DECENTRALIZED DIGITAL IDENTITY IN THE CONTEXT OF ETIAS, EES, AND BEYOND

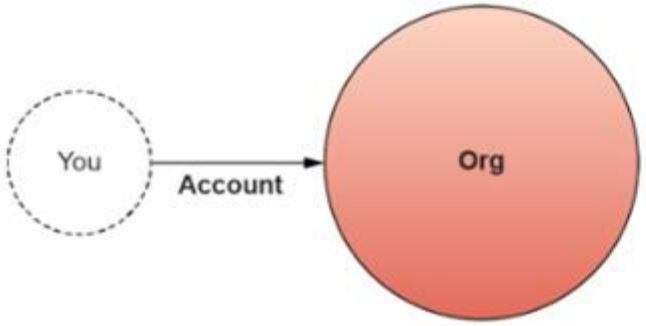
OCTOBER 12, 2022

accenture technology

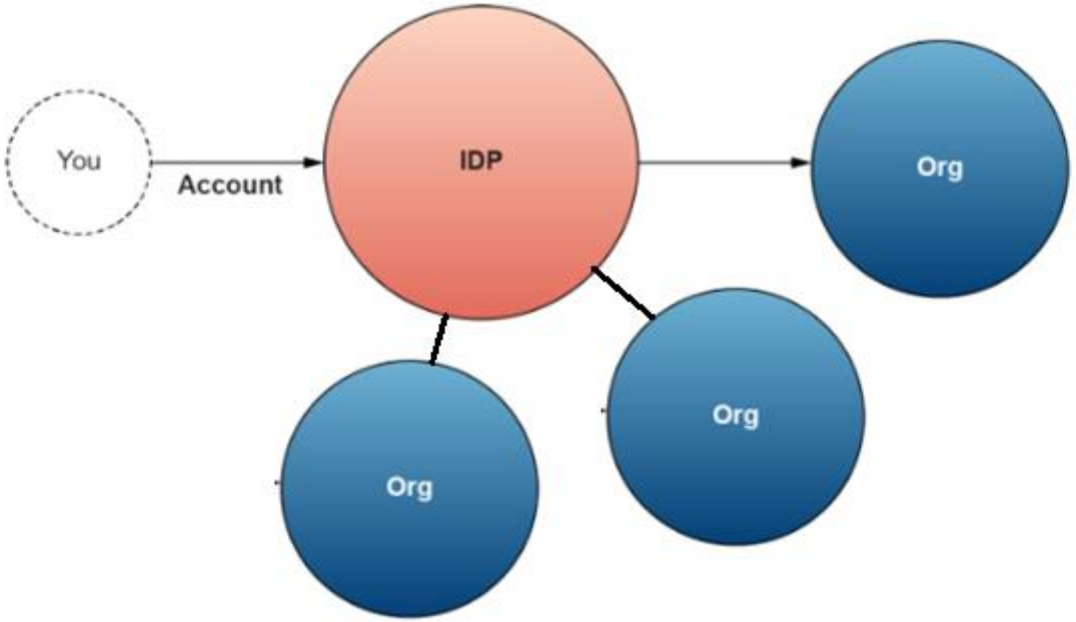
DECENTRALIZED DIGITAL IDENTITY

INTRODUCTION

Centralized Identity

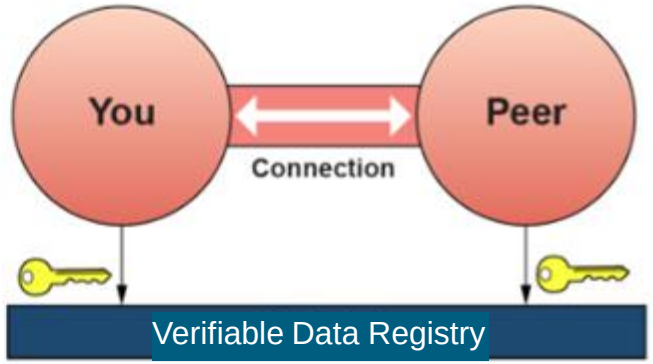


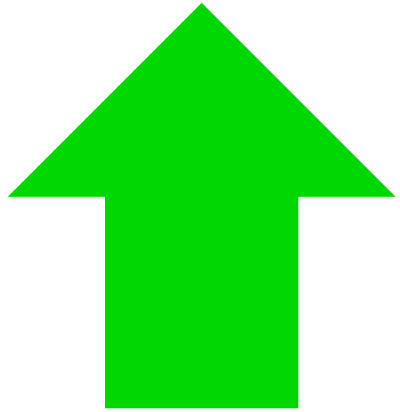
Federated Identity



Decentralized Digital Identity

Self-Sovereign Identity





DECENTRALIZED DIGITAL IDENTITY

Principles of Decentralized Digital Identity (aka, Self-Sovereign Identity):

- The ability for the subject to be in **possession and control** of verifiable identity attributes **from one or more issuers**
- The ability for the subject to **securely and selectively disclose** required information in a **privacy respecting manner** with informed consent - including **Zero Knowledge Proofs**
- The ability for an issuer to **revoke** the verifiable identity attributes they issued
- The ability to **cryptographically verify identity attributes** without a single, centralized authority

