and is formatted according to the X509 standard [2]; the other Certificate is dedicated for the digital signature purpose and is formatted according to the Qualified Certificate standards [3] and the EIDAS Regulation No 910/2014 The Certificates are embedded within cards that have been certified as meeting the control requirements defined within the Protection Profile for a Secure Signature Creation Device [13].

This document is the Certificate Policy (CP) for the Malta Resident Electronic Signature (Qualified) and Authentication Certificates.

The GOM has established the Malta Certification Authority (MCA) to control the policies of the GOM eID PKI and to audit compliance with these policies. The role of the MCA is detailed in section 1.3.1 of the Malta eID Certificate Practice Statement.

1.1.2. CP Overview

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 [1].

This Certificate Policy is the statement by the MCA of the set of named rules that indicates the applicability of the Malta Resident Electronic Signature (Qualified) and Authentication Certificates; it is supplemented by other practices detailed in the Malta eID Certificate Practice Statement

(CPS) document [14]. It meets the formal requirements of RFC3647 [1]. The manner in which this Certificate Policy is maintained is defined in section 1.2.1.

Document name and identification

This Certificate Policy is named “Certificate Policy for Malta Resident Electronic Signature (Qualified) and Authentication Certificates”.

1.1.1. Object Identifier

The Malta Resident Electronic Signature (Qualified) and Authentication Certificates are linked to this Certificate Policy through an Object Identifier (OID) that is physically held within the associated Certificate. By including an Object Identifier in its Certificate, MCA provides assurance of its conformance to the identified Certificate Policy requirements as published in RFC 3647 [1].

The Object Identifiers associated with this Certificate Policy are:

Class of certificate	Object Identifier
Malta Resident Electronic Signature (Qualified) Certificate	2.16.470.4.3.2
Malta Resident Electronic Authentication Certificate	2.16.470.4.3.3

The OIDs 2.16.470.4.3.2 and 2.16.470.4.3.3 are assigned within the arc registered to MCA, and assigned to the Malta eID PKI for Malta Resident Electronic Signature (Qualified) and Authentication Certificates respectively.

The Malta Resident Electronic Authentication Certificates also include the Identifier 0.4.0.2042.1.2, which conforms to ETSI TS 102 042 [19]

1.1.2. Policy qualifier

A policy qualifier is an attribute defined in the certificate policies extension. See section 7.1 for more details on which fields are supported by The Malta Resident Electronic Signature (Qualified) and Authentication Certificates.

MCA makes publicly available this Certificate Policy (CP) and its associated Certification Practices Statement (CPS). Subscribers and Relying Parties can use the link explicitly given in the policy qualifier of the Certificate Policy extension to download those documents.

1.2. PKI participants

1.2.1. Policy Management Authority

The Malta Certification Authority is the Policy Management Authority for the GOM. Its main goal is to define, supervise and maintain the overall framework of Malta PKI system including the definition of the policies under which the Malta eID PKI system operates.

The Malta Certification Authority through the management team referred to as the Malta PKI Management Board is responsible for:

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

- Supervising the correct implementation of the CPs in conformance with the CPS, and;
- The definition of the review requirements and processes relating to the implementation of the Malta eID CPS and supported CPs.

Further details on the role and responsibilities of the MCA are found in the Malta eID Certification Practices Statement [17].

All questions and comments regarding this Certificate Policy should be addressed to the representative of this Policy Management Authority:

Malta Certification authority
Gattard House
National Road
Blata l-Bajda, Malta

1.2.2. Certification Authorities

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

The CA that issues the Certificates covered by this Certificate Policy is the Malta Resident Electronic Identity CA (Malta Resident eID CA or Malta Resident CA)

1.2.3. Subscribers

A Subscriber is the person who applies for a Certificate. Within the GOM PKI there are several types of Subscribers, described in [17]. The Subscribers in the case of the present CP are the holders of the appropriate Electronic Resident Card.

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

- Authentication for persons of 14 years of age and above
- Digital Signature (Qualified Certificate), for persons of 16 years of age and above.

This CP covers the following class of Subscriber:

- Residents who are subscribers to the Malta Resident CA and who will hold a Electronic Resident Card;

Further details on the specific applicability, usage and community that apply to each End Entity Certificate class in the Resident PKI are described later on in this Certificate Policy.

1.2.4. Registration Authorities

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

Identity Malta (Expatriates) is responsible by delegation from Identity Malta (Identity Cards) for the processes associated with the registration, validation and issuance of the Electronic Resident Cards in conjunction with their associated embedded Certificates and Private Keys. For this purpose, it relies on the National Identity Management System (NIDMS). Further information on this can be found in the NIDMS Functional Specification Document [14].

The registration authority for the Resident Certification Authority is made of the Residence Card Management Identity Officer (RMIO), responsible to register (or update information on) the person identity in the national database, the Residence Card Management Authority Officer (RMAO), responsible for the registering of new Electronic Residence Card application, the Residence Card Management Authority Administrator (RMAA), responsible to validate the eligibility of the applicant to proceed with the application and the Central Registration Authority

Officer (CRAO) that reviews each RMAA approved application and passes them for production processing.

1.2.5. Revocation Authorities

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

The Revocation Authority for the Resident Certification Authority is made of Suspension and Revocation Authority Officer (SRAO) who validates suspension and revocation application requests on the basis of personal presentation of the requester at the Identity Malta (Identity Cards) offices, and Help Desk Officer (HDO) who processes suspension and revocation application requests.

