CY
FOR CYBERSECURITY

CONTACT

AUTHORS

ACKNOWLEDGEMENTS

LEGAL NOTICE

COPYRIGHT NOTICE

1. INTRODUCTION 6

1.1. PURPOSE OF THIS DOCUMENT 6

1.2. DIGITAL IDENTITY STANDARDS 6

1.3. RELATED EUROPEAN UNION LEGISLATION 7

2. SCOPE 8

2.1. BASIC MODEL 8

2.2. SCOPE OF THE ANALYSIS 10

3. SETTING THE SCENE 12

3.1. ROLE OF DIGITAL IDENTITY STANDARDS 12

3.2. STANDARDISATION ORGANISATIONS 12

3.3. TOPICS 17

4. ANALYSIS 18

4.1. EACH GROUP OF STANDARDS 18

4.2. GENERAL GROUPS OF STANDARDS 18

4.3. SPECIFIC GROUPS OF STANDARDS PROVIDING AUTHENTICATION CAPABILITIES 21

4.4. SPECIFIC GROUPS OF STANDARDS NOT PROVIDING AUTHENTICATION CAPABILITIES 48

4.5. SUMMARY 55

5. RECOMMENDATIONS 58

5.1. EUROPEAN UNION POLICYMAKERS 58

5.2. EUROPEAN STANDARDISATION ORGANISATIONS 58

5.3. EUROPEAN UNION AGENCY FOR CYBERSECURITY 59

ANNEX: ANALYSIS – DIGITAL IDENTITY WALLETS 61

A.1. INTRODUCTION TO DIGITAL IDENTITY WALLETS 61

A.2. STANDARDS RELATING TO THE EUROPEAN DIGITAL IDENTITY WALLET 64

A.3. ANALYSIS 68

-
-
-
-
-
-

1.

1.1. PURPOSE OF THIS DOCUMENT

1.2. DIGITAL IDENTITY STANDARDS

-
-
-
-

1.3. RELATED EUROPEAN UNION LEGISLATION

2.

2.1. BASIC MODEL

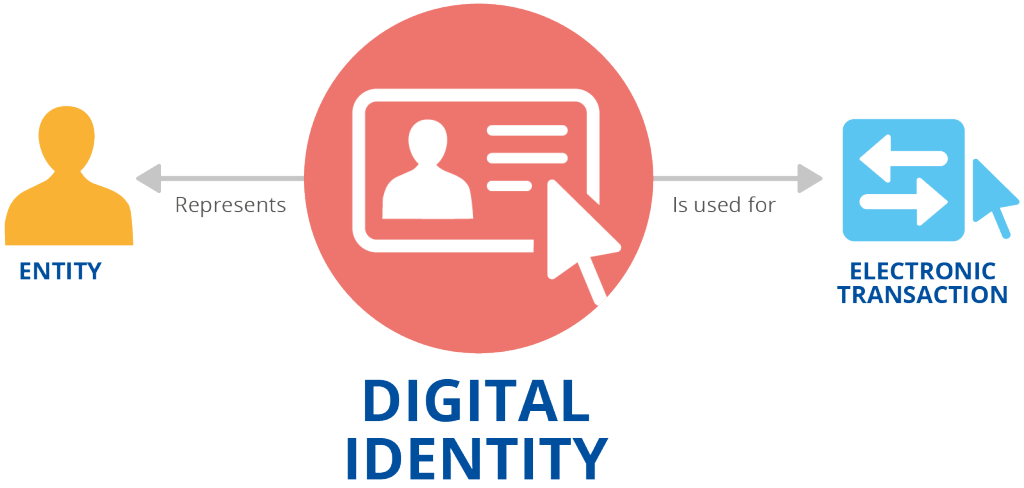
2.1.1. Digital identity

Digital identity **unique representation of a subject engaged in an online transaction**

Identity

set of attributes ... related to an entity

Figure 1:



