

Government of Malta PKI Disclosure Statement for Resident Authentication Certificates and Resident Qualified Electronic Signature Certificates

Date of Issue: 03/09/2019

Version Number: 2.1

This document discloses and summarizes important user information and provides further policy provisions relating to the Government of Malta Certificate Policy for Resident Authentication Certificates and Resident Qualified Electronic Signature Certificates.

Malta Electronic Certification Services (MECS) Ltd

Change Record

Date	Author	Version	QA	Description of Change
14/12/2018	DLR	1.3	MECS	Initial version for takeover by IMA, based on Citizen PDS.
12/02/2019	IMA	1.4	MECS	Review and updating for publication
14/03/2019	IMA	2.0	MECS	Revised for consistent versioning
17/06/2019	IMA	2.1	MECS	Updated for clarifications

Document Details

Detail	
Title	Government of Malta PKI Disclosure Statement for Resident Authentication Certificates and Resident Qualified Electronic Signature Certificates
Filing Reference	GOM_Resident_eID_PDS_V2.1_PUB
Owner	MECS
Change Authority / Approver	PMA
Distributor	PMA

Reviewers

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

Malta Electronic Certification Services (MECS) Ltd

Table of Contents

IMPORTANT NOTICE	4
1 Policy Authority & Certification Authority (TSP) Contact Info	4
2 Certificate Type, Validation procedures and usage	4
3 Reliance Limits	5
4 Subscriber Obligations	5
5 Certificate Status checking Obligations of Relying Parties.....	5
6 Limited Warranty & Disclaimer/Limitation of Liability	6
7 Applicable Agreements, Certification Practice Statement, Certificate Policy	6
8 Privacy Policy.....	6
9 Fees	6
10 Applicable Law & Dispute Resolution	6
11 Trust Marks & Audit	7
12 Identification of this Certificate Policy.....	7
13 Approved Registration Authorities	7
14 Approved Repositories.....	7
15 Eligible Subscribers	7
16 Eligible Relying Parties	7
17 Certificate Status Information	8
List of Acronyms.....	8
References	9

Malta Electronic Certification Services (MECS) Ltd

IMPORTANT NOTICE

The Government of Malta (GOM) has commissioned Malta Electronic Certification Services Ltd (MECS) as the Trust Service Provider¹ (TSP) responsible for the issuance and management of Identity Cards containing Resident Authentication Certificates and Resident Qualified Electronic Signature Certificates.

The purpose of this document is to:

- Summarise the key points of the GOM PKI Resident eID Certificate Policy [1] (hereafter referred to as the Certificate Policy) for the benefit of Subscribers and Relying Parties.
- Provide additional detail and further provisions that apply to the Certificate Policy and which are incorporated in it by reference.

The full Certificate Policy under which Certificates are issued is defined by two documents:

- PKI Disclosure Statement (this document).
- The GOM PKI Resident eID Certificate Policy.[1]

You must read the Certificate Policy [1], the Subscriber Agreement [2] and Relying Party Agreement [3] (as appropriate) located at <https://repository.qca.gov.mt/> before you apply for or rely on a Certificate issued by the TSP.

Certificates issued by the TSP reference the Certificate Policy [1] located at <https://repository.qca.gov.mt/> and consequently this document.

Terms used in this document are defined in the Glossary located at <https://repository.qca.gov.mt/>.

1 Policy Authority & Certification Authority (TSP) Contact Info

TSP

MECS Ltd
Onda Building
Aldo Moro Road
Marsa, MRS9065
Malta
Telephone: +356 25904900
E-mail: info.meecs@gov.mt

Policy Management Authority

CA Manager
Identity Malta Agency
Onda Building
Aldo Moro Road
Marsa, MRS9065
Malta
Telephone: +356 25904900
E-mail: enquiries@identitymalta.com

2 Certificate Type, Validation procedures and usage

The Certificate types are, and their permitted usage is, as follows:

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

¹ Also known as the Certification Authority.

Malta Electronic Certification Services (MECS) Ltd

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

All other use of certificates issued under this policy [1] is prohibited.

The registration process for Resident Authentication Certificates and Resident Qualified Electronic Signature Certificates involves face-to-face applicant registration.

3 Reliance Limits

No stipulation.

4 Subscriber Obligations

Subscribers² must comply with the requirements defined in the Subscriber Agreement [2] and Certificate Policy [1] located at <https://repository.qca.gov.mt/>.

The Subscriber warrants and represents that s/he:

- Accepts the procedures set by the TSP in the Certification Practice Statement [4] currently in effect located at <https://repository.qca.gov.mt/> for the provision of Certificates.
- When applying to the Registration Authority for the National Identity Card, s/he has submitted precise, accurate and complete information, and complied with the corresponding registration procedures.
- Will use or rely on keys or Certificates only for purposes permitted by the present document, the Certificate Policy [1], the Certification Practice Statement [4], and as appropriate, the Subscriber Agreement [2] or Relying Party Agreement [3], and for no other purpose.
- Gives an undertaking that s/he is the sole holder and user of the Private Keys within the National Identity Card linked to the Public Keys to be certified.
- Protects the Private Keys at all times against loss, disclosure, alteration or unauthorised use.
- Will immediately notify the TSP in such a manner as specified in the Subscriber Agreement [2] in the event of the compromise or suspected compromise of the Private Keys or the activation data (e.g. PIN codes).
- Will immediately inform the TSP of any changes to the data on the Certificates.

