

# Standards Inventory for the future of digital identity

## Deliverable 1: Reference Material

Scope:  
Standards  
EU Digital Identity Wallet  
Distributed Ledger Technologies  
Identity Proofing  
Verifiable Credential

Writer: [Mickaël Gaborit](#)

## Agenda

<b>1</b>	<b>INTRODUCTION</b>	<b>6</b>
1.1	RATIONALE	6
1.2	WHY BLOCKSTAND?	7
1.2.1	BLOCKCHAIN STANDARDIZATION EXPERTISE	7
1.2.2	SUPPORT FOR EUROPEAN STRATEGIC AUTONOMY	7
1.2.3	ENGAGEMENT AND COLLABORATION PLATFORM	7
1.2.4	INNOVATION AND FUTURE-PROOFING	8
1.2.5	ENSURING INTEROPERABILITY AND COMPLIANCE	8
1.3	SCOPE OF INTERNATIONAL ORGANIZATIONS	8
1.4	SCOPE OF NATIONAL ORGANIZATIONS	11
1.5	IMPACT	11
1.6	PURPOSE OF THE FINAL DOCUMENT	12
<b>2</b>	<b>REGULATORY REFERENCES</b>	<b>13</b>
2.1	EU BACKGROUND	13
2.2	EIDAS (ELECTRONIC IDENTIFICATION AUTHENTICATION AND TRUST SERVICES)	14
2.2.1	EIDAS WORKING GROUP	14
2.2.2	No 910/2014	14
2.2.3	CIR 2015/1501	14
2.2.4	CIR 2015/1502	14
2.2.5	PROPOSAL 2021/281 AMENDING No 910/2014	15
2.2.6	PROVISIONAL AGREEMENT 2021/0136	15
2.2.7	SSI EIDAS BRIDGE REFERENCE IMPLEMENTATION	15
2.3	CYBERSECURITY	15
2.3.1	2019/881	15
2.4	DRIVING LICENCES	15
2.4.1	2006/126/EC	15
2.5	EHEALTH	15
2.5.1	2011/24/EU	16
2.5.2	GUIDELINE ON THE ELECTRONIC EXCHANGE OF HEALTH DATA UNDER CROSS-BORDER DIRECTIVE 2011/24/EU (RELEASE 2)	16
2.6	EUROPASS	16
2.6.1	EDCL (EUROPEAN DIGITAL CREDENTIALS FOR LEARNING)	16
2.6.2	EDCI (EUROPEAN DIGITAL CREDENTIAL INFRASTRUCTURE)	16
2.6.3	EUROPASS - INTEROPERABILITY	17
<b>3</b>	<b>STANDARDIZATION REFERENCES</b>	<b>18</b>
3.1	ROLLING PLAN FOR ICT STANDARDISATION	18
3.2	EBSI (EUROPEAN BLOCKCHAIN SERVICES INFRASTRUCTURE)	18
3.2.1	EBSI API	18
3.2.2	EBSI VC FRAMEWORK	19
3.2.3	EBSI TOOLS	20
3.2.4	WALLET ARF (ARCHITECTURE AND REFERENCE FRAMEWORK)	20

# Standards Inventory for the future of digital identity

<b>3.3 AFNOR (ASSOCIATION FRANÇAISE DE NORMALISATION)</b>	<b>20</b>
3.3.1 COMMISSION DE NORMALISATION BLOCKCHAIN AFNOR/CN BLOCKCHAIN	21
3.3.2 PR NF Z64-951 - ÉTABLIR LA CONFIANCE DANS LES DONNÉES ENREGISTRÉES DANS LA BLOCKCHAIN	21
3.3.3 AFNOR/CN 171 - APPLICATIONS POUR L'ARCHIVAGE ET LA GESTION DU CYCLE DE VIE DU DOCUMENT	21
3.3.4 AFNOR NF Z42-013 - SPECIFICATIONS CONCERNING THE DESIGN AND THE OPERATION OF AN INFORMATION SYSTEM FOR ELECTRONIC INFORMATION PRESERVATION	21
<b>3.4 CEN (EUROPEAN COMMITTEE FOR STANDARDIZATION) AND CENELEC (EUROPEAN COMMITTEE FOR ELECTROTECHNICAL STANDARDIZATION)</b>	<b>22</b>
3.4.1 CEN/TC 224 - PERSONAL IDENTIFICATION & DEVICES	22
3.4.2 CEN/TS 16634:2014 - BIOMETRIC BORDER CONTROL RECOMMENDATIONS	25
3.4.3 CEN-CLC/JTC 19 - BLOCKCHAIN & DISTRIBUTED LEDGER	25
3.4.4 CEN EN 419 212-1 & 2 - APPLICATION INTERFACES FOR SECURE ELEMENTS USED AS QUALIFIED ELECTRONIC SIGNATURE (SEAL-) CREATION DEVICES	25
3.4.5 CEN EN 419 241-1 - TRUSTWORTHY SYSTEMS SUPPORTING SERVER SIGNING - PART 1: GENERAL SYSTEM SECURITY REQUIREMENTS	26
3.4.6 CEN EN 419 241-2 - TRUSTWORTHY SYSTEMS SUPPORTING SERVER SIGNING	26
3.4.7 CEN EN 419 221-5:2018 - PROTECTION PROFILES FOR TSP CRYPTOGRAPHIC MODULES	26
3.4.8 CEN/TC 251 - HEALTH INFORMATICS	27
<b>3.5 CSN (THE COMMONWEALTH STANDARDS NETWORK)</b>	<b>28</b>
3.5.1 CSN EN 419 211-2 - PROTECTION PROFILES FOR SECURE SIGNATURE CREATION DEVICE - PART 2: DEVICE WITH KEY GENERATION	28
<b>3.6 NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY)</b>	<b>28</b>
3.6.1 US-EU TRADE AND TECHNOLOGY COUNCIL - WORKING GROUP 1: TECHNOLOGY STANDARDS - SUBGROUP ON DIGITAL IDENTITY	28
3.6.2 NIST-800-63	29
3.6.3 NIST SP 800-160 Vol. 1 Rev. 1 - ENGINEERING TRUSTWORTHY SECURE SYSTEMS	29
<b>3.7 ENISA (EUROPEAN UNION AGENCY FOR CYBERSECURITY)</b>	<b>29</b>
3.7.1 ENISA SECURITY FRAMEWORK FOR QTSP	30
<b>3.8 ETSI (EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE)</b>	<b>30</b>
3.8.1 ETSI ISG PDL (INDUSTRY SPECIFICATION GROUP PERMISSIONED DISTRIBUTED LEDGER)	30
3.8.2 ETSI ISG IPE (IPV6 ENHANCED INNOVATION)	31
3.8.3 ETSI TC ESI (TECHNICAL COMMITTEE ELECTRONIC SIGNATURES AND TRUST INFRASTRUCTURES)	31
3.8.4 ETSI EN 319 401 - GENERAL POLICY REQUIREMENTS FOR TSP	31
3.8.5 ETSI TR 119 460 - SURVEY OF TECHNOLOGIES AND REGULATORY REQUIREMENTS FOR IDENTITY PROOFING FOR TRUST SERVICE SUBJECTS	31
3.8.6 ETSI TS 119 461 - ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI) - POLICY AND SECURITY REQUIREMENTS FOR TRUST SERVICE COMPONENTS PROVIDING IDENTITY PROOFING OF TRUST SERVICE SUBJECTS	31
3.8.7 ETSI TS 119 432 - ELECTRONIC SIGNATURES AND INFRASTRUCTURES (ESI) - PROTOCOLS FOR REMOTE DIGITAL SIGNATURE CREATION	32
3.8.8 DTS/ESI-0019471 - POLICY AND SECURITY REQUIREMENTS FOR ATTRIBUTE ATTESTATION SERVICES	33
3.8.9 DTS/ESI-0019472 - PROFILES FOR ATTRIBUTE ATTESTATIONS	33
3.8.10 DTS/ESI-0019462 - WALLET INTERFACES FOR TRUST SERVICES AND SIGNING	33
<b>3.9 ISO (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION)</b>	<b>34</b>
3.9.1 ISO/TC 46/SC 11 - ARCHIVES/RECORDS MANAGEMENT	34
3.9.2 ISO/TC 154 - PROCESSES, DATA ELEMENTS AND DOCUMENTS IN COMMERCE, INDUSTRY AND ADMINISTRATION	34
3.9.3 ISO/TC 321 - TRANSACTION ASSURANCE IN E-COMMERCE	35

## Standards Inventory for the future of digital identity

3.9.4	ISO/TC 215 - HEALTH INFORMATICS .....	35
3.9.5	ISO/TC 307 - BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGIES.....	35
3.9.6	ISO/TC 68/SC 8 - REFERENCE DATA FOR FINANCIAL SERVICES.....	39
3.9.7	ISO/TC 171/SC 1 - QUALITY, PRESERVATION AND INTEGRITY OF INFORMATION.....	39
<b>3.10</b>	<b>ISO/IEC JTC 1 .....</b>	<b>40</b>
3.10.1	ISO/IEC JTC 1/SC 37 - BIOMETRICS .....	40
3.10.2	ISO/IEC JTC 1/SC 27 - INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION .....	40
3.10.3	ISO/IEC JTC 1/SC 17 - CARDS AND SECURITY DEVICES FOR PERSONAL IDENTIFICATION.....	41
<b>3.11</b>	<b>ITU-T (INTERNATIONAL TELECOMMUNICATION UNION).....</b>	<b>42</b>
3.11.1	ITU-T SG3 - ECONOMIC AND POLICY ISSUES.....	42
3.11.2	ITU-T SG5: ENVIRONMENT, CLIMATE CHANGE AND CIRCULAR ECONOMY .....	42
3.11.3	ITU-T SG 11: SIGNALLING REQUIREMENTS, PROTOCOLS AND TEST SPECIFICATIONS.....	43
3.11.4	ITU-T SG13 - FUTURE NETWORKS, WITH FOCUS ON IMT-2020, CLOUD COMPUTING AND TRUSTED NETWORK INFRASTRUCTURE.....	43
3.11.5	ITU-T SG17 - SECURITY & IDENTITY MANAGEMENT.....	43
3.11.6	ITU-T SG20 - INTERNET OF THINGS, SMART CITIES AND COMMUNITIES.....	44
3.11.7	ITU X.509 .....	44
<b>3.12</b>	<b>UNECE (UNITED NATIONS ECONOMIC COMMISSION FOR EUROPE) .....</b>	<b>45</b>
<b>3.13</b>	<b>OASIS (ORGANIZATION FOR THE ADVANCEMENT OF STRUCTURED INFORMATION STANDARDS).....</b>	<b>46</b>
3.13.1	EEA COMMUNITY PROJECTS .....	46
3.13.2	EEA BASELINE PROTOCOL (STANDARD FOR UNIVERSAL VERIFIED STATE SYNCHRONIZATION & MULTIPARTY COORDINATION USING ZERO KNOWLEDGE).....	46
3.13.3	OASIS SECURITY SERVICES (SAML) TC .....	46
3.13.4	OASIS ELECTRONIC IDENTITY CREDENTIAL TRUST ELEVATION METHODS (TRUST ELEVATION) TC.....	46
3.13.5	OASIS DIGITAL SIGNATURE SERVICES EXTENDED (DSS-X) TC .....	46
3.13.6	OASIS EBXML MESSAGING SERVICES TC.....	47
3.13.7	OASIS BUSINESS DOCUMENT EXCHANGE (BDEX) TC .....	47
3.13.8	OASIS XRI DATA INTERCHANGE (XDI) TC (CLOSED).....	47
<b>3.14</b>	<b>OIDF (OPENID FOUNDATION).....</b>	<b>47</b>
3.14.1	WORKING GROUPS.....	47
3.14.2	STANDARDS.....	49
3.14.3	PARALLEL PROJECTS.....	50
<b>3.15</b>	<b>IETF (INTERNET ENGINEERING TASK FORCE) .....</b>	<b>50</b>
3.15.1	WORKING GROUPS.....	50
3.15.2	STANDARDS.....	52
<b>3.16</b>	<b>W3C (WORLD WIDE WEB CONSORTIUM).....</b>	<b>53</b>
3.16.1	W3C WORKING GROUP.....	53
3.16.2	W3C STANDARDS.....	53
3.16.3	W3C GITHUB PROJECTS.....	59
<b>3.17</b>	<b>DIF (DECENTRALIZED IDENTITY FOUNDATION).....</b>	<b>60</b>
3.17.1	WORKING GROUPS.....	60
3.17.2	DIF INTEROPERABILITY PROJECT.....	60
3.17.3	STANDARDS.....	60
<b>3.18</b>	<b>HYPERLEDGER.....</b>	<b>62</b>
3.18.1	ARIES .....	62
3.18.2	INDY.....	65

## Standards Inventory for the future of digital identity

<b>3.19</b>	<b>OWF (OPEN WALLET FOUNDATION)</b> .....	<b>65</b>
<b>3.20</b>	<b>INATBA (INTERNATIONAL ASSOCIATION OF TRUSTED BLOCKCHAIN APPLICATIONS)</b> .....	<b>65</b>
3.20.1	INATBA STANDARDS COMMITTEE .....	65
3.20.2	INATBA IDENTITY COMMITTEE .....	66
3.20.3	INATBA PRIVACY COMMITTEE .....	66
<b>3.21</b>	<b>EUBOF (EU BLOCKCHAIN OBSERVATORY AND FORUM)</b> .....	<b>66</b>
<b>3.22</b>	<b>KANTARA</b> .....	<b>66</b>
3.22.1	KANTARA USER-MANAGED ACCESS (UMA) 2.0 .....	66
3.22.2	KANTARA CONSENT RECEIPT SPECIFICATION .....	66
3.22.3	KANTARA BLINDING IDENTITY TAXONOMY .....	67
<b>3.23</b>	<b>IEEE (INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS)</b> .....	<b>67</b>
3.23.1	IEEE COMPUTER SOCIETY BLOCKCHAIN AND DISTRIBUTED LEDGERS (BDL) STANDARDS COMMITTEE 67	
3.23.2	IEEE CONSUMER TECHNOLOGY SOCIETY (CTSOC) STANDARDS COMMITTEE .....	67
<b>3.24</b>	<b>ICAO (INTERNATIONAL CIVIL AVIATION ORGANIZATION)</b> .....	<b>68</b>
3.24.1	ICAO Doc9303 - MACHINE READABLE TRAVEL DOCUMENTS .....	68
3.24.2	ICAO DTC - VIRTUAL COMPONENT DATA STRUCTURE AND PKI MECHANISMS .....	68
<b>3.25</b>	<b>EPC (EUROPEAN PAYMENTS COUNCIL)</b> .....	<b>68</b>
3.25.1	EPC004-16/ 2021 - SEPA INSTANT CREDIT TRANSFER - SCHEME RULEBOOK .....	68
3.25.2	EPC PSD3 (PAYMENT SERVICES DIRECTIVE) .....	69
<b>3.26</b>	<b>GSMA (GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS)</b> .....	<b>69</b>
3.26.1	GSMA SAM (SECURED APPLICATIONS FOR MOBILE) .....	69
3.26.2	GSMA EMBEDDED SIM .....	69
<b>3.27</b>	<b>CLOSED INITIATIVES</b> .....	<b>70</b>
3.27.1	E-SENS (ELECTRONIC SIMPLE EUROPEAN NETWORKED SERVICES) .....	70
3.27.2	STORK .....	70
3.27.3	SSEDIC (SCOPING THE SINGLE EUROPEAN DIGITAL IDENTITY COMMUNITY) .....	70
3.27.4	FIDIS (FUTURE OF IDENTITY IN THE INFORMATION SOCIETY) .....	70
3.27.5	PRIME - PRIVACY AND IDENTITY MANAGEMENT FOR EUROPE .....	70
3.27.6	ESSIF (EUROPEAN SELF SOVEREIGN IDENTITY FRAMEWORK) LABORATORY .....	71
<b>4</b>	<b><u>OTHER IDENTITY PROJECTS</u></b> .....	<b><u>72</u></b>
4.1	KERI (KEY EVENT RECEIPT INFRASTRUCTURE) .....	72
4.2	MATTR BBS+ SIGNATURE SCHEME .....	72
4.3	DIGITAL BAZAAR CREDENTIAL HANDLER API POLYFILL .....	72
4.4	SPRUCE DIDKIT .....	72
4.5	SCHEMA.ORG .....	73
4.6	PUBLIC SECTOR PROFILE OF THE PAN-CANADIAN TRUST FRAMEWORK .....	73

# 1 Introduction

## 1.1 Rationale

Digital Identity will be totally transformed (law, usages, standards), and every public or private organization should be aware about which standards are the basis to evaluate which standards will be transformed.

Consequently, they need a standard Inventory considering the future eIDAS rules and Wallet ARF (Architecture and Reference Framework) to ensure consistency, interoperability, and security in the implementation of electronic identification and authentication systems. This ARF is open to DLT.

Having a standard Inventory or set of standardized guidelines and best practices helps in the following ways:

- **Consistency:** A standard Inventory ensures that all organizations follow a common set of rules and practices, leading to consistent and uniform approaches to electronic identification and authentication. This consistency is crucial for seamless interactions between different systems and services.
- **Interoperability:** Standardization facilitates interoperability between various eIDAS-compliant systems, enabling smooth information exchange and interactions across different platforms. This interoperability is vital for public and private organizations to collaborate effectively and provide services to users seamlessly.
- **Security:** Adhering to standardized security measures helps organizations protect sensitive user data and ensures a higher level of cybersecurity. A standard Inventory can provide guidelines for implementing robust security protocols and safeguards against potential threats and vulnerabilities.
- **Compliance:** With future eIDAS rules and Reference Architecture Framework in mind, a standard Inventory can help organizations align with regulatory requirements and ensure compliance with relevant laws and guidelines. It provides a clear roadmap for organizations to follow while developing and deploying electronic identification and authentication systems.
- **Efficiency:** By following standardized practices, organizations can streamline their processes, reduce duplication of efforts, and achieve greater operational efficiency. This efficiency ultimately benefits both the organization and the users accessing their services.
- **Future-Proofing:** A standard Inventory can consider emerging technologies and evolving regulatory requirements, allowing organizations to future-proof their electronic identification and authentication systems. It enables organizations to stay ahead of the curve and adapt to changes in the digital landscape.