2.1.2. Means to support digital identity

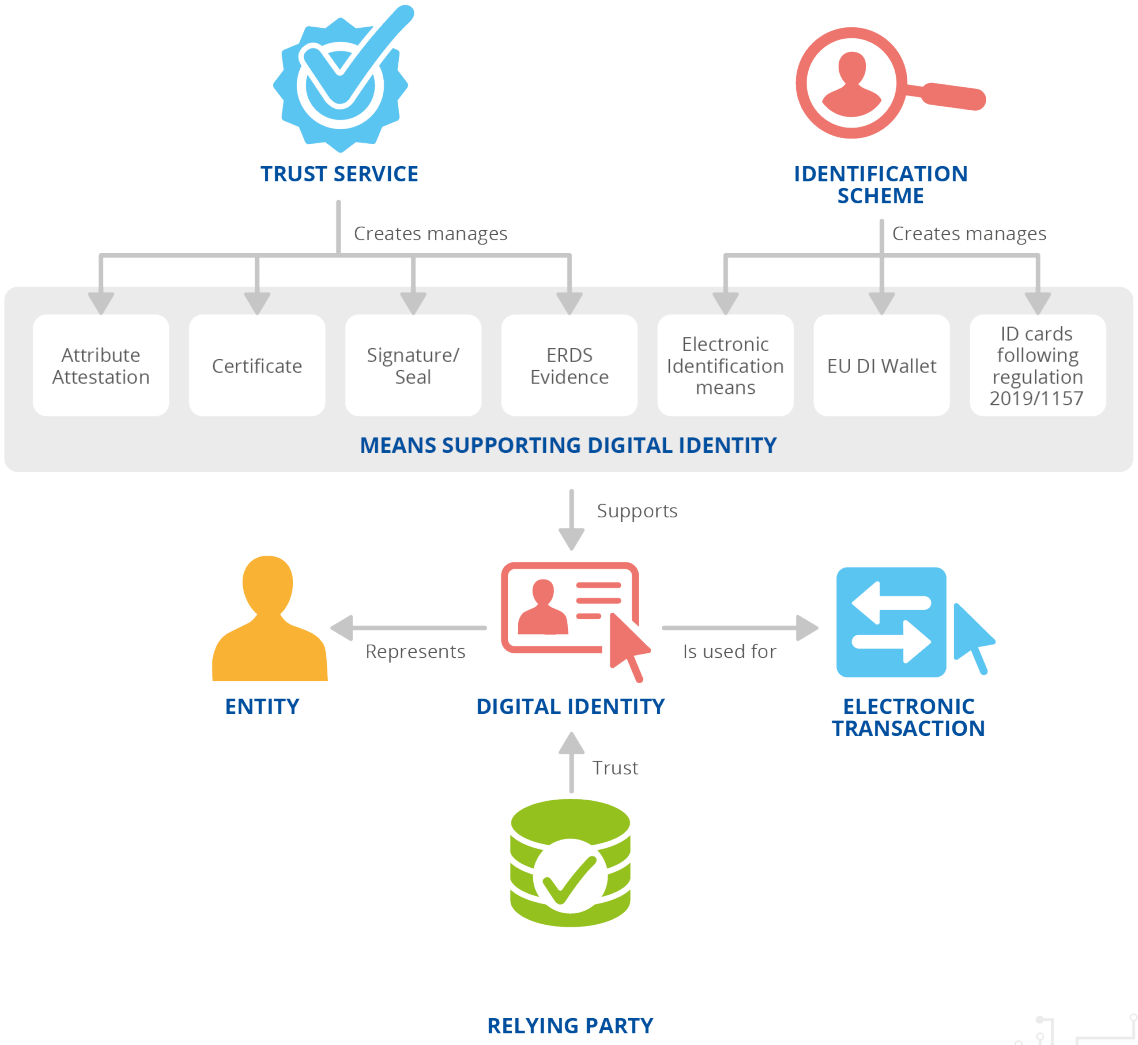
2.1.2.1. Means created and managed by trust services

-
-
-
-
-
-
-
-

2.1.2.2. Means created and managed by identification schemes

-
-
-

Figure 2



2.1.3. Supporting services

- **Timestamping authority.**

- **Signature validation service.**
- **Preservation service.**
- **Signature creation service.**

2.2. SCOPE OF THE ANALYSIS

3.