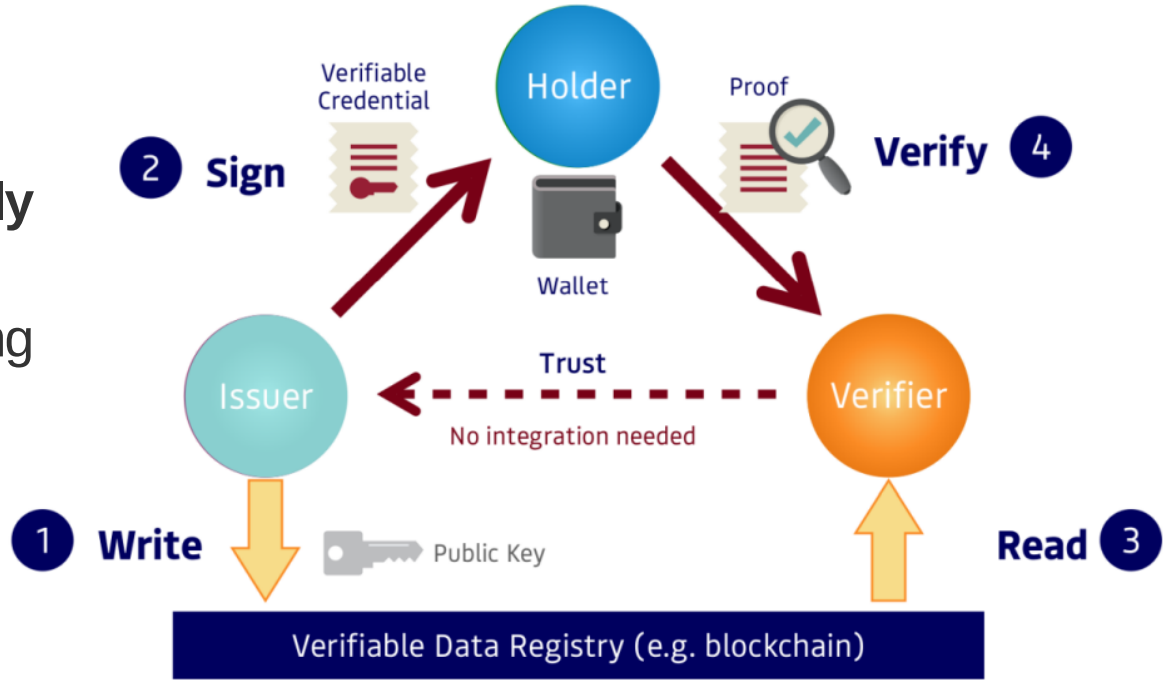
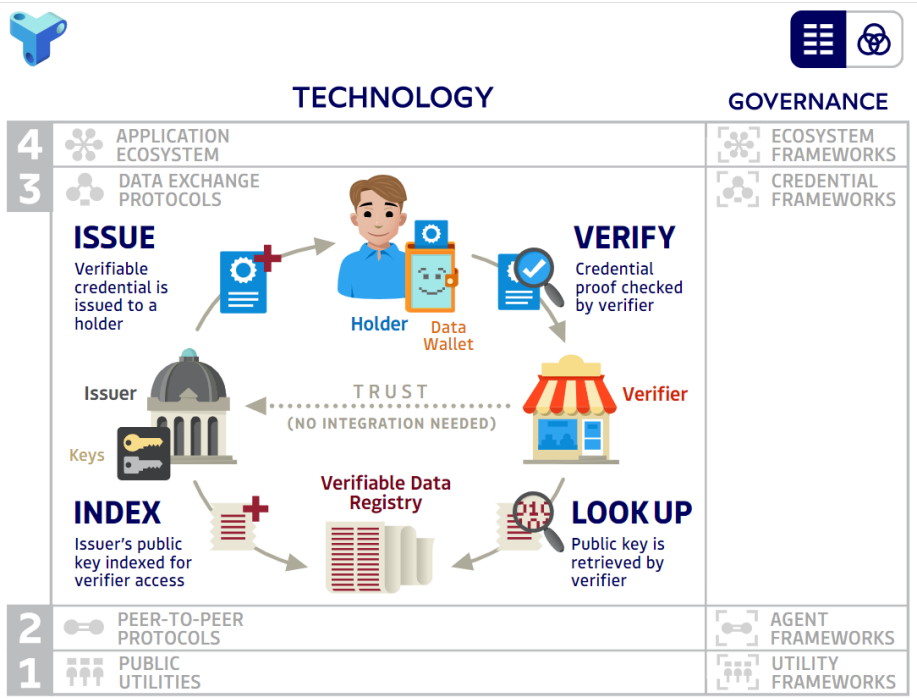


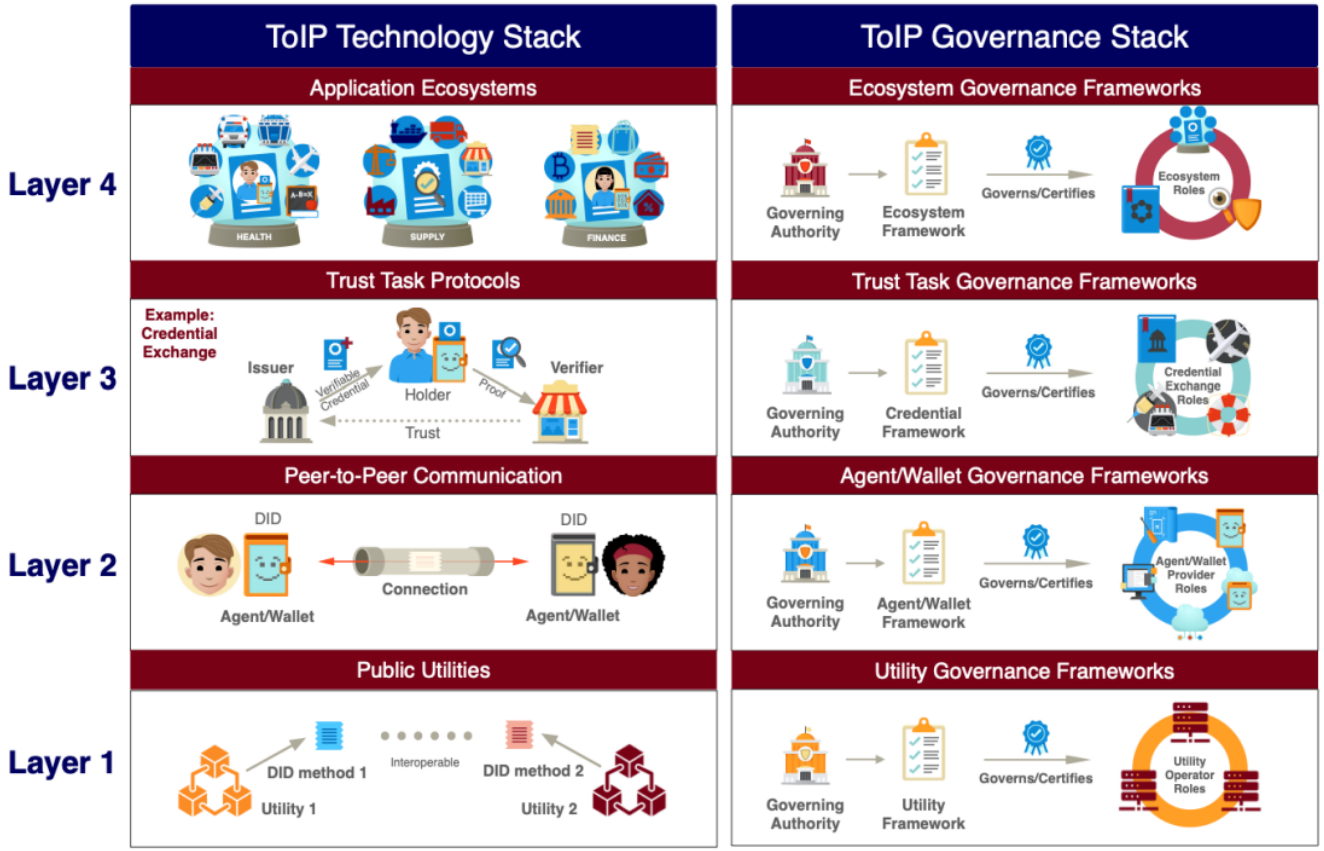
Figure 13. The four basic steps in the verifiable credential trust triangle