In summary, a standard Inventory is essential for public and private organizations to create a cohesive and robust ecosystem of electronic identification and authentication solutions. It fosters consistency,

interoperability, security, compliance, efficiency, and future readiness, all of which are vital for the successful implementation of eIDAS rules and Reference Architecture Framework.

### 1.2 Why Blockstand?

Blockstand is a pivotal initiative aimed at reinforcing the European Union's leadership in the global landscape of blockchain standardisation. This project underscores the significance of blockchain technology for the EU's industrial dominance on the international stage.

Blockstand's core mission is to ensure that the internationally applied standards in blockchain not only bolster European leadership in this cutting-edge domain but also reflect the continent's values and requirements. By coordinating the inputs of experts, Blockstand serves as a crucial instrument for supporting Europe's strategic autonomy, emphasizing the importance of blockchain standards that align with European principles and needs.

Utilizing Blockstand to create an inventory of standards impacting or impacted by the new eIDAS regulation was a logical step for several strategic and operational reasons, grounded in both the objectives of Blockstand and the significance of the eIDAS regulation in the context of Europe's digital transformation:

#### 1.2.1 Blockchain Standardization Expertise

Blockstand focuses on enhancing European leadership in global blockchain standardization. Since the eIDAS regulation plays a crucial role in establishing a regulatory framework for electronic identification and trust services across Europe, Blockstand's expertise in blockchain standardization could facilitate the integration of new blockchain standards and technologies within the eIDAS framework. This is particularly pertinent for aspects related to security, trust, and interoperability, which are fundamental to both the blockchain ecosystem and the eIDAS regulatory landscape.

#### 1.2.2 Support for European Strategic Autonomy

Blockstand aims to support European strategic autonomy in blockchain standardization, ensuring that international standards reflect European values and needs. The eIDAS regulation is central to the European Digital Single Market, aiming to enhance trust in electronic transactions. By aligning with Blockstand, there's an opportunity to ensure that the development and update of eIDAS-related standards are in harmony with European strategies and autonomy, especially in areas where blockchain technologies intersect with digital identity and trust services.

#### 1.2.3 Engagement and Collaboration Platform

Blockstand provides a platform for stakeholders to engage in standardization activities, offering a collaborative environment for experts, policymakers, and industry representatives. The eIDAS regulation necessitates broad consensus and alignment across different sectors and

## Standards Inventory for the future of digital identity

countries within the EU. Blockstand's infrastructure and community could serve as a crucial meeting ground for facilitating discussions, sharing best practices, and developing consensus on standards relevant to eIDAS.

### 1.2.4 Innovation and Future-Proofing





The eIDAS regulation is set to evolve with technological advancements and the changing needs of the digital economy. Blockstand's focus on blockchain implies a forward-looking approach to standardization, crucial for incorporating innovative solutions into the eIDAS framework. This includes exploring how distributed ledger technologies can enhance the security, efficiency, and interoperability of electronic identification and trust services.

### 1.2.5 Ensuring Interoperability and Compliance

Finally, Blockstand's work on creating a comprehensive inventory of blockchain standards can directly contribute to ensuring that new and existing eIDAS services are interoperable and compliant with emerging blockchain technologies. This is essential for the seamless operation of cross-border electronic transactions and services within the EU, promoting a cohesive and integrated Digital Single Market.

In summary, leveraging Blockstand's resources, expertise, and community platform for developing an inventory of eIDAS-impacting standards was a strategic choice to align blockchain innovation with EU regulatory frameworks, thereby supporting the digital and strategic autonomy of the European Union in the global digital landscape.

## 1.3 Scope of international organizations

Organizations		Scope	
	UNECE (United Nations Economic Commission for Europe)	Cross Border Trade	Global
	ICAO (International Civil Aviation Organization)	Aviation	Global
	IETF (Internet Engineering Task Force)	Internet	Global
	W3C (World Wide Web Consortium)	Internet	Global






## Standards Inventory for the future of digital identity

 <b>DIF</b>	DIF (Decentralized Identity Foundation)	Identity	Global
 <b>IEEE</b>	IEEE (Institute of Electrical and Electronics Engineers)	Electronics	Global
 <b>ISO</b>	ISO (International Organization for Standardization)	Standards	Global
 <b>ITU</b>	ITU-T (International Telecommunication Union)	Telecommunication	Global
 <b>GSMA™</b>	GSMA (Global System for Mobile communications)	Mobile Communications	Global
 <b>NIST</b>	NIST (National Institute of Standards and Technology)	Cybersecurity	US
 <b>eIDAS</b>	eIDAS (Electronic Identification Authentication and trust Services)	Digital Identity	Europe
 <b>CEN CENELEC</b>	CEN (European Committee for Standardization) and CENELEC (European Committee for Electrotechnical Standardization)	Standards	Europe
 <b>ebsi</b> European Blockchain	EBSI (European Blockchain Services Infrastructure)	Blockchain Trusted Ledgers	Europe
 <b>NGI</b> ESSIF-LAB	ESSIF (European Self Sovereign Identity Framework) Laboratory	Self-Sovereign Identity	Europe

## Standards Inventory for the future of digital identity

	ETSI (European Telecommunications Standards Institute)	Telecommunication	Europe
	ENISA (European Union Agency for Cybersecurity)	Cybersecurity	Europe
	EPC (European Payments Council)	Payment	Europe
	OIDF (OpenID Foundation)	Open Standards	Global
	OASIS (Organization for the Advancement of Structured Information Standards)	Open Standards	Global
	Kantara	Identity for Assurance	Global
	Hyperledger	Open Source Blockchain	Global
	OWF (Open Wallet Foundation)	Wallet	Global
	INATBA (International Association of Trusted Blockchain Applications)	Blockchain	Global
	EUBOF (EU Blockchain Observatory and Forum)	Blockchain	Europe

#### 1.4 Scope of national organizations

	SIS (Swedish Institute for Standards)	Standards	Sweden
	CSN (Commonwealth Standards Network)	Standards	Commonwealth of Nations
	AFNOR (Association Française de NORmalisation)	Standards	France

#### 1.5 Impact

Having a standard Inventory covering identity, certificates, e-signature, and secure elements in Europe can have several positive impacts:

- **Interoperability:** Standardization ensures that different systems and services across Europe can interact seamlessly, promoting cross-border interoperability. This facilitates the exchange of information and services, fostering a more connected and efficient digital environment.
- **Security:** A standardized approach enhances the security of digital identities, certificates, and e-signatures. It establishes consistent security measures and protocols, reducing vulnerabilities and enhancing protection against cyber threats and fraudulent activities.
- **Legal and Regulatory Compliance:** A standard Inventory ensures alignment with legal and regulatory requirements, such as those specified in eIDAS (Electronic Identification, Authentication, and Trust Services) Regulation. Compliance with such standards enhances trust and confidence in digital transactions within Europe.
- **User Trust and Confidence:** Standardization helps build trust and confidence among users in digital services and transactions. Users are more likely to adopt and use digital identity and signature solutions when they are backed by recognized and standardized frameworks.
- **Market Growth and Innovation:** A common standard encourages the growth and innovation of digital identity and signature solutions. Companies and startups can develop products and services more efficiently, knowing they conform to established standards, and this can foster healthy competition and spur technological advancements.
- **Cross-Border Services:** Standardization facilitates the provision of cross-border services within the EU. Users can access digital services across member states with greater ease, leading to improved efficiency and accessibility.

## Standards Inventory for the future of digital identity

- **Economic Benefits:** A harmonized approach to digital identity, certificates, e-signature, and secure elements can generate economic benefits. It streamlines processes, reduces operational costs, and encourages the adoption of digital services, contributing to overall economic growth.
- **Simplified User Experience:** Users benefit from a simplified and consistent user experience when interacting with various digital services across Europe.
- **Standardized processes** reduce confusion and friction, making it easier for individuals and businesses to engage in digital transactions.

In summary, having a standard Inventory for identity, certificates, e-signature, and secure elements in Europe creates a more secure, trusted, and efficient digital ecosystem. It promotes innovation, fosters cross-border services, and contributes to the growth of the European digital economy.

### 1.6 Purpose of the final document

This first deliverable is a curated collection of reference materials, including relevant standards organizations and technical specifications, to support further learning and understanding of the subject matter.

The second deliverable will be a comprehensive Standard Inventory Document, containing detailed guidelines, and description of standards for identity management, certificates, e-signature, and secure elements. It will cover topics such as authentication methods, digital certificates, cryptographic protocols, and security measures. It will contain a Summary Guide: A condensed version of the standard Inventory, providing a high-level overview of the key concepts and recommendations. This summary guide will be useful for quick reference and to introduce stakeholders to the main principles.

The last deliverable will be a comprehensive and practical guide for organizations, public and private. It will map following macro-features of wallet and identified standards:

- Secure Cryptographic Device
- Data Storage Components
- Wallet “PID/EAA Presentation” Creation Application (WCA)
- Wallet Driving Application (WDA)
- User interface
- Relying Party interface

## 2 Regulatory References

### 2.1 EU Background

In the context of the e-signatures Directive, in January 2010, the Commission mandated the ESOs to rationalise the standards for e-signatures and related trust services to form a coherent and up-to-date framework (mandate M/460).

The eIDAS Regulation adopted on 23 July 2014 addresses in one comprehensive piece of legislation, electronic identification, electronic signatures, electronic seals, electronic time stamping, electronic registered delivery services, electronic documents and certificate services for website authentication as core instruments for electronic transactions. To support the implementation of this highly technical regulation, further standardisation work will be needed. In the case of trust services, the planned secondary legislation refers extensively to the availability of standards as possible means to meet the regulatory requirements. Existing standards should be checked to take account of the protection of individuals with regard to personal data processing and the free movement of such data. Specific privacy by design standards should be identified and where needed developed. The accessibility needs of persons with disabilities should also be taken into account.

- 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
- Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework
- Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means
- Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification
- Commission Implementing Regulation (EU) 2015/806 of May 2015 laying down specifications relating to the form of EU trust mark for qualified trust Services
- Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies
- Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists
- Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down Standards for the security assessment of qualified signature on seal creation devices

## 2.2 eIDAS (Electronic IDentification Authentication and trust Services)

The “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”, which is commonly known as the “**eIDAS Regulation**” is expected to boost trust and efficiency for electronic transactions across Europe and beyond.

Within the framework of Mandate M / 460, which is an initiative of the European Commission with the objective of providing a coordinated response on the subject of the deployment of a single digital European market, ETSI (European Telecommunications Standards Institute) and CEN (European Committee for Standardization) and CENELEC (European Committee for Electrotechnical Standardization) were entrusted with the task of drawing up standards relating to the trust services provided for by eIDAS.

### 2.2.1 eIDAS Working Group

Group of [experts](#) dedicated to exchange of good practices and initiatives supporting electronic identification and trust services - Discuss and recommend solutions to proposed content for secondary legislation.

### 2.2.2 No 910/2014

Regulation (EU) [No 910/2014](#) (application at July 1st 2016, also known as [CIR 2015/1501](#)) 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.

A [provisional agreement on the Regulation amending Regulation \(EU\) No 910/2014](#) as regards establishing a framework for a European Digital Identity was reached on 8 November between the European Parliament and the Council.

### 2.2.3 CIR 2015/1501

This Regulation [CIR 2015/1501](#) (Commission Implementing Regulation) lays down **technical and operational requirements of the interoperability framework** in order to ensure the interoperability of the electronic identification schemes which Member States notify to the Commission.

### 2.2.4 CIR 2015/1502

The CIR 2015/1502 sets out **minimum technical specifications and procedures for assurance levels for electronic identification** means pursuant to Article 8(3) 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.

### 2.2.5 Proposal 2021/281 amending No 910/2014

The document [COM/2021/281 final](#) is a proposal amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.

### 2.2.6 Provisional agreement 2021/0136

A [provisional agreement](#) on the Regulation amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity was reached on 8 November between the European Parliament and the Council.

The [Council adopted the European framework for digital identity \(eID\) on 26<sup>th</sup> March 2024](#). The revised regulation will be published in the Official Journal of the EU in March or April 2024, and will enter into force twenty days after its publication. The regulation will be fully implemented by 2026.

### 2.2.7 SSI eIDAS Bridge reference implementation

The [SSI eIDAS bridge](#) is a pilot focusing on providing a cross-border identity solution compliant with the eIDAS trust framework. It opens a new way of implementing the eGovernment's once-only principle.

The eIDAS bridge refers to the component that will interconnect the SSI core solution to the eIDAS trust framework.

It allows anyone to issue credentials that can be trusted and ensures that the trust services provided by service providers who comply with the requirements in the Regulation can be accepted as evidence in legal proceedings.

## 2.3 Cybersecurity

### 2.3.1 2019/881

The document [32019R0881](#) is a regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)

## 2.4 Driving Licences

### 2.4.1 2006/126/EC

The document [32006L0126](#) was consolidated in 2020 within the [02006L0126-20201101](#) document.

## 2.5 eHealth

The [eHealth Network](#) is a voluntary network, set up under article 14 of Directive 2011/24/EU. It provides a platform of Member States' competent

authorities dealing with eHealth. The Joint Action supporting the eHealth Network (JAseHN) provides scientific and technical support to the Network.

### 2.5.1 2011/24/EU

The initial [32011L0024](#) directive of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare.

It was consolidated in the following [02011L0024-20140101](#) directive.

### 2.5.2 Guideline on the electronic exchange of health data under Cross-Border Directive 2011/24/EU (Release 2)

#### 2.5.2.1 Patient Summary for unscheduled care

This [guideline 2016112-co10](#) was adopted by consensus by the eHealth Network (21 November 2016).

#### 2.5.2.2 ePrescriptions and eDispensations

This [guideline 20161121-co91](#) was adopted by consensus by the eHealth Network (21 November 2016).

## 2.6 Europass

[Europass](#) is a free, personal tool for learning and working in Europe.

### 2.6.1 EDCL (European Digital Credentials for Learning)

[European Digital Credentials for Learning](#) are trust-worthy, digital records of learning achievements such as qualifications and diplomas. European Digital Credentials for Learning are signed by an issuing education and training institution and so have the same legal value as paper-based credentials. Receiving digital credentials is fast and simple.

Acting on the evident need to shift from paper-based certificates to digitally-signed credentials, the EU is stepping in to assist. The Commission is currently working on the EDCI (European Digital Credentials Infrastructure) which organisations can implement for free to issue digital credentials. The implementation will allow organisations to issue qualifications (like a degree or vocational training), apprenticeships or participation certificates efficiently through a secure, trustworthy and fraud-resistant digital infrastructure.

### 2.6.2 EDCI (European Digital Credentials Infrastructure)

The EDCI is a set of standards, services and software which allows institutions to issue digital, tamper-proof qualifications and other learning credentials within the European Education Area. With it learners, employers, education and training providers and other authorised bodies have a simple and trustworthy way of verifying the validity and authenticity of digital credentials.



### 2.6.3 Europass - Interoperability

New [Europass](#) promotes [interoperability](#) by defining a specific data model and vocabulary to express the information contained in Europass documents. This data model is realised in terms of an XML Schema as well as a JSON Schema which:

- describes the constraints on the structure and on the contents of Europass documents.
- establishes the preferred data interchange format between Europass and other software systems and applications.

The following schemas are downloadable on the Interoperability page.

2.6.3.1 Europass XML schema definition, v3.4.0

2.6.3.2 Europass XML schema documentation, v3.4.0

## 3 Standardization References

### 3.1 Rolling Plan for ICT standardisation

The [EU Rolling Plan](#) provides an overview of the needs for ICT standardisation activities to be undertaken in support of EU policy activities.

The Rolling Plan for ICT Standardisation is drafted by the European Commission in collaboration with the European Multi-Stakeholder Platform (MSP) on ICT Standardisation and is updated annually. It lists all the topics identified as EU policy priorities where standardisation, standards, or ICT technical specifications ought to play a key role in the implementation of the policy. It covers technologies of 'horizontal importance', ones whose application have a wide impact across different technical fields, in the context of ICT infrastructures and ICT standardisation.

This collection hosts the annual revisions of the plan in easy-to-access form and provides a platform to share and discuss standardisation activities included in the annual plans.

### 3.2 EBSI (European Blockchain Services Infrastructure)

The [EBSI](#) aims to leverage the power of blockchain for the public good. EBSI is an initiative of the European Commission and the European Blockchain Partnership.

EBSI would be structured as European Digital Infrastructure Consortium (EDIC), a legal framework established in December 2022 to enable member states to implement multi-country projects. This is based on the European Research Infrastructure Consortium model under which member states combine resources to build and run large and expensive science facilities.

EDICs, which should contribute to EU's Digital Decade 2030 objectives, are set up by the Commission in response to applications from at least three member states. The applicants are given a leading role in the governance of the projects, which can be based on new or existing infrastructure.

EBSI would be used for public administration, for example allowing Personal Identification Data, Driving Licenses and other documents to be recognized across the ledgers, and facilitating procedures such as VAT declarations. It could also support applications, such as the digital euro, or digital twins of cities, to help identify things like flood risks.

#### 3.2.1 EBSI API

EBSI offer [APIs](#) (application programming interface) for blockchain and identity solutions:

### 3.2.1.1 EBSI Authorisation API

EBSI Core Service responsible to issue Short Term Access Tokens to the EBSI Platform for legal entities, natural persons, and trusted Applications in exchange of their EBSI Verifiable Authorisation credential and their DID.