1.2.6. Relying Parties

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

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

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

1.2.7. Other Participants

For further information please refer to the Malta eID Certificate Practice Statement [17].

1.3. Certificate usage

1.3.1. Appropriate certificate uses

This CP refers to the usage of the following two Certificate classes

- Residence card Authentication Certificates;
- Residence card Digital Signing Qualified Certificates.

These Certificates are described below.

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

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

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

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

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

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

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

1.3.2. Prohibited certificate uses

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

1.4. Policy administration

1.4.1. Organization administering this document

The organization administering this CP is the Malta Certification Authority.

1.4.2. Contact person

Contact Person

Postal Address

The CA Manager
Gattard House
National Road
Blata l-Bajda
Malta

Phone: (356) 2123 4710

Fax: (356) 2123 4701

1.5. Definitions and acronyms

Definitions:

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

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

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

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

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

Certification Authority (CA): has the meaning set out in paragraph 1.3.2 of the CPS.

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

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

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

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

Certificate Revocation List (CRL): A signed list indicating a set of certificates that are no longer considered valid by the certificate issuer.

Certificate Trust Chain: An ordered list of Certificates that contains the End-Entity Certificate, intermediary Certificates and the Certificate for the Root CA such that a Relying Party may follow the trust chain up to and including the top level trust anchor. Within the National Identity

Cards the full Certificate Trust Chain is embedded within the card at the time of issuance and is not subsequently updated on the card. For example, the Certificate Trust Chain for the authentication Certificate contained on an Electronic Identity Card would comprise the Public Key Certificates for the authentication Certificate, the Malta Citizen eID CA and the Malta Root CA.

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

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

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

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

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

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

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

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

End Entity Certificate: For the purpose of this CP an End Entity Certificate is one of the following:

- Residence card Authentication Certificates;
- Residence card Digital Signing Qualified Certificates;;

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

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

- Certification Authorities (Root and subordinate);
- Registration Authorities;
- Subscribers;

- Relying Parties, and;
- Other Participants such as the OCSP responder and Time Stamping authority.

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

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

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

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

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

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

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

Qualified Certificate: A Certificate that has been issued in accordance with the EIDAS Regulation No 910/2014.

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

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

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

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

Secure Signature Creation Device: is a secure device handling the private key of the user. The smartcards used for the national Electronic Identity card and the National Electronic Resident card are examples of a Secure Signature creation Device and have been assessed against the appropriate Secure Signature Creation Device Protection Profile (PPSSCD) 13. The smartcards continue to benefit from this status under the new EIDAS Regulation No 910/2014 on the basis of the transitional measures (Art 51.1).

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

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

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

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

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

Subject: Entity to which a Certificate issued.

Subscriber: Entity that request and subscribes for a Certificate and for which it is either the Subject or not as more particularly described in paragraph 1.3.3 of the CPS.

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

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

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

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

Acronyms:

CA	Certification Authority
CAO	Certificate Authority Officer
CP	Certificate Policy
CPS	Certification Practice Statement
CRAO	Central Registration Authority Officer
CRL	Certificate Revocation List
CSP	Certification Service Provider
HDO	Help Desk Officer
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ISO	International Organisation for Standardisation
ITU	International Telecommunications Union
LCP	Lightweight Certificate Policy
LDAP	Lightweight Directory Access Protocol
LRAA	Local Registration Authority Administrator
LRAO	Local Registration Authority Officer
NIDMS	National Identity Management System
OID	Object Identifier
OPM	Office of Prime Minister
PIN	Personal Identification Number
PKCS	Public Key Certificates Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509) (IETF Working Group)
QCP	Qualified Certificate Policy
RA	Registration Authority

RAO	Registration Authority Officer
RFC	Request for Comments
RMAA	Residence Card Management Authority Administrator
RMAO	Residence Card Management Authority Officer
RMIO	Residence Card Management Identity Officer
RSA	A specific Public Key algorithm invented by Rivest, Shamir, and Adleman
SRAO	Suspension and Revocation Authority Officer
URL	Uniform Resource Locator

2. PUBLICATIONS AND REPOSITORY RESPONIBILITIES

2.1. Identification of entities operating repositories

The GOM eID repositories are made of the GOM eID Directory and its associated web site.

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

2.2. Distribution of Certification Information

The Resident CA Certificate and associated CRL are located at http://crt.qca.gov.mt/ResidentCA.crt and http://crl.qca.gov.mt/ResidentCA.crl respectively.

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

The above information can also be located at ldap.qca.gov.mt.

The CDP CRLs that are defined in the certificate profiles are also published to ldap.qca.gov.mt (see 7.1.11 of the present CP and chapter 11 of the CPS [17] for details).

The GOM Root CA and Resident CA also publish their also Certificate status information via OCSP. Certificate status information is available at http://ocsp.qca.gov.mt

The CPS [17] and the present CP will be published to a central repository: http://repository.qca.gov.mt

2.3. Time and Frequency of Publication

The Malta Resident eID CA will create new CRL every every hour on the hour. The CRL will have a validity of 6 days. The new CRL(s) will be added to the GOM eID Directory and its associated web site at the time following each new CRL entry's creation. The CRLs will include the expired certificates. Certificate status information will be published to OCSP at the time immediately following creation of the CRL.

