IDENTITY
MALTA

On behalf of the Government of Malta

MALTA
eIDAS NOTIFICATION
2021

IDENTITY
MALTA

Identity Malta
CASTAGNA Building,
Valley Road, Msida, Malta
t +356 2590 4900
e enquiries@identitymalta.com
w www.identitymalta.com

Identity Malta Agency ("IMA") on behalf of the Republic of Malta hereby notifies the European Commission of an electronic identification scheme to be published in the list referred to in Article 9(3) of Regulation (EU) No 910/2014.

Malta confirms the following:

i. the information communicated in this notification is consistent with the information which has been communicated to the Cooperation Network in accordance with Article 7(g) of Regulation (EU) No 910/2014; and

ii. the electronic identification scheme can be used to access at least one service provided by a public sector body in Malta.

Respectfully submitted,

Anton Sevasta
MECS Ltd.,
Responsible party

Stefan Rodoligo
IMA Chief Information Officer,
Technical implementation

Date:	19/02/2021
Object:	eIDAS Pre-notification
Ref:	
Dissemination:	Cooperation Network

TABLE OF CONTENTS

Contents

DEFINITIONS

2FA means two-factor authentication, a method of authentication incorporating two of three factors to include: something one has, who one is (such as biometric factors), and something one knows.

Biometrics has the same meaning as in Article 4(14) GDPR;

CA Certificate Authority which issues certificates for use in authentication and digital electronic signatures;

e-ID or **the Scheme** means the Electronic ID operated by the Identity Malta Agency on behalf of the Government of Malta as notified herein;

eIDAS Regulation means 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;

ENISA European Union Agency for Cybersecurity;

Expatriates means EEA, Swiss and Third-country Nationals;

Expatriates Unit means the department within the Agency entrusted with the issuance of Residence Documents and Residence Permits (as defined herein);

GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016;

ID Card means an identity document issued to Maltese Nationals under Part A of the Identity Cards and other Identity Documents Act and in compliance with Chapter II of Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019; in the context of this document, it can also refer to a residence document issued to EU Nationals under the same Act and Regulation.

Identity Cards Act means the Identity Card and other identity documents act, Chapter 258 of the Laws of Malta;

Identity document refers collectively to ID Cards, Residence Documents and Residence Permits (as all defined herein);

IDMO Identity Management Office, sometimes also referred as ID Cards Unit or e-ID Cards Unit. It is the department within IMA responsible for the e-ID and the issuance of Identity Cards (as defined herein);

IMA or the **Agency** means Identity Malta Agency of the Government of Malta established by Subsidiary Legislation 595.07 entitled "Identity Malta Agency

(Establishment) Order" to carry out functions and duties of the public administration in the matters related to visas, residence permits, work permits, passports, identity cards and other identity documents, acts of civil status and registration of public deeds;

MCA Malta Communication Authority, the supervisory body in accordance with EIDAS regulation of MECS Ltd. electronic identity means;

Ministry for Gozo refers specifically to the e-ID Cards and e-Residence Office within the Ministry for Gozo, responsible for issuing Identity documents to entitled individuals residing in Gozo;

MITA Malta Information Technology Agency;

QSCD Qualified Signature Creation Device;

QTSP Qualified Trust Service Provider;

RA means the Registration Authority;

Residence Document means an identity document issued to Nationals of any country of the European Economic Area and Switzerland under Part B of the Identity Cards Act and in compliance with Chapter III of Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019;

Residence Permit means an identity document issued to Third-country Nationals under Part B of the Identity Cards Act and in compliance with Regulation (EC) No 1030/2002 as amended by Regulation (EU) 2017/1954, and as implemented by Commission Implementing Decision C(2018) 7767;

Subscriber is the individual e-ID holder who signs the Subscriber's Agreement and is issued the authentication and the qualified electronic signing certificate and/or electronic identity account issued by the Government of Malta;

TSP means a Trust Service Provider;

1. General information

Title of the scheme	Maltese National ID (e-ID Card) Maltese Residence Document (e-RP Card)
Level(s) of assurance (low, substantial, high)	High

2. Authority responsible for the scheme

The authority responsible for the Scheme is Identity Malta Agency, acting under a mandate of the Maltese government.

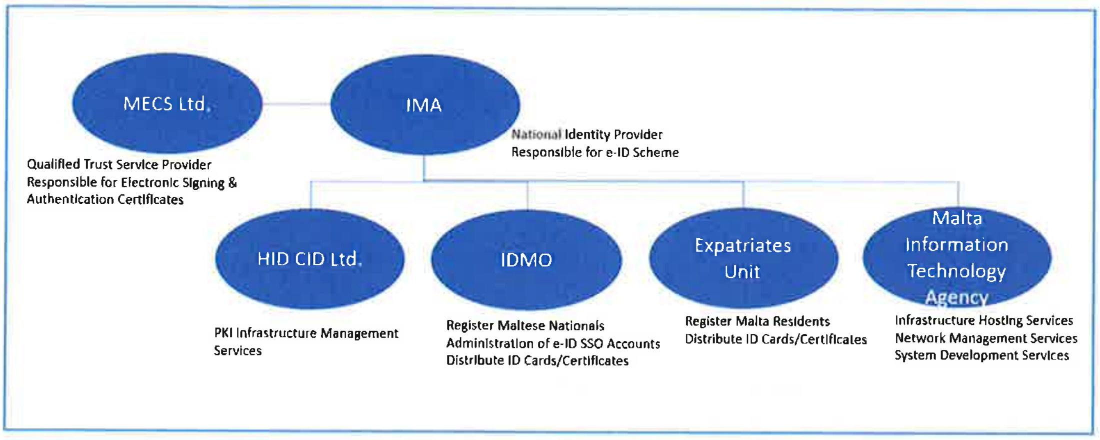
Technical and administration duties are led by IMA, which has two separate departments to register and issue identity documents. IDMO is the department of the authority responsible for the issuing of electronic identity cards to Maltese citizens and responsible for the registration of e-ID accounts. Whereas the Expatriates Unit of the authority is in charge of the processing and issuing of the Maltese Residence Document (e-RP Card).

	Identity Malta Agency (Head Office)	**IDMO**	**Expatriates**
Postal address	Castagna Building, Valley Road, Msida, MSD9020, Malta	Gattard House, National Road, Blata il-Bajda, Hamrun, Malta	Castagna Building, Valley Road, Msida, MSD9020, Malta
E-mail address	enquiries@identitymalta.com	infoeid@gov.mt	Eresidence.ima@gov.mt
Telephone No	(+356) 2590 4900	(+356) 2590 4300	(+356) 2590 4800

3. Information on relevant parties, entities, and bodies

Where there are multiple parties, entities or bodies, please list them all, in accordance with Article 3(2) and (3) of Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (notified under document C(2015) 7369) (Text with EEA relevance)

Malta National EIDAS e-ID Scheme


MECS Ltd.
Qualified Trust Service Provider
Responsible for Electronic Signing &
Authentication Certificates
IMA
National Identity Provider
Responsible for e-ID Scheme
HID CID Ltd.
PKI Infrastructure Management
Services
IDMO
Register Maltese Nationals
Administration of e-ID SSO Accounts
Distribute ID Cards/Certificates
Expatriates
Unit
Register Malta Residents
Distribute ID Cards/Certificates
Malta
Information
Technology
Agency
Infrastructure Hosting Services
Network Management Services
System Development Services

3.1. Entity which manages the registration process of the unique person identification data (name)

Name of entity which manages the registration process of the unique person identification data

Identity Malta Agency through IDMO (for Maltese Nationals) and Expatriates Unit (for Expatriates).

3.2. Party issuing the electronic identification means

Name of the party issuing the electronic identity means and indication of whether the party is referred to in Article 7(a)(i), (ii) or (iii) of Regulation (EU) No 910/2014

Identity Malta Agency through IDMO and Expatriates.