### 3.2.1.2 EBSI DID Registry API

Generic EBSI Core Service providing the capability of resolving EBSI Decentralised Identifiers (DIDs).

### 3.2.1.3 EBSI Ledger API

Use case applications access to all the available blockchain protocol interfaces and capabilities provided by the ledger nodes software running on MS hosted nodes.

### 3.2.1.4 EBSI Timestamp API

EBSI Core Service enabling to interact with the TimeStamp SC to timestamp hashes, supports timestamping records/versions (and linking the timestamps), verify timestamps.

### 3.2.1.5 EBSI Track and Trace API

Track and Trace (TnT) creates Proof of Origin.

### 3.2.1.6 EBSI Trusted Issuers Registry API

Generic decentralised registry holding information about trusted issuers, like public information, accreditations and other. All information is stored in the smart contract in form of Attribute envelopes (like Verifiable Credentials).

### 3.2.1.7 EBSI Trusted Policies Registry API

EBSI core service providing access to policies defined in Policies Registry Smart Contract.

### 3.2.1.8 EBSI Trusted Schemas Registry API

Register a new schema, update a registered schema, read and validate registered schemas.

## 3.2.2 EBSI VC Framework

EBSI offer tools and documentation needed to integrate solution with all systems that use the [EBSI framework for Verifiable Credentials](#).

### 3.2.2.1 EBSI VC Framework & W3C Verifiable Credentials

Learn more about the framework for Verifiable Credentials and Verifiable Presentations defined by W3C.

### 3.2.2.2 EBSI Data Models

Find information about the various data models used in EBSI, including those needed to build a Trust Chain, as well as use case-specific data models.

### 3.2.2.3 EBSI DID Methods

Discover the proposed EBSI Decentralized Identifiers Methods, as well as security considerations to follow.

### 3.2.2.4 EBSI E-signing and e-sealing

Find guidelines for issuers and holders on how to sign and seal a Verifiable Credential

### 3.2.2.5 EBSI Trust Model

Learn about the EBSI trust model and find out how to set up a Trust Chain.

### 3.2.2.6 EBSI Credential Status Framework

Find a general overview of revocation methods for Verifiable Credentials, as well as guidelines on choosing the right revocation strategy.

### 3.2.3 EBSI Tools

EBSI offers [toolkit](#) to streamline development, including smart contract compilers, APIs, tests, wallet services, and documentation about the libraries needed to interact with the EBSI ecosystem.

### 3.2.4 Wallet ARF (Architecture and Reference Framework)

The purpose of the [document](#) is to provide a set of the specifications needed to develop an interoperable European Digital Identity (EUDI) Wallet Solution based on common standards and practices.

The ARF is a living document, as part of a feedback loop. Its specifications will feed into the reference implementation (RI), which is the basis for and supports the large-scale pilots (LSPs), whose feedback and proposals feed back into the ARF.

As a document it has no legal standing, but LSPs should follow it for their pilots.

National implementations of wallets must be based on the RI, but can include their own software aiming to be open source and opt out of optional modules and plugins. There is a minimum set of modules, but details on these areas are pending.

## 3.3 AFNOR (Association Française de NORmalisation)

With 1,480 members of [AFNOR](#) Association, a workforce of 1,170, 39 offices in the world et 69,000 customers, the AFNOR Group designs and deploys solutions based on voluntary standards around the world. The Group serves the general interest in its standardization activities and provides services in such competitive sectors as training, professional and technical information and intelligence, assessment and certification.

4 business Units: Normalisation, Éditions, Compétences, certification.

### 3.3.1 Commission de Normalisation Blockchain AFNOR/CN BLOCKCHAIN

The Blockchain standardization commission brings together the players concerned, who define by consensus between the participants, the priorities to be given according to their specific needs and interests. Currently, the parties have defined priorities:

- terminology: define what is meant by blockchain (in technology, in law), agree on the necessary vocabulary, the taxonomy.
- architecture / modeling: conceptualize the architecture of a blockchain development based on use cases, distinguish the network / service layers, allow the definition of a functional model between the actors and the interfaces according to the exchanges of information, avoid fragmentation of technology, verify that the model allows all existing representations.

CN Blockchain covers the same field of activity as ISO/TC 307 Blockchain and electronic distributed ledger technologies.

### 3.3.2 PR NF Z64-951 - Établir la confiance dans les données enregistrées dans la blockchain

This [Standard](#) is in Design since 2020.

### 3.3.3 AFNOR/CN 171 - Applications pour l'archivage et la gestion du cycle de vie du document

This [commission](#) mirrors ISO/TC 171 "Document management applications".

CN 171 includes a "DIGITAL SAFE" working group in charge of a reference project on the preservation of documents in digital media.

### 3.3.4 AFNOR NF Z42-013 - Specifications concerning the design and the operation of an information system for electronic information preservation

The AFNOR NF Z42-013 [standard](#) becomes an international standard Published under the title "ISO 14641-1:2012 - Electronic archiving – Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation", the standard covers specifications for the design and operation of computer systems used for electronic archiving. A standard now available to companies around the world!

Shortly after the publication of the NF Z42-013 standard in 2009, AFNOR brought this document to the International Organization for Standardization (ISO) so that it could possibly be incorporated into an international standard.

Following this proposal and the involvement of the members of the French delegation to promote this standard, the ISO/TC 171/SC3 technical committee "Document management applications - General" organized a vote among the 14 member countries. Most members voted for the transposition of the French standard into an international standard.

Digital documents are used daily by companies or organizations. They can be opened in one click, received and distributed via e-mail... But their conservation is often necessary within a computer system.

The ISO 14641-1 standard allows companies to find out about the specifications relating to the technical and organizational measures to be implemented for the recording, archiving, consultation and communication of digital documents in order to ensure the conservation and integrity of these. These specifications aim to ensure that digital documents are captured, archived, returned and communicated in such a way that it is possible to ensure that the archived document retains the same value as the original document throughout the retention period. .

The standard is primarily aimed at organizations and companies wishing to implement computer systems in which they can archive digital documents. It also targets IT service companies and software publishers who wish to design systems to ensure the finality and integrity of digital documents and companies providing third-party digital document archiving services on behalf of their clients.

The AFNOR CN 171 commission has developed standard NF Z42-013 and contributed to [ISO 14641:2018](#).

### 3.4 CEN (European Committee for Standardization) and CENELEC (European Committee for Electrotechnical Standardization)

The European Committee for Standardization (CEN, French: Comité Européen de Normalisation) is a public standards organization whose mission is to foster the economy of the European Single Market and the wider European continent in global trading, the welfare of European citizens and the environment by providing an efficient infrastructure to interested parties for the development, maintenance and distribution of coherent sets of standards and specifications.

The CEN was founded in 1961. Its 34 national members work together to develop European Standards (ENs) in various sectors to build a European internal market for goods and services and to position Europe in the global economy. CEN is officially recognized as a European standards body by the European Union, European Free Trade Association and the United Kingdom; the other official European standards bodies are the European Committee for Electrotechnical Standardization (CENELEC) and the ETSI (European Telecommunications Standards Institute).

#### 3.4.1 CEN/TC 224 - Personal identification & devices

[CEN/TC 224](#) 'Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment' develops standards for strengthening the interoperability and security of personal identification and its related personal devices, systems, operations and privacy. CEN/TC 224 addresses sectors such as Government/Citizen, Transport, Banking, e-Health, as well as Consumers and

providers from the supply side such as card manufacturers, security technology, conformity assessment body and software manufacturers.

AFNOR is the technical secretariat.

#### 3.4.1.1 Working Groups

A specific Working Group CEN/TC 224/WG 20 is dedicated to European Digital Identity Wallets:

- CEN/TC 224/WG 11 - Transport applications
- CEN/TC 224/WG 17 - Protection Profiles in the context of SSCD
- CEN/TC 224/WG 18 - Biometrics
- CEN/TC 224/WG 19 - Breeder Documents
- CEN/TC 224/WG 20 - Ad Hoc Group on European Digital Identity Wallets

#### 3.4.1.2 CEN/TC 224/WG 20 - Ad Hoc Group on European Digital Identity Wallets

The [Ad Hoc Group](#) has met online five times and has at this moment 37 registered members

The work of the Ad Hoc Group has been focused on identifying and putting together relevant bricks

(1) in a Gap Analysis document, CEN/TC 224/WG 20 N 23. Relevant existing standards and standards work in progress has been identified but is not complete

(2). Missing work items have been identified in the Gap Analysis document

(3). The group has been working on a Gap Analysis as a roadmap and it is not yet finalized

(4). We have found overlaps in standards and also of work in progress which needs to be resolved.

Cooperation is needed between organizations working in the area of authentication and also organizations that are looking specifically focused on the eIDAS Wallet.

Liaison is required between involved parties within the EU, see attached Gap Analysis document, CEN/TC 224/WG20 N 23, (8). Focus is recommended on work related to the Wallet.

The Ad Hoc group recommends a NWI for the continuation of the Gap Analysis. A NWI proposal is drafted and attached to this report.

The Gap Analysis working document should be made available to ETSI/ESI and sent to Nick Pope, vice chair ETSI TC ESI.

Work in the area needs to continue and several outstanding questions need to be resolved.

### 3.4.1.3 Relevant standardization committees

The following international and European standardisation committees are relevant for CEN/TC 224:

- ISO/IEC JTC 1/SC 17 "Cards and personal identification"
- ISO/IEC JTC 1/SC 27 « IT Security techniques »
- ISO/IEC JTC1/SC37 « Biometrics »
- ISO/TC 68/SC 7 « Core Banking »
- CEN/TC 251 "Health informatics", for healthcare applications
- CEN/TC 278 "Road transport and traffic telematics", for surface transport applications
- CEN/TC225 "AIDC technologies"
- ETSI Electronic Signature Infrastructure Committee

### 3.4.1.4 Relevant European legislations

The following European legislations or policy initiatives are relevant for CEN/TC224:

- Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC on electronic signatures
- Directive 1995/46/EC on data protection and Regulation proposal on general data protection
- Directive 58/2002/EC on processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) and its amendment 2009/136/EC
- A series of other texts related to the processing of personal data: Regulation (EC) 45/2001, Commission Decisions 2001/497/EC, 2002/16/EC and 2004/915/EC, Directive 2006/24/EC and communications COM(2007) 228 final, COM(2007) 87 final, COM(2012) 10 final 2012/0010 (COD)
- Regulation 2252/2004 on Standards for security features and biometrics in passports and travel documents issued by Member State completed by the other related documents COM(2007)0619, C6-0359/2007 and 2007/0216(COD)
- Directive 2007/64/EC on payment services as well as the proposal of revision. The Green Paper of the European Commission "Towards an integrated European market for card, internet and mobile payments" and the Euro Retail Payment Board launches by the European Central Bank is a framework for CEN/TC224 for further standardisation activities
- The White Paper of the European Commission defining a roadmap to a Single European Transport Area - Towards a competitive and resource efficient transport system (2011).



### 3.4.2 CEN/TS 16634:2014 - Biometric Border Control Recommendations

[CEN/TS 16634:2014](#) 'Personal identification - Recommendations for using biometrics in European Automated Border Control' is a Technical Specification primarily focusing on biometric aspects of Automated Border Control (ABC) systems.

Drawing on the first European and international ABC deployments, it aims to disseminate best practice experiences with a view to ensure consistent security levels in European ABC deployments. Furthermore, the best practice recommendations given here shall help make border control authorities' processes more efficient, speeding up border clearance, and delivering an improved experience to travellers.

### 3.4.3 CEN-CLC/JTC 19 - Blockchain & Distributed Ledger

[CEN-CLC/JTC 19](#) 'Blockchain and Distributed Ledger Technologies' focuses on European requirements for Distributed Ledger Technologies and proceeds with the identification and possible adoption of standards already available or under development in other SDOs (especially ISO TC 307), which could support the EU Digital Single Market and/or EC Directives/Regulations. In the context of the revision of the rules on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation), CEN-CLC/JTC 19 will address the development of standards in support of electronic identification.

### 3.4.4 CEN EN 419 212-1 & 2 - Application interfaces for secure elements used as qualified electronic signature (seal-) creation devices

This standard describes an application interface and behaviour of the SSCD in the context of Identification, Authentication and Signature (IAS) services.

This multi-part document covers the following topics:

- Part 1: Introduction: This part introduces the different parts of the series and gives the main notions and common definitions.
- Part 2: Basic services: This part describes the specifications for signature (and seal) generation, including user verification, password-based authentication protocols, establishment of a secure channel and key generation. A specific annex deals with seal, and another one with remote signature.
- Part 3: Device authentication: This part describes device authentication protocols, including data structures, Card-Verifiable (CV) certificates and key management.
- Part 4: Privacy specific protocols: This document describes privacy specific protocols.
- Part 5: Trusted eServices: This document describes additional trusted e-services in the context of signature

including Client/Server authentication, role authentication, symmetric key transmission between a remote server and a SE, signature cryptographic verification.

### 3.4.5 CEN EN 419 241-1 - Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements

This [document](#) specifies security requirements and recommendations for Trustworthy Systems Supporting Server Signing (TW4S) that generate digital signatures.

The TW4S is composed at least of one Server Signing Application (SSA) and one Signature Creation Device (SCDev) or one remote Signature Creation Device.

A remote SCDev is a SCDev extended with remote control provided by a Signature Activation Module (SAM) executed in a tamper protected environment. This module uses the Signature Activation Data (SAD), collected through a Signature Activation Protocol (SAP), in order to guarantee with a high level of confidence that the signing keys are used under sole control of the signer.

The SSA uses a SCDev or a remote SCDev in order to generate, maintain and use the signing keys under the sole control of their authorized signer. Signing key import from CAs is out of scope.

So when the SSA uses a remote SCDev, the authorized signer remotely controls the signing key with a high level of confidence.

A TW4S is intended to deliver to the signer or to some other application, a digital signature created based on the data to be signed.

This standard:

- provides commonly recognized functional models of TW4S;
- specifies overall requirements that apply across all of the services identified in the functional model;
- specifies security requirements for each of the services identified in the TW4S;
- specifies security requirements for sensitive system components which may be used by the TW4S.

This standard is technology and protocol neutral and focuses on security requirements.

### 3.4.6 CEN EN 419 241-2 - Trustworthy Systems Supporting Server Signing

The [CEN EN 419 241 Part 2](#) is covering “Protection Profile for QSCD for Server Signing” (dated 2018-05-11)

### 3.4.7 CEN EN 419 221-5:2018 - Protection Profiles for TSP Cryptographic Modules

The CEN EN 419 221 Part 5 is covering “Cryptographic Module for Trust Services”.

### 3.4.8 CEN/TC 251 - Health informatics

Two standards establishing an International Patient Summary, EN 17269:2019 and CEN/TS 17288:2020, were recently developed by [CEN/TC 251](#) 'Health informatics'. These standards cover the requirements for exchanging a core, essential dataset of healthcare data to support the continuity of care for a patient, whenever and wherever it is needed

#### 3.4.8.1 EN 17269:2019 - The International Patient Summary

This [EN 17269:2019](#) standard formalises the dataset required to share information about the medical background and history of a patient from the patient's country of affiliation with a healthcare professional in another country where unscheduled treatment is required

#### 3.4.8.2 CEN/TS 17288:2020 - The International Patient Summary: Guideline for European Implementation

This [CEN/TS 17288:2020](#) Technical Specification (TS) provides implementation guidance to support the use of the International Patient Summary dataset in a European context.

The focus of this technical specification takes into consideration European specific jurisdictional requirements, needs and contexts that Europe requires to be satisfied for effective implementation.

It addresses both functional and non-functional requirements for the dataset's interchange. As part of the usability of the International Patient Summary, European perspectives, directives and regulations contextualise and add value to generic reference implementations for use by Member States.

The TS applies the refined European Interoperability Framework (ReEIF), which describes legal, organisational, semantic and technological considerations for interoperability. These considerations highlight the eHealth Network's (eHN) guidance for cross-border care and underpin the care process.

The TS formalises principles to support the safe and legitimate use of patient summary data and afford protection for efficient cross-border data interchange within scenarios for unscheduled care. This Technical Specification gives selection criteria and provides examples of various transport formats and terminologies shown to be suitable for interchanging the International Patient Summary dataset. Compliance, deployment & migration Guidance are also included. The TS distinguishes between cross-border only requirements for interchanging the dataset and those that are generally applicable within national borders.

### 3.5 CSN (The Commonwealth Standards Network)

The [CSN](#) aims to tackle non-tariff barriers and promote strong trade amongst all Commonwealth states through the participation, adoption and implementation of international standards.

The CSN aims to increase its members technical and institutional capacity to use and participate in the development of international standards via existing international standards organisations such as ISO and IEC. International standards play an important role in promoting productivity and efficiency, reducing costs, removing barriers to trade, and driving economic growth. As such, the CSN is especially relevant to National Standards Bodies (NSBs) from Commonwealth nations that are looking to boost their international trade capabilities.

#### 3.5.1 CSN EN 419 211-2 - Protection profiles for secure signature creation device - Part 2: Device with key generation

This [CSN EN 419211-2](#) European Standard specifies a protection profile for a secure signature creation device that may generate signing keys internally: secure signature creation device with key generation (SSCD KG).

### 3.6 NIST (National Institute of Standards and Technology)

The National Institute of Standards and Technology (NIST) is an agency of the United States Department of Commerce whose mission is to promote American innovation and industrial competitiveness.

NIST's activities are organized into physical science laboratory programs that include nanoscale science and technology, engineering, information technology, neutron research, material measurement, and physical measurement. From 1901 to 1988, the agency was named the National Bureau of Standards

#### 3.6.1 US-EU Trade and Technology Council - Working Group 1: Technology Standards - Subgroup on Digital Identity

Over the course of 2023, the Digital Identity Subgroup of the EU-US Trade and Technology Council (TTC) Working Group 1: Technology Standards (WG1) held a series of government-to-government technical exchanges between the European Commission (EC) and a US federal interagency group led by the National Institute of Standards and Technology (NIST) within the US Department of Commerce.