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

2.4. Access Control on Repositories

Only trusted and controlled staff have write and change access on these repositories. The GOM eID PKI has ensured that appropriate security measures have been implemented to protect these repositories and to monitor access and maintenance.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of names

The GOM uses a genuine, unambiguous, clearly distinguishable and unique X.500 Distinguished Name (DN) in the Malta Resident Electronic Signature (Qualified) and Authentication Certificates subject name fields in accordance with RFC 5280 [2

3.1.2. Need for names to be meaningful

The Resident DN will be derived from the Certificate request created by the NIDMS on the basis of the registration data. It is the responsibility of the RA to ensure the meaningfulness of the Resident DN during the registration process.

CN	[First name Surname (Authentication or Signature)]
Surname	Family name
Given Name	First name(s)
Serial number	MBUN (meaningless but unique number)

C	MT

(Country codes MUST follow the format of two letter country codes, specified in [R16], *ISO/IEC 3166, Codes for the representation of names of countries and their subdivisions – 1997)*.

3.1.3. Uniqueness of names

The Distinguished Names of the Resident Certificate are unique and are constructed as described in section [10].

3.1.4. Recognition, authentication, and role of trademarks

The GOM does not accept trademarks, logos or otherwise copyrighted graphic or text material for inclusion in its Resident Certificates.

3.2. Initial identity validation

Residents must apply for the Electronic Resident Card by completing an initial registration process at a Residence Card Management Authority Office where their credentials are validated and biometric data (photograph and written signature) captured by the Residence Card Management Authority Officer (RMAO)

3.2.1. Method to prove possession of private key

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

3.2.2. Data needed for Subscriber registration

NIDMS verifies by appropriate means and on the basis of a documented procedure [14], the identity, and if applicable, all specific attributes thereof of applicants of a Resident Certificate.

3.2.3. Records for Subscriber registration

NIDMS records all information used to verify the identity of the requestor identity. The records shall be kept securely archived for the entire lifetime of the GOM eID PKI.

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

Certificate renewal requests are not allowed for Resident Certificates. All update requests for Certificates embedded upon an Electronic Resident Card are treated as an initial request and

shall result in the issuance of a new Electronic Resident Card and associated embedded key and Certificate.

3.4. Identification and authentication for revocation request

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

a) holders of Electronic Identity Cards or of e-Residence documents (hereinafter referred to as Identification Documents);
b) any person who has a power of attorney to manage Identification Documents on behalf of the holders;
c) any reliable third-party which shall be established as such by Identity Malta (Identity Cards) – 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).

In all cases, requests for revocation and/or suspension can only be made with regards to either both the authentication Certificate and the signature Certificate or solely to the signature Certificate. Requests for revocation and/or suspension regarding authentication Certificate alone shall not be considered (unless the signature Certificate has already been suspended/revoked).

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

a) online (through e-mail or webportal);
b) phoning the Identity Malta (Identity Cards) Helpdesk;
c) calling personally at the Identity Malta (Identity Cards) premises;
d) through an authenticated request

In all cases, such applications are processed by the Identity Malta (Identity Cards) Helpdesk. Authentication of persons submitting requests online or by phone is made through phone contact by Identity Malta (Identity Cards) Helpdesk who would verify the identity through confirmation of any of the applicant's personal data.

In order for a revocation of Certificates to be carried out, the applicant has to personally call at the Identity Malta (Identity Cards) Office and on presentation of his/her identification (or alternative) document (except in cases where the request is made by the afore-mentioned reliable third-parties). In all other cases Identity Malta (Identity Cards) shall only limit itself to temporary suspending the Certificates – the applicant would be asked to call personally at Identity Malta (Identity Cards) so that revocation could then be completed.

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

3.5. Identification and authentication for re-key after revocation

Re-certifying a Resident Certificate following its revocation is not permitted. A new Certificate with a new key pair for the revoked Resident Certificate must be obtained in order to continue valid operational service. The application must be made to NIDMS who is the only body that can

sanction such a request. The same identification and authentication procedure as the first request is applied for re-key request.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Who can submit a certificate application

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

Certificate applications may only be made by Residents.

In addition the following criteria are applied when issuing Electronic Resident Cards

- Authentication Certificate *only* for persons of 14 years of age and above that are have not yet reached 16 years old.
- Authentication *and* Digital Signature (Qualified Certificate) for persons of 16 years of age and above.

4.1.2. Subscriber's registration process

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

1.1 Initial registration process

Residents must apply for the Electronic Identity Card by completing an initial registration process at a Residence Card Management Authority Office, where their credentials are validated and biometric data captured by the Residence Card Management Authority Officer (RMAO).

1.2 Request for card and keys generation

Upon successful completion of this initial registration process, the Residence Card Management Authority Administrator (RMAA) shall authorise the generation of an Electronic Identity Card.

1.3 Card personalisation

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

1.4 Certification

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

1.5 Card completion and testing

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

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

1.6 Hand over to resident

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

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

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

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

The National Identity Management System operates the identification and authentication processes that are followed for the issuance of an Electronic Resident card and associated embedded keys and Certificates issuance according to section 4.1 and according to procedures described in a confidential and internal document.

4.3. Certificate issuance

4.3.1. CA actions during Certificate issuance

The CA is configured in such a manner that it will only accept certification requests relating to the Electronic Resident Cards from NIDMS that have been entered by a RMAO, approved by the RMAA.