DECENTRALIZED DIGITAL IDENTITY



https://trustoverip.org/wp-content/toip-model/

TRUST Over IP FOUNDATION



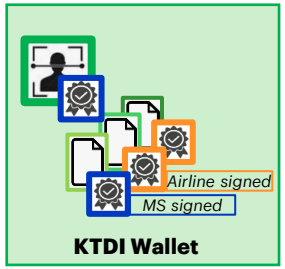
DECENTRALIZED DIGITAL IDENTITY

KTDI Known Traveller Digital Identity

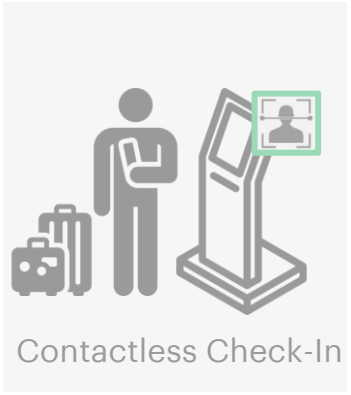
https://vimeo.com/343652153

DECENTRALIZED DIGITAL IDENTITY

KTDI Known Traveller Digital Identity

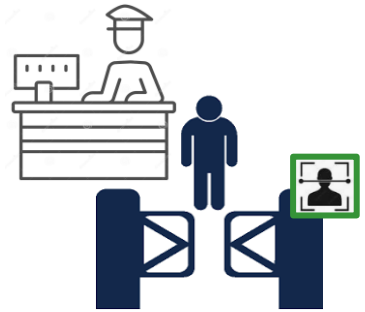


In-person Digitalization, including live image capture
High LOA

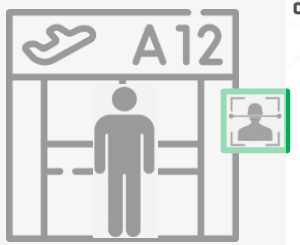


Contactless Travel

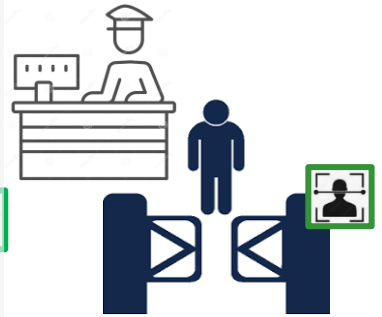
Contactless
Security Check Point



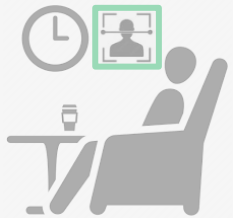
Contactless Arrival



Contactless
Boarding



Contactless Exit
(where applicable)



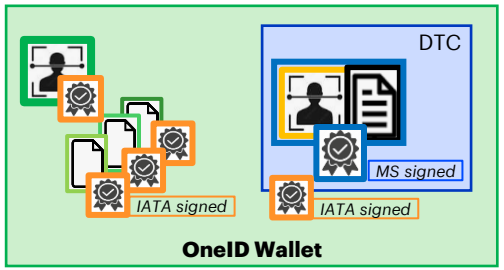
Lounge Access /
Shopping

DECENTRALIZED DIGITAL IDENTITY

Developing two Recommended Practices

1. Digitalization of Admissibility
2. Contactless Travel

Remote Digitalization, including live selfie image capture
Medium LOA



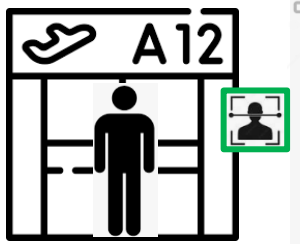
Contactless Check-In

Contactless Bag Drop

Contactless Travel

Contactless Security Check Point

Contactless Arrival



Contactless Boarding

Contactless Exit (where applicable)

Lounge Access / Shopping

ICAO MRTD

ICAO MRTD

A Brief History:

- The International Civil Aviation Organization (ICAO) is the United Nations agency created to promote aviation understanding, facilitation and security through cooperative multilateral regulation. In carrying out these broad responsibilities, ICAO establishes international standards for travel documents, in accordance with the Chicago Convention.
- The ICAO began to explore different approaches for machine readable travel documents (MRTDs) in meetings during 1969, culminating in 1980 with the publication of the first edition of Document 9303, titled “A Passport with Machine Readable Capability.”
- In 1995, ICAO clearly recognized the desirability of pursuing the use of biometrics in travel documents as the single best way to link the document and its rightful “owner.”
- In 1998, Malaysia became the first country to issue an electronic (aka, biometric) passport.
- **Globally interoperable Decentralized Digital Identity** - 193 Member States currently participate in ICAO MRTD program with 101 issuing e-Passports.

ICAO MRTD

ICAO Document 9303 defines:

- **Identity Cards**
  - TD1 Size Machine Readable Official Travel Documents
- **[Paper] Visas**
  - Specifications for TD2 Size Machine Readable Official Travel Documents (MROTDs)
  - Machine Readable Visas
- **Passports [Books]**
  - Specifications for Machine Readable Passports (MRPs) and other TD3 Size MRTDs

ICAO MRTD

We will focus on:

- **ePassports**
  - ePassport Books
  - ePassport Cards
- **DTC Type 1**
  - Virtual Component (VC)