During a government-to-public workshop event held in Brussels in March 2023, the EC and the US government committed to undertake a transatlantic mapping exercise with the objective of finding commonalities between the EU and US approaches to digital identity, under the [WG1 Digital Identity Subgroup](#).

This subgroup has asked for feedback on the [DRAFT EU-US TTC WG-1 Digital Identity Mapping Exercise Report](#), as well as use cases and areas of potential US-EU cooperation on digital identity, by the end of February 2024.

### 3.6.2 NIST-800-63

Released in June 2017, the NIST Special Report 800-63-3 defines requirements for federal agencies implementing digital identity services.

These NIST standards are primarily concerned with ensuring that someone is who they say they are before granting them access to a digital service. These digital identity standards and other cybersecurity frameworks are part of a larger government strategy to reduce identity theft and fraud.

The NIST Special Publication (SP) 800-63 document suite provides technical requirements for federal agencies implementing digital identity services in a four-volume set:

- [SP 800-63-3 Digital Identity Guidelines](#)
- [SP 800-63A Enrollment and Identity Proofing](#)
- [SP 800-63B Authentication and Lifecycle Management](#)
- [SP 800-63C Federation and Assertions](#)

### 3.6.3 NIST SP 800-160 Vol. 1 Rev. 1 - Engineering Trustworthy Secure Systems

This [publication](#) describes a basis for establishing principles, concepts, activities, and tasks for engineering trustworthy secure systems. Such principles, concepts, activities, and tasks can be effectively applied within systems engineering efforts to foster a common mindset to deliver security for any system, regardless of the system's purpose, type, scope, size, complexity, or the stage of its system life cycle. The intent of this publication is to advance systems engineering in developing trustworthy systems for contested operational environments (generally referred to as systems security engineering) and to serve as a basis for developing educational and training programs, professional certifications, and other assessment criteria.

## 3.7 ENISA (European Union Agency for Cybersecurity)

[ENISA](#) was created in 2004 by EU Regulation No 460/2004 under the name of European Network and Information Security Agency.

ENISA's Regulation is the EU Regulation No 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing EU Regulation No 526/2013 (Cybersecurity Act).

The Agency works closely together with the EU Members States and other stakeholders to deliver advice and solutions as well as improving their cybersecurity capabilities. It also supports the development of a cooperative response to large-scale cross-border cybersecurity incidents or crises and since 2019, it has been drawing up cybersecurity certification schemes.

### 3.7.1 ENISA Security Framework for QTSP

This [document](#) proposes a security framework to achieve compliance with Article 19 of the eIDAS Regulation, to which both non-QTSP and QTSP (Qualified Trust Service Providers) are subject.

Nevertheless, Article 19.1 states that the security measures “shall ensure that the level of security is commensurate to the degree of risk”. to achieve compliance with Article 19 (valid for both, QTSPs and non-QTSPs), this series of documents recommend that the level of security implemented by non-QTSP, expected to follow ‘best practices’ when operating with due diligence, is equivalent to the one of QTSP. For this reason, the security practices applied by QTSPs are also relevant to – and can also be followed by – non-QTSPs.

### 3.8 ETSI (European Telecommunications Standards Institute)

Independent, not-for-profit, standardization organization in the field of information and communications. [ETSI](#) supports the development and testing of global technical standards for ICT-enabled systems, applications and services.

Under the standardisation mandate M/460 on e-signatures, [ETSI TC ESI](#) provided an initial set of upgraded and new standards within a rationalized framework. ETSI TC ESI provides standards for introducing the overall framework of standards, for trust service providers supporting digital signatures but also preservation services, edelivery services, for (remote) signature creation and validation, for cryptographic suites and for trust service status lists providers.

#### 3.8.1 ETSI ISG PDL (Industry Specification Group Permissioned Distributed Ledger)

[ETSI ISG PDL](#) is committed to analyse and provide the foundations for the operation of permissioned distributed ledgers, with the ultimate purpose of creating an open ecosystem of industrial solutions to be deployed by different sectors, fostering the application of these technologies, and therefore contributing to consolidating the trust and dependability on information technologies supported by global, open telecommunications networks. The ISG PDL incorporates research and new development results in the field as they become available, especially in aspects related to smart contracts, interoperability among ledgers, data management, and trust and reputation support. The group is actively working to facilitate the coordination and cooperation between relevant standardization bodies and open source projects. ETSI via ISG PDL has published Specifications on the Distributed Blockchain “Smart contracts” and “reference architecture”. It is now working on the Specification of Redactable Block, Block Hashing, Reputation, etc. and collaborating with TC ESI on eIDAS and in support of smart contracts in the Data Act proposal context.

### 3.8.2 ETSI ISG IPE (IPv6 Enhanced innovation)

[ISG IPE](#) studies how IPv6 could be applied to blockchain technology. The GR “IPv6-based Blockchain” outlines how the properties of IPv6, can be leveraged to achieve new direct payment mechanisms for users of the blockchain. IPE is working on GR “IPv6 and Cloud using Data Block Matrix for Food Supply Chain Tracking and Tracing” which introduces blockchain technology in the Food Supply Chain for food tracking and tracing.

### 3.8.3 ETSI TC ESI (Technical Committee Electronic Signatures And Trust Infrastructures)

[TC ESI](#) plans to work on policy and security requirements for use of ledgers as a trust service in support of smart contracts as well as on the use of EU Digital Identity Wallets and advanced and qualified electronic signatures / seals for identification with smart contracts. Such standards will support both the proposed Data Act and the proposed eIDAS2 regulation which establishes a framework for trust services in regard to the creation and maintenance of (qualified) electronic ledgers.

### 3.8.4 ETSI EN 319 401 - General Policy Requirements for TSP

The [ETSI EN 319 401](#) (Final draft V2.3.1) specifies general policy requirements relating to **Trust Service Providers** (TSPs) that are independent of the type of TSP. It defines policy requirements on the operation and management practices of TSPs.

Other specifications refine and extend these requirements as applicable to particular forms of TSP. The present document does not specify how the requirements identified can be assessed by an independent party, including requirements for information to be made available to such independent assessors, or requirements on such assessors.

### 3.8.5 ETSI TR 119 460 - Survey of technologies and regulatory requirements for identity proofing for trust service subjects

The [ETSI TR 119 460](#) provides the results of a survey on the technologies, legislations, specifications, guidelines and standards related to or used for identity proofing. The present document provides a “point in time” picture of the identity proofing landscape at the time of edition, i.e. September 2020. It aims to be rather broad and serves as a basis for, ETSI DTS/ESI-0019461 *“Policy and security requirements for trust service components providing identity proofing of trust service subjects”* that addresses identity-proofing for trust service providers.

### 3.8.6 ETSI TS 119 461 - Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for trust service components providing identity proofing of trust service subjects

Identity proofing is the process of verifying with the required degree of reliability that the purported identity of an applicant is correct. The scope of the [ETSI TS 119 461](#) (**Electronic Signatures and Infrastructures** (ESI); Policy and security requirements for trust service components providing identity

proofing of trust service subjects) document is identity proofing of applicants to be enrolled as subjects or subscribers of a **Trust Service Provider (TSP)**.

Identity proofing can be carried out by the TSP as an integral part of the trust service provisioning. It can also be the task of a specialized **Identity Proofing Service Provider (IPSP)** acting as a subcontractor to the TSP; such a separate IPSP can provide services to several TSPs. The present document applies to both of these scenarios.

This document aims to meet the general requirements of the international community to provide trust and confidence in electronic transactions, including, amongst others, applicable requirements from Regulation (EU) No 910/2014.

This document poses policy and security requirements specific to identity proofing covering applicable technologies and use cases, resulting in identity proofing to a **Baseline Level of Identity Proofing (LoIP)** that is considered applicable to all relevant ETSI trust services standards.

### 3.8.7 ETSI TS 119 432 - Electronic Signatures and Infrastructures (ESI) - Protocols for remote digital signature creation

The present [document](#) specifies protocols and interfaces applicable when the process of creating AdES digital signatures as defined by ETSI TS 119 102-1 [i.7] and/or digital signature values, as result of Data To Be Signed Representations signatures, is carried out by a distributed solution comprised of two or more systems/services/components.

The present document is limited to remote server signing, i.e. the signing key is held in a remote shared service.

NOTE: Remote signature creation with local signing, i.e. the signing key is held with the signer's personal device but other steps in the signature creation are carried out by means of networked services, is a possible solution but protocols for such architecture are not covered in the present document.

Finally, the present document specifies two bindings, each one in a different syntax (XML and JSON), for each of the protocols mentioned above.

As far as it has been possible and suitable, the protocols have re-used constructs of CSC JSON and OASIS DSS-X XML specifications. When this has not been possible the present document specifies new components semantically and also syntactically in the two formats: XML and JSON.

The authorized signer's use of its key for signing requires users to provide multiple proofs of their claimed identity before being granted access to the needed set of resources. The way in which the user identity verification process is carried out by the service provider or any suggestion concerning



the usage of multi-factor authentication mechanisms is out of the scope of the present document.

### 3.8.8 DTS/ESI-0019471 - Policy and Security requirements for Attribute Attestation Services

Scope of work to be undertaken by the [DTS/ESI-0019471](#): The goal of this NWI is to specify policy and security requirements of attribute attestation trust service providers and the attribute attestation services they provide.

More specifically this WI shall specify:

- Policy and security requirements on attribute verification and generation of attestations by the trust service provider;
- Policy and security requirements on attribute attestation status validation services;
- Requirements for assessing the trustworthiness of the attribute attestation; and
- Requirements on personal data processing

### 3.8.9 DTS/ESI-0019472 - Profiles for Attribute Attestations

The goal of the [DTS/ESI-0019472](#) is to specify profiles for Attribute Attestations. More specifically this WI shall specify:

- Semantics for the components of attribute attestations. This will include, among others, information as listed in Annex V of eIDAS 2.0.
- Binding of semantics to one or more syntaxes.

The work to be done will assess a range of syntaxes such as Verifiable Credentials, SAML, JWT, X.509 Attribute Certificates and others.

The standard will not limit the types of attributes carried in an Attribute Assertion.

Separate standardization may be required to define interfaces for the management and use of Attribute Attestations.

### 3.8.10 DTS/ESI-0019462 - Wallet interfaces for trust services and signing

The goal of this [WI](#) is to specify interfaces enabling interaction of wallet and trust services including signing. More specifically this WI shall specify:

- A wallet interface to trust service providers for the purpose of issuing attribute attestations and certificates to the wallet;
- A wallet interface to trust service providers when acting as relying party in providing its services;
- An interface for creation of electronic signature where the QSCD is managed by TSP;
- Other use cases for the creation of electronic signatures and other trust services and possible requirements for interfaces;

This Work Item will take into account concurrent work on Attribute attestations policies and Attribute attestations profiles.

### 3.9 ISO (International Organization for Standardization)

#### 3.9.1 ISO/TC 46/SC 11 - Archives/records management

It is the ISO [Committee](#) responsible for developing standards on records/archives management. Our foundation standard is ISO 15489 Records management. Part 1 of this Standard has been revised and replaced in 2016 as ISO 15489 Records management - Principles and concepts, with other updated parts under development. In addition, we have a range of other standards and technical reports including the ISO 30300 series, Management systems for records. See the list of our standards and our current projects at the right. You can find more information in the Projects section.

##### 3.9.1.1 ISO/WD TR 24332 - Blockchain and Distributed Ledger Technology in relation to authoritative records, records systems, and records management

This [standard](#) is under development.

#### 3.9.2 ISO/TC 154 - Processes, data elements and documents in commerce, industry and administration

The ISO Technical Committee, [ISO/TC 154](#) addresses standardisation and registration of business, and administration processes and supporting data used for information interchange between and within individual organizations and supports standardisation activities in the area of industrial data.

Ongoing work:

- Requirements and roles & responsibilities for fulfilling trusted e-communications in commerce, industry and administration
- Qualified trust services for long-term signature of kinds of electronic documents
- Validation of long-term signature
- Trusted (or qualified) electronic registered delivery services (or platform)
- Dematerialisation and proof of dematerialisation
- Requirements for providing trusted e-communications in the mobile environment
- Requirements for providing trusted e-communications in the cloud environment

Projects include the ISO 14533 series of standards for Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles.

### 3.9.3 ISO/TC 321 - Transaction Assurance in e-Commerce

The ISO Technical Committee [ISO/TC 321](#) addresses standardisation in the field of “transaction assurance in e-commerce related upstream/downstream processes”, including the following:

- Assurance of transaction process in e-commerce (including easier access to e-platforms and estores);
- Protection of online consumer rights including both prevention of online disputes and resolution process;
- Interoperability and admissibility of inspection result data on commodity quality in cross-border e-commerce;
- Assurance of e-commerce delivery to the final consumer.

### 3.9.4 ISO/TC 215 - Health informatics

[ISO/TC 215](#) define the standardization in the field of health informatics, to facilitate capture, interchange and use of health-related data, information, and knowledge to support and enable all aspects of the health system.

#### 3.9.4.1 ISO 27269:2021 - Health informatics – International patient summary

The [ISO 27269:2021](#) document defines the core data set for a patient summary document that supports continuity of care for a person and coordination of their healthcare. It is specifically aimed at supporting the use case’ scenario for ‘unplanned, cross border care’ and is intended to be an international patient summary (IPS). Whilst the data set is minimal and non-exhaustive, it provides a robust, well-defined core set of data items. The tight focus on this use case also enables the IPS to be used in planned care. This means that both unplanned and planned care can be supported by this data set within local and national contexts, thereby increasing its utility and value.

It uses the European Guideline from the eHN as the initial source for the patient summary requirements, then takes into consideration other international patient summary projects to provide an interoperable data set specification that has global application.

This document provides an abstract definition of a Patient Summary from which derived models are implementable. Due to its nature therefore, readers should be aware that the compliance with this document does not imply automatic technical interoperability; this result, enabled by this document, can be reached with the conformity to standards indicated in the associated technical specification and implementation guides.

### 3.9.5 ISO/TC 307 - Blockchain and distributed ledger technologies

This technical committee is divided into 8-7 Working groups, and developing several [standards around Blockchain](#).

#### 3.9.5.1 ISO/TC 307/WG 2 Security, privacy and identity

The work of the working group WG 2 Security, privacy and identity **was transferred** in 2019 in the working group JWG 4 Joint ISO / TC 307 - [ISO /](#)

[IEC JTC 1/ SC 27 WG](#): Blockchain and distributed ledger technologies and IT Security techniques.

### 3.9.5.2 ISO/TC 307/WG 3 Smart contracts and their applications

This WG published the [ISO/TR 23455:2019](#) named “Blockchain and distributed ledger technologies – Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems”

This document provides an overview of smart contracts in BC/DLT systems; describing what smart contracts are and how they work. It also discusses methods of interaction between multiple smart contracts. This document focuses on technical aspects of smart contracts. Smart contracts for legally binding use and applications will only be briefly mentioned in this document.

### 3.9.5.3 ISO/TC 307/JWG 4 Joint ISO/IEC JTC 1/SC 27 WG: Security, privacy and identity for Blockchain and DLT

Linked to ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection.

### 3.9.5.4 ISO/AWI 7603 - Decentralized Identity standard for the identification of subjects and objects (UD)

A [standard](#) for the design and use of decentralized and self-sovereign identification of subjects (legal entities and natural persons) and objects, assets within the design of Blockchain and DLT Systems, in conjunction with Verifiable Credentials (VCs). The standard will refer to available identification standards from ISO as well as other standardization bodies, such as W3C, GLEIF, IETF, ITU, IEEE, etc. and non-standardization global consortiums, such as DIF, TOIP, and the Kantara Initiative.

Purpose is to support developers to deliver cost and time efficient development of high quality Blockchain and DLT systems for managing identity across a defined architectural stack. To create awareness of available standards of subjects (legal entities and natural persons) and objects and to give an overview of existing identifier standards.

### 3.9.5.5 ISO TS 23516 - Blockchain & DLT – Interoperability Framework

This [document](#) specifies a framework, recommendations and requirements for interoperability between DLT systems, between DLT and entities outside the DLT system, the relationship and interactions between these and cross-cutting aspects.

### 3.9.5.6 ISO 22739:2020 - Blockchain & DLT – Vocabulary (REPLACED)

This [document](#) provides fundamental terminology for blockchain and distributed ledger technologies.

Will be replaced by the following [ISO/CD 22739](#).

### 3.9.5.7 ISO/CD 22739 - Blockchain & DLT – Vocabulary

This [document](#) provides fundamental terminology for blockchain and distributed ledger technologies.

### 3.9.5.8 ISO/WD TR 6039 - Blockchain & DLT - Identifiers of subjects and objects for the design of blockchain systems

This [standard](#) is under development.

### 3.9.5.9 ISO/DTR 23644 - Blockchain & DLT - Overview of trust anchors for DLT-based identity management (TADIM) (UD)

This [standard](#) is under development.

### 3.9.5.10 ISO/WD TR 23642 - Blockchain & DLT - Overview of smart contract security good practice and issues (UD)

This [standard](#) is under development.

### 3.9.5.11 ISO/PRF TR 23247 - Blockchain & DLT - Overview of existing DLT systems for identity management

This [standard](#) is under development.

### 3.9.5.12 ISO/DTR 3242 - Blockchain & DLT - Use cases

This [standard](#) is under development.

### 3.9.5.13 ISO TS 23257:2022 - Blockchain & DLT - Reference Architecture

This [standard](#) was published in February 2022.

### 3.9.5.14 ISO/TS 23258:2021 - Blockchain & DLT – Taxonomy and Ontology

This [document](#) specifies a taxonomy and an ontology for blockchain and distributed ledger technologies (DLT). The taxonomy includes a taxonomy of concepts, a taxonomy of DLT systems and a taxonomy of application domains, purposes and economy activity sections for use cases. The ontology includes classes and attributes as well as relations between concepts.