The request will be entered and approved by authorised personnel using the appropriate local interface. The approved details will be passed to the appropriate dedicated card management system component where the key pair(s) will be generated upon the appropriate card and the Certificate request(s) will be created using the correct format.

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

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

Subscribers will be notified at the time of application by the RMAO of the timescales within which their card will be ready for collection.

The Certificates will be provided to the Subscriber embedded inside the Electronic Residents Card when collected from the RMA office and accepted by the Resident in accordance with the terms of the Subscriber Agreement.

4.4. Certificate Acceptance

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

4.5. Key pair and certificate usage

Subscribers shall only use key pairs and their associated Certificates for purposes defined within this Certificate Policy in section 1.4.1.

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

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

The Electronic Resident Card has been certified against the appropriate protection profile as a Secure Signature Creation Device (SSCD) [13] and continues to benefit from this status in line with the transitional measures (Art 51.1) of the EIDAS Regulation No 910/2014.

4.6. Certificate Renewal

Certificate renewal is not allowed by the GOM eID PKI.

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

4.7. Certificate Re-Keying

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

4.8. Certificate Modification

Certificate modification is not allowed by the GOM eID PKI.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for revocation

If the CA or RA (through a NIDMS Office) is notified of at least one of the following circumstances then the Certificate must be revoked. The card holder is responsible for promptly reporting any suspicion of card or PIN compromise in addition to the relevant subset of reasons listed below.

Possible reasons for the revocation of a Certificate will include:

- The Certificate contains invalid information;
- The Electronic Resident Card of the Subscriber was reported factually lost, stolen, disclosed or otherwise compromised/misused;
- The Subscriber is no longer authorized to use the Certificate (see Section 1.3).
- The Subscriber does not comply with the GOM eID CPS and/or the present CP;
- The Subscriber requests that the Certificate is revoked through a local Registration Authority office;
- The CA or RA responsible does not comply with GOM eID CPS, or;
- The CA terminates its operation.

In all cases, requests for revocation can only be made with regards to either both the authentication Certificate and the signature Certificate or solely to the signature Certificate.

Requests for revocation regarding authentication Certificate alone shall not be considered (unless the signature Certificate has already been suspended/revoked).

4.9.2. Revocation checking requirement for Relying Parties

Before a Certificate is used, Relying Parties must check its validity and then use the Certificate solely in compliance with this Certificate Policy and the Malta eID Certificate Practice Statement (CPS) [17].

4.9.3. Circumstances for suspension

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

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

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

In all cases, requests for suspension can only be made with regards to either both the authentication Certificate and the signature Certificate or solely to the signature Certificate. Requests for suspension regarding authentication Certificate alone shall not be considered (unless the signature Certificate has already been suspended/revoked).

4.9.4. Suspension checking requirement for Relying Parties

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

4.9.5. Subscriber's revocation process

As described in section 3.4, requests for revocation of Certificates embedded within the Electronic Resident Card shall only be supported through a request authenticated by the National Identity Management System. After the approval of request, the Resident CA will change the status of the Certificate referred to in the request to revoked and will generate a new Certificate Revocation List (CRL). The time for generation of a new CRL will be a maximum of 6 hours from receipt of the request by the Resident CA.

The Resident CA will publish CRL information to the GOM eID Directory and will also update the status information available to relying parties through the OCSP service.

Revocation of an Electronic Resident Card will automatically result in the card being no longer able to conduct digital transactions and the revocation of the associated End Entity Certificates stored within the card.

4.10. Certificate Status Services

Certificate Status information will be published to OCSP by the Resident eID CA within the GOM eID PKI. See section 2.2

The Malta Resident Electronic Signature (Qualified) and Authentication Certificates each contain a CDP extension which points to the OCSP server which will contain the latest revocation data of the Resident eID CA. Further details on this are provided in section 7.1.10 of this CP.

4.11. End of Subscription

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

4.12. Key Escrow and Recovery

Key escrow or key recovery are not supported by the GOM eID PKI.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical controls

GOM eID PKI implements physical controls on its premises that host and operate Resident Certificate key lifecycle management functions. See [17] for more details.

5.2. Procedural controls

GOM eID PKI follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties in the fields of the electronic signature-related technologies. More details are given in [17].

5.3. Personnel controls

5.3.1. Qualifications, experience and clearance requirements

GOM eID PKI conducts an initial investigation of all members of staff, including outsourcing staff, who are candidates to serve in trusted roles to make a reasonable attempt to determine their competence, experience and trustworthiness. Members of staff in trusted positions provide official documents attesting they are of good character and have no prior convictions for serious crimes. See more details in [17].

5.3.2. Background check procedures

The GOM eID PKI follows the GOM background check procedures.

5.3.3. Training requirements

The GOM eID PKI makes available to their personnel appropriate education, training and awareness plans related to the role they execute.

5.3.4. Retraining frequency and requirements

The GOM eID PKI provides appropriate retraining and training updates for personnel as the need evolves.

5.3.5. Sanctions for unauthorized actions

The GOM eID PKI will follow the GOM procedures for imposing sanctions for deliberate or repeated wrong behaviour or unauthorised actions.

