Government of Malta PKI Glossary

Date of Issue: 20/04/2020

Version Number: 1.1

This Glossary defines terms and acronyms used by the GOM eID PKI in its Certificate Policies, Certification Practice Statement, PKI Disclosure Statements, Subscriber Agreements and Relying Party Agreements.

Change Record

Date	Author	Version	QA	Description of Change
11/01/2019	Gerry Hay	0.1 draft	IMA Compliance	Initial version
21/01/2019	Gerry Hay	1.0 final	IMA Compliance	Corrected format and added a few entries to prepare for publishing
17/04/2020	IMA	1.1	IMA	Added definitions

Document Details

Detail	
Title	Government of Malta PKI Glossary
Filing Reference	GOM_PKI_Glossary_V1.1_PUB
Owner	MECS
Change Authority / Approver	Policy Management Authority (PMA)
Distributor	PMA

Reviewers

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

Table of Contents

1 Terms 4

2 Acronyms 7

1 Terms

Admin: See "Administrator".

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 Identity Card.

Administrator Card: A card used for Authentication purposes, issued to natural persons who have the role of Operators and Administrators within the National Identity Management System.

Advanced Electronic Signature (AES): An Electronic Signature that: is uniquely linked to the signatory; is capable of identifying the signatory; is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Agreements: The Subscriber Agreement and the Relying Party Agreement.

Authentication: An electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed.

Card Management System: Technical system used for Identity Card and Administrator Card management. This includes the management of key pair generation and the request/receipt of Certificates from the Certificate Authority.

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

Certificate Authority (CA): Technical certificate generation service that is used by a Certification Services provider that creates and assign public key certificates.

Certification Authority: A Trust Service Provider that creates and assigns public key certificates.

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

Certificate Generation Service: Creates and signs certificates based on the identity and other attributes verified by the registration service. This can include key generation.

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

Certificate Revocation List (CRL): Signed list indicating a set of certificates that have been revoked by the certificate issuer.

Certification Practice Statement (CPS): A statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates.

Certification Service(s): Refers to the following PKI related services: Registration Service; Certificate Generation Service; Dissemination Service; Revocation Management Service; Revocation Status Service, Subject Device Provision Service.

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

Citizen eID: See "Electronic Identity Card".

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.

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.

Electronic ID (eID): A service provided by the Government of Malta to identify citizens and residents electronically using a username and password, which can be linked to their electronic identity or resident card as a second factor of authentication.

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

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

Electronic Signature: Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.

Electronic Time Stamp: Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.

End Entity: The Subject at the end of a Certificate chain that holds a Certificate e.g. natural person, legal person, or device.

GOM eID PKI: The Public Key Infrastructure used by the Government of Malta for the provision and support of Certificate related services for the National Identity Card schemes.

Malta Certification Authority: means 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 Trust Service Provider for the GOM PKI.

National Identity Card: The collective term used to refer to the Electronic Identity Card and the Electronic Resident Card issued by the National Identity Management System.

National Identity Management System (NIDMS): 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.

PKI Disclosure Statement: An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI.

Policy Management Authority (PMA): The body established to govern the GOM PKI and specify PKI policy.

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

Pseudonymity: The use of a pseudonym corresponding to a name or a surname by which the person is commonly known, which name and, or surname is to be indicated by the words "known as" at the discretion of the authorised officer, and to be included in the body of an identity document and/or in the Certificates, as the case may be. (as defined in Article 2 of Cap. 258)

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

Public Key Infrastructure: A hierarchical system of trust creating public-private key pairs where the public keys can be verified from a trusted source, and private keys are kept secret to complement (the public key) during encryption and decryption or other cryptographic techniques.

Qualified Certificate (for electronic signature): A certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I of eIDAS Regulation No 910/2014.

Qualified Electronic Signature: An advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

Qualified Electronic Signature Creation Device (QSCD) An electronic signature creation device that meets the requirements laid down in Regulation 910/2014 Annex II.[1]

Registration service: Verifies the identity and if applicable, any specific attributes of a subject. The results of service are passed to the Certificate Generation Service.

Relying Party: Natural or legal person that relies upon an electronic identification or a trust service. Relying Parties include parties verifying a digital signature using a public key certificate.

Relying Party Agreement: The agreement between Relying Parties and the Trust Service Provider which contains the legal terms and conditions governing acceptance and use of Certificates by Relying Parties.

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

Resident eRP: See "Electronic Resident Card".

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.

Revocation Status Service: Provides certificate revocation status information to relying parties.

[1] The smartcards used for the Identity Card are certified as Secure Signature Creation Devices in accordance with Article 3(4) of Directive 1999/93/EC and are considered as qualified electronic signature creation devices under EIDAS Regulation 910/2014 on the basis of the transitional measures (Art 51.1).

Root CA: The computer that serves as the top of the PKI hierarchy such that all certificates in that organization's PKI can be traced back to a computer, which serves as the single/origin point of trust.

Signatory: A natural person who creates an electronic signature.

Subject: Entity identified in a certificate as the holder of the private key associated with the public key given in the certificate.

Subject Device Provision Service: Prepares, and provides or makes available secure cryptographic devices, or other secure devices, to subjects.

Subscriber: A legal or natural person bound by agreement with a Trust Service Provider to any Subscriber obligations.

Subscriber Agreement: The agreement between a Subscriber and a Trust Service Provider which contains the legal terms and conditions governing the use of a Certificate and eID.

Time Stamp: See Electronic Time Stamp.

Trust Service: An electronic service normally provided for remuneration which consists of: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services;

Trust Service Provider (TSP): A natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider.

Trustworthy System: An information system or product implemented as either hardware and/or software that produces reliable and authentic records which are protected against modification and additionally ensures the technical and cryptographic security of the processes supported by it.

UniCERT Programmatic Interface (UPI): The UniCERT Programmatic Interface (UPI) is an advanced UniCERT component that allows integrators to programmatically take advantage of the certificate request and authorization processing functionality of UniCERT. It is customizable and comes with a developer's toolkit to create the functionality needed for customised applications and/or devices to interact with UniCERT

2 Acronyms

CA	Certificate Authority
CAO	Certificate Authority Operator
CP	Certificate Policy
CPS	Certification Practice Statement
CRAO	Central Registration Authority Officer
CRL	Certificate Revocation List
GOM	Government of Malta

HDO	Help Desk Officer
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ISO	International Organisation for Standardisation
ITU	International Telecommunications Union
LDAP	Lightweight Directory Access Protocol
LRAA	Local Registration Authority Administrator
LRAO	Local Registration Authority Officer
NIDMS	National Identity Management System
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Certificates Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509) (IETF Working Group)
QCP	Qualified Certificate Policy
RA	Registration Authority
RAO	Registration Authority Officer
RFC	Request for Comments
RMAA	Residence Card Management Authority
RMAO	Residence Card Management Authority Officer
RMIO	Residence Card Management Identity Officer
RSA	A Public Key algorithm invented by Rivest, Shamir, and Adleman
SHA	Secure Hashing Algorithm
SRAO	Suspension and Revocation Authority Officer
UPI	UniCERT Programmatic Interface
URL	Uniform Resource Locator