3.1. ROLE OF DIGITAL IDENTITY STANDARDS

3.2. STANDARDISATION ORGANISATIONS

3.2.1. European Standardisation Organisations (ESOs) and standards

-
-
-
-
-
-
-

-
-
-

3.2.2. International Standardisation Organisations (SDOs) and standards

-
-
-
-
-
-
-
-

3.2.3. National standardisation bodies and specialised agencies

- **ANSSI**
  -
  -
  -
- **BSI**
  -
  -
- **British Standards Institute**
  -
- **NIST**
  -
  -

3.2.4. Industrial bodies

- **Certification Authority Browser Forum**
  -
  -

- **Cloud Signature Consortium (CSC)**
  -
- **Financial Action Task Force (FATF)**
  -
- **FIDO**
  -
  -
-
  -
- **Organization for the Advancement of Structured Information Standards (OASIS)**
  -
- **OpenID**
  -
- **SOG-IS**
  -
- **World Wide Web Consortium (W3C)**

-
-
-

3.3. TOPICS

-
-
-
-
-
-
-
-
-
-
-
-

4.

4.1. EACH GROUP OF STANDARDS

-
-
-
-
-
-

4.2. GENERAL GROUPS OF STANDARDS

4.2.1. General standards used in identity management

-
-

-

4.2.1.1. Identity proofing

4.2.1.2. Biometrics

4.2.2. General standards used in trust services

4.2.2.1. Layer 1: trust anchor distribution

4.2.2.2. Layer 2: cryptographic standards

4.2.2.3. Layer 3: governance frameworks

-
-

-
-

4.2.2.4. Layer 4

4.3. SPECIFIC GROUPS OF STANDARDS PROVIDING AUTHENTICATION CAPABILITIES

4.3.1. International Civil Aviation Organization electronic machine-readable travel documents and the eIDAS token

4.3.1.1. Layer 1

4.3.1.2. Layer 2

Agents and devices

Authentication capabilities

-
-
-
-

may

-
-
-
-
-

4.3.1.3. Layer 3

Technical format: the logical data structure electronic machine-readable travel document structure

-
-

Governance frameworks

-

-
-
-
-

-
-

-
  -
  -
  -
-
  -
  -
-
-
-

-
-
-
-

-
-
-

4.3.1.4. Layer 4

4.3.1.5. Analysis

ICAO e-MRTDs and the eIDAS token	
Coverage of the identity management life cycle	
Maturity of the standards	
Authentication capabilities	
User sole control and dependencies	
Data-protection-enhancing technologies	
Trust model	

4.3.2. Mobile Driving Licence (mDL/mdoc) and Mobile eID

Authentication capabilities

-
-

4.3.2.3. Layer 3

Technical formats: mdoc CBOR and mdoc signed JWT

4.3.2.4. Layer 4

4.3.2.5. Analysis

mDLs/mdocs and mobile electronic identification	
Coverage of the identity management life cycle	
Maturity of the standards	
Authentication capabilities	
User sole control and dependencies	

Data-protection-enhancing technologies	
Trust model	

4.3.3. X.509 certificates (PKI-PMI)

4.3.3.1. Layer 1

4.3.3.2. Layer 2

Agents and devices

- **ISO/IEC 19790 and FIPS PUB 140-3**

- **CEN/TS 419 221, Parts 1–4, and CEN EN 419221-5**

Authentication capabilities

4.3.3.3. Layer 3

Technical formats: X.509 public key certificates and X.509 attribute certificates

-
-
-
-

-
-
-
-
  -

Governance frameworks

-
-
-
-

4.3.3.4. Layer 4

Sector-specific X.509 certificates

Governance frameworks

4.3.3.5. Analysis

eIDAS X.509 certificates (PKI/PMI)	
Coverage of the identity management life cycle	
Maturity of the standards	
Authentication capabilities	
User sole control and dependencies	
Data-protection-enhancing technologies	