☒ *Article 7(a)(i)*

☐ *Article 7(a)(ii)*

☐ *Article 7(a)(iii)*

3.3. Party operating the authentication procedure

Name of party operating the authentication procedure

The Scheme comprises both electronic identification and electronic signature services, both of which are operated by Malta Electronic Certification Services Limited (MECS Ltd). MECS Limited serves as the Qualified Trust Service Provider (QTSP) on behalf of the Government of Malta. MECS Limited is responsible for the issuance and management of certificates including the Authentication and Digital Electronic Signing Certificates on the ID cards issued by IMA. The day to day operations have been outsourced to IMA which also handles the policy management services. The day to day operations includes the revocation status service and managing the Root and issuing CAs for the identity cards used in the Scheme.

The Scheme can be used in the e-ID login portal (https://eid.gov.mt/) operated by the Government of Malta, in order to access a range of e-government services.

3.4. Supervisory body

Name of the supervisory body

Malta Communications Authority ("MCA")

Postal address: Valletta Waterfront, Pinto Wharf, Floriana, FRN1913, Malta
E-mail address: eidas@mca.org.mt
Telephone No: +356 2133 6840

4. Description of the electronic identification scheme

Document(s) may be enclosed for each of the following descriptions.

(a) Briefly describe the scheme including the context within which it operates and its scope

The Maltese e-ID Scheme is managed by IMA through its Identity Management Office (IDMO) and Expatriates Unit. The said scheme is based on two electronic identifications means, that is the Maltese e-ID card and the e-residence documents issued to foreign nationals residing in Malta. Both of these are issued by an EIDAS-certified QTSP (MECS Ltd.). The electronic identification means can be used to log into a web portal that allows access to other websites. Currently, Malta uses this portal for eGovernment services.

Technically, all Maltese e-IDs and e-RPs are PKI-based solutions, where the private key is stored on a secure module of the chip. Smart card-based solutions (e-ID card, e-RP card) have public key certificates in addition to a public certificate repository, also stored on the smart card. The storage includes the subscriber, the intermediate, and the root QCA public certificates. There are two versions of the card available now. The current version is a contactless polycarbonate composite card and supports protocols using ISO 14443 standards. The previous card has a visible chip and is read through a reader with contact, supporting the ISO 7816 protocols. The previous version will be in circulation for about 10 more years ending around the year 2030 when the last ones have expired. The present notification comprises both versions.

The chips are EIDAS QSCD-certified devices. These are smart card-based solutions, which protect the private key from unauthorized access, copying, or tampering. Identity data – the person's first name, last name, and unique identifier (serial number) – is stored in the public key certificate.

The certificates can be used for authentication or electronic signing. Malta offers them in order to integrate a high-assurance ID with a means of electronic authentication or a legal signature that can be used in cross-border transactions. The certificate from the e-ID scheme is used for the Maltese Government's e-ID login portal as a 2nd factor authentication (2FA) which can be used optionally on the portal. The secure chip is accessed only when in possession of the card through a hardware-based card reader and providing evidence that the private authentication key is in the hand of the user. Service providers (from the public or private sector) can choose to force 2FA to create a higher level of security when accessing their service. Only the card-equipped user can access the website when using this option. The e-ID login portal can be used as a Single Sign On (SSO) portal with high assurance when this 2-factor authentication option is chosen by the service provider. It is through this SSO that Maltese Citizens and Malta Residents can access government services online.

The Maltese e-ID card is issued to natural persons who are citizens of Malta. The card stores two electronic certificates within a chip sealed within the card body. Communication is only possible through contactless communication, secured by means of the PACE protocol. The certificates enable electronic identification through the authentication certificate and the digital signing certificate. Through use of the secret PINs the chip can use the private key to prove possession of the card through a cryptographic operation. The e-ID card can also be used as a means to sign documents legally for the holder of the card. The e-residence document is composed of the same components to be issued to natural persons that are foreign nationals. Authentication certificates are available on cards for those natural persons 14 and over. Signing certificates are included for those requesting a card who are over 18 years of age.

Natural persons are registered through an in-person process to ensure the identity of the card recipient. Biometrics are gathered in-person and the necessary checks are made on the authentication of the documents used to apply for the cards. E-ID card registration and issuance is handled by the Identity Malta Agency ID Cards Unit. E-resident document registration and issuance is handled by the Expatriates Unit within Identity Malta Agency.

Security features are built into the card itself in compliance with Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement.

e-ID cards are issued either in person to be picked up upon verification of the address of the applicant or if the applicant has received a card before, then the card can be delivered through registered mail with a signature and return of the old card due upon receipt.

Cards for Maltese Citizens have a validity period of 10 years for Citizens 18 years and older, 2 years for Citizens that are younger. E-ID cards are not issued until age 14. E-residence documents are valid for a maximum of 5 years for those under 14. They are valid for a maximum of 4 years between 14 and 17 years of age, and a maximum of 10 years at 18 years and older. The certificates on the chip correspond with these validity dates.

When applying for an e-ID card or e-residence document, applicants may subscribe for an e-ID login account, which is required to access Government online services. Following the receipt of an application by the ID Cards Unit, IMA verifies the identity of the applicant and an activation link is sent to the email provided by the applicant during their card application process. The card can then be linked to act as a 2nd factor for authentication of government services.

The e-ID was introduced in year 2014 and was updated in 2020. Modernization of the Scheme involved the introduction of a new portal and dashboard accessible on https://eid.gov.mt and is integrated with government services that are offered online so that citizens and residents can authenticate themselves. Security features have been enhanced, and a new page dedicated to privacy and security have been introduced. On this page, the e-ID user is able to adjust certain features related to privacy and security, including the Government entities and relying parties that have been previously granted access.

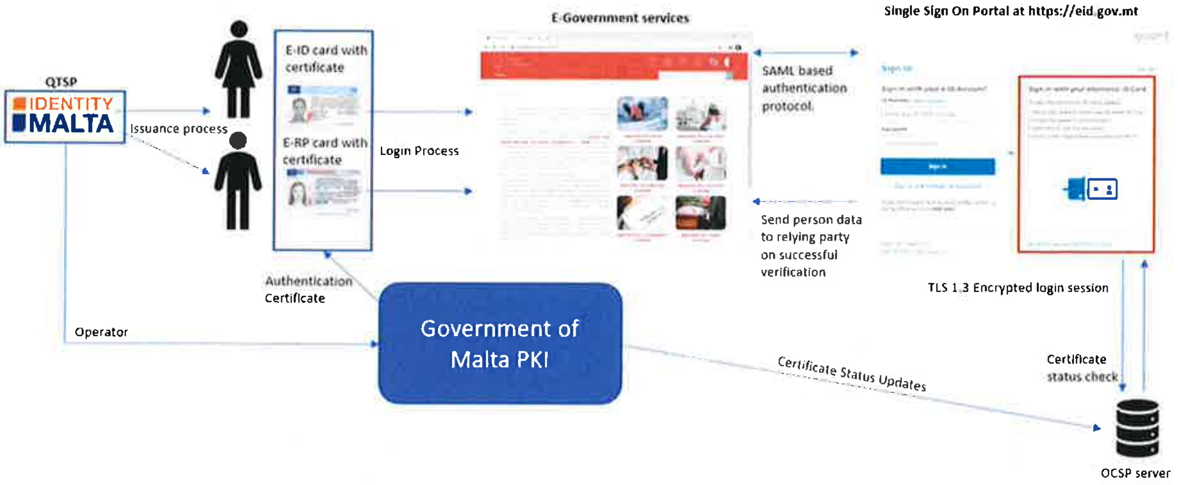
In the management of the eID scheme, the following parties are involved:

- As the issuing and registration authority, Identity Malta Agency performs the registration of applicants as well as the issuance of the physical cards themselves.
- MECS Ltd. serves as the QTSP under eIDAS and is audited by a Certified Audit Body every two years to maintain its QTSP status.
- The supervisory body, MCA ensures that MECS ltd. and Identity Malta Agency adhere to the security, privacy and assurance standards as regulated by the eIDAS legislation.
- HID CID Limited has been engaged by the Government of Malta for the supply of identity documents that are manufactured and inspected using processes that adhere to the most well-known and respected compliance standards in the industry. HID CID Limited also operate the PKI infrastructure on behalf of Identity Malta Agency.