ICAO MRTD

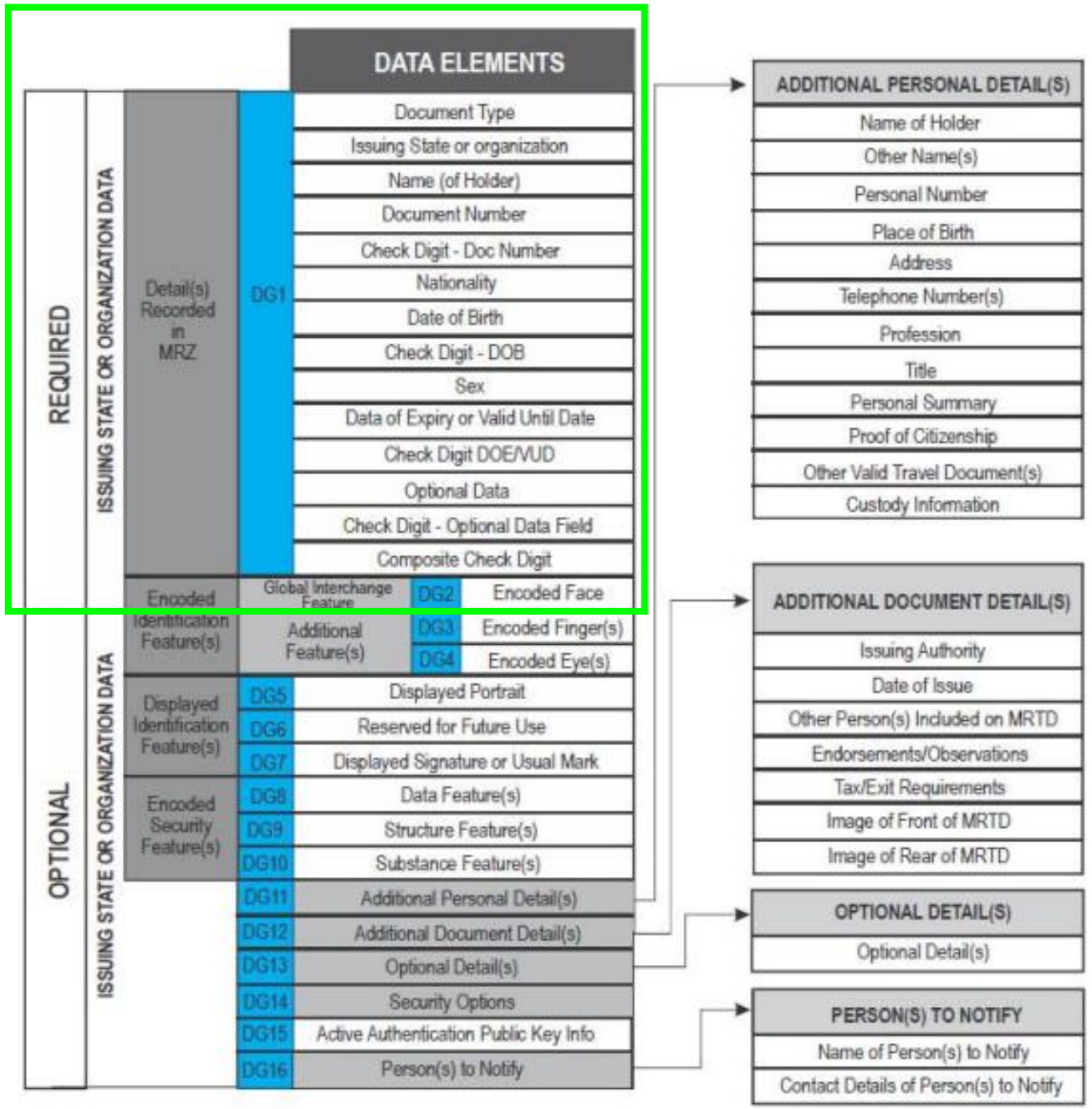
Logical Data Structure (LDS)

- *Current version 1.7*

ICAO Doc 9303 Machine Readable Travel Documents

Part 1: Introduction
Part 2: Specifications for the Security of the Design, Manufacture and Issuance of MRTDs
Part 3: Specifications Common to all MRTDs
Part 4: Specifications for Machine Readable Passports (MRPs) and other TD3 Size MRTDs
Part 5: Specifications for TD1 Size Machine Readable Official Travel Documents (MROTDs)
Part 6: Specifications for TD2 Size Machine Readable Official Travel Documents (MROTDs)
Part 7: Machine Readable Visas
Part 8: Emergency Travel Documents
Part 9: Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs
Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)
Part 11: Security Mechanisms for MRTDs
Part 12: Public Key Infrastructure for MRTDs
Part 13: Visible Digital Seals

https://www.icao.int/publications/pages/publication.aspx?docnum=9303



ICAO MRTD

Digital Travel Credentials (DTCs)

Technical Report Published

- **Type 1 -** eMRTD bound DTC – consist of a DTC-VC only, with the eMRTD as a physical authenticator
  - The virtual component is an exact copy of the electronic document data, with exceptions noted
  - In accordance with the guiding principles, an eMRTD bound DTC is considered to be issued by a Travel Document Issuing Authority, because it is derived from the Authority's data
  - The traveller MUST have their physical eMRTD in their possession while traveling
- **Type 2** - eMRTD- PC bound – consists of DTC-VC and an DTC-PC in addition to the eMRTD
  - The physical device serves as the DTC-PC, with the eMRTD as the alternate or as a fallback
  - The virtual component will be an exact copy of the electronic document data, with exceptions noted in section 7
  - The VC contains a link to the physical component
  - The VC may contain additional data at the discretion of the issuing authority
  - The traveller SHOULD have their physical eMRTD in their possession while traveling
- **Type 3** - PC bound – consists of a DTC-VC and a DTC-PC but NO eMRTD
  - Only the physical device will serve as the DTC-PC
  - The virtual component will use the exact same data elements as defined in the logical data structure of Doc. 9303, with exceptions noted.
  - The VC may contain additional data at the discretion of the issuing authority
  - There SHALL be a distinguishable identifier to recognise the document as a virtual credential without an eMRTD as an alternate or as a fallback
  - May have its own document characteristics (ID [passport] number, validity period, digital signature, etc)

ICAO MRTD

DTC Type 1

Value		Comments
DTCContentInfo		
version	m	Value = v1
DTCData	m	
dtcSOD	c	MUST be present if DTC is eMRTD Bound or eMRTD-PC Bound. This field MUST NOT be present if DTC is PC Bound.
dtcDG1	m	
dtcDG2	m	
dtcDG3 – dtcDG16	o	
dtcSecurityInfo	c	See Section 2.1.2
DTCIdentifier	m	See Section 2.1.2.1
DTCDOE	m	See Section 2.1.2.2
SecurityInfos	m	See Section 2.1.2.3
ActiveAuthenticationPublicKeyInfo	c	See Section 2.1.2.4
dtcOtherInfos	o	The dtcOtherInfos is for internal State or organization use.
DTCTBS	c	Contains the hash value of each data value in DTCData. MUST be present if DTC is eMRTD-PC Bound or PC Bound. This field MUST NOT be present if DTC is eMRTD Bound.
DTCSignerInfo	c	MUST be present if DTC is eMRTD-PC Bound or PC Bound. This field MUST NOT be present if DTC is eMRTD Bound.