5.3.6. Independent contractor requirements

Independent contractors are subject to the same background, trustworthiness and competence check. GOM eID PKI conducts such investigations and handle all collected information in strict confidence and shall comply with the requirements of the applicable legislation on the protection of personal data.

Contractors in trusted positions provide official documents attesting they are of good character and have no prior convictions for serious crimes.

5.3.7. Documentation supplied to personnel

The GOM eID PKI makes available appropriate documentation to its personnel during training, retraining or under other circumstances. See [17] for more details.

5.4. Audit logging procedures

The GOM eID PKI implements audit logging procedures that include physical access and logical logs implemented for the purpose of monitoring and maintaining a secure environment. See [17] for more details.

Logical access is logged for all GOM eID PKI components. Generated logs include the following PKI components:

- Database activities and events transactions,
- Operating systems in windows event logs,
- PKI system logs.

5.5. Records archival and retention

5.5.1. Types of records archived

The retained records and archival process is described in [17].

5.5.2. Retention period for archive

The CPS [17] associated to this CP details the retention period of the items to be recorded.

5.5.3. Protection of archive

The CPS [17] associated to this CP details the protection mechanism of the archived items.

5.5.4. Requirements for time-stamping of records

The CPS [17] associated to this CP highlights how GOM eID PKI implements requirement for time-stamping of records.

5.5.5. Procedures to obtain and verify archive information

The CPS [17] associated to this CP describes the procedure to obtain and verify archived items.

5.6. Key Changeover

GOM eID PKI CA keys update and changeover procedure is detailed in [17].

5.7. Compromise and Disaster Recovery

The GOM eID PKI has implemented a business continuity plan to ensure business continuity and to prevent from a disaster. More detail is given in [17].

5.8. CA or RA termination

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

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

- Inform all Subscribers, cross-certifying CA's and Relying Parties with which the CA has agreements or other form of established relations;
- Inform the Malta Communications Authority and the Government of Malta of the termination and its possible consequences;
- Hand over its activities to another CA of the same quality and security level; if this is not possible, revoke the Certificates two (2) months after having informed the Subscribers and archive all relevant Certificate information;
- If possible, make publicly available information of its termination at least 3 month prior to termination;
- Publish the last CRL issued after the revocation of the last unexpired and unrevoked Certificate on the GMCA Information URI.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

The GOM CAs key pair generation and installation as well as internal PKI key pair generation and installation (e.g. such as key pair for security officers, SSL certificates) are described in [17].

6.1.1. Key Pair Generation

The key pairs associated with the Electronic Resident Card will be generated and stored upon the card itself, within a secure module that has been validated against the appropriate protection profile for a Secure Signature Creation Device and continue to benefit from this status in line with the transitional measures (Art 51.1) of the EIDAS Regulation No 910/2014.

This operation is performed by the card management component of the Malta National Identity Management System.

- For each Electronic Resident Card applicant that is approved that is 16 years old and above, two key pairs will be generated on the card, one for the Resident authentication Certificate, the other for the Resident signature (Qualified) Certificate. The Public Key associated with each of these key pairs will be submitted securely into the PKI where they will be sent to the Resident CA for signing.

- For each Electronic Resident Card applicant that is 14 years old and above, but under 16 years, a single key pair will be generated on the card, the authentication Certificate. The associated Public Key will be submitted securely into the PKI where it will be sent to the Resident CA for signing.

6.1.2. Private Key Delivery to Subscriber

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

The sole control on the key by the Subscriber is insured during the issuance process by generating and storing the Private Key upon the card and then distributing the PIN to the registered address of the Subscriber. As such only the Subscriber has access to both the card and the associated PIN.

6.1.3. Public Key Delivery to Certificate Issuer

The Card Management System component of NIDMS will generate the Certificate service request and deliver this to the Resident CA.

The Certificate will be returned to NIDMS from the Resident CA using the PKCS#7 format and will then be embedded onto the Electronic Resident Card containing the associated key pair.

6.1.4. CA Public Key Delivery to Relying Parties

The Root CA Public Key and Resident CA Public Key will be embedded into the Electronic Resident Card prior to the card being handed over to the applicant.

These Certificates will also be available on the GOM eID Directory and its associated web site. See 2.2

6.1.5. Key Sizes

Key size for all Malta Resident Electronic Signature (Qualified) and Authentication Certificates will contain 2048 bit public keys.

6.1.6. Public Key Parameters Generation and Quality Checking

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

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

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

Certificate	Key Usage
Resident Card Authentication Certificate	Digital Signature
Resident Card Signing (Qualified) Certificate	Non repudiation

Certificate	Key Usage

6.2. Private Key Protection and Cryptographic Module Engineering Control

6.2.1. Cryptographic Module Standards and Controls

The key pairs associated with the Electronic Resident Card will be generated and stored upon the card itself, within a secure module that has been validated against the appropriate protection profile for a Secure Signature Creation Device [13].

6.2.2. Private Key m of n Multi-Person Control

Not applicable

6.2.3. Private Key backup

Private key backup for Resident Certificate is not supported

6.3. Other Aspects of Key Pair Management

6.3.1. Certificate Operational Periods and Key Pair Usage Periods

The validity period of the Malta Resident Electronic Signature (Qualified) Certificate is a variable validity, expressed in the Certificate request from the National Identity Management System, with a maximum of 10 years.