Issuance of the e-ID card and the e-RP card is described in section 2.2.1. of the corresponding LoA mapping in Section 5 of this document.

eID technical descriptions are provided in section 2.3.1. of the corresponding LoA mapping in Section 5 of this document.

Assurance requirements come from European legislation (i.e., the eIDAS Regulation, GDPR, etc.) and national legislations (i.e., the Electronic Commerce Act, the Identity Card and Other Identity Documents Act, and other national acts) for both public and private parties involved.


QTSP
IDENTITY MALTA
Issuance process
E-ID card with certificate
E-RP card with certificate
Login Process
E-Government services
SAML based authentication protocol.
Single Sign On Portal at https://eid.gov.mt
Send person data to relying party on successful verification
TLS 1.3 Encrypted login session
Authentication Certificate
Operator
Government of Malta PKI
Certificate Status Updates
Certificate status check
OCSP server

(b) Where applicable, list the additional attributes which may be provided for the natural persons under the scheme if requested by a relying party.

The Scheme supports the minimal data set required under EIDAS. A comprehensive overview of attributes (including any additional attributes) that can be requested and provided to relying parties under this scheme are:

ID Card Number
Full Name
Date of Birth
Email
Sex
Address
Telephone Number
Mobile Number
Fax Number
Photo
Title

(c) Where applicable, list the additional attributes which may be provided for legal persons under the scheme if requested by a relying party.

Maltese e-IDs are used only for identification of natural persons; therefore, no additional attributes are provided for legal persons under the scheme if requested by a relying party.

4.1. Applicable supervisory, liability and management regime

4.1.1. Applicable supervisory regime

Describe the supervisory regime of the scheme with respect to the following: (where applicable, information shall include the roles, responsibilities and powers of the supervising body referred to in point 3.4, and the entity to which it reports. If the supervising body does not report to the authority responsible for the scheme, full details of the entity to which it reports shall be provided)

(a) supervisory regime applicable to the party issuing the electronic identification means

As already established in point 3.4 above, the MCA is the designated national supervisory authority in relation to the electronic identification means.

The MCA applies the same degree of diligence towards the Scheme and comparable supervision as it would towards qualified trust service providers. Notably, the MCA maintains a list of qualified trust service providers which are supervised by it, together with information related to the qualified trust services provided by them. This list complies with the Electronic Identification Regulation. MCA holds the necessary powers and adequate resources to ensure that the requirements of the eIDAS Regulation are followed and take action in cases that the said Regulation requirements are not met. MCA can audit or require an audit from a Certified Audit Body (CAB) of entities that it certifies. Its duties are (but not limited to):

- the assessment of qualified status of trust services and issuance of licenses to provide trust services;
- the managing of trust list of Maltese trust service providers;
- supervising of notified trust services providers in meeting the established requirements;
- collecting, analyzing, solving security incidents, and informing them to ENISA;

MECS Ltd. currently enlists the Services of a CAB to audit the entire QTSP operations (including the authentication procedure) every two years. Those findings are supplied to MCA every time it is audited, for evaluation purposes. Every significant change to the QTSP system is audited on an ad-hoc basis to support MECS Ltd. eIDAS certification on behalf of the MCA.

(b) supervisory regime applicable to the party operating the authentication procedure

See point 4.1.1. (a) above. Authentication is performed using the certificates on the identity card and validated by the OCSP or CRL revocation status service. Both are under the responsibility of MECS Ltd. and supervised by the MCA.

4.1.2. Applicable liability regime

(a) liability of the Member State under Article 11(1) of Regulation (EU) no 910/2014

Liability for ensuring that the person data used in authentication is representing the correct person. Also, liability for ensuring the authentication method is available, is free to public sector bodies, and isn't too difficult to connect to.

The liability of Malta is stated in Malta's national legislation.

As one of the first Member States to legislate in the field of eCommerce, today the Maltese national legislation on eID and Trust Services is harmonious with the EIDAS Regulation and permits Malta to benefit from cross-border authentication and digital signing in to eGovernment services. The main piece of legislation in this regard is the Electronic Commerce Act, Chapter 426 of the Laws of Malta which act went through various amendments by virtue of Act XXXV of 2016 ensures compliance with the measures provided for in Regulation (EU) 910/2014 (EIDAS) to have in place one consolidated piece of legislation in line with EU requirements.

(b) liability of the party issuing the electronic identification means under Article 11(2) of Regulation (EU) no 910/2014

Liability for ensuring that the EID means is issued to the correct person.

The liability regime (including liability limitations and constraints) has been implemented in accordance with the requirements of the eIDAS Regulation for qualified trust services, which has been amended with limited variation to encompass the identification functionalities of the Scheme.

The liability of the QTSP issuing the EID means, being MECS Ltd., is governed by clause 16 of the Subscriber's Agreement signed by e-ID holders registering for their e-ID card and e-ID account issued by the Government of Malta. Notably, the QTSP does not assume any 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's Agreement and/or which exceeds the indicated limitations of any such use or reliance.

In any case, and to the extent permitted by law, the QTSP'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) maximum 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 under the Subscriber's Agreement where such failure arises from a force majeure event that is an event beyond the TSP's reasonable direct control, as defined under the said Agreement.

(c) liability of the party operating the authentication procedure under Article 11(3) of Regulation (EU) no 910/2014

Liability for ensuring that the authentication procedure is operating properly (i.e. the system should not keep the correct person out or allow someone to impersonate someone else)

MECS Ltd. is the party that assumes the responsibility of the authentication procedure involved in the Scheme. MECS Ltd. oversees the operations of the certificate issuance and the certificate revocation status service. MECS is liable to the extent required by the eIDAS Regulation, noting (as stated above) that its liability as a QTSP has been extended to also address the identification components of the Scheme, as captured in the Subscriber's Agreement.

Except for indemnity obligations set out in the Subscriber's Agreement, the Subscriber shall not hold the Government of Malta responsible (including in relation to the e-ID Portal when logging on to e-government applications) for any cessation, interruption or delay in the performance of its obligations defined under the said Agreement in clause 23 (f) provided that the Government (i) shall have given the Subscriber written notice thereof promptly and, in any event, within five (5) days of discovery thereof and (ii) shall take all reasonable steps reasonably necessary under the circumstances to mitigate the effects of the force majeure event upon which such notice is based.

Of particular relevance is Article 3 of the Electronic Commerce Act, Chapter 426 of the Laws of Malta, which states that Malta cannot hold transactions invalid because they take wholly or partly by means of one or more electronic communications. This is in-line with the EIDAS regulation which states that no cross-border transactions may be denied legal effect solely by the fact that the transactions are conducted through electronic means. Thereby codifying the situations where of digital transactions by electronic communication is legal and increasing the liability of the authentication mechanism (provided that it is using MECS Ltd. authentication or signing certificate for the transaction).

4.1.3. Applicable management arrangements

Describe the arrangements for suspending or revoking of either the entire identification scheme or authentication, or their compromised parts.

For individual revocations, the Authentication and Signing certificates of an e-ID or e-RP card can be revoked at the request of the Subscriber in the following cases:

a) If the e-ID, Private Keys or PINs of the Subscriber have been, or are suspected to have been, compromised or are insecure in any way;

b) If any of the information contained in the Certificate, or the identification and authentication information has been changed, altered, or is otherwise no longer accurate or complete.

Furthermore, the TSP can revoke certificates for the following reasons: if any of the information in the Certificate changes; If the TSP and/or the RA knows or has reason to suspect that the Private Keys or password or PIN number of the Subscriber have been compromised; If the Subscriber fails to comply with their obligations under their applicable Subscriber Agreement; or for any other reasons the TSP and/or the RA deems necessary.