MUST NOT be present if DTC is eMRTD bound

ICAO MRTD

ICAO has been discussing these capabilities for several years under LDS 2.0 but they have not been operationalized [but are supported in DDI]:

- **Electronic Travel Stamps**
  - Standardized content and format, and protection from tampering.
  - The benefit of adding this travel data in digital format include greater consistency, enhanced security, and ease of access and viewing.
- **Electronic Visas**
  - Application will allow for electronic visas to be added to the document almost instantaneously, bolstering client service and reducing the costs associated with designing, shipping, and storing visas/travel stamps.
  - Adding the visa directly to the document also reduces the need to rely on databases containing this information, which could facilitate transit travel, support third party validation, and mitigate the impacts of network outages or connection errors.
- **Additional Biometrics Post Issuance**
  - The ability to add secondary biometrics (iris and fingerprint) post-issuance provides States with more choices in national policy regarding secondary biometric storage and trusted traveller programs.
  - In instances where the photo of the holder can no longer be used, States could add an updated photo of the holder, which could result in fewer replacement passports being issued, less unnecessary delays at border control, and more dependability on facial recognition.

ISO mDL

ISO MDL

ISO/IEC 18013-X INFORMATION TECHNOLOGY — PERSONAL IDENTIFICATION — ISO-COMPLIANT DRIVING LICENSE

- **ISO/IEC 18013-1:2018** PART 1: PHYSICAL CHARACTERISTICS AND BASIC DATA SET
- **ISO/IEC 18013-2:2020** PART 2: MACHINE-READABLE TECHNOLOGIES
- **ISO/IEC 18013-3:2017** PART 3: ACCESS CONTROL, AUTHENTICATION AND INTEGRITY VALIDATION
- **ISO/IEC 18013-3:2017/AMD 1:2022** PART 3: ACCESS CONTROL, AUTHENTICATION AND INTEGRITY VALIDATION - AMENDMENT 1: PACE PROTOCOL
- **ISO/IEC 18013-4:2019** PART 4: TEST METHODS
- **ISO/IEC 18013-5:2021** PART 5: MOBILE DRIVING LICENCE (MDL) APPLICATION
- **ISO/IEC AWI TS 18013-6** [UNDER DEVELOPMENT] PART 6: MDL TEST METHODS
- **ISO/IEC AWI TS 18013-7** [UNDER DEVELOPMENT] PART 7: MOBILE DRIVING LICENCE (MDL) ADD-ON FUNCTIONS
    - Unattended use cases
    - Issuer-verified mDLs

ISO MDL

ISO/IEC DIS 18013-5:2020(E)

Figure 1 shows the interfaces in scope for this document. The explanation of each interface is:

1) This is the interface between the issuing authority infrastructure and the mDL. This interface is out of scope for this document.
2) This is the interface between the mDL and the mDL Reader. This interface is specified in this document. The interface can be used for connection setup and for offline data retrieval.
3) This is the interface between the issuing authority infrastructure and the mDL Reader. This interface is specified in this document. The interface can be used for the online data retrieval method.

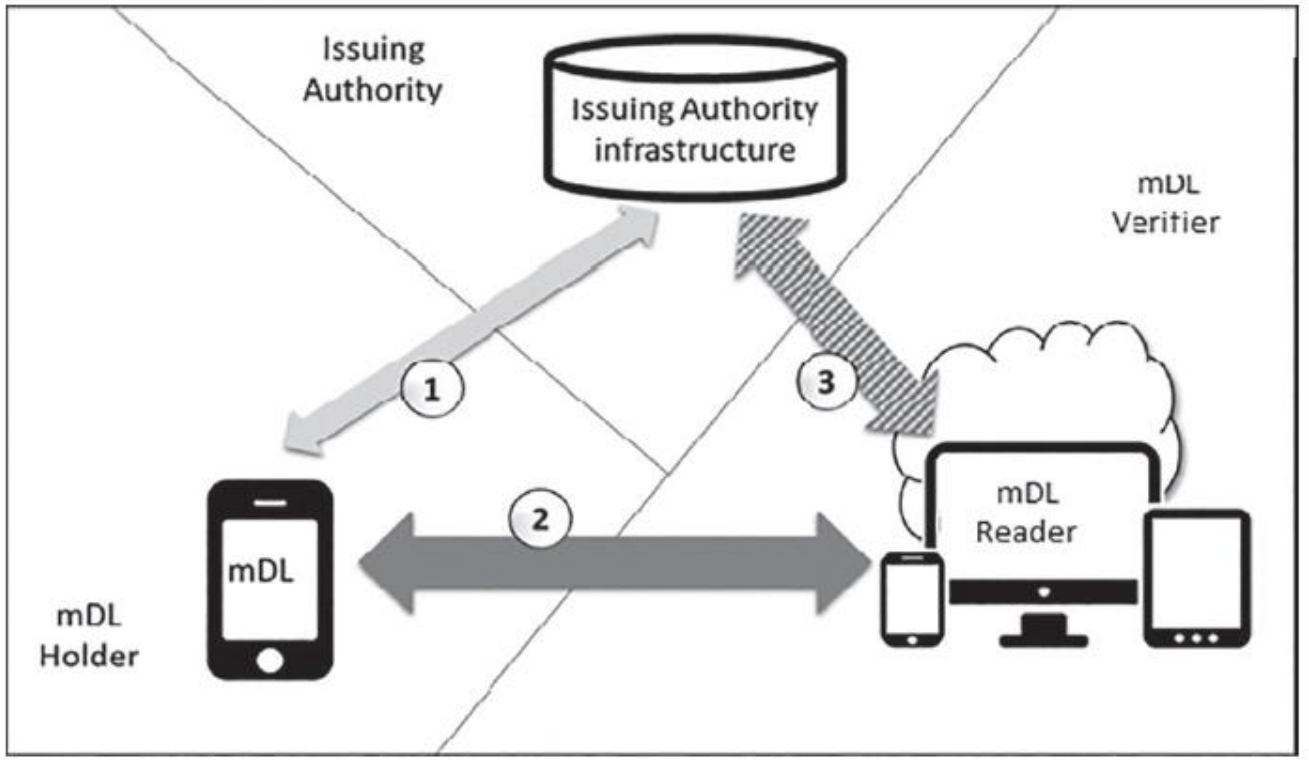
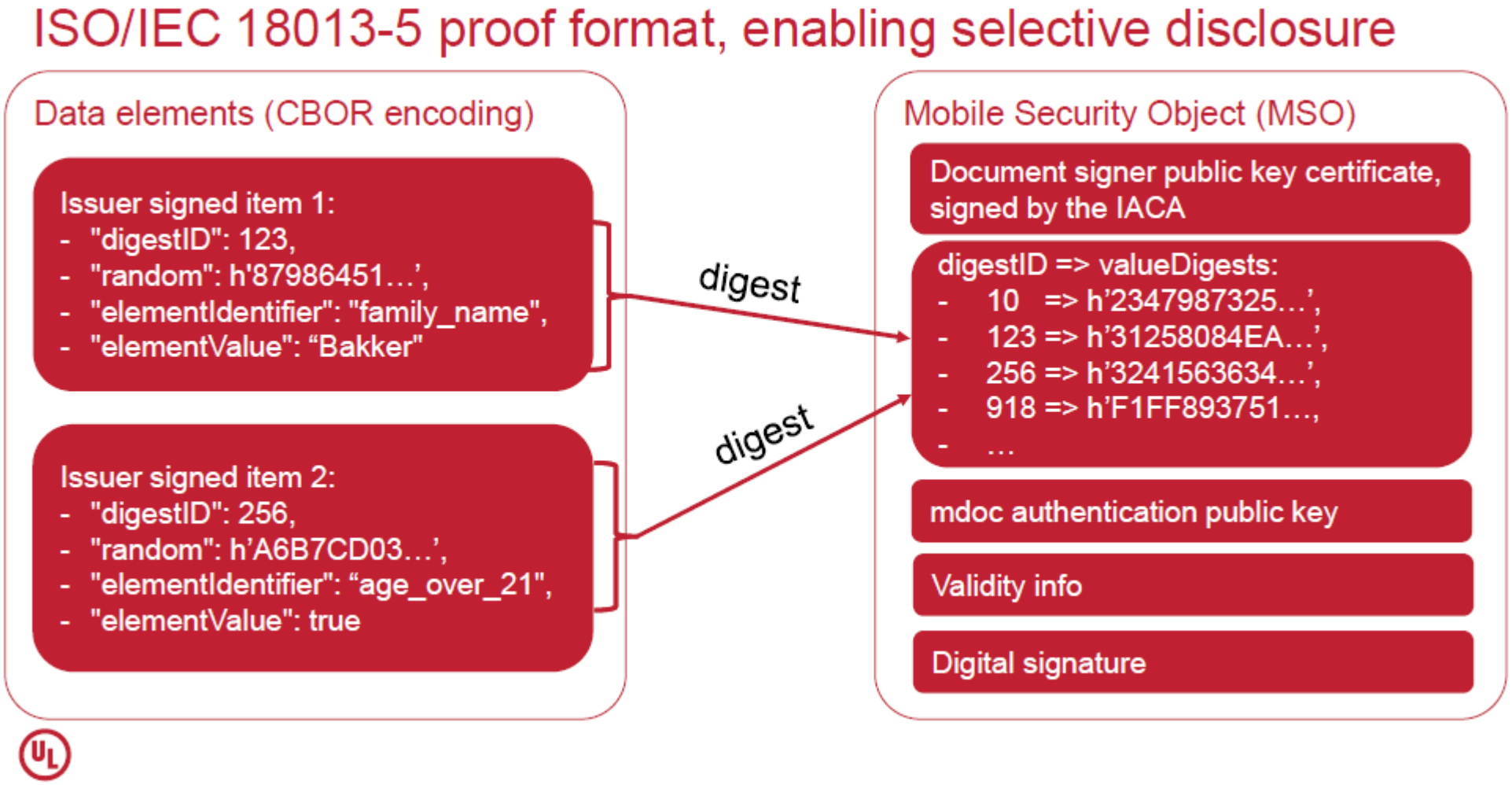