The validity period of the Malta Resident Electronic Authentication Certificate is a variable validity, expressed in the Certificate request from the National Identity Management System, with a maximum of 10 years.

6.4. Activation Data Generation and Installation

6.4.1. Activation Data Protection

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

6.5. Computer Security Controls

The GOM eID PKI shall implement computer security controls as defined within the eID PKI security implementation document [18].

6.6. Life cycle technical controls

The GOM eID PKI shall implement life-cycle technical controls including the execution of tools and procedures to ensure that operational systems and networks adhere to their configured security. Please refer to the Malta eID Certificate Practice Statement [17] for information

6.7. Network security controls

The GOM eID PKI shall implement network security controls as defined within the NIDMS infrastructure document. See more details in [11].

7. CERTIFICATE AND CRL PROFILES

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

7.1. Certificate profile

The Malta Resident Electronic Signature (Qualified) and Authentication Certificates are drafted according to RFC 5280 [2].

In addition the Resident Signature (Qualified) Certificate conforms to RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile [3].

7.1.1. Version

The version field indicates the X.509 version of the Certificate format. The Malta Resident Electronic Signature (Qualified) and Authentication Certificates are compliant with version 3 of the X.509 recommendation [2], allowing for Certificate extensions.

7.1.2. Serial Number

The field serial number specifies the unique, numerical identifier of the Certificate within all Public-Key Certificates issued by the same CA.

The Malta Resident Electronic Identity CA will assign a unique serial number to the Malta Resident Electronic Signature (Qualified) and Authentication Certificates.

7.1.3. Signature

The signature field determines the cryptographic algorithm used by a CA to sign a Certificate. The algorithm identifier, which is a number registered with an internationally recognized standards organization, specifies both the Public-Key algorithm and the hashing algorithm used by the CA to sign Certificates.

The signing algorithm used by the Malta Resident Electronic Identity CA to sign the Malta Resident Electronic Signature (Qualified) and Authentication Certificates is (2048 bit) 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. Issuer

The Issuer field identifies the certification authority that has signed and issued the Certificate. Issuer is structured as a "Distinguished Name", that is a hierarchically structured name, composed of attributes, most of which are standardised in the X.500 attributes.

The Distinguished Name associated with Resident Electronic CA is made of the following attributes:

CN	Malta Resident Electronic Identity CA
OU	Class Qualified
O	Government of Malta
C	MT

7.1.5. IssuerAltName

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

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

7.1.6. Validity

The validity field indicates the time interval during which Malta Resident Electronic Identity CA Certificate is valid, and over which the issuing CA maintains Certificate status information.

The validity period should be interpreted as the period when, before and after which the Certificate should not be trusted.

The validity period is expressed in two fields: not before and not after.

- Not before: expresses the date on which the Certificate validity period begins, and

- Not after: expresses the date on which the Certificate validity period ends.

The validity period of the Malta Resident Electronic Signature (Qualified) Certificate is a variable validity, expressed in the Certificate request from the National Identity Management System, with a maximum of 10 years.

The validity period of the Malta Resident Electronic Authentication Certificate is a variable validity, expressed in the Certificate request from the National Identity Management System, with a maximum of 10 years.

7.1.7. Subject

The Subject field identifies the subject holding the Private Key corresponding to the Public Key published in the Certificate. Subject is structured as a set of attributes, defined in the X.500 attributes.

The subject of the Malta Resident Electronic Signature (Qualified) and Authentication Certificates are formatted with the following attributes which are derived from the Resident Certificate request made on behalf of the Subscriber through the National Identity Management System:

CN	[First name Surname (Authentication or Signature)]
Surname	Family name
Given Name	First name(s)
Serial number	MBUN (meaningless but unique number)
C	MT

7.1.8. Subject Public Key Info

The Subject Public Key Info field is used to carry the (2048 bit) Public Key being certified and identify the algorithms with which the key has been generated.

7.1.9. Key usage

The Key Usage extension field specifies the purpose of the key contained in the Certificate.

The possible key purposes identified by the X.509v3 standard are the following: a) digital signature, b) non-repudiation, c) key encipherment, d) data encipherment, e) key agreement, f) key certificate signing, g) CRL signing, h) encipher only, i) decipher only.

In the Malta Resident Electronic Signature (Qualified) Certificate, the following flag is asserted and marked as critical:

- Non repudiation

In the Malta Resident Electronic Authentication Certificate, the following flag is asserted and marked as critical:

- Digital signature

7.1.10. Basic constraints

The Basic Constraints extension specifies whether the subject of the Certificate may act as a CA or only as an end-user.

In the Malta Resident Electronic Signature (Qualified) and Authentication Certificates, the Subject Type value is set to “end entity”, with Path Length constraint not asserted, and this extension is marked not critical.

7.1.11. CRL Distribution Point

The CRL Distribution Points extension identifies the CRL distribution point or points to which a Certificate user should refer to ascertain if the Certificate has been revoked. A Certificate user can obtain a CRL from an applicable distribution point or it may be able to obtain a current complete CRL from the authority directory entry.

The status of the Malta Resident Electronic Identification Digital Signature (QC) and Authentication Certificates can be obtained from an http location identified by the following URL:

URL=http://crl.qca.gov.mt/residentca.crl

or from a directory identified by the following URL:

URI=ldap://ldap.qca.gov.mt/cn=ResidentCA,o=Government of Malta,c=MT?certificateRevocationList?base

7.1.12. Certificate Policy Qualifier

A policy qualifier is defined in the Certificate Policies extension. This extension provides a mechanism for a Certificate issuer to distribute information regarding the policies under which the Certificate has been issued and the purposes for which the Certificate may be used.