Currently, the TSP does not offer certificate suspensions.

The process for suspension or revocation of the applicable trust service is defined in the Termination Plan for the PKI of MECS Ltd. The present Termination Plan indicates the requirements and procedures to be followed, and the responsibilities of the parties involved, during the termination of a TSP and of its related services, as well as the subsequent decommissioning of those PKI Certificate Services used by the QTSP to manage Certificates, in accordance with the GOM Certificate Policies (CPs) for the issuance of Qualified and non-Qualified Certificates. In summary, the suspension or revocation is coordinated with the supervisory body (MCA). The MCA is notified first for either case. In both cases, the situation would be notified to the European Commission by the MCA.

Suspension is enacted when the electronic identification means has been compromised in part or in whole. Operations of the compromised area for MECS Ltd would be suspended until such time when the issue is remediated.

In case of a revocation, there are two versions - planned versus unplanned. The planned revocation would see a gradual shutdown of operations as the responsibilities are transferred to a replacement operator. The replacement operator is chosen by the MCA.

The unplanned revocation is generally used in case of a compromise of the system that is unrecoverable or there is no longer a trusted relationship between the operator and the issued EID means. The unplanned revocation would see a transfer of responsibilities to the MCA until such a time that the replacement can be chosen. The certificates affected in the unplanned revocation will be invalidated. In both cases, the MCA will oversee the transfer of the authentication means to a new party.

4.2. Description of the scheme components

Describe how the following elements of Commission Implementing Regulation (EU) 2015/1502 (1) have been met in order to reach a level of assurance of an electronic identification means under the scheme the Commission is being notified of: (include any standards adopted)

4.2.1. Enrolment

(a) Application and registration

Registration for Maltese Citizens is done at birth where the child is assigned a National ID number, which is then used in applying for an ID after they turn 14.

<u>First-time National ID applicants must fill in and submit the following documentation:</u>

- Form ID 10 – Application for a Maltese Identity Card with a recent passport-size photo attached, signed by the authorized witness who signed Section D;

- Previous Residence Card (whenever the applicant acquired Maltese citizenship and formerly held a Residence Permit card bearing an "A" number);
- A letter of confirmation or certificate issued by the Citizenship Unit as proof of being a Maltese citizen. This proof is not necessary under certain circumstances.

Those who are applying for residence documents must do the following:

- A natural person seeks to apply and enquires at the Expatriates office, they will have to fill out the application form.
- Applicants should also supply the relative documentation. (there are different documentation requirements depending on what program is applied for)
- Supply Form ID-1A (case dependent)
- Subsequently, the applicant is required to personally call at the offices of the Agency in order to capture the required biometric data in line with applicable legislation.

Thereby the e-ID and e-RP card recipients each go through a verification process with a high level of assurance. During this process, the correctness of the application is confirmed by local stakeholders to confirm that the person exists under the claimed identity. Thereafter, IMA verifies their evidentiary documentation in order to ensure that the documentation is indeed for and about that person. Finally, the person submitting the documents is brought in in-person, so that we can see face-to-face that they are real and are to be associated to the identity card via picture, or signature, or fingerprints.

EID SSO logon account application is included with the ID-10 form for the e-ID card and the ID-1A form for the e-RP. The EID is granted by the following steps:

- An email address must be provided on the application for the identity document along with explicit approval to create an EID SSO login.
- Following the receipt of the application by the IDMO, IMA employees confirm the identity to be given the account.
- IMA sends an email to the email address listed on the application.
- The person clicks the link in the email or pastes it into their browser.
- The e-ID SSO portal verifies the correct identity using details such as National ID number, Document number, Application reference number
- The applicant must then create a secure password (alphanumeric, mixed-case, >8 characters, not containing name or ID number)
- Password is then able to be used to gain access to SSO portal.
- Service providers can request additional levels of authentication where the person will need to use their card to provide a 2nd factor for login using a PIN and authentication certificate.

(b) Identity proofing and verification (natural person)

Identity-proofing and verification (natural person) is described in section 2.1.2. of the corresponding LoA mapping in Section 5 of this document.

(c) Identity proofing and verification (legal person)

As the identity cards are only issued to Natural Persons this option is not available in Malta.

(d) Binding between the electronic identification means of natural and legal persons

As the identity cards are only issued to Natural Persons this option is not available in Malta.

4.2.2. Electronic identification means management

(a) Electronic identification means characteristics and design (including, where appropriate, information on security certification)

Electronic identification means characteristics and design are described in section 2.2.1. of the corresponding LoA mapping in Section 5 of this document.

(b) Issuance, delivery and activation

Issuance, delivery, and activation is described in section 2.2.2. of the corresponding LoA mapping in Section 5 of this document.

(c) Suspension, revocation and reactivation

In this context the provision relates to the processes used to suspend, revoke or reactivate an electronic identification means issued to specific natural or legal person. This is distinct from the requirements set out in 4.1.3. that relate to the suspension of an authentication mechanism or scheme itself.

Suspension, revocation, and reactivation is described in section 2.2.3. of the corresponding LoA mapping in Section 5 of this document.

(d) Renewal and replacement

Renewal and replacement is described in section 2.2.4. of the corresponding LoA mapping in Section 5 of this document.

4.2.3. Authentication

Describe the authentication mechanism including terms of access to authentication by relying parties other than public sector bodies.

In general, there are no restrictions for the use of Maltese eID-based electronic authentication other than those listed in the respective Subscriber's Agreement. IMA provides an ID card, which is in-turn housing a secure chip which stores an authentication certificate. Malta intends for this certificate to connect individuals to eGovernment services and perhaps partner services (relying parties) may integrate their systems with this technology in the future. Technically, certificate-based authentication is an establishment of SSL/TLS communication using the client certificate. This means everyone (public or private sector) can use it. The authentication method is depicted above in section 4 (a) of this document.

There are two methods for verifying the authentication certificate in use is valid. One can use the OSCP service for checking certificate validity with the CA. On the other hand, the CRL is publicly available, but, since CRL technology has its limitations, it is rarely used by the public sector and only with systems where reliability requirements are low.

4.2.4. Management and organization

(a) General provisions on management and organization

General provisions are described in section 2.4.1. of the corresponding LoA mapping in Section 5 of this document.

(b) Published notices and user information

Published notices and user information is described in section 2.4.2. of the corresponding LoA mapping in Section 5 of this document.

(c) Information security management

Information security management is described in section 2.4.3. of the corresponding LoA mapping in Section 5 of this document.

(d) Record keeping

Record keeping is described in section 2.4.4. of the corresponding LoA mapping in Section 5 of this document.

(e) Facilities and staff

Facilities and staff are described in section 2.4.5. of the corresponding LoA mapping in Section 5 of this document.

(f) Technical controls

Technical controls are described in section 2.4.6. of the corresponding LoA mapping in Section 5 of this document.

(g) Compliance and audit

Compliance and audit are described in section 2.4.7. of the corresponding LoA mapping in Section 5 of this document.

4.3. Interoperability requirements

Describe how the interoperability and minimum technical and operational security requirements under Commission Implementing Regulation (EU) 2015/1501 (1) are met. List and attach any document that may give further information on compliance, such as the opinion of the Cooperation Network, external audits, etc.

The Scheme has been extensively tested and is currently being used for eGovernment services. The national EIDAS node has been separately evaluated by the EC and found to support the interoperability and minimum technical and operational security requirements under Commission Implementing Regulation (EU) 2015/150 as a result. The node is currently certified under EIDAS regulation by the European Commission. Therefore, it is currently interoperable and in operation now. The eIDAS Node permits Maltese citizens to use the digital public services of other EU member states and, correspondingly, gives European citizens access to the digital services of the Maltese Government. The Node is compliant with the EU Interoperability Framework. It enables the mutual recognition of national electronic identity schemes and strengthens Malta's position in meeting its obligations and harnessing opportunities for interoperability under the eIDAS Regulation.