Figure 1 — mDL interfaces

ISO MDL



ISO MDL

Issuers can share verifiable information with Holder	
mDL	Out of scope for ISO/IEC 18013-5 (will be covered in ISO/IEC AWI TS 23220-3 which is currently under development)
SSI	In-scope through secure, pairwise pseudonymous channels

Issuers can revoke verifiable information shared with Holder	
mDL	Out of scope for ISO/IEC 18013-5 (expiry dates can be provisioned)
SSI	In-scope by utilising one of the available revocation methods

Holders can selectively disclose verifiable information	
mDL	Yes because each Issuing Authority creates a unique digest for each data element where the entire digest is signed by an MDOC Security Object during the issuance process using approved (e.g., NIST, BSI, ANSI) cryptographic algorithms for authentication
SSI	Yes, for each Verifiable Credential from each Issuer when JSON LD BBS+ or AnonCreds are used to create a Verifiable Presentation

ISO MDL

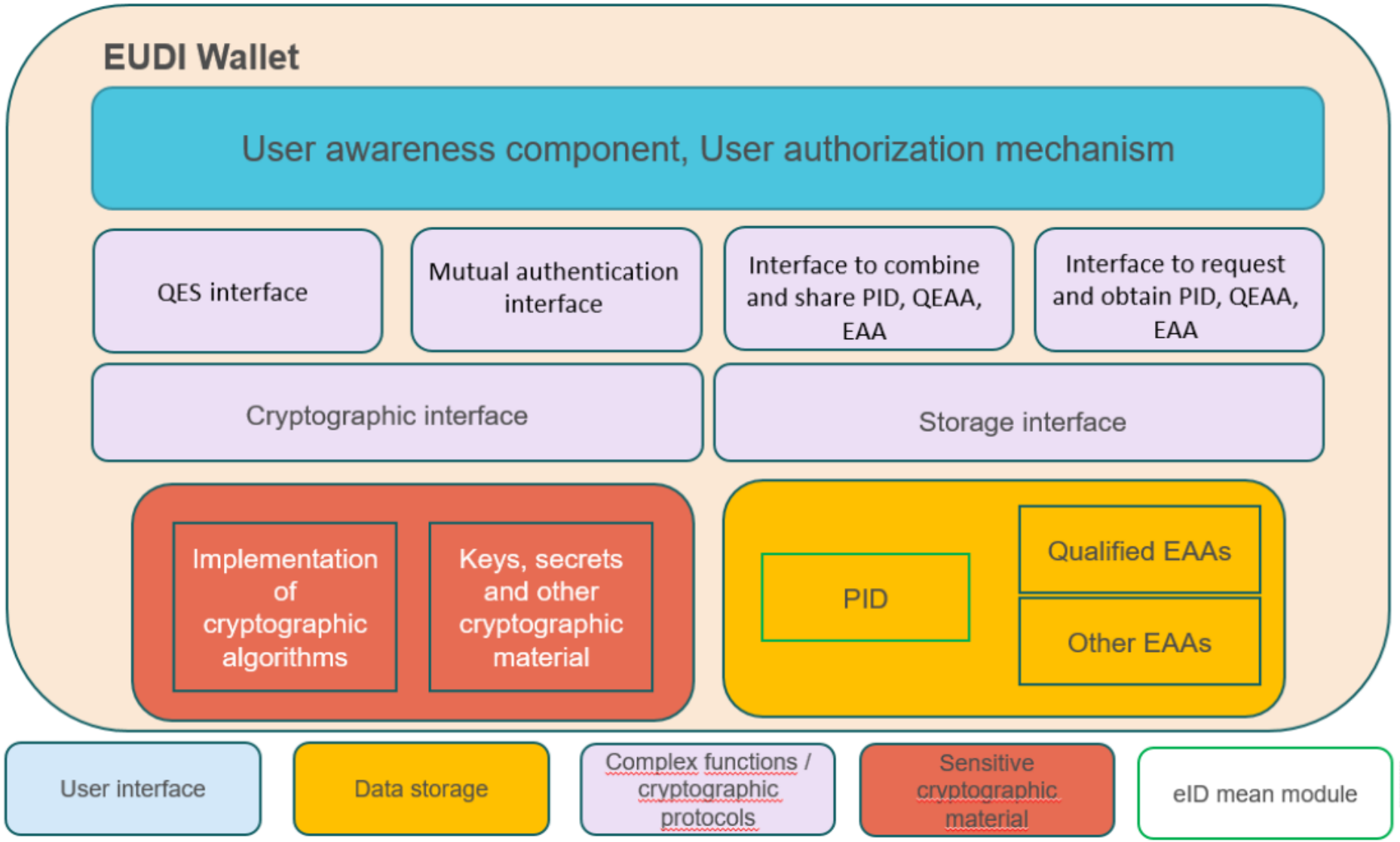
Holders can prove something without sharing personal information (ZKP)	
mDL	Yes, with predetermined, pre-negotiated predicates and variables such as “age over 18” [where age is the predicate and years is the variable]
SSI	Yes, for each Verifiable Claim within a Verifiable Credential and without predetermined predicates or variables when JSON LD BBS+ or AnonCreds are used to create a Verifiable Presentation