5 Certificate Status checking Obligations of Relying Parties

Relying Parties must comply with the requirements defined in the Relying Party Agreement [3] located at <https://repository.qca.gov.mt/>.

The Relying Party shall check the validity of a Certificate on which they may wish to rely and all Certificates in the Certificate Chain. 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

² The Subscriber Agreement applies to Resident Subscribers.

Malta Electronic Certification Services (MECS) Ltd

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.

6 Limited Warranty & Disclaimer/Limitation of Liability

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 the Subscriber Agreement [2] and/or which exceeds the indicated limitations of any such use or reliance. 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 Electronic Signatures, transactions or claims relating to such Certificate. 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 CA's works or materials, insurrection or other civil disorder, war or military operations, or explosions.

7 Applicable Agreements, Certification Practice Statement, Certificate Policy

The full Certificate Policy [1], Subscriber Agreement [2], Relying Party Agreement [3], Certification Practice Statement [4] and any other associated agreements are published by the TSP and made available at <https://repository.qca.gov.mt/>.

8 Privacy Policy

The Privacy Policy governing the processing of personal data by the TSP shall be found at Section 18 of the Subscriber's Agreement. [2]

The latest version of the Subscriber's Agreement [2] is located at <https://repository.qca.gov.mt/>.

9 Fees

Not applicable.

10 Applicable Law & Dispute Resolution

The Certificate Policy [1] is governed, construed and interpreted in accordance with the laws of Malta. 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.

11 Trust Marks & Audit

Audit shall be carried out on a periodic basis and using an accredited Conformity Assessment Body as required by the eIDAS Regulation No 910/2014 [5].

12 Identification of this Certificate Policy

This Certificate Policy [1] has been assigned the following Object Identifiers (OIDs).

Class of certificate	Object Identifier
GOM PKI Resident Qualified Electronic Signature Certificate	2.16.470.4.3.2
GOM PKI Resident Authentication Certificate	2.16.470.4.3.3

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

13 Approved Registration Authorities

The following Registration Authorities have been approved by the TSP to register Subscribers under this Certificate Policy [1]:

- GOM PKI IMA Registration Authority.

14 Approved Repositories

The following publicly available Repositories have been approved by the TSP under this Certificate Policy [1]

- <https://repository.qca.gov.mt/>
- <https://crt.qca.gov.mt/>
- <https://crl.qca.gov.mt/>

15 Eligible Subscribers

The following types of Subscribers are eligible to be issued with Certificates under this Certificate Policy [1]:

- Maltese Residents in accordance the Malta Identity Card Act, Chapter 258 Laws of Malta [6].

16 Eligible Relying Parties

The following types of Relying Parties are eligible to rely on Certificates issued under this Certificate Policy [1] and the Relying Party Agreement [3]:

- Government of Malta: Malta Financial Services Authority (MFSA)
- Government of Malta: Commissioner For Revenue (CFR)

Malta Electronic Certification Services (MECS) Ltd

- Other parties and persons are also eligible to rely on Certificates issued under this Certificate Policy insofar as (i) this is legally required under mandatory provisions of the eIDAS Regulation No 910/2014 [5], notably in relation to the Citizen Qualified Electronic Signature Certificates; or (ii)s, as they come to agreement with MECS to abide by the Relying Party Agreement and corresponding Certificate Policy, shall become eligible relying parties and may not be reflected here. To contact the TSP regarding becoming an eligible relying party, one may send an email to info.mecs@gov.mt.

For the avoidance of doubt, all types of Relying Parties as described above shall be bound by the warranty, disclaimer and liability provisions as set out above.

17 Certificate Status Information

Certificate status information shall be made available via CRLs and the OCSP protocol. CRL Certificate status information shall include status information on expired Certificates.

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

To support Subscribers and Relying Parties and provide flexibility to users, the GOM PKI is in multiple locations and formats. Details are defined in the certificate policy [1]. This document provides guidance to assist users in checking certificate status via the various mechanisms.

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

List of Acronyms

Acronym	Meaning
CA	Certificate Authority
CFR	(Malta's) Commissioner For Revenue
CRL	Certificate Revocation List
eIDAS	Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
GOM	Government Of Malta
IMA	Identity Malta Agency
MECS	Malta Electronic Certification Services
MFSA	Malta Financial Services Agency
OCSP	Online Certificate Status Protocol
OID	Object Identifiers
PKI	Public Key Infrastructure
TSP	Trust Services Provider

Malta Electronic Certification Services (MECS) Ltd

References

- [1] Certificate Policy for Government of Malta Resident Authentication Certificates and Qualified Electronic Signature Certificates [\[link\]](#)
- [2] Subscriber Agreement For (a) The E-ID Account and (b) Certificates Within the Residence Permit / Document [\[link\]](#)
- [3] (Government of Malta) Relying Party Agreement [\[link\]](#)
- [4] Government of Malta Electronic Identity Scheme Certification Practice Statement [\[link\]](#)
- [5] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [\[link\]](#)
- [6] Identity Card and Other Identity Documents Act – Chapter 258 of the Laws of Malta [\[link\]](#)