The audience includes but is not limited to academics, architects, customers, users, tool developers, regulators, auditors and standards development organizations.

### 3.9.5.15 ISO TS 23259 - Blockchain & DLT – Legally binding smart contracts

This [standard](#) is under development.

### 3.9.5.16 ISO/TR 23576:2020 - Blockchain & DLT – Security management of digital asset custodians

This [document](#) discusses the threats, risks, and controls related to:

## Standards Inventory for the future of digital identity

- systems that provide digital asset custodian services and/or exchange services to their customers (consumers and businesses) and management of security when an incident occurs;
- asset information (including the signature key of the digital asset) that a custodian of digital assets manages.

This document is addressed to digital asset custodians that manage signature keys associated with digital asset accounts. In such a case, certain specific recommendations apply.

The following is out of scope of this document:

- core security controls of blockchain and DLT systems;
- business risks of digital asset custodians;
- segregation of customer's assets;
- governance and management issues.

### 3.9.5.17 ISO/NP 25126 - Information security controls based on ISO/IEC 27002 for distributed ledger services

This [standard](#) provides security controls and implementation guidance for distributed ledger service providers and distributed ledger service customers.

There is a strong need for standardisation to provide a baseline and structure for assurance and collaborative governance of DLT. This is particularly true across government organisations and regulated industry sectors. There is demand across all industry sectors, including but not limited to the use cases identified in ISO TR 3242:2022, Blockchain and distributed ledger technologies – Use cases. Areas where this is particularly important include cross-border financial services, cross-border trade and customs tariff management, supply chains involving controlled goods and regulated items.

With this standard, DLT service providers could enhance their security and potentially become certified. DLT service customers could use the certification to select their DLT service providers. Also, bodies performing audit and certification for DLT service providers could use the standard to review the information security controls according to this document. Financial industries already need to certify for ISO and a controls specific standard would assist anyone in this area. This would improve compliance, interoperability and collaboration across the financial sector and prospectively others to align all service providers, contractors and third parties to be uniform and measure/ evaluate them better.

Although there are national, international and industry standards for information security and cybersecurity, including for specific technologies such as cloud services, there are no DLT security standards available with sufficient controls that could be implemented and operated by the responsible governance bodies.

The intention is that this proposed standard should provide DLT specific controls and guidance that would be an extension of the ISO 27002 control set.

### 3.9.6 ISO/TC 68/SC 8 - Reference data for financial services

#### 3.9.6.1 ISO 17442-1:2020 - Legal entity identifier (LEI) – Part 1: Assignment

This [document](#) specifies the minimum elements of an unambiguous legal entity identifier (LEI) scheme to identify the legal entities relevant to any financial transaction.

#### 3.9.6.2 ISO 17442-2:2020 - Legal entity identifier (LEI) – Part 2: Application in digital certificates

This [document](#) specifies a standardised way of embedding the legal entity identifier (LEI) code, as represented in ISO 17442-1, in digital certificates, represented by the International Telecommunications Union (ITU) Recommendation X.509 and its ISO equivalent standard, ISO/IEC 9594-8.

It specifies the structure of a public key certificate conforming with ISO/IEC 9594-8 in which the LEI is embedded.

#### 3.9.6.3 ISO/WD TR 6277 - Blockchain and distributed ledger technologies - Data flow model for blockchain and DLT use cases (obsolete or under development?)

No more info about the [ISO TR 6277](#) standard.

Under Technical Committee: [ISO/TC 307](#) Blockchain and distributed ledger technologies.

### 3.9.7 ISO/TC 171/SC 1 - Quality, preservation and integrity of information

#### 3.9.7.1 ISO 14641-1:2012 - Electronic archiving – Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation

The scope of this [standard](#) is:

- Control processes
- Quality of input and output
- Production control, statistical evaluations
- Physical aspects of storage and preservation (short and long term)
- Operating equipment
- Evaluation of characteristics of use
- Qualification of processes
- Terminology - Vocabulary
- Integrity of information

3.9.7.2 ISO 14641-1:2018 - Electronic archiving — Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation

This [Standard](#) replace the ISO 14641-1:2012.

3.10 [ISO/IEC JTC 1](#)

3.10.1 ISO/IEC JTC 1/SC 37 - Biometrics

[ISO/IEC JTC 1/SC 37](#) is responsible for the standardisation of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks, biometric application programming interfaces, biometric data interchange formats, related biometric profiles and other standards in support of technical implementation of biometric systems, evaluation criteria to biometric technologies, methodologies for performance testing and reporting, cross-jurisdictional and societal aspects of biometric implementation. The complete list of standards published or under development, can be found in on the SC 37 homepage.

Published standards and ongoing projects related to the topics include the series of biometric data interchange standards for different biometric modalities, biometric technical interfaces, related biometric profiles and other standards in support of technical implementation of biometric systems, and cross jurisdictional and societal aspects of biometric implementation. Representative projects include revisions to some of the ISO/IEC 19794 series for Biometric data interchange formats, ISO/IEC 29794 series for Biometric sample quality and ISO/IEC 39794 series for Extensible biometric data interchange formats. These projects include generic extensible data interchange formats for the representation of data, a tagged binary data format based on an extensible specification in ASN.1 and a textual data format based on an XML schema definition (both capable of holding the same information). The ISO/IEC 30107 series for Biometric presentation attack detection and ISO/IEC 24779 series for Cross-Jurisdictional and societal aspects of implementation of biometric technologies - pictograms, icons and symbols for use with biometric systems are multi-part standards of relevance.

3.10.2 ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection

[ISO/IEC JTC 1/SC 27](#), is responsible for international IT security. The most relevant standards to electronic identification and trust services are developed by SC 27/WG 5 Identity Management and Privacy Technologies. After completion of foundational frameworks, specifically, the ISO/IEC 24760 series A framework for identity management and ISO/IEC 29100 for Privacy framework, priorities for WG 5 are related standards and Standing Documents on supporting technologies, models, and methodologies. WG 5's Projects include:



## Standards Inventory for the future of digital identity

- A framework for identity management - Part 1: Terminology and concepts (ISO/IEC 24760-1, 2nd edition:2019)
- A framework for identity management - Part 2: Reference framework and requirements (ISO/IEC 24760-2, 1st edition:2015)
- A framework for identity management - Part 3: Reference framework and requirements (ISO/IEC 24760-3, 1st edition:2016)
- Privacy framework (ISO/IEC 29100, 1st edition:2011; Amendment 1:2018)
- Privacy architecture framework (ISO/IEC 29101, 2nd edition:2018)
- A framework for access management (ISO/IEC 29146, 1st edition:2016)
- Requirements for partially anonymous, partially unlinkable authentication (ISO/IEC 29191, 1st edition:2012)
- Privacy enhancing data de-identification terminology and classification of techniques (ISO/IEC 20889, 1st edition:2018)
- Privacy impact assessment - methodology (ISO/IEC 29134, 1st edition:2017)
- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management - Requirements and guidelines (ISO/IEC 27701, 1st edition:2019)
- WG 5 Standing Document 2 - "Privacy references list"
- WG 5 Standing Document 4 - "Standards Privacy Assessment"

ISO/IEC JTC 1 SC 27 is working in close collaboration with CEN/CLC/JTC 13 'Cybersecurity and Data protection' on eIDAS related standardisation activity.

### 3.10.2.1 ISO/NP 24946 Requirements and guidance for improving, preserving, and assessing the privacy capability of DLT systems.

The [document](#) specifies DLT related requirements and provides guidance for controllers and processors holding responsibility and accountability for privacy protected data processing.

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

[ISO/JTC 1/SC 17](#) Cards and security devices for personal identification is responsible for standardisation and interface associated with their use in inter-industry applications and international interchange in the area of:

- Identification and related documents,
- Cards,
- Security devices and tokens

#### 3.10.3.1 ISO/IEC 18013-5 - Driving licence identification by mobile

[ISO/IEC 18013-5](#) establishes interface specifications for the implementation of a driving licence in association with a mobile device. This document specifies the interface between the mDL and mDL reader and the interface between the mDL reader and the issuing authority infrastructure. This document also enables parties other than the issuing authority (e.g. other issuing authorities, or mDL verifiers in other countries) to:

## Standards Inventory for the future of digital identity

- use a machine to obtain the mDL data;
- tie the mDL to the mDL holder;
- authenticate the origin of the mDL data;
- verify the integrity of the mDL data.

The following items are out of scope for this document:

- how mDL holder consent to share data is obtained;
- requirements on storage of mDL data and mDL private keys.

3.10.3.2 ISO/IEC AWI TS 18013-7 - Mobile driving licence add-on

[ISO/IEC AWI TS 18013-7](#) is under development.

3.10.3.3 ISO/IEC DIS 23220-1 - Generic system architectures of mobile eID systems

[ISO/IEC DIS 23220-1](#) is under development

3.10.3.4 ISO/IEC AWI 23220-2 - Data objects and encoding rules for generic eID systems

[ISO/IEC AWI TS 23220-2](#) is under development.

3.10.3.5 ISO/IEC DIS 23220-4 - Protocols and services for operational phase

[ISO/IEC AWI TS 23220-4](#) is under development.

### 3.11 ITU-T (International Telecommunication Union)

Some blockchain related activities are taking place in SG5, SG11, SG13 and SG20, and Identity activities in SG3, SG11, SG13, SG17 and SG20.

#### 3.11.1 ITU-T SG3 - Economic and policy issues

[ITU-T SG3](#) is responsible, inter alia, for studying international telecommunication/ICT policy and economic issues and tariff and accounting matters (including costing principles and methodologies), with a view to informing the development of enabling regulatory models and frameworks. SG3 is also tasked with a study on the economic and regulatory impact of the Internet, convergence (services or infrastructure) and new services. SG3 is currently working on a guideline for digital identity under the new Question 9/3 - economic and policy aspects of big data and digital identity in international telecommunications services and networks. SG3 has a draft Recommendation on “Guidelines for digital identity” (D.DigID) under development.

#### 3.11.2 ITU-T SG5: Environment, climate change and circular economy

[ITU-T SG5](#) has approved Recommendation L.1317 “Guidelines on energy efficient blockchain systems” which focuses on blockchain energy demands and how these can be optimized. This Recommendation aims to explain the energy demand of blockchain, to define the blockchain energy model and to

describe the energy efficiency parameters that can be calibrated in order to enhance the corresponding energy efficiency.

### 3.11.3 ITU-T SG 11: Signalling requirements, protocols and test specifications

[ITU-T SG11](#) is developing draft Recommendation Q.DIVS-IMT2020 “Signalling Requirements and Protocol for Providing Network-oriented Data Integrity Verification Service based on Blockchain in IMT-2020 network” and Q.BaaS-iop-reqts “Interoperability testing requirements of blockchain as a service”.

### 3.11.4 ITU-T SG13 - Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructure

[ITU-T SG13](#) published three technical reports on trust provisioning for future ICT infrastructures and services and five Recommendations (ITU-T Y.3051-Y.3055). There are currently seven more work items under development covering areas such as Decentralized Trustworthy Network Infrastructure (Y.DNI-fr), trust index for ICT infrastructures and services (Y.trust-index) etc. SG13 is developing a [Standardisation roadmap on Trustworthy Networking and Services](#) including Quantum Enhanced Networks.

ITU-T SG13 also studies quantum technologies, in particular, quantum key distribution networks (QKDN) to increase the security of networks communication. It approved four Recommendations (ITU-T Y.3800-3804) and has seven open work items about QKDN. A flipbook “[Trust in ICT](#)” (2017) gives a snapshot of main concepts for Trust as applied to ICT and overview of standardisation efforts worldwide to date.

### 3.11.5 ITU-T SG17 – Security & Identity Management

[ITU-T SG17](#) is responsible for the study and coordinate the work on security and identity management. It has approved Recommendations:

- ITU-T X.1058 “Information technology - Security techniques - Code of practice for Personally Identifiable Information protection”
- ITU-T X.1148 “Framework of de-identification process for telecommunication service providers”
- ITU-T X.1212 “Design considerations for improved end-user perception of trustworthiness indicators”
- ITU-T X.1250 “Baseline capabilities for enhanced global identity management and interoperability”
- ITU-T X.1252 “Baseline identity management terms and definitions”
- ITU-T X.1403 “Security considerations for using distributed ledger technology data in identity management”
- ITU-T X.1451 “Risk identification to optimize authentication”
- ITU-T X.1363 “Technical framework of personally identifiable information (PII) handling system in IoT environment” and is developing six draft Recommendation in this domain: (X.5Gsec-t, X.sec-QKDN-tn, X.smsrc, X.scpa, X.sgos, X.rdda).

### 3.11.6 ITU-T SG20 - Internet of Things, smart cities and communities

[ITU-T SG20](#) is the lead study group for IoT identification. It studies what the identification systems are capable of in terms of fulfilling the requirements of IoT and SC&C including security, privacy and trust; how authentication technologies can work with identification systems; what options or measures are available for identification of IoT objects; how identification mechanisms can support interoperability in IoT and SC&C and mitigate risks, among others. It approved Recommendations:

- ITU-T Y.4459 “Digital entity architecture framework for IoT interoperability”
- ITU-T Y.4807 “Agility by design for Telecommunications/ICT Systems Security used in the Internet of Things”
- ITU-T Y.4808 “Digital entity architecture framework to combat counterfeiting in IoT” etc. It is currently working on several draft Recommendations on the topic (Y.IoT-IoD-PT, Y.Data.Sec.IoT-Dev, Y.FW.IC.MDSC, Y.IoT-Ath-SC, Y.IoT-CSIADE-fw, Y.IoT-ITS-ID, Y.IoT-Smartcity-Risk , Y.oneM2M.SEC.SOL).

Under the Security, Infrastructure and Trust Working Group led by ITU under the Financial Inclusion Global Initiative (a joint programme of the ITU, World Bank and Bank for International Settlements and supported by the Gates Foundation), [studies on strong authentication technologies applications for digital financial services](#) are being undertaken. The studies describe several widely-adopted technical and policy standards that support strong authentication mechanisms. The examples of strong authentication and advanced authentication systems are categorized as either enrolment or authentication for the use of DFS. These two use case categories primarily impact users of DFS. The use of identity verification and authentication system based on DLT are also being studied.

ITU-T SG20 has approved the following recommendations:

- Y.4560 “ Blockchain-based data exchange and sharing for supporting Internet of things and smart cities and communities ”,
- Y.4561 “Blockchain-based Data Management for supporting Internet of things and smart cities and communities”,
- Y.4907 “Reference architecture of blockchain-based unified KPI data management for smart sustainable cities”
- Y.4476 “OID-based resolution framework for transaction of distributed ledger assigned to IoT resources”.

### 3.11.7 ITU X.509

[X.509](#) is an International Telecommunication Union (ITU) standard defining the format of public key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web. They are also used in offline applications, like electronic signatures.

An X.509 certificate binds an identity to a public key using a digital signature. A certificate contains an identity (a hostname, or an organization, or an individual) and a public key (RSA, DSA, ECDSA, ed25519, etc.), and is either signed by a certificate authority or is self-signed. When a certificate is signed by a trusted certificate authority, or validated by other means, someone holding that certificate can use the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key.

X.509 also defines certificate revocation lists, which are a means to distribute information about certificates that have been deemed invalid by a signing authority, as well as a certification path validation algorithm, which allows for certificates to be signed by intermediate CA certificates, which are, in turn, signed by other certificates, eventually reaching a trust anchor.

X.509 is defined by the International Telecommunications Union's "Standardization Sector" (ITU-T), in ITU-T SG17 and is based on ASN.1, another ITU-T standard.

The last recommendation was produced through a joint activity with ISO and IEC.

### 3.12 UNECE (United Nations Economic Commission for Europe)

The UNECE in its Recommendation [14 outlines base elements to take into account in the use of electronic authentication methods](#). It recommends that the authentication methods should be chosen considering the nature of the electronic transaction and the relationship between the parties involved in the exchange. Not all electronic exchanges require the highest level of reliability.

The mission of UN/CEFACT (Centre for Trade Facilitation and Electronic Business) is to improve the ability of business, trade and administrative organizations from developed, developing and transitional economies to exchange products and relevant services effectively. Its principal focus is on facilitating national and international transactions through the simplification and harmonization of processes, procedures, and information flows in order to contribute to the growth of global commerce.

Further work is being developed on this topic within UN/CEFACT, named [White Paper on Trusted Transboundary Environment](#).

UN/CEFACT also published another White Paper named [eDATA Verifiable Credentials for Cross Border Trade](#) describing a highly scalable operating model for digitization and trust of cross border trade based on verifiable credentials, linked data, and decentralized identifiers. It provides national regulators with implementation guidance that will facilitate the following outcomes.

### 3.13 OASIS (Organization for the Advancement of Structured Information Standards)

[OASIS](#) was founded under the name “SGML Open” in 1993. It began as a consortium of vendors and users devoted to developing guidelines for interoperability among products that support the Standard Generalized Markup Language (SGML). The consortium changed its name to “OASIS” in 1998 to reflect an expanded scope of technical work.

#### 3.13.1 EEA Community Projects

The EEA Community Projects, formerly known as the Ethereum OASIS Open Project, is the hub for open source-based standards development in the Ethereum industry.

It aims to facilitate Ethereum’s longevity, interoperability, and ease of integration and intends to develop documentation and shared test suites that facilitate new features and enhancements to the Ethereum protocol.

The projects seek to address interoperability of implementations. EEA projects include Ethereum projects like the Baseline Protocol and JSON-RPC API documentation under its stewardship.

#### 3.13.2 EEA Baseline Protocol (Standard for Universal Verified State Synchronization & Multiparty Coordination Using Zero Knowledge)

The Baseline Protocol OASIS Open Project combines advances in cryptography, messaging, and blockchain to deliver secure and private business processes at low cost via the public Ethereum Mainnet.