4.4. Supporting documents

List here all supporting documentation submitted and state to which of the elements above they relate. Include any domestic legislation which relates to the electronic identification provision relevant to this notification. Submit an English version or English translation whenever available.

Level of Assurance Mapping for EID Scheme

- eIDAS Malta Level of Assurance - v1.0.docx

National Qualified Trust Service Provider Listing

- https://tsl.mca.org.mt/MT_TSL.pdf

National legislation related to Trust Service Providers

- Malta Electronic Commerce Act - https://legislation.mt/eli/cap/426/eng/pdf

National Legislation on Issuance of e-ID and e-RP cards

- Malta Identity Card and other Identity Documents Act
  https://legislation.mt/eli/cap/258/eng/pdf

Liability related documents

- e-ID Subscriber's Agreement
  https://repository.qca.gov.mt/ID_Subscriber_Agreement_V2.4_PUB.pdf
- e-RP Subscriber's Agreement
  https://repository.qca.gov.mt/eRP_Subscriber_Agreement_V2.4_PUB.pdf

5. Level of Assurance Mapping

1 Document Approval (Malta EID Scheme Level of Assurance)

Approved by	Position	Signature	Date
Stefan Rodoligo	CIO		
Anton Sevasta	CEO		

1.1 Document Management Team

Name & Surname	IMA Position	Initials
Maurizio Banavage	IT Security & Procedure Manager	MB
Greg Smith	IT Security Manager	GS
Joanna Attard	Legal Officer	JA

1.2 Revision History

REVISION NUMBER			REVISION DATE	SUMMARY OF CHANGE/S	AUTHOR
1.0			14/12/2020	Initial Document	MB
1.10			15/01/2021	Merged LoA Document	GS
1.11			11/05/2021	Added High Assurance 2.3.1.6	JA
1.12			07/10/2021	Document format Arrangement	MB

Contents

1.3 Introduction

This document maps the characteristics of Malta eID Scheme to the standard requirements based on the eIDAS Levels of Assurance in line with the Commission Implementing Regulation (EU) 2015/1502 of 8th September 2015 which sets out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8 (3) of Regulation (EU)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 .
This document covers the Level of Assurance achieved by Identity Malta Agency which should meet the requirements for level of assurance standard 'high'.
A full overview of the system is given in the Maltese eID Pre-Notification documents which cover what type of Cryptography is used and the types of ID Cards issued.

1.4 Definitions

The following words are used within this guidance:

- 'applicant' when describing someone who is trying to authenticate or has yet to be proven to be the legitimate natural person.
- 'subject' when describing the legitimate natural person that is, or to be, represented by the electronic identification means.

The 'subject' and 'applicant' effectively become one and the same when an authentication has successfully been performed.

Throughout this Level of Assurance map, the term *document* is to be understood to refer to both physical and electronic documents. The term *evidence* is to be understood to refer to physical and electronic evidence, and all other forms nationally accepted.

(1) 'authoritative source' means any source irrespective of its factor or form that can be relied on and provide accurate data, information/evidence as proof of identity;

(2) 'authentication factor' means a way of acknowledgement to bound a person that falls into a possession, knowledge or inherit base authentication;

(3) 'CAN' means Card Access Number, printed on the front of a physical card to help prevent electronic eavesdropping on wireless cards;

(4) 'cryptographic' means the use of a process to change information into unrecognizable data which cannot be unscrambled unless a key is used to get back the original information (the study these processes is called 'cryptography');

(5) 'dynamic authentication' means a cryptography electronic progress or other techniques to provide a means of creating on demand an electronic proof that the subject is in control or in possession of the identification that changes with each authentication between the subject and the system verifying the subject's identity;

(6) 'HSM' means Hardware Security Module;

(7) 'IMA' means Identity Malta Agency;

(8) 'information security management system' means a set of procedures and processes that are designed to assess risks levels related to information security;

(9) 'MDS' means Minimum Data Set for person data, as set by Commission Implementing Regulation (EU) 2015/1501, which outlines pieces of information needed for interoperability;

(10) 'OCSP' means Online Certificate Status Protocol, a service available to remotely check if a certificate has been revoked and is still valid;

(11) 'PIN' means personal identification number;

(12) 'QSCD' means Qualified Signature Creation Device creating electronic digital signatures under the EIDAS Regulation;

(13) 'SA' means Subscriber's Agreement, an agreement given to the subscriber of the Trust Service providing the authentication and qualified signature certificate;

(14) 'Single Sign-On' means one set of credentials that can be used for multiple services when verified as authentic by an identity service provider.

(15) '2FA' or two factor authentication means using two of three factors to authenticate. The factors commonly used are: 1 – information someone knows, 2 – an object someone has, and 3 – who someone is (such as biometric factors).

2 Technical specifications and procedures

The elements of technical specifications and procedures outlined in this Annex shall be used to determine how the requirements and criteria of Article 8 of Regulation (EU) No 910/2014 shall be applied for electronic identification means issued under an electronic identification scheme.

GUIDANCE:
The requirements in 2.1-2.2 refers to requirements to the enrolment and issuance process. They are functional requirements which must be met at the latest when the eID is used.

2.1 Enrolment

2.1.1 Application and registration

HIGH (Same as LOW)

1. Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means.

2.1.1.1 Current IMA Procedure

The terms and conditions are listed in the Subscriber Agreement (SA) for the e-ID Account and Certificates within the National Electronic Identity Card. It is relayed to the applicant and IMA ensures that the Applicant has read and agreed to the terms which thereafter are signed for our records.

2. **Ensure the applicant is aware of recommended security precautions related to the electronic identification means.**

2.1.1.2 Current IMA Procedures

Recommended security precautions are listed in our SA in section 5. The SA is relayed to the applicant and IMA ensures that the Applicant has read and agreed to the terms which thereafter are signed for our records.

3. Collect the relevant identity data required for identity proofing and verification.

2.1.1.3 Current IMA Procedure

Currently this is achieved through the Identity Card Applications (forms listed in section 3.3 below). Since these applications and associated paperwork is carried over through registration, issuance of card, and SSO account creation.

2.1.2 Identity proofing and verification (natural person)

LOW

1. The person can reasonably be assumed to be in possession of evidence recognized by the Member State in which the application for the electronic identity means is being made and representing the claimed identity.

2.1.2.1 Current IMA Procedures

The same verification process is to be followed for the creation of an SSO account and submission of the application form with supporting documentation when registering for an e-ID card or residence document. IMA gathers the information which is nationally recognized as evidence in order to issue the card and create the SSO account using the same application. In case the SSO account is not applied for at application stage, applicants can get an SSO account based on their nationally recognized ID card that has been previously issued.

2. The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid.

2.1.2.2 Current IMA Procedures

One of the required processes at the application stage is that any evidence and supporting documentation submitted is vetted and verified to be genuine and valid prior to the e-ID card being issued. The data from the documentation is double-checked to ensure valid entries are made into the registration database.

3. It is known by an authoritative source that the claimed identity exists, and it may be assumed that the person claiming the identity is one and the same.

2.1.2.3 Current IMA Procedures

The registration of birth assigns a national number, to which the e-ID is processed and linked accordingly. Residence Permits are based upon internationally recognized identity documents and verified to be genuine.

SUBSTANTIAL

Level Low, plus one of the alternatives listed in points 1 to 4 have to be met:

1. The person has been verified to be in possession of evidence recognized by the Member State in which the application for the electronic identity means is being made and representing the claimed identity

and

the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person

and

steps have been taken to minimize the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked, or expired evidence;

2.1.2.4 Current IMA Procedures

The SSO account will always be associated with a single national ID number, so that will not change who is represented. The process to apply will be based on a nationally recognized piece of evidence, which is a previous card (if available; see below).