Verifiers can authenticate information	
mDL	Yes, by authenticating against each Issuer’s public key and using digests for each identity element
SSI	Yes, by referring to Decentralised Identifiers (containing public keys) that can be anchored both on decentralised public key infrastructures (DPKI’s) as well as with traditional centralised PKI’s

Verifiers can interpret the information	
mDL	Yes, by referring to nameSpace(s) for each Issuing Authority; e.g., AAMVA namespace for the collaborating driving license issuers of the US and Canada
SSI	Yes, by referring to Schema registries maintained by groups of Issuers that collaborate in a Trust Framework or within a shared Verifiable Data Registry

EIDAS REVSION

EIDAS REVISION



EIDAS REVISION

Edge Authentication to access Wallet:

Additionally, the EUDI Wallet shall require the user to use two-factor authentication in a combination of at least two authentication factors for certain use cases, satisfying the requirements for LOA high:

- ***a proof of knowledge;***
- ***a proof of possession;***
- ***a proof of inherence.***

EIDAS REVISION

With the proposed requirement of LOA High for user authentication which mandates multi-factor authentication where one factor may be “proof of inherence” we refer to (EU) 2015/1502 assurance levels for electronic identification for guidance:

Assurance level	Elements needed
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 recognised 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;

EES / ETIAS

DECENTRALIZED DIGITAL IDENTITY

(EU) 2017/2226 - establishing an **Entry/Exit System (EES)** to register entry and exit data … of third-country nationals crossing the external borders

Article 15

Facial image of third-country nationals

1. Where it is necessary to create an individual file or to update the facial image referred to in point (d) of Article 16(1) and point (b) of Article 17(1), the facial image shall be taken live.

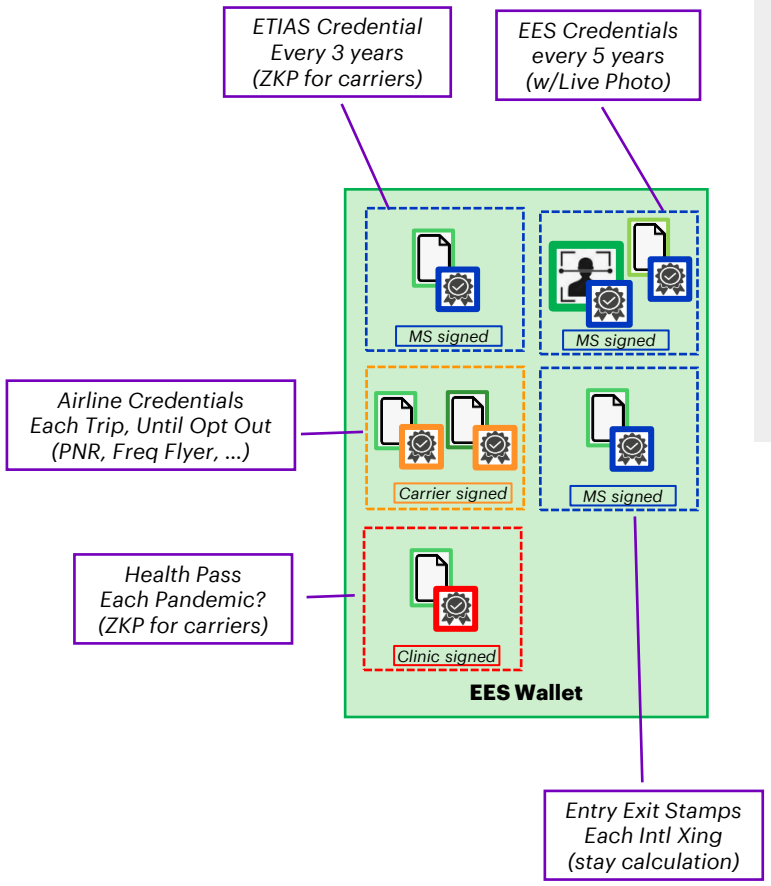
2. By way of derogation from paragraph 1, in exceptional cases where the quality and resolution specifications set for the enrolment of the live facial image in the EES cannot be met, the facial image may be extracted electronically from the chip of the electronic Machine Readable Travel Document (eMRTD). In such cases, the facial image shall only be inserted into the individual file after electronic verification that the facial image recorded in the chip of the eMRTD corresponds to the live facial image of the third-country national concerned.

3. Each Member State shall transmit once a year a report on the application of paragraph 2 to the Commission. That report shall include the number of third-country nationals concerned, as well as an explanation of the exceptional cases faced.

4. The facial image of third-country nationals shall have sufficient image resolution and quality to be used in automated biometric matching.