#### 3.13.3 OASIS Security Services (SAML) TC

[OASIS SS SAML TC](#) maintains and extends the widely used Security Assertion Markup Language (SAML, also ITU-T Recommendation X.1141) standard. A [profile of SAML](#) is used for cross-border identification and authentication of citizens in the [eIDAS nodes provided by the eID Building Block of the Connecting Europe Facility \(CEF\)](#). SAML is also used at national level in Member States.

#### 3.13.4 OASIS Electronic Identity Credential Trust Elevation Methods (Trust Elevation) TC

The [OASIS Trust Elevation TC](#) defines a set of standardized protocols that service providers may use to elevate the trust in an electronic identity credential presented to them for authentication.

#### 3.13.5 OASIS Digital Signature Services eXtended (DSS-X) TC

The [OASIS DSS-X TC](#) defines standard Digital Signature Service Core Protocols, Elements, and Bindings. The latest version provides both JSON- and XML-based request/response protocols for signing and verifying, including updated timestamp formats, transport and security bindings and metadata discovery methods. This TC works in close liaison with the ETSI.

### 3.13.6 OASIS ebXML Messaging Services TC

The [OASIS ebXML Message TC](#) maintains the OASIS ebMS3 (also ISO 15000-1) standard and the AS4 standard (also ISO 15000-2). AS4 is [profiled](#) as the message exchange protocol of the [eDelivery Building Block of the Connecting Europe Facility](#). Several dozens policy domains use eDelivery for cross-border secure and reliable exchange of documents and data. AS4 is also used in the [EESSI system for digitalisation in social security coordination](#).

### 3.13.7 OASIS Business Document Exchange (BDXR) TC

The [OASIS Business Document Exchange TC](#) provides complementary eDelivery specifications for service location and capability lookup.

### 3.13.8 OASIS XRI Data Interchange (XDI) TC (closed)

The [Technical Committee](#) was closed by OASIS TC Administration on 05 October 2020 and is no longer active. Archives of its work remain publicly accessible and are linked from this page.

## 3.14 [OIDF \(OpenID Foundation\)](#)

Set of standards and related certification profiles addressing identity transactions over the internet. [10 active working groups](#) are:

### 3.14.1 Working Groups

#### 3.14.1.1 AB/Connect WG

The AB/Connect working group is a combined working group of the Artifact Binding (AB) Working Group and the Connect Working Group aimed at producing the OAuth 2.0 based “OpenID Connect” specifications.

#### 3.14.1.2 Enhanced Authentication Profile (EAP) WG

The purpose of this working group is to develop a security and privacy profile of the OpenID Connect specifications that enable users to authenticate to OpenID Providers using strong authentication specifications. The resulting profile will enable use of IETF Token Binding specifications with OpenID Connect and integration with FIDO relying parties and/or other strong authentication technologies.

#### 3.14.1.3 eKYC & IDA WG

The eKYC and Identity Assurance (eKYC & IDA) WG is developing extensions to OpenID Connect that will standardise the communication of assured identity information, i.e. verified claims and information about how the verification was done and how the respective claims are maintained.

#### 3.14.1.4 Financial-grade API (FAPI) WG

The goal of FAPI is to provide JSON data schemas, security and privacy recommendations and protocols to:

- enable applications to utilize the data stored in the financial account,

- enable applications to interact with the financial account, and
- enable users to control the security and privacy settings.

### 3.14.1.5 FastFed WG

The purpose of this Working Group is to develop a meta-data document specification, APIs, and workflow to enable an administrator to federate an identity provider and a hosted application that supports one or more of OpenID Connect, SAML, and SCIM and enable configuration changes to be communicated between the identity provider and hosted application.

### 3.14.1.6 HEART WG

The HEART Working Group intends to harmonize and develop a set of privacy and security specifications that enable an individual to control the authorization of access to RESTful health-related data sharing APIs, and to facilitate the development of interoperable implementations of these specifications by others

### 3.14.1.7 International Government Assurance Profile (iGov) WG

The purpose of this working group is to develop a security and privacy profile of the OpenID Connect specifications that allow users to authenticate and share consented attribute information with public sector services across the globe. The resulting profile will enable standardized integration with public sector relying parties in multiple jurisdictions. The profile will be applicable to, but not exclusively targeted at, identity broker-based implementations.

### 3.14.1.8 MODRNA WG

The MODRNA (Mobile Operator Discovery, Registration & authentication) WG will develop a profile of OpenID Connect intended to be appropriate for use by mobile network operators (MNOs) providing identity services to RPs and for RPs in consuming those services as well as any other party wishing to be interoperable with this profile.

Additionally, it will identify and make recommendations for additional standards items.

### 3.14.1.9 Research & Education (R&E) WG

The purpose of this working group is to develop a set of profiles for the OpenID Connect specifications to ease the adoption of OpenID Connect in the Research and Education (R&E) sector. The profiles will take into account existing practices of federated identity management in the R&E sector, current international standards to represent users that belong to R&E institutions, as well as the existing international trust fabric based on R&E identity federations and multi-lateral trust exchange. The working group will also actively look for the engagement of the R&E international community.

### 3.14.1.10 Shared Signal & Events WG

The goal of Shared Signals & Events is to provide data sharing schemas, privacy recommendations and protocols to:



## Standards Inventory for the future of digital identity

- Share information about important security events in order to thwart attackers from leveraging compromised accounts from one Service Provider to gain access to accounts on other Service Providers (mobile or web application developers and owners).
- Enable users and providers to coordinate in order to securely restore accounts following a compromise.

Internet accounts that use email addresses or phone numbers as the primary identifier for the account will be the initial focus.

### 3.14.2 Standards

#### 3.14.2.1 OIDF Self-Issued OpenID Provider v2

OpenID Connect defines mechanisms by which an End-User can leverage an OpenID Provider (OP) to release identity information (such as authentication and claims) to a Relying Party (RP) which can act on that information.

This [specification](#) extends OpenID Connect with the concept of a Self-Issued OpenID Provider (Self-Issued OP), an OP which is within the End-User's local control. End-Users can leverage Self-Issued OPs to authenticate themselves and present claims directly to the RPs. This allows users to interact with RPs directly, without relying on third-party providers or requiring the End-User to operate their own hosted OP infrastructure.

#### 3.14.2.2 OIDF OpenID Connect Credential Provider

In OpenID Connect today the existing ways to communicate End-User claims to relying parties are the `id_token` and the `userinfo` endpoint, however these mechanisms alone are unsuitable for the style of indirect presentation of claims to relying parties via a holder, as the relying party must be able to authenticate the authority of the holder to be presenting the claims on behalf of the End-User.

Instead in order to support this style of flow, this [specification](#) defines a new vehicle for communicating End-User claims called a "credential". In addition to this definition this specification defines how an existing OpenID Provider can be extended to issue "credentials" to holders.

#### 3.14.2.3 OIDF OpenID Connect for Verifiable Presentations

This [specification](#) defines an extension of OpenID Connect to allow presentation of claims in the form of W3C Verifiable Credentials as part of the protocol flow in addition to claims provided in the `id_token` and/or via `Userinfo` responses.

#### 3.14.2.4 OIDF OpenID Connect for Identity Assurance

This [specification](#) defines an extension of OpenID Connect for providing Relying Parties with Verified Claims about End-Users. This extension facilitates the verification of the identity of a natural person.

### 3.14.3 Parallel projects

#### 3.14.3.1 Bcgov: Verifiable Credential Authentication with OpenID Connect (VC-AuthN OIDC)

This [repository](#) is the home of a project to achieve verifiable credential based authentication using OpenID Connect, executed by [Matr](#).

DID Communication (DIDComm) is used as the messaging protocol between the OP and IW. DIDComm, is an emerging messaging protocol that is being incubated and developed under the Hyperledger Aries Project with much of the current protocol documentation residing under the Aries RFC repository.

The [VON](#) (Verifiable Organizations Network) is based on Hyperledger Indy distributed ledger technology, and initiated by the Governments of British Columbia, Ontario and Canada.

### 3.15 IETF (Internet Engineering Task Force)

#### 3.15.1 Working Groups

[Electronic identification and trust services including e-signatures](#) is dedicated to deliver:

Action 1. Build on the work done under Mandate M/460, in the following way: address the trust service providers (TSP) providing signature creation services, the TSPs providing signature validation services, and standards for trust application service providers. Support harmonisation of identity proofing, particularly in relation certificate issuance and remote signing.

Action 2. Take ongoing EU policy activities into account in standardisation, e.g. in ISO/IEC JTC 1/SC 27/WG 5 (identity management and privacy technologies) and other working groups of ISO/IEC JTC 1/SC 27. Furthermore, in order to promote the strengths of the European approach to electronic identification and trust services at global level and to foster mutual recognition of electronic identification and trust services with non-EU countries, European and international standards should be aligned wherever possible. The promotion and maintenance of related European approaches, which especially take into account data protection considerations, in international standards should be supported.

Action 3. Support and improve the development of interoperable standards by facilitating the organisation of plugtests (interoperability events) and developing and enhancing conformity testing tools. Such interoperability events may address CAdES, XAdES, PAdES, ASiC, use of trusted lists, signature validation, remote signature creation and validation, e-delivery services, preservation services, etc.

Action 4. Foster the development of standards supporting the implementation of the measures derived from the revision of the eIDAS regulation, aimed to improve its effectiveness, extend its benefits to the private sector and promote trusted digital identities for all Europeans.

The IETF Working Groups are:

#### 3.15.1.1 Web Authorization Protocol (oauth) WG

The [Web Authorization Protocol \(OAUTH\) WG](#) developed a protocol suite that allows a user to grant a third-party Website or application access to the user's protected resources, without necessarily revealing their long-term credentials, or even their identity. It also developed security schemes for presenting authorisation tokens to access a protected resource.

The ongoing standardisation effort within the OAUTH Working Group is focusing on enhancing interoperability of OAUTH deployments.

#### 3.15.1.2 Public Notary Transparency (TRANS) WG

The [Public Notary Transparency \(TRANS\) WG](#) develops a standards-track specification of the Certificate Transparency protocol (RFC6962) that allows detection of the miss-issuance of certificates issued by CAs or via ad-hoc mapping by maintaining cryptographically verifiable audit logs.

#### 3.15.1.3 Automated Certificate Management Environment (ACME) WG

The [Automated Certificate Management Environment \(ACME\) WG](#) specifies conventions for automated ITU X.509 certificate management, including validation of control over an identifier, certificate issuance, certificate renewal, and certificate revocation. The initial focus of the ACME WG is on domain name certificates (as used by web servers), but other uses of certificates can be considered as work progresses.

#### 3.15.1.4 JWM (JSON Web Message)

[JSON Web Message](#) (JWM) is a flexible way to encode application-level messages in JSON for transfer over a variety of transport protocols. JWMs use JSON Web Encryption (JWE) to protect integrity, achieve confidentiality, and achieve repudiable authentication; alternatively, or in addition, they use JSON Web Signatures (JWS) to associate messages with a non-repudiable digital signature.

#### 3.15.1.5 Decentralization of the Internet Research Group (DINRG) WG

The [DINRG WG](#) investigate open research issues in decentralizing infrastructure services such as trust management, identity management, name resolution, resource/asset ownership management, and resource discovery. The focus of DINRG is on infrastructure services that can benefit from decentralization or that are difficult to realize in local, potentially connectivity-constrained networks. Other topics of interest are the investigation of economic drivers and incentives and the development and operation of experimental platforms. DINRG will operate in a technology- and solution-neutral manner, i.e., while the RG has an interest in distributed ledger technologies, it is not limited to specific technologies or implementation aspects.

### 3.15.2 Standards

#### 3.15.2.1 OAuth 2.0

OAuth 2.0 is the industry-standard protocol for authorization. OAuth 2.0 focuses on client developer simplicity while providing specific authorization flows for web applications, desktop applications, mobile phones, and living room devices. This [specification](#) and its extensions are being developed within the Web Authorization Protocol (oauth) WG.

#### 3.15.2.2GNAP (Grant Negotiation and Authorization Protocol)

This [document](#) defines a mechanism for delegating authorization to a piece of software, and conveying that delegation to the software. This delegation can include access to a set of APIs as well as information passed directly to the software.

This evolution of OAuth aims to address limitations of OAuth 2.0.

#### 3.15.2.3JOSE (JSON Object Signing and Encryption)

[Standards](#) for signing and encrypting data -- primarily identity tokens -- on the web. Header parameters (JWE & JWS) and payload claims (JWT) are both registered in an IANA Registry.

#### 3.15.2.4Signing HTTP Messages

This [document](#) describes a mechanism for creating, encoding, and verifying digital signatures or message authentication codes over content within an HTTP message.

This mechanism supports use cases where the full HTTP message may not be known to the signer, and where the message may be transformed (e.g., by intermediaries) before reaching the verifier.

#### 3.15.2.5Cryptographic Hyperlinks (Hashlink)

When using a hyperlink to fetch a resource from the Internet, it is often useful to know if the resource has changed since the data was published. Cryptographic hashes, such as SHA-256, are often used to determine if published data has changed in unexpected ways. Due to the nature of most hyperlinks, the cryptographic hash is often published separately from the link itself.

This [specification](#) describes a data model and serialization formats for expressing cryptographically protected hyperlinks. The mechanisms described in the document enables a system to publish a hyperlink in a way that empowers a consuming application to determine if the resource associated with the hyperlink has changed in unexpected ways.

#### 3.15.2.6RFC 6960

This [RFC 6960](#) (Request For Comments) for OCSP (Online Certificate Status Protocol) document specifies a protocol useful in determining the current

status of a digital certificate without requiring Certificate Revocation Lists (CRLs).

Additional mechanisms addressing PKIX operational requirements are specified in separate documents. This document obsoletes RFCs 2560 and 6277.

#### 3.15.2.7 RFC 5280

This [RFC 5280](#) (Request For Comments) specifies a protocol useful in determining the current status of a digital certificate without requiring Certificate Revocation Lists (CRLs). Additional mechanisms addressing PKIX operational requirements are specified in separate documents. This document obsoletes RFCs 2560 and 6277. It also updates RFC 5912.

#### 3.15.2.8 RFC 8259

This [RFC 8259](#) (Request For Comments) defines a small set of formatting rules for the portable representation of structured data.

### 3.16 W3C (World Wide Web Consortium)

The W3C Credentials Community Group discusses credential storage and exchange systems for the web. Some of their ideas are being discussed in the Web Payments Interest Group via the Verifiable Claims Task Force (as of January 2016).

#### 3.16.1 W3C Working Group

##### 3.16.1.1 W3C DID Working Group

The mission of the [Decentralized Identifier Working Group](#) is to standardize the DID URI scheme, the data model and syntax of DID Documents, which contain information related to DIDs that enable the aforementioned initial use cases, and the requirements for DID Method specifications.

The co-chairs of the group are Daniel Burnett (Invited Expert) and Brent Zundel (Evernym). The staff contact is Ivan Herman. The group is chartered until September 2021.

##### 3.16.1.2 W3C VC Working Group

The mission of the Verifiable Credentials (formerly known as Verifiable Claims) Working Group ([VCWG](#)) is to make expressing and exchanging credentials that have been verified by a third party easier and more secure on the Web. The Working Group is now in maintenance mode.

There is a corresponding [VC Working Group Github](#).

#### 3.16.2 W3C Standards

##### 3.16.2.1 W3C VC Data Model

The Verifiable Claims Working Group specifies ways to make expressing, exchanging, and verifying claims easier and more secure on the Web. It

released the [Verifiable Credentials Data Model V1.1](#), providing a mechanism to express these sorts of credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable.

There is a corresponding [VC Data Model Github](#).

#### 3.16.2.2W3C VC JSON

The Data Model can be encoded in JSON (JavaScript Object Notation) RFC 8259, mapping is described [here](#).

#### 3.16.2.3W3C VC Schema Specification

The VC Data Model specifies the models used for Verifiable Credentials and Verifiable Presentations, and explains the relationships between three parties: issuer, holder, and verifier. A critical piece of infrastructure out of the scope of those specifications is the Credential Schema. This [specification](#) provides a mechanism to express a Credential Schema and the protocols for evolving the schema.

#### 3.16.2.4W3C VC Implementation Guidelines 1.0

The [VC Implementation Guidelines](#) provides implementation guidance for Verifiable Credentials.

#### 3.16.2.5W3C VC Revocation List

This [specification](#) describes a privacy-preserving, space-efficient, and high-performance mechanism for publishing the revocation status of Verifiable Credentials.

#### 3.16.2.6W3C Credential Handler

This [specification](#) defines capabilities that enable third-party Web applications to handle credential requests and storage.

#### 3.16.2.7W3C VC Presentation Request Specification

This [specification](#) describes a declarative JSON-based query language used by applications to perform requests from wallets and agents. The results of the requests are always wrapped in a Verifiable Presentation.

#### 3.16.2.8W3C VC HTTP API

Verifiable credentials provide a mechanism to express credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable. This [specification](#) provides data model and HTTP protocols to issue, verify, present, and manage data used in such an ecosystem.

#### 3.16.2.9W3C VC Use Cases

The [W3C Note of 24 September 2019](#) is a collection of use cases for the Verifiable Credentials Data Model 1.0 and helps to better understand that Specification.

### 3.16.2.10W3C DID Use Cases & requirements

This [document](#) sets out use cases and requirements for a new type of identifier that has 4 essential characteristics:

- decentralized: there should be no central issuing agency;
- persistent: the identifier should be inherently persistent, not requiring the continued operation of an underlying organization;
- cryptographically verifiable: it should be possible to prove control of the identifier cryptographically;
- resolvable: it should be possible to discover metadata about the identifier.

Although existing identifiers may display some of these characteristics, none currently displays all four.