Trust model	

4.3.4. Security Assertion Markup Language and the eIDAS regulation

-
-
-

-

4.3.4.1. Layer 1

-
-

-

4.3.4.2. Layer 2

Agents and devices

Authentication capabilities

4.3.4.3. Layer 3

Technical format: SAML assertion

- **Authentication**
- **Attribute.**
-

Governance framework

4.3.4.4. Layer 4

4.3.4.5. Analysis

SAML and the eIDAS regulation	
Coverage of the identity management life cycle	
Maturity of the standards	
Authentication capabilities	
User sole control and dependencies	
Data-protection-enhancing technologies	
Trust model	

4.3.5. OpenID Connect

4.3.5.1. Layer 1

4.3.5.2. Layer 2

Agents and devices

Authentication capabilities

4.3.5.5. Analysis

OpenID Connect / OpenID Connect with SIOP	
Coverage of the identity management life cycle	
Maturity of the standards	
Authentication capabilities	
User sole control and dependencies	
Data-protection-enhancing technologies	
Trust model	

4.3.6. FIDO2

-
-
-
-

-

4.3.6.1. Layer 1

4.3.6.2. Layer 2

Agents and devices

Authentication capabilities

4.3.6.3. Layer 3

Technical formats: Public credential source, authentication assertion

Trust model	

4.3.7. Self-Sovereign Identity

4.3.7.1. Layer 1

4.3.7.2. Layer 2

Agents and devices

Authentication capabilities

4.3.7.3. Layer 3

Technical formats: Verifiable Credentials/Presentations

4.3.7.4. Layer 4

4.3.7.5. Analysis

Self-Sovereing Identity	
Coverage of the identity management life cycle	
Maturity of the standards	
Authentication capabilities	
User sole control and dependencies	
Data-protection-enhancing technologies	
Trust model	

4.4. SPECIFIC GROUPS OF STANDARDS NOT PROVIDING AUTHENTICATION CAPABILITIES

4.4.1. Advanced electronic signature/seals (AdES)

4.4.1.1. Layer 1

4.4.1.2. Layer 2

Agents and devices

-
-
-
-
-
-

-

Authentication capabilities

4.4.1.3. Layer 3

Technical formats: CadES, XadES, PadES, AsIC, JadES

-
  -
-
  -
  -
-
  -

-
-
  -
  -
  -
-
-
-
-

Governance frameworks

-
-
-
    -
-
-
-

4.4.1.4. Layer 4

4.4.1.5. Analysis

Advanced electronic signature/seals (AdES)	
Coverage of the identity management life cycle	
Maturity of the standards	
Authentication capabilities	

User sole control and dependencies	
Data-protection-enhancing technologies	
Trust model	

4.4.2. ERDS evidence

4.4.2.1. Layer 1

4.4.2.2. Layer 2

4.4.2.3. Layer 3

Technical formats: ERDS evidence set

-
-

Governance frameworks

-
-
-
-

-
-
-
-

4.4.2.4. Layer 4

4.4.2.5. Analysis

ERDS evidence	
Coverage of the identity management life cycle	
Maturity of the standards	
Authentication capabilities	
User sole control and dependencies	
Data-protection-enhancing technologies	
Trust model	

4.5. SUMMARY

-

	eMRTD (ISO 7501 – ICAO 9303)	eIDAS Token (TR-03110-2)	mDL (ISO/IEC 18013-5)	mID (ISO/IEC 23220)	X509 PKI certificates (ISO/IEC 9594-8)	SAML eIDAS (ITU-T	OpenID Connect	OpenID Connect with SIOP	FIDO2 (ITU-T X.1277 and X.1278)	SSI
Formal standard										
Personal Identification Data (PID) format										
(Qualified) Electronic Attestation of Attributes format										
Subject's offline authentication										
Subject's online authentication (LoA)										
Relying party's offline authentication										
Relying party's online authentication										
Device binding (e.g. smart phone)										
Use of secure element (level of confidence)										

User sole control										
Initially designed for law enforcement										
Need of centralised identity provider										
Selective disclosure										
Non traceability/unlinkability										
Support for the identity management lifecycle										
Trust model										
Maturity of the standards										

5.