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R2226&rid=1

DECENTRALIZED DIGITAL IDENTITY



In-person Digitalization, including live image capture

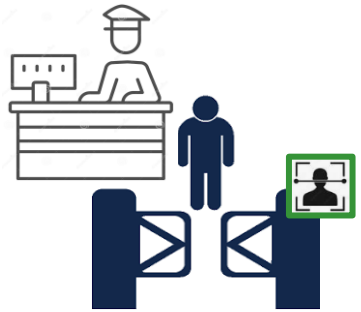
High LOA

- Consular Office,
- Registration Desk,
- Authorized 3rd Party,
- Supervised Remote

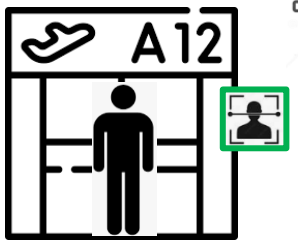
Contactless Check-In

Contactless Bag Drop

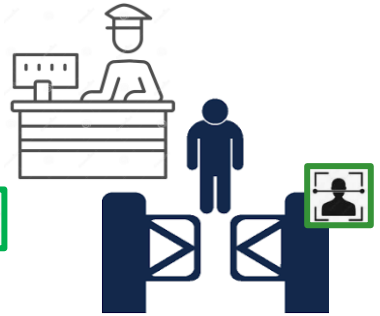
Contactless
Security Check Point



Contactless Arrival



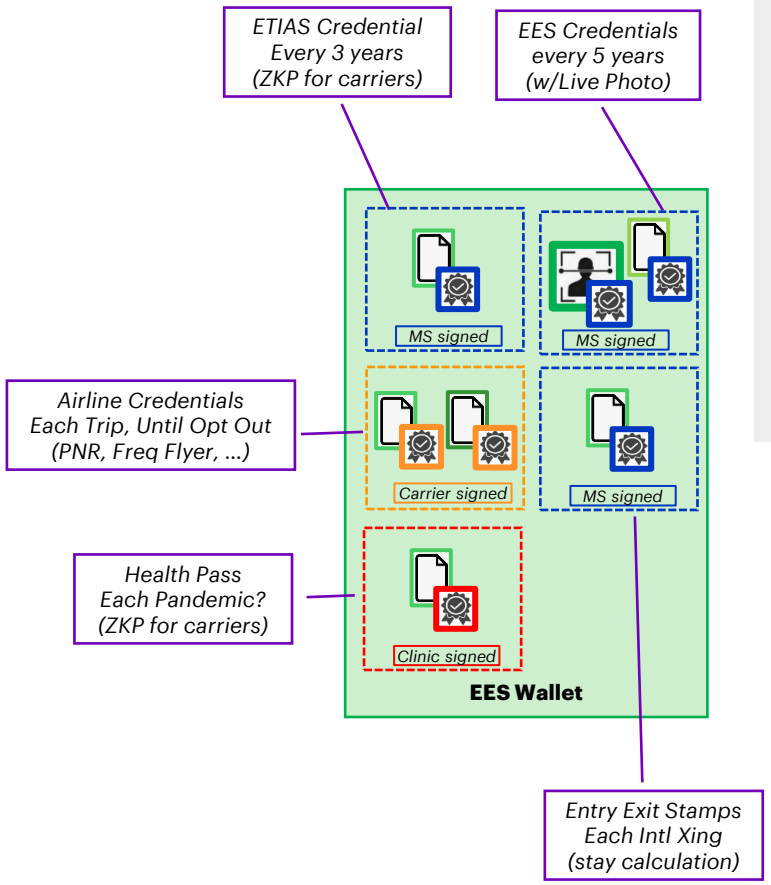
Contactless
Boarding



Contactless Exit
(where applicable)

Lounge Access /
Shopping

DECENTRALIZED DIGITAL IDENTITY



In-person Digitalization, including live image capture

High LOA

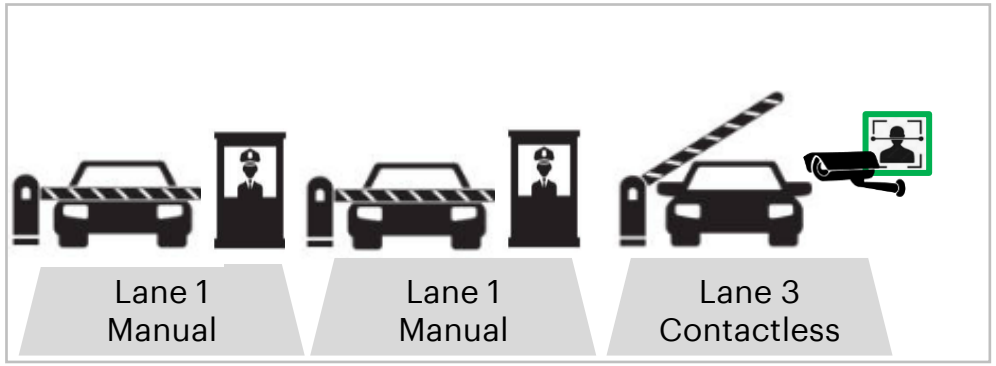
- Consular Office,
- Registration Desk,
- Authorized 3rd Party,
- Supervised Remote

Crossing Registration

- Traveler's EES Creds
- Traveler's ETIAS Creds
- Vehicle Info

Please use Lane 3
11-OCT-2022
Noon – 14:00

Lane 3
Approach



STANDARDS

ISO/IEC JTC 1/SC 17 Cards and security devices for personal identification

ISO/IEC JTC 1/SC 17/AG 1	Registration Management Group (RMG)	Working group
ISO/IEC JTC 1/SC 17/CAG 1	Chair's Advisory Group	Working group
ISO/IEC JTC 1/SC 17/WG 1	Physical characteristics and test methods for ID-cards	Working group
ISO/IEC JTC 1/SC 17/WG 3	Traveller identification	Working group
ISO/IEC JTC 1/SC 17/WG 4	Generic interfaces and protocols for security devices	Working group
ISO/IEC JTC 1/SC 17/WG 8	Integrated circuit cards without contacts	Working group
ISO/IEC JTC 1/SC 17/WG 10	Motor vehicle driver licence and related documents	Working group
ISO/IEC JTC 1/SC 17/WG 11	Application of biometrics to cards and personal identification	Working group
ISO/IEC JTC 1/SC 17/WG 12	Drone license and drone identity module	Working group
CEN/TC 224	Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment	
ISO/IEC JTC 1/SC 17/JWG ??	General purpose personal identification? Identity Wallets?	Joint Working Group?

CONTACT INFO

Daniel Bachenheimer
Digital Identity Innovations | Technology Lead
Office: Arlington, VA | USA
Direct: +1 703.947.1659 | Mobile: +1 202.251.7073
Email: daniel.bachenheimer@accenture.com

ISO/IEC SC 37 (Biometrics) Liaison Officer to TC 307 (Blockchain)
ISO/IEC SC 37 (Biometrics) Liaison to eu-LISA
ISO/IEC SC 37 (Biometrics) Liaison to Frontex