### 3.16.2.11W3C Decentralized Identifiers (DIDs) v1.0

The [Decentralized Identifiers \(DIDs\) v1.0](#) document specifies the DID syntax, a common data model, core properties, serialized representations, DID operations, and an explanation of the process of resolving DIDs to the resources that they represent.

### 3.16.2.12W3C DID Specification Registries

The [DID Specification Registries](#) serves as an official registry for all known global parameters, properties, and values used by the Decentralized Identifier ecosystem

### 3.16.2.13W3C DID Method Rubric

The communities behind Decentralized Identifiers (DIDs) bring together a diverse group of contributors who have decidedly different notions of exactly what "decentralization" means.

Rather than attempting to resolve this potentially unresolvable question, we propose a rubric — a scoring guide used to evaluate performance, a product, or a project — that teaches how to evaluate a given DID Method according to one's own requirements.

This [rubric](#) presents a set of criteria which an Evaluator can apply to any DID Method based on the use cases most relevant to them. We avoid reducing the Evaluation to a single number because the criteria tend to be multidimensional and many of the possible responses are not necessarily good or bad. It is up to the Evaluator to understand how each response in each criteria might illuminate favorable or unfavorable consequences for their needs.

### 3.16.2.14W3C DID Method for Static Cryptographic Keys

This [specification](#) describes a non-registry based DID Method based on expanding a cryptographic public key into a DID Document. This approach

provides the simplest possible implementation of a DID Method that is able to achieve many, but not all, of the benefits of utilizing DIDs.

### 3.16.2.15W3C DID web Method Specification

DIDs that target a distributed ledger face significant practical challenges in bootstrapping enough meaningful trusted data around identities to incentivize mass adoption. This [document](#) propose using a new DID method in conjunction with blockchain-based DIDs that allows them to bootstrap trust using a web domain's existing reputation.

### 3.16.2.16W3C Web Cryptography API

This [specification](#) describes a JavaScript API for performing basic cryptographic operations in web applications, such as hashing, signature generation and verification, and encryption and decryption. Additionally, it describes an API for applications to generate and/or manage the keying material necessary to perform these operations. Uses for this API range from user or service authentication, document or code signing, and the confidentiality and integrity of communications.

### 3.16.2.17W3C Web Authentication: An API for accessing Public Key Credentials

This [specification](#) defines an API enabling the creation and use of strong, attested, scoped, public key-based credentials by web applications, for the purpose of strongly authenticating users. Conceptually, one or more public key credentials, each scoped to a given WebAuthn Relying Party, are created by and bound to authenticators as requested by the web application. The user agent mediates access to authenticators and their public key credentials in order to preserve user privacy. Authenticators are responsible for ensuring that no operation is performed without user consent. Authenticators provide cryptographic proof of their properties to Relying Parties via attestation. This specification also describes the functional model for WebAuthn conformant authenticators, including their signature and attestation functionality.

### 3.16.2.18W3C Cryptographic Key Management Systems for the Web

Cryptographic authentication systems enable more secure interactions among machines, individuals, and organizations. These systems often use public-private key cryptography or encryption mechanisms to manage both cryptographic material and operations utilizing that material. This [specification](#) provides a common data model and interface for interacting with these systems enabling one to perform secure cryptographic operations on keypairs such as creating, wrapping, unwrapping, signing, encrypting, and decrypting.



### 3.16.2.19W3C Encrypted Data Vaults

We store a significant amount of sensitive data online, such as Personally Identifying Information (PII), trade secrets, family pictures, and customer information. The data that we store is often not protected in an appropriate manner. This [specification](#) describes a privacy-respecting mechanism for storing, indexing, and retrieving encrypted data at a storage provider. It is often useful when an individual or organization wants to protect data in a way that the storage provider cannot view, analyze, aggregate, or resell the data. This approach also ensures that application data is portable and protected from storage provider data breaches.

### 3.16.2.20W3C Universal Wallet

This [specification](#) describes a portable, extensible, JSON-LD wallet, supporting digital currencies and credentials.

### 3.16.2.21W3C JSON-based Serialization for Linked Data

This [specification](#) describes a superset of the features defined in [JSON-LD 1.0](#) and, except where noted, documents created using the 1.0 version of this specification remain compatible with JSON-LD 1.1.

### 3.16.2.22W3C CBOR-based Serialization for Linked Data

CBOR is a compact binary data serialization and messaging format. This [specification](#) defines CBOR-LD 1.0, a CBOR-based format to serialize Linked Data. The encoding is designed to leverage the existing JSON-LD ecosystem, which is deployed on hundreds of millions of systems today, to provide a compact serialization format for those seeking efficient encoding schemes for Linked Data. By utilizing semantic compression schemes, compression ratios in excess of 60% better than generalized compression schemes are possible. This format is primarily intended to be a way to use Linked Data in storage and bandwidth constrained programming environments, to build interoperable semantic wire-level protocols, and to efficiently store Linked Data in CBOR-based storage engines.

### 3.16.2.23W3C Authorization Capabilities for Linked Data

[Authorization Capabilities for Linked Data](#) (ZCAP-LD for short) provides a secure way for linked data systems to grant and express authority utilizing the object capability model. Capabilities are represented as linked data objects which are signed with Linked Data Proofs. ZCAP-LD supports delegating authority to other entities on the network by chaining together capability documents. "Caveats" may be attached to capability documents which may be used to restrict the scope of their use, for example to restrict the actions which may be used or providing a mechanism by which the capability may be later revoked

The following [repository published by MATTR](#) contains a linked data proof implementation for creating BBS+ Signatures using BLS12-381 key pairs.

### 3.16.2.24W3C BBS+ Signatures

This [specification](#) describes the BBS+ Signature Suite created in 2020 for the Linked Data Proof specification. The Signature Suite utilizes BBS+ signatures to provide the capability of zero knowledge proof disclosures.

### 3.16.2.25W3C Data Privacy Vocabulary

The [DPV](#) provides terms (classes and properties) to describe and represent information related to processing of personal data based on established requirements such as for the EU General Data Protection Regulation (GDPR). The DPV is structured as a top-down hierarchical vocabulary with the core or base concepts of personal data categories, purposes of processing and types of processing, data controller(s) associated, recipients of personal data, legal bases or justifications used, technical and organisational measures and restrictions (e.g. storage locations and storage durations), applicable rights, and the risks involved.

### 3.16.2.26W3C VC Engineering Privacy

Three related but distinct privacy enhancing strategies: "data minimization," "selective disclosure," and "progressive trust." These enhancements are enabled with cryptography.

The goal of this [paper is to enable decision makers](#), particularly non-technical ones, to gain a nuanced grasp of these enhancements along with some idea of how their enablers work. We describe them below in plain English, but with some rigor. This knowledge will enable readers of this paper to be better able to know when they need privacy enhancements, to select the type of enhancement needed, to assess techniques that enable those enhancements, and to adopt the correct enhancement for the correct use case.

### 3.16.2.27W3C ActivityPub

The [ActivityPub protocol](#) is a decentralized social networking protocol based upon the [ActivityStreams] 2.0 data format. It provides a client to server API for creating, updating and deleting content, as well as a federated server to server API for delivering notifications and content.

### 3.16.2.28W3C & DIF Confidential Storage

We store a significant amount of sensitive data online, such as personally identifying information (PII), trade secrets, family pictures, and customer information. The data that we store is often not protected in an appropriate manner.

This [specification](#) describes a privacy-respecting mechanism for storing, indexing, and retrieving encrypted data at a storage provider. It is often useful when an individual or organization wants to protect data in a way that the storage provider cannot view, analyze, aggregate, or resell the data. This approach also ensures that application data is portable and protected from storage provider data breaches.

### 3.16.3 W3C Github Projects

#### 3.16.3.1 W3C DID Test Suite

This [test suite](#) performs interoperability tests on the W3C Decentralized Identifier specification and is maintained by the W3C DID Working Group

#### 3.16.3.2 W3C Signing HTTP Messages Working Group Test Suite

The [test suite](#) will check an implementation that generates and validates signatures compliant with Signing HTTP Messages to ensure conformance with the specification.

This suite requires a functioning installation of nodejs (>v8.12), and specifically the npm command (>v6.4).

#### 3.16.3.3 W3C VC Test Suite

This [repository](#) contains the W3C Verifiable Credentials Working Group test suite. Any conforming implementation MUST pass all tests in the test suite.

#### 3.16.3.4 W3C VC Examples

This [repository](#) hosts example credentials, as well as documents needed to construct them. When contributing an example, you are encouraged to provide everything needed to generate and verify a credential. Do your best not to include ANY broken links or missing documentation. If possible, try to make the credential id resolvable as well.

#### 3.16.3.5 W3C Digital Identity Guidelines (NIST-800-63) Comments

This [document](#) serves as a collection of the W3C Credentials Community Group responses to Digital Identity Guidelines (NIST-800-63) Request for Comments. Please note that this is not an official W3C position, but the compendium of feedback from the Credentials Community Group, which is a group consisting of W3C members, W3C working group participants, industry, and the general public.

#### 3.16.3.6 W3C Decentralized Identifier Core Registries`

This [repository](#) contains a registry created by the W3C Decentralized Identifier Working Group (DID WG) for the purpose of enhancing DID ecosystem interoperability.

#### 3.16.3.7 W3C VC API Goals

The W3C CCG VC APIs are a set of RESTful API definitions conforming with the OpenAPI 3.0 Specification (formerly known as Swagger) for the roles of Issuer, Verifier, and Holder as described in the VC Data Model specification. These APIs provide a [standard set of interfaces](#) by which interoperability may be tested and verified by various parties who leverage Verifiable Credentials (VCs).

### 3.17 DIF (Decentralized Identity Foundation)

#### 3.17.1 Working Groups

#### 3.17.2 DIF Interoperability Project

A [project](#) to demonstrate continuous technical demonstration of interoperability between DID Methods, Wallets, Agents, Encrypted Data Vaults, and Verifiable Credentials.

The project consists of a series of tools and web applications.

- Meeting page/agendas
- Meeting recordings

#### 3.17.3 Standards

##### 3.17.3.1 DIF & Aries DID Peer Method Specification

This document defines a "peer" DID Method that conforms to the [DID Spec](#). The method can be used independent of any central source of truth, and is intended to be cheap, fast, scalable, and secure. It is suitable for most private relationships between people, organizations, and things. We expect that peer-to-peer relationships in every blockchain ecosystem can benefit by offloading pairwise and n-wise relationships to peer DIDs.

##### 3.17.3.2 DIF & Aries DIDComm Messaging

The purpose of this [document](#) is to provide a secure, private communication methodology built atop the decentralized design of DIDs.

##### 3.17.3.3 DIF Well Known DID Configuration

Making it possible to connect existing systems and Decentralized Identifiers (DIDs) is an important undertaking that can aid in bootstrapping adoption and usefulness of DIDs. One such form of connection is the ability of a DID controller to prove they are the same entity that controls an origin.

The [DID Configuration resource](#) provides proof of a bi-directional relationship between the controller of an origin and a DID via cryptographically verifiable signatures that are linked to a DID's key material. This document describes the data format of the resource and the resource location at which origin controllers can publish their DID Configuration.

##### 3.17.3.4 DIF Presentation Exchange 2.0.0

This [Presentation Exchange](#) specification codifies a Presentation Definition data format Verifiers can use to articulate proof requirements, and a Presentation Submission data format Holders can use to describe proofs submitted in accordance with them.

This specification is designed to be both Claim format and transport envelope agnostic, meaning an implementer can use JSON Web Tokens (JWTs), Verifiable Credentials (VCs), JWT-VCs, or any other JSON Claim format, and convey them via Open ID Connect, DIDComm, Credential

Handler API, or any other transport envelope. The goal of this flexible format- and transport-agnostic mechanism is to enable unified procedures and code, thereby reducing potentially redundant code and processing requirements.

### 3.17.3.5 DIF Identity Hub

Identity Hub is a DRAFT [specification](#) under development. It incorporates requirements and learnings from related work of many active industry players into a shared specification that meets the collective needs of the community.

The specification will be updated to incorporate feedback, from DIF members and the wider community, with a reference implementation being developed within DIF that exercises the features and requirements defined here. We encourage reviewers to submit GitHub Issues as the means by which to communicate feedback and contributions.

### 3.17.3.6 DIF Credential Manifest

The [Credential Manifest](#) is a common data format for describing the inputs a Subject must provide to an Issuer for subsequent evaluation and issuance of the credential(s) indicated in the Credential Manifest.

### 3.17.3.7 DIF Sidetree

Sidetree is a protocol for creating scalable Decentralized Identifier networks that can run atop any existing decentralized anchoring system (e.g. Bitcoin, Ethereum, distributed ledgers, witness-based approaches) and be as open, public, and permissionless as the underlying anchoring systems they utilize. The protocol allows users to create globally unique, user-controlled identifiers and manage their associated PKI metadata, all without the need for centralized authorities or trusted third parties. The [syntax of the identifier and accompanying data model](#) used by the protocol is conformant with the W3C Decentralized Identifiers specification. Implementations of the protocol can be codified as their own distinct DID Methods and registered in the W3C DID Method Registry.

### 3.17.3.8 DIF DID Universal Resolver

The [Universal Resolver](#) resolves Decentralized Identifiers (DIDs) across many different DID methods, based on the W3C DID Core 1.0 and DID Resolution specifications. It is a work item of the DIF Identifiers&Discovery Working Group.

### 3.17.3.9 DIF DID Universal Registrar

The [Universal Registrar](#) creates/updates/deactivates Decentralized Identifiers (DIDs) across many different DID methods, based on the W3C DID Core 1.0 and DID Registration specifications.

## 3.18 [Hyperledger](#)

### 3.18.1 Aries

#### 3.18.1.1 Aries Protocol Implementations

Hyperledger Aries allows trusted online peer-to-peer interactions based on decentralized identities and verifiable credentials. Aries includes a protocol definition, tools, and reference implementations. The Aries protocol supports identities rooted in a variety of distributed ledgers or blockchains. This approach to identity is often called Self Sovereign Identity (SSI).

Key components of an Aries solution are:

- agents,
- DID communications,
- protocols
- and key management

There are 2 types of Aries RFCs:

- describe individual features (in the [features folder](#))
- explain concepts underpinning many features (in the [concepts folder](#))

#### 3.18.1.2 Aries RFC 0231: Biometric Service Provider

This [specification](#) characterize the functions and schema that biometric service providers (BSPs) must implement to ensure a uniform interface to clients: wallets and agents.

For example, current Automated Biometric Information Systems (ABIS) and other standards (IEEE 2410, FIDO) provide a subset of services but often require proprietary adaptors due to the fragmented history of the biometric market: different modalities (face, fingerprint, iris, etc.) require different functions, schema, and registration information.

More recently, standards have begun to specify functions and schema across biometric modalities. This specification will adopt these approaches and treat biometric data within an encrypted envelope across modalities.

#### 3.18.1.3 Aries RFC 0270: Interop Test Suite

This [document](#) describes the goals, scope, and interoperability contract of the Aries Interop Test Suite. Does NOT serve as a design doc for the test suite code, or as a developer guide explaining how the test suite can be run; see the test suite codebase for that.

#### 3.18.1.4 Aries RFC 0289: The Trust Over IP Stack

This [document](#) introduces a complete architecture for Internet-scale digital trust that integrates cryptographic trust at the machine layer with human trust at the business, legal, and social layers.

### 3.18.1.5 Aries RFC 0281: Aries Rich Schemas

The [proposed schemas](#) are JSON-LD objects. This allows credentials issued according to the proposed schemas to have a clear semantic meaning, so that the verifier can know what the issuer intended. They support explicitly typed properties and semantic inheritance. A schema may include other schemas as property types, or extend another schema with additional properties. For example a schema for "employee" may inherit from the schema for "person."

Schema objects are processed in a generic way defined in Rich Schema Objects Common.

### 3.18.1.6 Aries RFC 0104: Chained Credentials

This [document](#) describes a set of conventions, collectively called chained credentials, that allows data in a verifiable credential (VC) to be traced back to its origin while retaining its verifiable quality. This chaining alters trust dynamics. It means that issuers late in a chain can skip complex issuer setup, and do not need the same strong, globally recognizable reputation that's important for true roots of trust. It increases the usefulness of offline verification. It enables powerful delegation of privileges, which unlocks many new verifiable credential use cases.

Chained credentials do not require any modification to the standard data model for verifiable credentials; rather, they leverage the data model in a simple, predictable way. Chaining conventions work (with some feature variations) for any W3C-conformant verifiable credential type, not just the ones developed inside Hyperledger.

### 3.18.1.7 Aries RFC 0013: Data Overlays

This [document](#) describes a standard approach to data capture that separates raw schema building blocks from additional semantic layers such as data entry business logic and constraints, knowledge about data sensitivity, and so forth.

### 3.18.1.8 Aries RFC 0167: Data Consent Lifecycle

This [RFC](#) illustrates a reference implementation for generating a consent proof for use with DLT (Distributed Ledger Technology). Presenting a person controlled consent proof data control architecture and supply chain permissions, that is linked to the single consent proof.

The objective of this RFC is to move this reference implementation, once comments are processed, to a working implementation RFC, demonstrating a proof of consent for DLT.

This RFC breaks down key components to generate an explicit consent directive with the use of a personal data processing notice (PDP-N) specification which is provided with this RFC as a template for smart privacy. Appendix - PDP - Notice Spec (DLC Extension for CR v2)

## Standards Inventory for the future of digital identity

This reference RFC utilises a unified legal data control vocabulary for notification and consent records and receipts (see Appendix A), maintained by the W3C Data Privacy Vocabulary Control Community Group (DPV), where the unified data control vocabulary is actively being maintained.

This RFC modularizes data capture to make the mappings interchangeable with overlays (OCA -Ref), to facilitate scale of data control sets across contexts, domains and jurisdictions.