The above steps are taken by the Maltese government authority responsible for the issuance of the cards to process the person's identity and assure proper attribution. The information submitted on the application form is verified as accurate and true by cross-checking it with the national identity database which is controlled by IMA, and which qualifies as an authoritative source. A previously issued card is usually used as evidence to issue a new card. Where no card is available for a re-issuance of an e-ID card, then a reputable witness must be produced to vouch for that person and sign their application. In case a card is stolen, a police report must be submitted as evidence to serve as proof that the card had actually been stolen before proceeding with the re-issuance of the card The same methods are used for the e-RP to provide evidence. The initial application is different in that a foreign identity document instead of birth records is used to match identifying information with a person. These must be checked by the police as to their authenticity. The applicants are also confirmed by their employer to be the person who is receiving the e-RP.

HIGH

Requirements of either point 1 or 2 have to be met:

1. Level substantial, plus one of the alternatives listed in points a to c has to be met:

a. Where the person has been verified to be in possession of photo or biometric identification evidence recognized by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source;

and

the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source;

or

b. Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level substantial, then the entity responsible for the registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council or by an equivalent body

and

steps are taken that the results of this previous procedure remain valid;

2.1.2.5 Current IMA Procedures

During the card application process these biometrics are captured through live enrolment and used to match the person data on the card with the person receiving the card. A Collection Letter is issued once the card is printed and is ready for collection.

2.1.3 Identity proofing and verification (legal person)

2.1.3.1 Current IMA Procedures

This is not available, legal person's identity cards are not issued in this scheme.

2.1.4 Binding between the electronic identification means of natural and legal persons

2.1.4.1 Current IMA Procedures

Not Applicable since Malta does not currently issue electronic identification means to legal persons, but only to natural persons.

2.2 Electronic identification means management

2.2.1 Electronic identification means characteristics and creation

SUBSTANTIAL

1. The electronic identification means utilizes at least two authentication factors from different authentication factor categories.

2.2.1.1 Current IMA Procedure

To utilize the authentication certificate upon the card, two factors must be used. One factor is that the person must hold the card and the second factor is knowing the PIN. One must hold the card to get access to the correct private key in order to authenticate as the subject on the SSO portal. Furthermore, one must know the PIN to use the private key on the card for this authentication.

2. The electronic identification means is designed so that it can be assumed to be used only if under the control of the subject to whom it belongs.

2.2.1.2 Current IMA Procedure

Prior to the issuance process, several steps are taken to issue the card to only those people to whom it belongs. The PINs letter is used as proof of address and brought in to retrieve the card. The IMA clerk verifies the subject after they look and cross-identify the person data on the card with the person in front of them. That person then controls the PINs and the card. Subsequently, the e-ID scheme can only allow the SSO login with 2FA if that card and verified PIN is used to log in. Subscribers are informed of their obligation to maintain control over the card, and to ensure the confidentiality of the PIN.

HIGH

Level substantial, plus:

1. The electronic identification means protects against duplication and tampering against attackers with high attack potential.

2.2.1.3 Current IMA Procedure

The authentication certificate is secured on a qualified signature creation device (QCSD) which keeps the private key from being copied for use elsewhere. This secures one factor of the 2FA as the ID Card issued to the subject is the unique key used in authentication. The use of 2FA is also protected with communication encryption to prevent against man-in-the-middle or replay attacks. The embedded chip in the card is certified to a Common Criteria protection profile at Evaluated Assurance Level 5+. Furthermore, the other factor of the access PIN is set when the subscriber first sets up the card and will be known only by them.

2. The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.

2.2.1.4 Current IMA Procedure

The responsibilities of the subscriber for the protection of his identity are set out in the Subscriber's Agreement. IMA issuing the e-ID means on a physical card allows the subscriber to protect its use. A subscriber protects its use by physically holding the card, generally in someone's personal wallet or bag, thereby controlling who has access to the card itself. In order to use the certificates on the chip, personal PINs are needed and communication with the card's chip cannot be initiated without possessing the Card Access Number (CAN) or the Machine-Readable Zone (MRZ) printed on the physical card. The CAN/MRZ is used to prevent nearby card readers from accessing the chip because what is printed on the card is assumed to be unknown.

2.2.2 Issuance, delivery, and activation

HIGH

The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs.

2.2.2.1 Current IMA Procedure

ID cards (including the incorporated certificates) are handed to the person who can prove his identity and picking up in person, or by signature of receiving registered mail and turning in their old card for comparison.

2.2.3 Suspension, revocation, and reactivation

LOW

1. It is possible to suspend and/or revoke an electronic identification means in a timely and efficient manner.

2.2.3.1 Current IMA Procedure

IMA has an obligation to revoke certificates within twenty-four (24) hours as stated in our own Certificate Policy available from the repository listed in the Notes section 3.3.4 below. Suspension is not currently an option. The subscriber requesting a revocation should do so by submitting the request in person to verify the correct person is authorized to make the request.

2. The existence of measures taken to prevent unauthorized suspension, revocation and/or reactivation.

2.2.3.2 Current IMA Procedure

A verification process is done by our helpdesk before revocation. Revocation requests are generally handled in-person. In the case that helpdesk is not readily able to make a verification of a person's identity, being the subject of the revocation, then helpdesk may ask for supplementary information to prove the identity of someone requesting revocation.

3. Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met.

2.2.3.3 Current IMA Procedure

IMA revokes the certificates on the card and then the assurance requirements are met because a new certificate/ID card would have to be issued. The assurance requirements are met through the application and issuance procedure ensuring that the identity card is issued to the same person who applies for the same card. Reactivation of the same certificates is not currently available with the e-ID Scheme.

2.2.4 Renewal and replacement

LOW

Considering the risks of a change in the person identification data, renewal or replacement needs to meet the same assurance requirements as initial identity proofing and verification or be based on a valid electronic identification means of the same, or higher, assurance level.

2.2.4.1 Current IMA Procedure

The applicant must hand in the old card issued and then sign a release form to hand over the new card to the unit in charge within IMA. This implies a new face to face identification process. Any changes in address are substantiated by the person bringing in a mailed PIN letter or Collection Letter to prove their address. Changes in identity data must be substantiated with official certificates (e.g. birth certificate, marriage certificate) issued by the official Public Registry serving as proof of the change of identity.

HIGH

Level low, plus:

Where renewal or replacement is based on a valid electronic identification means, the identity data is verified with an authoritative source.

2.2.4.2 Current IMA Procedure

Malta does currently allow for the use of valid electronic identification means to start an application process for a new ID on the web portal https://singlepermit.gov.mt. The e-ID SSO portal can be used to gain access to this site by verifying the valid e-ID logon account. The verification process ensures us that only the person whose information IMA received through the e-ID login account creation process will access the account for the card renewal process of that person.

2.3 Authentication

This section focuses on the threats associated with the use of the authentication mechanism and lists the requirements for each assurance level. In this section controls are understood to be commensurate to the risks at the given level.

2.3.1 Authentication mechanism

LOW

1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity.

2.3.1.1 Current IMA Procedure

The electronic identification means is used with the Single Sign On portal to provide authentication data, which data is verified through the OCSP server as valid before allowing the user through and sending personally identifying data to the relying party. Once a user has logged on, the system creates a session cookie that will help identify them as a valid user if they want to access another relying party's service without typing in a password.

2. Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline.

2.3.1.2 Current IMA Procedure

Through the use of the SSO portal, the identification data is protected by the connection to the site using TLS 1.3 encryption and authentication. The SSO portal is hosted in a data center that is protected by following ISO guidance as evidenced by its ISO 27001 certification, with technical, administrative, and physical controls in accordance with the state of the art to prevent compromise of the data. Symmetric algorithms are used for encryption of personal data during transmission.

3. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.