The Malta Resident Electronic Signature (Qualified) Certificate uses the following policy:

- OID= 2.16.470.4.3.2 [OID for Malta Resident Electronic Signature (Qualified) Certificate Policy]

The Malta Resident Authentication certificate uses the following two policies:

- OID= 0.4.0.2042.1.2 [ETSI 102 042] [19]

- OID= 2.16.470.4.3.3 [OID for Malta Resident Electronic Authentication Certificate Policy]

OID= 2.16.470.4.3.2 and OID= 2.16.470.4.3.3 both refer to this Certificate Policy, since it covers both the Digital Signature (Qualified) certificates and Authentication certificates issued by the Malta Resident Electronic Identity CA

The GOM publishes its PKI practices in a repository identified by the following URL:
URL= http://repository.qca.gov.mt

7.1.13. Authority Key Identifier

The Authority Key Identifier extension identifies the Private Key used by an issuer to sign a Certificate, when the issuer has multiple signing keys (either due to multiple concurrent key pairs or due to changeover).

By identifying the signing key, the Authority Key Identifier makes it possible to verify the signature of a Certificate and therefore to validate the Certificate. This extension is always non-critical.

This field is present in the Malta Resident Electronic Signature (Qualified) and Authentication Certificates.

7.1.14. Subject Key identifier

The Subject Key Identifier field identifies the Public Key being certified. It enables distinct keys used by the same subject to be differentiated (either due to multiple concurrent key pairs or due to changeover).

A key identifier has to be unique with respect to all key identifiers for the subject with which it is used. This extension is always non-critical.

This field is present in the Malta Resident Electronic Signature (Qualified) and Authentication Certificates.

7.1.15. Name constraint

The Name Constraint extension is not used in the Malta Resident Electronic Signature (Qualified) and Authentication Certificates.

7.1.16. Policy constraint

The policy constraint extension is not used in the Malta Resident Electronic Signature (Qualified) and Authentication Certificates.

Chapter 10 summarizes the Malta Resident Electronic Signature (Qualified) and Authentication Certificate profiles.
Details of other Certificates issued by the GOM eID PKI are provided in the Malta eID Certificate Practice Statement (CPS) [17]

Details of the Certificate Revocation Lists issued by the GOM eID PKI are provided in the Malta eID Certificate Practice Statement (CPS) [17]

Details of the Online Certificate Status Protocol certificate issued by the GOM eID PKI are provided in the Malta eID Certificate Practice Statement (CPS) [17]

7.2. CRL profile

The Resident CRL is drafted according to RFC 5280 [2]. Its profile is detailed in section 11.3.

7.2.1. Version

The version field indicates the X.509 version of the CRL format. CRL signed by the Government of Malta Resident CA is compliant with version 2 of the X.509 recommendation [2], allowing for CRL extensions.

7.2.2. Algorithm OID

The signing algorithm used by the Resident CA to sign the CRL is RSA with SHA256, its Object Identifier is { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}.

7.2.3. Issuer

The issuer field identifies the certification authority that has signed and issued the CRL. Issuer is structured as a “Distinguished Name”, that is a hierarchically structured name, composed of attributes, most of which are standardized in the X.500 attributes.

The issuer of the Resident CRL is formatted with the following attributes:

CN	Malta Resident Electronic Identity CA
OU	Class Qualified
O	Government of Malta
C	MT

7.2.4. ThisUpdate

This field indicates the time at which the CRL has been produced. This field is formatted in UTC time.

7.2.5. NextUpdate

NextUpdate indicates when the next CRL will be produced (at the latest). This field is also formatted in UTC time. CRLs issued by the Resident CA are refreshed at least every 6 hours. All CRLs issued by the Resident CA will be valid for 6 days (plus any grace period).

7.2.6. RevokedCertificates

This field inventories the revoked Certificates. It lists the serial number of revoked Certificates and gives the date and time of revocation in UTC time.

7.2.7. Authority Key Identifier

See 7.1.13.

7.2.8. CRL Number

This field specifies the serial number of the CRL.

7.2.9. Reason Code

This extension specifies the reason why the entry was revoked. Possible values are:

CRLReason ::= ENUMERATED { unspecified (0), keyCompromise (1), caCompromise (2), affiliationChanged (3), superseded (4), cessationOfOperations (5)}.

The Resident CRL profile is summarized in section 11.3.

7.2.10. ExpiredCertsonCRL

Indicates CRL includes expired certificates [OID 2.5.29.60].

8. COMPLIANCE AUDIT AND RISK ASSESSMENTS

8.1. Assessment topic

Malta Certification Authority shall submit a Conformity Assessment Report in fulfillment of the requirements of the EIDAS Regulation No 910/2014 by 1st July 2017 and every 2 years after that. Periodic compliance inspections will also be conducted to ensure that the Malta eID PKI follows the processes stated in this CP and its associated CPS.

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

8.2. Frequency or circumstances of risk assessment

The GOM eID PKI shall be audited on a periodic basis not exceeding 24 months on its policies, including this CPS.