### 3.18.1.9 Aries RFC 0103: Indirect Identity Control

This [RFC](#) compares and contrasts three forms of indirect identity control that have much in common and that should be explored together: delegation, guardianship, and controllership. Recommends mechanisms that allow identity technology to model each with flexibility, precision, and safety. These recommendations can be applied to many decentralized identity and credentialing ecosystems--not just to the ones best known in Hyperledger circles.

### 3.18.1.10 Aries RFC 0430: Machine-Readable Governance Frameworks

This [document](#) explains how governance frameworks are embodied in formal data structures, so it's possible to react to them with software, not just with human intelligence.

### 3.18.1.11 Aries RFC 0051: DKMS (Decentralized Key Management System) Design and Architecture

This [design and architecture for a decentralized key management system \(DKMS\)](#) has been developed by **Evernym** Inc. under a contract with the U.S. Department of Homeland Security Science & Technology Directorate.

This fourth draft is being released on 29 Mar 2019 to begin an open public review and comment process in preparation for DKMS to be submitted to a standards development organization such as OASIS (Organization for the Advancement of Structured Information Standards) for formal standardization.

### 3.18.1.12 Aries Protocol Test Suite

The [APTS](#) (Aries Protocols Test Suite), allows you to test your agent for Aries compatibility and automatize it.

### 3.18.1.13 Aries Cloud Agent Python (ACA-Py)

This [github](#) is a foundation for building Verifiable Credential (VC) ecosystems. It operates in the second and third layers of the Trust Over IP framework (PDF) using DIDComm messaging and Hyperledger Aries protocols. The "cloud" in the name means that ACA-Py runs on servers (cloud, enterprise, IoT devices, and so forth), and is not designed to run on mobile devices.



### 3.18.2 Indy

#### 3.18.2.1 Indy: Anonymous Credential Protocol

This [document](#) describes the protocol for Camenisch-Lysyanskaya signatures and the anonymous credentials they enable.

### 3.19 OWF (Open Wallet Foundation)

The [OWF](#) is a consortium of companies and non-profit organisations collaborating to drive global adoption of open, secure and interoperable digital wallet solutions as well as providing access to expertise and advice through our Government Advisory Council.

The OWF aims to set best practices for digital wallet technology through collaboration on standards-based OSS components that issuers, wallet providers and relying parties can use to bootstrap implementations that preserve user choice, security and privacy.

The OpenWallet Foundation is a project of Linux Foundation Europe.

### 3.20 INATBA (International Association of Trusted Blockchain Applications)

[INATBA](#), the International Association of Trusted Blockchain Applications, has been launched with the support of the European Commission on 3 April 2019.

It brings together representatives of the stakeholders across the value chain: industry, startups and SMEs, policy makers, international organisations, regulators, civil society and standard-setting bodies to support blockchain and Distributed Ledger Technology (DLT) to be mainstreamed and scaled-up across multiple sectors.

It offers developers and users of DLT a global forum to interact with regulators and policy makers and bring blockchain technology to the next stage. On 11-13 November 2019 INATBA together with EU Blockchain Observatory and forum, Alastria and the European Commission co-organised the Global blockchain congress CONVERGENCE, of which the next iteration is being anticipated in 2023.

INATBA has several Working Group:

#### 3.20.1 INATBA Standards Committee

The [standardization WG](#) support the development and adoption of interoperability guidelines, specifications and global standards, to enhance trusted, traceable, user-centric digital services, liaise with standards development organisations and to develop contributions to standardisation, such as use cases and requirements. Relevant for standardisation are also the interoperability and governance working groups.

### 3.20.2 INATBA Identity Committee

The [Identity WG](#) aims at facilitating the exchange of ideas, best practices and domain-specific knowledge between the digital identity and blockchain communities, including researchers, governments and international institutions. The Working Group supports and fosters the creation of an identity ecosystem for interoperable, trusted blockchain services. This will be achieved by providing compliance and foundational layers for the governance and interoperability of identity systems that can be used in blockchain applications.

### 3.20.3 INATBA Privacy Committee

The [Privacy WG](#) gathers mutual interest amongst INATBA members to obtain more guidance and particular help from the regulators. This may lead to issued guidance, on the European level from the EDPB, change of current regulations and taking this key technology into account when drafting new regulations.

### 3.21 [EUBOF \(EU Blockchain Observatory and Forum\)](#)

The [EU Blockchain Observatory and Forum](#)'s goal is to create a community to discuss and highlight key developments of blockchain technology and strengthen partnerships in Europe and beyond. It is committed to enhancing the understanding of the blockchain technology, its applications, and the larger economic ecosystems in which it can play an important role.

### 3.22 [Kantara](#)

#### 3.22.1 Kantara User-Managed Access (UMA) 2.0

This [document](#) is a federated authorization framework that defines an extension OAuth 2.0 grant type and uses OAuth and federated identity technologies in various other ways.

It defines how resource owners can control protected-resource access by clients used by arbitrary requesting parties, where the resources reside on any number of resource servers, and where a centralized authorization server governs access based on resource owner policies.

#### 3.22.2 Kantara Consent Receipt Specification

A Consent Receipt is record of authority granted by a Personally Identifiable Information (PII) Principal to a PII Controller for processing of the Principal's PII. The record of consent is human-readable and can be represented as standard JSON.

This [specification](#) defines the requirements for the creation of a consent record and the provision of a human-readable receipt. The standard includes requirements for links to existing privacy notices & policies as well as a description of what information has been or will be collected, the purposes for that collection as well as relevant information about how that information will be used or disclosed. This specification is based on current privacy and

data protection principles as set out in various data protection laws, regulations and international standards.

### 3.22.3 Kantara Blinding Identity Taxonomy

This [BIT](#) (Blinding Identity Taxonomy) Initiative (revised December 2019) provide the needed common standards to help protect the identity of any governed entity, and to contribute to .

BIT classifies 49 different elements which require cryptographically encoding to prevent the re-identification of any governed entity, including organisations and individuals.

Some of these elements can directly identify organisations and individuals, such as a name, physical address or bank account details, and some of them can do so indirectly, such as a photo, IP address or cookie browser identifier.

### 3.23 [IEEE \(Institute of Electrical and Electronics Engineers\)](#)

The [IEEE](#) has [standards and pre-standards activities relevant to Electronic Identification and Trust Services](#), including dealing with blockchain technology and biometric identification.

Relevant Standards Activities and Active Standards are:

- IEEE P2048.4 - Standard for Virtual Reality and Augmented Reality: Person Identity
- IEEE P2049.3 - Standard for Human Augmentation: Identity
- IEEE Std 2410-2019, IEEE Standard for Biometric Open Protocol
- IEEE P2733, Standard for Clinical Internet of Things (IoT) Data and Device
- Interoperability with TIPPSS - Trust, Identity, Privacy, Protection, Safety, Security
- IEEE P2790, Standard for Biometric Liveness Detection
- IEEE P2799, Standard for Confirming and Conveying Identity Over the Internet

#### 3.23.1 IEEE Computer Society Blockchain and Distributed Ledgers (BDL) Standards Committee

This [Committee](#) manages the development of standards within the area of blockchains and distributed ledgers, including standards for relevant data formats, the development and implementation of blockchains and distributed ledger systems, and for applications of blockchains and distributed ledgers to specific sectors, industries, and processes.

#### 3.23.2 IEEE Consumer Technology Society (CTSoc) Standards Committee

The field of interest of this [committee](#) is engineering and research aspects of the theory, design, construction, manufacture or end-use of mass-market electronics, systems, software and services for consumers.

The Standards Committee shall develop standards covering the field of interest defined in the IEEE Consumer Technology Society Constitution.

In the event that the Standards Committee determines that a new standard is needed but does not fall within the purview of the Standards Committee's subcommittees, the Standards Committee itself may elect to sponsor the standard.

### 3.24 ICAO (International Civil Aviation Organization)

The [ICAO](#) is a specialized and funding agency of the United Nations. It changes the principles and techniques of international air navigation and fosters the planning and development of international air transport to ensure safe and orderly growth. The ICAO Council adopts standards and recommended practices concerning air navigation, its infrastructure, flight inspection, prevention of unlawful interference, and facilitation of border-crossing procedures for international civil aviation

Relevant Standards Activities and Active Standards are:

#### 3.24.1 ICAO Doc9303 - Machine Readable Travel Documents

[ICAO Doc9303](#) consists of various separate documents in which general (applicable to all MRTDs) as well as MRTD form factor specific specifications are grouped.

These specifications are not intended to be a standard for national identity documents. However, a State whose identity documents are recognized by other States as valid travel documents shall design its identity documents such that they conform to the specifications of Doc 9303-3 and Doc 9303-4, Doc 9303-5 or Doc 9303-6.

#### 3.24.2 ICAO DTC - Virtual Component Data Structure and PKI Mechanisms

This [WG3TF5 N0290 TR](#) technical report (Version - 1.2, October 2020) specifies the file structure of the Digital Travel Credentials (DTC) and the associated PKI to support the DTC.

Authors are ISO/IEC JTC 1/SC 17 - Cards and security devices for personal identification WG3/TF5.

### 3.25 EPC (European Payments Council)

The [EPC](#) was founded in 2002. It calls itself "the decision-making and coordination body of the European banking industry in relation to payments". The main task of the EPC is the development of the Single Euro Payment Area. The 74 members are banks and banking associations.

#### 3.25.1 EPC004-16/ 2021 - SEPA Instant Credit Transfer - Scheme Rulebook

The [EPC004-16/ 2021 rulebook](#) makes reference to various defined terms which have a specific meaning in the context of this Rulebook.

In this Rulebook, a defined term is indicated with a capital letter. A full list of defined terms can be found in Section 7 of this Rulebook. The Rulebook may make reference to terms that are also used in the Payment Services Directive (PSD).

### 3.25.2 EPC PSD3 (Payment Services Directive)

The terms used in this Rulebook may not in all cases correspond in meaning to the same or similar terms used in the PSD. On June 28, 2023, the European Commission (EC) published a set of new legislative proposals, notably for a [Third Payment Services Directive \(PSD3\)](#) and a Payment Services Regulation (PSR).

It foresees changes to the foundational framework of the European payments market and is likely to have a material impact on the players subject to it, both from a legal and operational perspective.

### 3.26 GSMA (Global System for Mobile communications)

The GSM Association (originally Groupe Spécial Mobile) is a lobby organisation that represents the interests of mobile network operators worldwide. More than 750 mobile operators are full GSMA members and a further 400 companies in the broader mobile ecosystem are associate members. The GSMA represents its members via industry programmes, working groups and industry advocacy initiatives

#### 3.26.1 GSMA SAM (Secured Applications for Mobile)

The [Secured Applications for Mobile specification](#) defines a capability allowing cellular connected Devices to use a wide range of secured applets within an eUICC. Such applets can be managed by a service provider, and may be paired with applications running in the Device itself. The work will focus on the eUICC where the secured applets will operate independently and outside of any eUICC Profile.

#### 3.26.2 GSMA Embedded SIM

The GSMA's [Embedded SIM Specification](#) provides a single, de-facto standard mechanism for the remote provisioning and management of machine to machine (M2M).

GSMA Embedded SIM is a vital enabler for Machine to Machine (M2M) connections including the simple and seamless mobile connection of all types of connected machines.

In the M2M market the SIM may not easily be changed via physical access to the device or may be used in an environment that requires a soldered connection, thus there is a need for 'over the air' provisioning of the SIM with the same level of security as achieved today with traditional removable SIM.

### 3.27 Closed initiatives

#### 3.27.1 e-SENS (Electronic Simple European Networked Services)

[e-SENS](#) is a large-scale pilot launched within the ICT policy support programme (ICT PSP), under the competitiveness and innovation framework programme (CIP). The aim of the project is to develop an infrastructure for interoperable public services in Europe. It builds upon and consolidates building blocks such as eID, e-Documents, e-Delivery, and e-Signature etc. from previous pilot projects and integrates them into a European digital platform for cross-sector, interoperable eGovernment services.

#### 3.27.2 STORK

[STORK](#) is a EU co-funded project to establish a European eID interoperability platform that will allow citizens to establish new e-relations across-borders, just by presenting their national eID.

The STORK 2.0 project was the continuation of STORK and has worked on extending the specification to roles and mandates.

In the context of the eIDAS Regulation and the implementing act on the interoperability framework for eID technical specifications are being developed for the eIDAS nodes. These technical specifications will provide further details on technical requirements as set out in the Regulation. The specifications for the eIDAS were developed through Member State collaboration in a technical sub-committee of the eIDAS Expert Group.

#### 3.27.3 SSEDIC (Scoping the Single European Digital Identity Community)

[SSEDIC](#) is an ICT PSP funded Thematic Network launched in December 2010 for a 3 years assignment. The SSEDIC network represents 35 partners and more than 30 associated partners who joined the network in the first project year.

The objective of SSEDIC is to provide a neutral platform for all the stakeholders of eID (electronic identity) to work together and collaborate to prepare the agenda for a proposed Single European Digital Identity Community as envisaged by the Digital Agenda (DAE) in its Key Action 16.

#### 3.27.4 FIDIS (Future of Identity in the Information Society)

[FIDIS](#) opened in 2004, and closed in 2009 ([CORDIS link](#)).

#### 3.27.5 PRIME - Privacy and identity management for Europe

The [PRIME](#) project receives research funding from the Community's Sixth Framework Programme and the Swiss Federal Office for Education and Science. From March 2004 until February 2008, 16 M€, 20 partners, W3C involved as subcontractor.

### 3.27.6 ESSIF (European Self Sovereign Identity Framework) Laboratory

Self-sovereign identity (SSI) supports identity management in a safe and reliable internet allowing secure transactions and eliminating logins. SSI aims to empower EU organisations to make secure and innovate transactions with stakeholders saving billions of euro on administrative expenses. SSI integration will also generate new jobs and business opportunities. However, even though SSI solutions have expanded worldwide, the vast majority target specific problems in specific fields and rarely interoperate.

The EU-funded [eSSIF-Lab](#) project is an innovation project aiming to reinforce internet reliability with electronic identities through the development and adoption of SSI technologies. The end goal is to advance the broad uptake of SSI as a next-generation open and trusted digital identity solution.

This Lab was closed in December 2022, sharing feedbacks to the [EBSI](#) roadmap and the legal, security, and technical governance.

## 4 Other identity projects

### 4.1 KERI (Key Event Receipt Infrastructure)

[KERI](#) is a decentralized identity framework (and system), ledger-less which means it doesn't need to use a ledger at all or ledger-portable which means that its identifiers are not locked to any given ledger and may switch as needed. In other words KERI identifiers are truly portable.

KERI uses best practices for key management which include a novel key rotation scheme called pre-rotation. This simplifies key management infrastructure. Pre-rotation is also post-quantum secure. KERI supports enterprise scalability features such as delegated identifiers that support hierarchical key management infrastructure.

KERI is open Apache2, hosted by the DIF which operates under the umbrella of the Linux Foundation, and founded by [Samuel M. Smith](#) from Sovrin and Consensus.

### 4.2 MATTR BBS+ Signature Scheme

This [document](#) describes the BBS+ signature scheme. The scheme features many important properties:

- The signature is over a group of Pedersen commitments--signatures can be created blinded or un-blinded.
- The signature is encoded as a single group element and two field elements.
- Verification requires 2 pairing operations.
- Simple signature schemes require the entire signature and message be disclosed during verification. BBS+ allows a fast and small zero-knowledge signature proof of knowledge to be created from the signature and the public key. This allows the signature holder to selectively reveal any number of signed messages to another entity (none, all, or any number in between).

### 4.3 Digital Bazaar Credential Handler API polyfill

The [CHAPI polyfill](#) provides a number of features that enable the issuance, holding, presentation, and general management of Verifiable Credentials, Authorization Capabilities, and a variety of other cross-origin credentials.

### 4.4 Spruce DIDkit

[DIDKit](#) provides Verifiable Credential and Decentralized Identifier functionality across different platforms. DIDKit's core libraries are written in Rust due to Rust's expressive type system, memory safety, simple dependency web, and suitability across different platforms including embedded systems, but the comprehensive DIDKit SDK includes many libraries and interfaces for using it almost everywhere.



#### 4.5 [Schema.org](#)

[Schema.org](#) is a collaborative, community activity with a mission to create, maintain, and promote schemas for structured data on the Internet, on web pages, in email messages, and beyond.

Schema.org vocabulary can be used with many different encodings, including RDFa, Microdata and JSON-LD. These vocabularies cover entities, relationships between entities and actions, and can easily be extended through a well-documented extension model. Over 10 million sites use Schema.org to markup their web pages and email messages. Many applications from Google, Microsoft, Pinterest, Yandex and others already use these vocabularies to power rich, extensible experiences.

Founded by Google, Microsoft, Yahoo and Yandex, Schema.org vocabularies are developed by an open community process, using the public-schemaorg@w3.org mailing list and through GitHub.

- Schemas: The actual schemas, arranged in a hierarchy, with a page for each item in the schema.
- The full type hierarchy: The full type hierarchy, in a single file.
- Frequently asked questions
- Data model: a brief note on the data model used, etc.
- Style Guide: naming conventions and related patterns for schema authoring.
- Developers: developer-oriented information about schema.org
- Vocabulary definition download: download definition files for core vocabulary and extensions.
- Extension Mechanism: The extension mechanism that can be used to extend the schemas.
- Schema.org COVID-19 response: US CDC Data Table fields
- Overview of dataset-related vocabulary.

#### 4.6 [Public Sector Profile of the Pan-Canadian Trust Framework](#)

The [PCTF](#) is a model that consists of a set of agreed-on concepts, definitions, processes, conformance criteria, and an assessment approach. It is not a “standard” as such, but is, instead, a framework that relates and applies existing standards, policies, guidelines, and practices, and where such standards and policies do not exist, specifies additional criteria. The role of the PCTF is to complement existing standards and policies such as those concerned with security, privacy, and service delivery.