2.3.1.3 Current IMA Procedure

The authentication mechanism requires three parties to verify on behalf of the service provider. The subscriber with a computer and connected ID card, the SSO portal, and the Certificate Status Service. The first party of the electronic identification uses the qualified signature creation device that keeps the communication secure. No private keys travel outside of the ID Card itself to prevent manipulation. The communication channel to the second party is secured through technical controls using TLS 1.3. This ensures that replays and eavesdropping cannot take place. The validity of the certificate is then checked through a secure communication established through the OCSP server (or the CRL under the control of the Government of Malta). This authentication and encryption will help prevent eavesdropping (leading to replay) and man in the middle attacks.

SUBSTANTIAL

Level low, plus:

1. The release of person identification data shall be preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication process.

2.3.1.4 Current IMA Procedure

The validation of the authentication certificate information is done dynamically using the OCSP server to ensure validity at the time of authentication for each separate session. Session cookies (and their level of authentication) are checked to make sure that they are valid before granting access to any systems protected by the SSO login portal.

2. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.

2.3.1.5 Current IMA Procedure

The verification of the electronic identification takes place partially through the qualified signature creation device that keeps the communication secure. The communication channel is secured through technical controls using TLS 1.3. This authentication and encryption will help prevent 3rd party or middleman attacks. The validity is checked through a secure communication, which is established through the OCSP server (or the CRL under the control of the Government of Malta)

HIGH

Level substantial, plus:

The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.

2.3.1.6 Current IMA Procedure

The three levels of assurance according to eIDAS are based on the ISO/IEC 2915 standard, which is the basis for many assurance frameworks. For that purpose, IMA considers each requirement of the Implementing Regulation and explains how the Malta eID meets the requirements for Level of Assurance 'high' on the basis of;

Identity assurance:
In-person ID proofing at registration authority
ID verification using official government sources and documents

2FA/Multi-factor

Authentication assurance:
Must access private data/keys stored on tamper-resistant hardware token
Cryptographic protection of personally identifying information (PII)
"Possession" (eID card) and "Knowledge" (PIN).

The corresponding private keys are securely stored on the chip of the eID card (Citizen ID card or residence permit) of the card holder. As part of the cryptographic protocols, the imprinted CAN number is always required to securely release the data. The corresponding PIN of the card holder is then required to unlock the chip of the eID card throughout the authentication process.

The Malta eID is based on two authentication factors from the different authentication factor categories "possession" (eID card) and "knowledge" (PIN). Both factors apply for both authentication and signing.

The private keys required for authentication with the eID and the identification data of the subject are stored on the chip of the card holder´s eID (QSCD). The chip hard- and software of the Malta eID card are certified according to the protection profiles for secure signature creation device EN 419211-2:2013 - Protection profiles for secure signature creation device - Part 2: Device with key generation, 18 May 2013, BSI-CC-PP-0059-2009-MA-02.

These Protection Profiles define the functional and assurance requirements for the chip hard- and software of the Malta eID card. This includes security functional requirements (SFRs) to protect the private keys and identity information against duplication and tampering.

2.4 Management and organization

All participants providing a service related to electronic identification in a cross-border context ("providers") shall have in place documented information security management practices, policies, approaches to risk management, and other recognized controls so as to provide assurance to the appropriate governance bodies for the electronic identification schemes in the respective Member States that effective practices are in place. Throughout section 2.4, all requirements/elements shall be understood as commensurate to the risks at the given level.

2.4.1 General provisions

LOW

1. Providers delivering any operational service covered by this Regulation are a public authority or a legal entity recognized as such by national law of Member State, with an established organization and fully operational in all parts relevant for the providing of the services.

2.4.1.1 Current IMA Procedure

Operations are under strict control of the government and respective entities.

2. Providers comply with any legal requirements incumbent on them in connection with operation and delivery of the service including, the types of information that may be sought, how identity proofing is conducted, what information may be retained and for how long.

2.4.1.2 Current IMA Procedure

MECS Limited, which acts as the QTSP on behalf of the Government of Malta, is bound by the eIDAS legislation and other applicable laws both at national and European level. IMA is also bound by GDPR and the applicable EU and national laws on data protection, particularly regulating the retention and collection of information IMA is authorized to collect. Finally, MECS Limited assumes liability as it is contractually bound to respect the terms of the Scheme.

3. Providers are able to demonstrate the ability to assume the risk of liability for damages, as well as having sufficient financial resources for continued operations and providing of the services.

2.4.1.3 Current IMA Procedure

MECS Ltd. has resources to continue operating the services as a QTSP in accordance with the requirements of EIDAS and is utilizing a revenue generating agency to ensure the required sufficient financial resources. These assurances in relation to financial stability benefit the Scheme as well. In addition to revenue from normal operations, MECS Ltd. is insured to cover the liability of the risk of damages pertaining to eIDAS itself. There is also a PKI Termination Plan in place so that both IMA and the national supervisory body (MCA) are prepared in the eventuality of a severe failure of the service.

4. Providers are responsible for the fulfilment of any of the commitments outsourced to another entity, and compliance with the scheme policy, as if the providers themselves had performed the duties.

2.4.1.4 Current IMA Procedure

Responsibility is built into the eIDAS regulation applicable to MECS Ltd. as the QTSP providing all services on behalf of the Government of Malta. IMA is responsible for the operational processes, but the liability for e-IDAS compliance stays with MECS Ltd.

5. Electronic identification schemes not constituted by national law shall have in place an effective termination plan. Such a plan shall include orderly discontinuations of service or continuation by another provider, the way in which relevant authorities and end users are informed, as well as details on how records are to be protected, retained, and destroyed in compliance with the scheme policy.

2.4.1.5 Current IMA Procedure

IMA has a current Termination Plan for the PKI QTSP procedures in place. The termination plan covers the steps that are to be followed in case of a scheduled termination as well as an unscheduled termination. It also summarizes the notification of such an action, who gets notified, and contact details.

Published notices and user information

LOW

1. The existence of a published service definition that includes all applicable terms, conditions, and fees, including any limitations of its usage. The service definition shall include a privacy policy.

2.4.1.6 Current IMA Procedure

The repository of the applicable documents is available publicly through the website at https://repository.qca.gov.mt (see Notes section 3.3.4).

2. Appropriate policy and procedures are in place in order to ensure that users of the service are informed in a timely and reliable fashion of any changes to the service definition and to any applicable terms, conditions, and privacy policy for the specified service.

2.4.1.7 Current IMA Procedure

The Certificate policy and the Certification Practice statement are posted publicly when made official through repository.qca.gov.mt. This document repository is referenced on the certificates themselves to ensure that all subjects can get directed to the policy and procedures used.

3. Appropriate policies and procedures are to be put in place that provide for full and correct responses to requests for information.

2.4.1.8 Current IMA Procedure

Customer Care and Enquiries are handled through Unit based policies and procedures. GDPR requests are handled through our data protection email address and follow the applicable data protection policies already in place.

2.4.2 Information security management

LOW

There is an effective information security management system for the management and control of information security risks.

2.4.2.1 Current IMA Procedure

A Risk Assessment Process and Policy is in place to cover the effective management and control of information security risks. The process goes through the step by step procedure used for enumerating risks, evaluating risks, and then making a plan to remediate them. The policy outlines what parties have responsibilities in the process, what scope there are for the Risk Assessments, and a directive to use the process described above. Our IMA ISMS evaluates risk on a yearly basis and implements a Risk Treatment Plan to adhere to when addressing risks. There is also a separate ISMS in place for the PKI infrastructure itself.

The server hosting facility for the EID Scheme, owned by MITA, is an ISO 27001 certified environment with the management and processes to support that certification.

2.4.3 Record keeping

LOW

1. Record and maintain relevant information using an effective record-management system, taking into account applicable legislation and good practice in relation to data protection and data retention.

2.4.3.1 Current IMA Procedure

Electronic records are kept in our backups server systems and network storage. Records of Identity Document issuance are kept in a paper filing system and electronic records databases. Security controls are in place for the systems to protect them against disclosure to unauthorized parties. Data retention is controlled by internal processes.