5.1. EUROPEAN UNION POLICYMAKERS

Recommendation 1

Recommendation 2

Recommendation 3

Recommendation 4

Recommendation 5

5.2. EUROPEAN STANDARDISATION ORGANISATIONS

Recommendation 6

Recommendation 7

Recommendation 8

-
-
-

Recommendation 9

Recommendation 10

5.3. EUROPEAN UNION AGENCY FOR CYBERSECURITY

Recommendation 11

standards

Recommendation 12

Recommendation 13

Recommendation 14

Recommendation 15

A.1. INTRODUCTION TO DIGITAL IDENTITY WALLETS

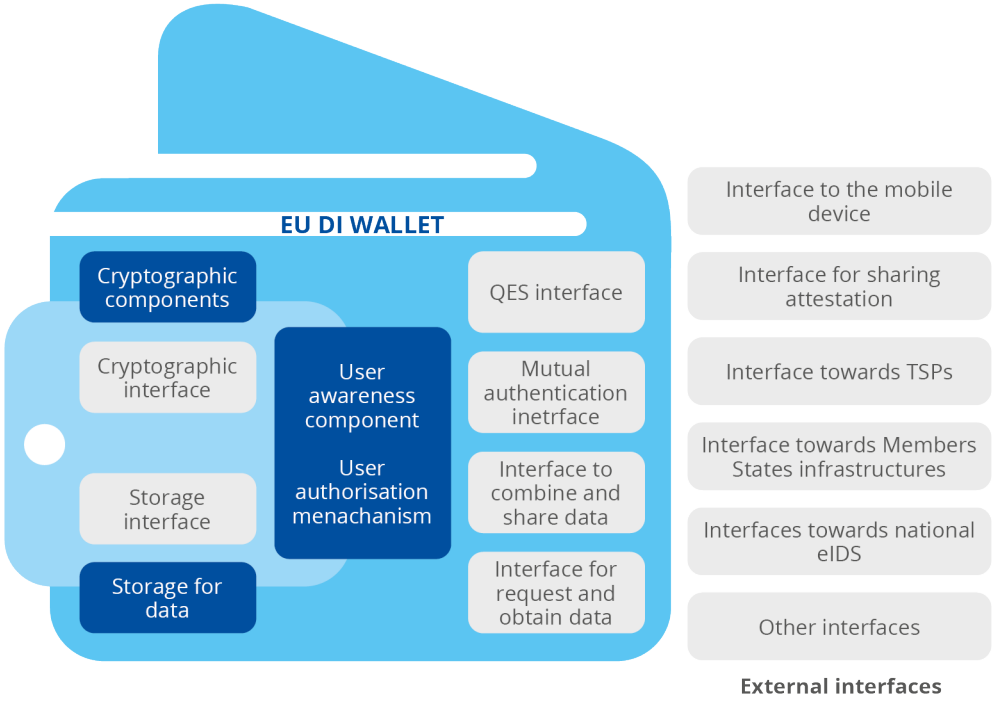
Digital Identity: Leveraging the SSI concept to build trust

European Digital Identity Architecture and Reference Framework Outline

European Digital Identity Architecture and Reference Framework Outline

European Digital Identity Architecture and Reference Framework Outline

Figure 3:


EU DI WALLET
Cryptographic components
Cryptographic interface
Storage interface
Storage for data
User awareness component
User authorisation menachanism
QES interface
Mutual authentication inetrface
Interface to combine and share data
Interface for request and obtain data
Interface to the mobile device
Interface for sharing attestation
Interface towards TSPs
Interface towards Members States infrastructures
Interfaces towards national eIDS
Other interfaces
External interfaces

-
-
-
-
-
-

-
-
-

-
-
-

-
-
-

-
-
-
-
-

Figure 4

The harmonised interfaces that allow direct access to the internal and external mobile device cryptographic security that the EUDI Wallet can use to perform cryptographic security functions are an essential and instrumental function.