This CPS shall be assessed in recognition of the role of the GOM eID PKI as the Certified Service Provider (CSP) for the provision of Qualified Certificates for use as described within the EIDAS Regulation No 910/2014 and the Laws of Malta.

8.3. Identity/qualifications of assessor

To carry out the audits there will be an independent Conformity Assessment Body appointed by the Malta Certification Authority in line with the requirements of the Malta Communications Authority.

8.4. Auditor's relationship to assessed entity

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

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

8.5. Topics covered by assessment

The compliance audit will include the control requirements defined within the EIDAS Regulation No 910/2014.

8.6. Actions taken as a result of deficiency

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

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

8.7. Communication of results

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

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

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

8. OTHER BUSINESS AND LEGAL MATTERS

PKI participants associated with this CP are bound to the legal conditions outlined in section 9 of the CPS [17]. This CP has no further legal provisions.

9. REFERENCES

1. RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework.
2. RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.
3. RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile.
4. ISO/IEC 27001:2005 and related standards on information security and infrastructure.
5. Not in use.
6. Not in use
7. IDENTITY CARD ACT (CAP. 258) Identity Cards (Issue and Validity) (Amendment) Regulations, 2008 Government Gazette of Malta No. 18,170 - 04.01.2008
8. RFC 2560: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
9. RFC 6277: Online Certificate Status Protocol Algorithm Agility. (Updates RFC 2560)
10. Chapter 426, Laws of Malta also known as the Electronic Commerce Act III of 2001 (amended 2002, 2004, 2005, twice in 2007, 2010 and 2016)
11. eID PKI Network Architecture V1.7, 2012
12. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
13. CEN/ISSS PPSSCD-Type3-v105 25th July 2001: Secure Signature creation Device Type 3 – Protection Profile.
14. NIDMS_Functional_Specification Issue 1.0 Final
15. NIDMS PKI Specification v2.1
16. MITA Security Policy.
17. Certification Practices Statement for the Government of Malta Electronic Identity System.
18. PKI security implementation, Vx, 2102

19. ETSI TS 102 042 V1.2.3 (2006-12) “Technical Specification Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates”.

10. ANNEX

11.1. Malta Resident Digital Signature (QC) certificate profile

Malta eID Resident digital signature Certificate Profile		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	Sha2RSA	
Issuer	CN	Malta Resident Electronic Identity CA
	OU	Class Qualified
	O	Government of Malta
	C	MT
Validity	Variable validity, expressed in registration request, with maximum 10 years	
Subject	Resident DN	Resident Distinguished Name from registration request. See 7.1.6
Public Key Length/Type	2048bits	
Extensions		
Authority Key Identifier	sha1 of the Public Key of Malta Resident CA	
Subject Key Identifier	sha1 of the Public key of registration request	
Basic Constraints	Subject Type= end entity Path Length Constraint = none	
Key Usage (Critical)	Non repudiation	
CRL Distribution Point	URL=http://crl.qca.gov.mt/residentca.crl URI=ldap://ldap.qca.gov.mt/cn=ResidentCA,o=Government of Malta,c=MT?certificateRevocationList?base	
Certificate Policy	OID= 2.16.470.4.3.2 URL=http://repository.qca.gov.mt UserNotice = Trust Service Provider: Malta Electronic Certification Services Ltd (MECS Ltd) – NTRMT-C43419	
qcStatement	id-etsi-qcs 1 1 [Certs are qualified] id-etsi-qcs 4 1 [Certs are installed on SSCDs] id-etsi-qcs 5 PDS URL Location = http://repository.qca.gov.mt Language = en id-etsi-qcs 6 OID = 0.4.0.1862.1.6.1 [esign]	

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

11.2. Malta Resident Authentication certificate profile

Malta eID Resident Authentication Certificate Profile		
Version	3	
Serial number	Allocated automatically	
Signature Algorithm	Sha2RSA	
Issuer	CN	Malta Resident 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	Resident DN	Resident Distinguished Name from registration request. See 7.1.6
Public Key Length/Type	2048bits	
Extensions		
Authority Key Identifier	sha1 of the Public Key of Malta Resident CA	
Subject Key Identifier	sha1 of the Public key of registration request	
Basic Constraints	Subject Type= end entity Path Length Constraint = none	
Key Usage (Critical)	Digital signature	
CRL Distribution Point	URL=http://crl.qca.gov.mt/residentca.crl URI=ldap://ldap.qca.gov.mt.mt/cn=ResidentCA,o=Government of Malta,c=MT?certificateRevocationList?base	

Certificate Policy	OID=0.4.0.2042.1.2 OID= 2.16.470.4.3.3 URL=http://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=http://crt.qca.gov.mt/ ResidentCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.qca.gov.mt

11.3. Malta Resident CRL profile

Malta eID CRL signed by Malta Resident CA		
Version	2	
Signature Algorithm	Sha2RSA	
Issuer	CN	Malta Resident Electronic Identity CA
	OU	Class Qualified
	C	MT
ThisUpdate	[Time of issue]	
NextUpdate	Time of issue + 6 days	
Revoked Certificates	UserCertificate	certificate serial number
	RevocationDate	revocation time
CRL Extensions		
Authority Key Identifier	Sha1 of the Public Key of Malta Resident CA	
CRL Number	CA assigned unique name	
ExpiredCertsonCRL	Indicates CRL includes expired certificates [OID 2.5.29.60]	