2. Retain, as far as permitted by national law or other national administrative arrangement, and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed.

2.4.3.2 Current IMA Procedure

Electronic records are kept according to best practice principles, following the lapse in period of the retention policies, electronic records will be deleted. Records of Identity Document issuance are kept in accordance with national laws, GDPR, and requirements for evidence in case of legal proceedings.

2.4.4 Facilities and staff

LOW

1. The existence of procedures that ensure that staff and subcontractors are sufficiently trained, qualified and experienced in the skills needed to execute the roles they fulfil.

2.4.4.1 Current IMA Procedure

All new employees are screened before being offered a job with IMA. IMA Human Resources department screens employees resumes and checks references to ensure that they possess the necessary qualifications and knowledge to fulfill the role descriptions. This includes an interview, an ICT test and getting copies of certificates and review of the police conduct. Employees are also asked to sign their job description.

2. The existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures.

2.4.4.2 Current IMA Procedure

HR ensures that each section is meeting its own resource requirements. HR does numerous meetings with the different Head of Sections to ensure that all units have the necessary human resources and see where employees need training.

3. Facilities used for providing the service are continuously monitored for, and protect against, damage caused by environmental events, unauthorized access and other factors that may impact the security of the service.

2.4.4.3 Current IMA Procedure

Facilities have protection against theft, fire, and electricity outages. Maintenance agreements are in place to ensure that all equipment is in a state of good repair. Server rooms and equipment are monitored continuously for detection of environmental and malicious threats.

4.Facilities used for providing the service shall ensure access to areas holding or processing personal, cryptographic, or other sensitive information is limited to authorized staff or subcontractors.

2.4.4.4 Current IMA Procedure

The facilities for holding and processing personal, cryptographic, or other sensitive information is limited to authorized staff or subcontractors. Access cards and biometric scanners are used to access physical locations and accounts for logging into these systems are controlled for role-based-authentication-control thereby ensuring that only authorized and qualified people are accessing information according to their role. Contractual agreements are in place regulating and restricting access solely to authorized personnel.

2.4.5 Technical controls

LOW

1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.

2.4.5.1 *Current IMA Procedure*

There are technical controls in place to manage the confidentiality, integrity, and availability of the information processed. This includes, but is not limited to, unique usernames and passwords, high-availability systems in separate physical locations to maintain availability, the maintenance of multiple backups, two-factor authentication used for registration of persons, two-factor authentication used in the administration of the PKI operations.

2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation, and replay.

2.4.5.2 *Current IMA Procedure*

Communication channels are protected through encryption throughout the systems and available to the public using TLS 1.3, internally the communication is on segmented networks used for the scheme only. Cryptography is instituted by policy for PKI systems with standards for minimum key-length of cryptography used in communication and storage. All cryptography that is used is compliant with relevant regulations, agreements, and legislation.

3. Access to sensitive cryptographic material, if used for issuing electronic identification means and authentication, is restricted to the roles and applications strictly requiring access. It shall be ensured that such material is never persistently stored in plaintext.

2.4.5.3 *Current IMA Procedure*

The issuing systems' sensitive cryptographic material is restricted to roles and applications that require access. There are physical and technical controls to ensure that persons who do not require access to do their work are not allowed to access those materials. Such measures include access controls for doors for physical biometric control upon entry or access cards, technical controls include role-based access control using unique usernames and passwords. Key making material is kept in a hardware security module in an encrypted state.

4. Procedures exist to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents, and security breaches.

2.4.5.4 Current IMA Procedure

The management of the changes to the systems involved are under change management procedures and are governed by a change management policy. Likewise, the test environments used to develop software used to access sensitive systems in the scheme are contained within secured environments (physical and technical controls).

Risk assessments are completed on a yearly basis to examine current levels and changes in assets, threats, and vulnerabilities, which may or can impact operations of the current trust services. Risk management roles and responsibilities are defined via the Risk Management Policy. Security breaches and incidents are governed by the Information Security Incident Management Procedure.

5. All media containing personal, cryptographic or other sensitive information are stored, transported and disposed of in a safe and secure manner.

2.4.5.5 Current IMA Procedure

Personal, cryptographic, or other sensitive information are stored on encrypted media and/or stored in physically secure locations, transported via documented means, and disposed of in a safe and secure manner, including destruction of storage media, decommissioning of equipment and shredding paper upon the lapse of the established retention period.

SUBSTANTIAL

Level low, plus:

Sensitive cryptographic material, if used for issuing electronic identification means and authentication, is protected from tampering.

2.4.5.6 Current IMA Procedure

The current use of cryptography is held to industry best practices and written into policy. Key lengths for symmetric algorithms must be at least 256, and asymmetric to use at least 2048. FIPS 140-2 standards are used to help determine the security of the modules we use. Additionally, communication must use TLS 1.2 at a minimum.
HSMs are utilized to encrypt the private keys used in issuing electronic identification means. The Root CA also remains offline.
For the physical environment, there are several physical access controls such as door access card readers, security guards, procedural controls, dual control in our highest security zone, keys to access server racks, safe storage (i.e. storing in a safe) of passwords and access cards for systems used for cryptographic controls, and security cameras and alarms for detection and prevention.
Visitors are also signed in and escorted when untrusted personnel are needed for consultation or auditors need access to the facility.

2.4.6 Compliance and audit

HIGH

1. The existence of periodical independent external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.

2.4.6.1 Current IMA Procedure

Independent audits are performed by the CAB every two years for certification or with every substantial change in the Qualified Trust Service to ensure continued compliance with relevant policies. Independent penetration testing is also performed by independent third bodies ensuring that MECS' security requirements are in place adhering to current security best practices.

2. Where a scheme is directly managed by a government body, it is audited in accordance with the national law.

2.4.6.2 Current IMA Procedure

Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the internal market, the e-IDAS Regulation was transposed into Maltese law by means of Act XXXV of 2016. In accordance with the e-IDAS Regulation, MCA acts as the national supervisory body to supervise trust service providers. MECS Limited is supervised by MCA to ensure that its QTSP status is in place. The responsibilities of the authority, as the competent regulator, are laid down in Articles 23A, 23B and 23C of the Electronic Commerce Act, Chapter 426 of the Laws of Malta.

3 Additional Information

3.1 Contact List

3.1.1 Identity Malta

Head Office – Castagna Building, Valley Road, Msida MSD9020, Malta
Phone – (+356) 2590 4900
email – info.mecs@gov.mt

3.1.2 Exigy

Head Office – 66, Dun Karm Street, Birkirkara BKR9038, Malta
Phone – (+356) 2011 2000
email – info@exigy.com

3.1.3 HID - CID

Maplewood, Crockford Lane, Chineham Business Park, Basingstoke, United Kingdom, RG24 8YB
phone – (+44) 7748 321987
email - liz.bird@hidglobal.com

3.1.4 MITA

Head Office, Gattard House, National Road, Blata l-Bajda HMR9010, Malta
Phone – (+356) 2599 2777
email – info.mita@gov.mt

3.2 Certification & Audits

EIDAS certification held by QTSP MECS Ltd., audited by official Certification Audit Body, and supervised by MCA.
Datacenter certification for ISO 27001 held by the MITA organization.

3.3 Check Forms

3.3.1 ID-10

Form application for filing to receive a National ID Card.
https://identitymalta.com/wp-content/uploads/2019/10/Form-ID-10_Application-for-ID-Card-1.pdf

3.3.2 ID-1A

Form application for filing to receive a Residence Document.
https://identitymalta.com/wp-content/uploads/2019/10/CEA-Form-ID-1A.pdf

3.3.3 Notes

Certificate Policies, Certification Practice Statement, Subscriber's Agreements, Relying Party Agreement, PKI Glossary, PKI Disclosure Statements, CRLs, and Malta PKI-CA public certificates are stored in the MECS Ltd. public repository here: https://repository.qca.gov.mt