Solution	Advantage	Disadvantage
Internal trusted execution environment (T.E.E.)		
External cryptographic device		
Remote cryptographic component		
Hybrid		

A.2. STANDARDS RELATING TO THE EUROPEAN DIGITAL IDENTITY WALLET

not to define the EUDI Wallet standards

Defining the ‘how’ would require specific work to set out a concrete interoperable implementation of the EUDI Wallet.

Name	Document reference	Standard supports wallet	Current version / publication year
Cards and security devices for personal identification – Building blocks for identity management via mobile devices – Part 1: Generic system architectures of mobile eID systems			
Cards and security devices for personal identification – Building blocks for identity management via mobile devices – Part 3: Protocols and services for installation and issuing phase			
Cards and security devices for personal identification – Building blocks for identity management via mobile devices – Part 4: Protocols and services for operational phase			
Cards and security devices for personal identification – Building blocks for identity management via mobile devices – Part 2: Data objects and encoding rules for generic eID-System			
QR Code bar code symbology specification			
Aztec Code bar code symbology specification			
Data Matrix bar code symbology specification			
Information technology – Automatic identification and data capture techniques – JAB			

Code polychrome bar code symbology specification			
Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures			
Concise Binary Object Representation (CBOR)			
CBOR Object Signing and Encryption (COSE)			
Client to Authenticator Protocol (CTAP)			

Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)	**ISO/IEC 18092:2013**	**Devices supporting the wallet**	**2013**
Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1) – Technical Corrigendum 1			
Near Field Communication; Interface and Protocol (NFCIP-1)			
Cards and security devices for personal identification – Building blocks for identity management via mobile devices – Part 5: Trust models and confidence level assessment			

A.3. ANALYSIS

European Digital Identity Architecture and Reference Framework Outline

major gaps

-
-

This functional requirement specification (FRS) must reference the relevant chapters of European and international standards when possible.

A.3.1. Functional requirements

Area	Standard	Applicability	Status
Functional Requirements			

Functional Testing Requirements			
Functional certification scheme			

Area	Standard	Applicability	Status
Requirements			
Functional Testing Requirements			
Functional certification scheme			

Area	Standard	Applicability	Status
Requirements			

Functional Testing Requirements			
Functional certification scheme			

Area	Standard	Applicability	Status
Requirements			

Functional Testing Requirements			
Functional certification scheme			

Area	Standard	Applicability	Status
Requirements			
	Self-Issued OpenID Provider v2	**Potential communication protocol for mutual authentication to relying party**	**Unspecified**
	RFC 8446 TLS 1.3	**Potential communication protocol for mutual authentication to relying party**	**Published**
	TR-03147	**Identity proofing requirements**	**Published**
Functional Testing Requirements			
Functional certification scheme	**Not available**		

Area	Standard	Applicability	Status
Requirements			

Functional testing requirements			
Functional certification scheme			

Area	Standard	Applicability	Status
Requirements			
Functional testing requirements			

Functional certification scheme			

Area	Standard	Applicability	Status
Requirements			

Functional testing requirements			
Functional certification scheme			

A.3.2. Interface requirements

Area	Standard	Applicability	Status
Functional requirements			
Functional testing requirements			
Functional audit requirements			

Area	Standard	Applicability	Status
Requirements			
Functional testing requirements			
Functional audit requirements			

Area	Standard	Applicability	Status
Requirements			
Functional testing requirements			
Functional audit requirements			

Area	Standard	Applicability	Status
Requirements			
Functional testing requirements			

Functional audit requirements			

Area	Standard	Applicability	Status
Requirements			
Functional testing requirements			
Functional audit requirements			

Area	Standard	Applicability	Status
Requirements			
Functional testing requirements			
Functional audit requirements			

ABOUT ENISA

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu