DRAFT EU-US TTC Digital Identity Mapping Exercise Report

22 December 2023

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

Table of Contents

Executive Summary

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.

This report provides the preliminary results of the initial transatlantic mapping exercise. It includes a mapping of definitions, assurance levels, and references to international standards across the NIST Digital Identity Guidelines (Special Publication 800-63, Revision 3) and 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.

The EC and the US established comparisons at three levels: a taxonomical approach to concepts used in each framework; a mapping of the different levels of assurance of the digital identities systems considered in the EU and the US; and a listing of international standards referenced in each authoritative document.

The NIST guidelines provide technical requirements for organisations implementing digital identity services, and while their use is mandatory for US federal agencies, adoption of the guidelines is not compulsory for other organisations or sectors unless otherwise prescribed through policy. The EU, however, has proposed a mandatory regulatory model to be adopted by the EU Member States. The distinct standards ecosystems on either side of the Atlantic are acknowledged in this report as well, with their commonalities and differences informing this mapping exercise.

A key takeaway from this report is that there are no major concepts that do not map to a companion concept, and any differences in the specific use of terms are minor. Where EC and US approaches differ most is on the topic of trust services, which are not explicitly addressed in NIST SP 800-63. As with the definitions mapping, the EU and US approaches to levels of assurance share significant commonalities, with both frameworks relying on three ascending levels to indicate increasing confidence in the means of identification. However, the NIST guidelines separate out the three ascending levels of assurance into three components—identity, authentication, and federation assurance levels—while the EU regulation relies solely on one overarching component: levels of assurance. Section 3 summarizes the findings of the mapping exercise. A multi-tab spreadsheet detailing the results of the mapping exercise may be viewed HERE as well.

Representatives of the WG1 Digital Identity Subgroup will build on the success of the first part of the mapping process with two further elements: collecting feedback on open questions that will need to be addressed in the future; and selecting potential use cases that could facilitate EU and US interest in the cross-border use of digital identities. In the future, a similar mapping could be envisaged upon the finalisation of NIST SP 800-63, Revision 4, and development of Implementing Regulations and

other supporting guidance relevant once the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity has been adopted.

To begin working towards this second phase of the mapping process, the EC and the US are actively seeking feedback from communities with subject matter expertise in digital identity, privacy, human-centred design, and cybersecurity; organisations that have designed or implemented digital identity systems within the EU, the US, or in cross-border contexts; and others with equities related to the topic of digital identity. Additional details and instructions for providing feedback are included in sections 4 and 5 of this report.

Introduction

The EU-US Trade and Technology Council (TTC) was formed at the EU-US Summit in June 2021 by US President Joseph R. Biden, European Commission President Ursula von der Leyen and European Council President Charles Michel. The TTC's overall objective is to promote EU and US competitiveness and prosperity and the spread of democratic, market-oriented values by increasing transatlantic trade and investment in products and services of emerging technology. In this way our technological and industrial leadership will be strengthened, innovation boosted, and critical and emerging technologies and infrastructure protected and promoted. Through the TTC, the EU and US cooperate on the development and deployment of new technologies based on shared democratic values, including respect for human rights, that encourage compatible standards and regulations.

Working Group 1: Technology Standards (WG1) has advanced collaboration in the promising area of digital identity. The Digital Identity Subgroup under WG1 has held a series of government-to-government technical exchanges, and in March 2023 a public event was jointly hosted to engage with subject matter experts from government, industry, civil society, and academia. During this event, representatives of the subgroup announced their intent to develop a transatlantic mapping of digital identity resources, initiatives, and use cases. The aim is to advance transatlantic pre-standardisation research efforts, facilitate interoperability, and streamline implementation guidance while respecting human rights.

The preliminary results of the initial transatlantic mapping exercise are enclosed in this report and include a mapping of definitions, assurance levels, and references to international standards across the NIST Digital Identity Guidelines (Special Publication 800-63, Revision 3) (henceforth NIST Special Publication 800-63-3) and 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 (henceforth EU No 910/2014 or eIDAS regulation).

The publication of this draft mapping is a first step in a larger process to support the outcomes of the TTC.

1. Purpose and methods

The mapping exercise presented in this document is a first step towards building a shared understanding of digital identity initiatives on both sides of the Atlantic. In the future, the contents of this report could be used as a resource to understand and coordinate approaches towards use of electronic identities, which could yield positive impacts not only for international trade and electronic commerce, but also for improved delivery of essential services, opportunities for trusted research collaborations between partners of different institutions, and enhanced confidence in everyday transactions online.

Both sides of the Atlantic aim to provide easier and more secure access to online services to their citizens, with shared values of privacy, security, civil liberties, equity, accessibility, and interoperability.

Trust, security, and usability of digital identities are of paramount importance to facilitate widespread adoption by individuals and organizations. Strong transatlantic cooperation on emerging technologies and standardisation can contribute to creating the conditions for meaningful strides in adoption to occur.

The EU aims to provide access to digital identities to one hundred per cent of its citizens by 2030, as part of Europe's Digital Decade 2030 targets. The US government has included in its National Cybersecurity Strategy the objective of supporting the development of a Digital Identity Ecosystem and has highlighted digital identity as a critical and emerging technology in its US Government National Standards Strategy. Both sides of the Atlantic aim to provide easier and more secure access to online services to their citizens, with shared values of privacy, security, civil liberties, equity, accessibility, and interoperability.

However, the two frameworks being compared in this exercise have some different fundamentals.

The NIST guidelines provide technical requirements for organisations implementing digital identity services, and while their use is mandatory for US federal agencies, adoption of the guidelines is not compulsory for other organisations or sectors unless otherwise prescribed through policy. The NIST guidelines are currently undergoing their fourth major revision, with publication anticipated in 2024.

The EU model is based on a regulation that is directly applicable by the EU Member States. In November 2023, the European Parliament and the Council reached a provisional agreement on a new European Digital Identity Framework. Once adopted, the regulation will require Member States to offer European Digital Identity Wallets to citizens, residents and businesses. The draft EU Regulation is currently under legislative scrutiny and must be voted by the Parliament and formally adopted by the Council before it will enter into force.

Given the status of both the EU Regulation and the NIST Digital Identity Guidelines, the mapping exercise between the EU and the US approaches included only the current, stable versions of text, and has established comparisons at three different levels:

- a comprehensive taxonomical approach to concepts used in each of the frameworks.
- a detailed mapping of the different levels of assurance considered in the EU and the US
- a listing of international standards referenced in each authoritative document.

This initial report on the mapping exercise between the digital identity approaches in the EU and the U.S aims to cover these first three steps. It will be complemented in the coming months with at least two additional elements, including:

- open questions across the ecosystem affecting use and interoperability of digital identity systems that will need to be addressed in the future through cooperative transatlantic effort.
- a selection of potential use cases for transatlantic cooperation that highlight the need for and value of enabling the cross-border use of digital identities.

The focus on specific use cases for cross-border cooperation and the identification of issues or problems that may need further work can be very relevant as part of pre-standardisation research in the field.

It is important to note that digital identity approaches are in constant evolution in the EU and the US The exercise presented in this report takes as a reference the latest published versions of the respective authoritative documents:

- NIST Special Publication 800-63-3: Digital Identity Guidelines.
- 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) 2015/1502 of 8 September 2015 on setting 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 (Text with EEA relevance).

2. Standards ecosystems in the EU and the US

The EU and the US have developed distinct comprehensive standards ecosystems for digital identity. These ecosystems present key differences in their areas of focus, format, and applications across the public and private sectors. However, they also share commonalities as both ecosystems tackle the same challenges and threats around digital identity, which are on the rise due to the increased digitalisation of societies and economies.

Both the EU and the US are currently in the process of updating their identity frameworks to provide guidance to the public and private sectors on how to safeguard an individual's digital identity against the latest cyberthreats, and to support the increasingly mobile-based manner by which individuals manage their identity and engage with services both online and offline.

However, they also share commonalities as both ecosystems tackle the same challenges and threats around digital identity, which are on the rise due to the increased digitalisation of societies and economies.

2.1 US identity guidelines

The US identity guidelines take the format of 'Digital Identity Guidelines' published by NIST (NIST Special Publication 800-63). These guidelines are grouped into four volumes:

(i) Base Volume - digital identity and risk management
(ii) Volume A - identity proofing and enrolment
(iii) Volume B - authentication and lifecycle management
(iv) Volume C - federation and assertions

These guidelines define technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions. They provide mandatory technical requirements for US federal agencies implementing digital identity services, and cover identity proofing and authentication of users (both public and internal) interacting with government IT systems over open networks. One example of a system where they are required is the US government's Login.gov, a unified login for federal government services. The NIST guidelines are not mandatory requirements outside of the US federal government level unless otherwise specified by law but are recommended for consideration by private sector organisations and state, local, tribal, and territorial governments.

NIST is currently updating its NIST Special Publication 800-63 as part of the fourth revision of these guidelines. This revision process was kicked off by a call for comments in September 2020, followed by a first draft update and accompanying second comment period, launched in December 2022. The

second comment period closed in April 2023. At the time of this report's publication, NIST is actively adjudicating over 3 000 unique comments with the intent to issue a second draft accompanied by a third round of public comment across all four volumes. NIST aims to adopt the fourth revision of the guidelines by US federal fiscal year 2024.

2.2 EU identity framework

The EU identity principles are set down in legislation via the eIDAS Regulation (EU Regulation 910/2014) and its eight implementing acts. This legislation establishes the basis for cross-border recognition of electronic identity (eID) schemes within the EU by mandating the set-up of infrastructure to facilitate cross-border interactions involving identification and defining the concept of an 'eIDAS-notified' eID scheme.

An eIDAS-notified eID scheme is one which is developed at the Member State level and, upon notification to the European Commission, undergoes a peer review conducted by other Member States against three levels of identify assurance ('low', 'substantial', or 'high'). The Regulation, its implementing acts, and associated guidance establish the technical standards and processes that must be followed in the context of eIDAS-notified eID schemes and the mandated cross-border infrastructure.

The eIDAS Regulation and its associated implementing acts will be revised by the EU Digital Identity Wallet Regulation that will be adopted in 2024 and come into force by 2026. The associated implementing acts will also be revised because new implementing acts are developed during the twelve months following adoption. The revised Regulation will mandate that each EU Member State issues a digital wallet that is compliant with the technical standards and specifications established by the revised implementing acts. Individuals will be able to store their identities in these wallets by onboarding via an eIDAS-notified eID scheme at level of assurance 'high'. These wallets will also be certified at assurance level high in line with EU cybersecurity and privacy requirements in place.

2.3. Mapping EU and US identities

This report maps active guidance on digital identity in the EU and the US and does not include a mapping of the proposed revisions to the NIST guidelines (i.e. Revision 4 of NIST SP 800-63) or to the future EU Digital Identity Wallet regulation.

The preliminary mapping exercise has three parts:

(i) mapping the definitions that exist in the respective reference documents in order to identify commonalities and differences.
(ii) mapping the identity assurance frameworks and levels that exist.
(iii) mapping the international standards referenced by each authoritative document.

Table 1. US framework for assessing identity systems

Identity assessment type	Description	Levels
Identity assurance level (IAL)	A category that conveys the degree of confidence that a person's claimed identity is their real identity, as defined in [NIST SP 800-63-3] in terms of three levels	IAL 1 (Some confidence) IAL 2 (High confidence) IAL 3 (Very high confidence)
Authenticator assurance level (AAL)	A measure of the strength of an authentication mechanism and, therefore, the confidence in it, as defined in [NIST SP 800-63-3] in terms of three levels	AAL1 (Some confidence) AAL2 (High confidence) AAL3 (Very high confidence)
Federation assurance level (FAL)	A category that describes the federation protocol used to communicate an assertion containing authentication and attribute information (if applicable) to an RP, as defined in [NIST SP 800-63-3] in terms of three levels	FAL 1 (Some confidence) FAL 2 (High confidence) FAL 3 (Very high confidence)

This differs from the EU, where there is one set of levels, the eIDAS 'Levels of Assurance', which are set out in Commission Implementing Regulation (EU) 2015/1502. The term 'level of assurance' refers to the degree of confidence in the claimed identity of a person. The level of assurance of an eID scheme is determined by several elements, including, among other factors, the process of obtaining the eID schemes, how the eID means is managed, and how authentication is performed. The three levels of assurance are as follows:

Table 2. EU systems for assessing levels of eID assurance

Identity assessment type	Description	Levels
eIDAS levels of assurance (LOA)	Assurance levels should characterise the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned	**Low (LOA 1):** e.g. enrolment is performed by self-registration on a webpage, without any identity verification **Substantial (LOA 2):** e.g. enrolment is performed by providing and verifying identity information, and authentication by using a username and a password and a one-time password sent to an individual's mobile phone **High (LOA 3):** e.g. enrolment is performed by registering in person in an office, and authentication by using a smartcard such as a national ID card

3. Results and observations

In a comparison of NIST Special Publication (SP) 800-63-3 and EU No 910/2014, there were no major concepts that did not map to a companion concept, and any differences in the specific use of terms were minor. The mappings, therefore, provide an effective tool for translating requirements and coordinating approaches towards use of electronic identities. A discussion of each of the mapping exercises—definitions, levels of assurance, and international standards references—follows. A multi-tab spreadsheet detailing the results of the mapping exercise may be viewed HERE as well.

In a comparison of NIST Special Publication 800-63, Revision 3 and EU No 910/2014, there were no major concepts that did not map to a companion concept, and any differences in the specific use of terms were minor.

3.1 Definitions

There is significant overlap across the definitions used in NIST SP 800-63-3 and EU No 910/2014. Although the wording is different for many definitions, in most cases the meaning is nearly identical. Where the EC and US approaches differ most is on the topic of trust services, which are not explicitly addressed in NIST SP 800-63. Specifically, the scope of EU No 910/2014 includes concepts such as qualified electronic signatures, node operators, and conformity assessment bodies, whereas the NIST guidance maintains an implementation-agnostic tone organised around a general set of roles and responsibilities, technologies, and processes. A table of common concepts and definitions is offered below to illustrate the similarities between the EU and US approaches, through three categories: ‘no match’, ‘partial match’, and ‘identical match’.

Notably, the mapping exercise did not find any terms which fell under the ‘no match’ category, highlighting the high level of similarity among EU and US digital identity concepts and definitions.

Table 3. Common concepts and definitions

Concept No match Partial match Identical match	NIST Definitions (SP 800-63-3)	EU No 910/2014 Definitions
Authentication	**Authentication:** verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources.	**Authentication:** electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed.
Authoritative source	**Authoritative source:** an entity that has access to, or verified copies of, accurate information from an issuing source such that a CSP can confirm the validity of the identity evidence supplied by an applicant during identity proofing. An issuing source may also be an authoritative source. Often, authoritative sources are determined by a policy decision of the agency or CSP before they can be used in the identity proofing validation phase.	**Authoritative source:** any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity.
Authentication factor	**Authentication factor:** the three types of authentication factors are something you know, something you have, and something you are. Every authenticator has one or more authentication factors.	**Authentication factor:** a factor confirmed as being bound to a person, which can be possession-based (something the person owns), knowledge-based (something the person knows) or inherent (something based on a physical attribute).
Certificate	**Public key certificate:** a digital document issued and digitally signed by the private key of a certificate authority that binds an identifier to a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key	**Certificate for electronic signature:** electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person.

	(see also RFC 5280).	
Identity	**Identity:** an attribute or set of attributes that uniquely describe a subject within a given context.	**Person identification data:** a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person, to be established.
Person identification data	**Personally identifiable information:** information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.	
Signature	**Digital signature:** an asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation, but not confidentiality protection.	**Electronic signature:** data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.
Relying party	**Relying party:** an entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.	**Relying party:** natural or legal person that relies upon an electronic identification or a trust service.
Risk management	**Risk management:** the programme and supporting processes to manage information security risk to organisational operations (including mission, functions, image, reputation), organisational assets, individuals, other organisations, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.	**Information security management system:** a set of processes and procedures designed to manage to acceptable levels risks related to information security.

3.2 Levels of assurance

As with the definitions mapping, the EU and US approaches to levels of assurance are more alike than they are different, each leveraging three ascending levels to indicate increasing confidence in the means of identification. Importantly, however, the NIST guidelines separate out the three ascending levels of assurance into three distinct components—identity, authentication, and federation assurance levels—while the EU relies on one overarching component.

Table 4. Approach to assurance level mapping

NIST SP 800-63-3 *Identity assurance level (IAL)* *Authenticator assurance level (AAL)* *Federation assurance level (FAL)*	**EU No 910/2014** *Level of assurance (LOA)*
IAL1, AAL1, FAL1	LOA1, Low
IAL2, AAL2, FAL2	LOA2, Substantial
IAL3, AAL3, FAL3	LOA3, High

For **identity proofing and enrolment**, the levels of assurance were compared according to four components:

1. Evidence requirements
2. Validation process
3. Verification method
4. Issuance and binding[1]

For **authentication**, the levels of assurance were compared according to eight components:

1. Allowed authenticators
2. Information security
3. Binding*
4. Issuance*
5. Suspension and revocation
6. Renewal and replacement
7. Cryptographic validation
8. Threats addressed

[1] *Note that issuance and binding content is compared across both identity and authentication assurance levels. Address confirmation is included under identity proofing and enrolment.*

3.2.1 Summary of LOA1 (IAL1/AAL1) mapping

The lowest level of assurance for identity proofing and enrolment (LOA1/IAL1) is nearly identical for NIST SP 800-63-3 and EU Regulation 910/2014.

Similarities between NIST SP 800-63-3 and EU Regulation 910/2014 at LOA1/IAL1

- No minimum requirements for evidence, validation, or verification.

Differences between NIST SP 800-63-3 and EU Regulation 910/2014 at LOA1/IAL1

- NIST SP 800-63-3: no minimum requirements for address confirmation.
- EU Regulation 910/2014: requirements for address confirmation related to binding, in which identity proofing of a natural person acting on behalf of a legal person should be verified as having been performed at level low or above; the binding should be established on the basis of nationally recognised procedures; and the natural person should not be known by an authoritative source to be in a status that would prevent that person from acting on behalf of the legal person.
- Following issuance, the electronic identification means should be delivered via a mechanism by which it can be assumed to reach only the intended person.

Similarities between NIST SP 800-63-3 and EU Regulation 910/2014 at LOA1/AAL1

- Both LOA1 and AAL1 are designed to address guessing, eavesdropping, and replay attacks.
- Both are characterised by a single authentication factor, and they both acknowledge the need for information security management, some requirements for issuance and binding, some requirements for revocation and suspension, and some requirements for renewal and replacement.

Differences between NIST SP 800-63-3 and EU Regulation 910/2014 at LOA1/AAL1

- The requirements for NIST AAL1 are more specific and action-oriented, whereas the authentication-related requirements for EU LOA1 consist largely of outcome statements.
- The NIST guidance calls out a minimum requirement for cryptographic validation while EU Regulation 910/2014 does not.

3.2.2 Summary of LOA2 (IAL2/AAL2) mapping

The mid-tier level of assurance for identity proofing and enrolment (LOA2/IAL2) has some similarities between NIST SP 800-63-3 and EU Regulation 910/2014, though the NIST guidance is more specific.

Similarities between NIST SP 800-63-3 and EU Regulation 910/2014 at LOA2/IAL2

- Verification for both NIST IAL2 and EU LOA2 centres on the applicant's possession of identity evidence. NIST IAL2 further specifies that knowledge-based verification (KBV) is not allowed for in-person identity verification.

Differences between NIST SP 800-63-3 and EU Regulation 910/2014 at LOA2/IAL2

- **Identity proofing**
  - NIST IAL2 allows for remote or in-person identity proofing and requires either one piece of superior or strong evidence; or two pieces of strong evidence; or one piece of strong evidence plus two pieces of fair evidence.
  - EU LOA2 does not specify a presence requirement for proofing and defers to Member State-recognised evidence.
- **Evidence validation**
  - NIST IAL2 requires that each piece of evidence be validated with a process that can achieve the same strength as the evidence presented.
  - EU LOA2 requires that evidence be checked to determine that it is genuine or that, according to an authoritative source, it is known to exist and relates to a real person, and that steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents. Validation leveraging an authoritative source is not required at EU LOA2.
- **Address confirmation**
  - NIST IAL2 requires address confirmation and specifies that valid records to confirm the address must originate from the issuing source or an authoritative source.
  - EU LOA2 enumerates binding requirements that build on EU LOA1's requirement that the natural person being identity-proofed is not known by an authoritative source to be in a status that would prevent that person from acting on behalf of the legal person. LOA2 increases the burden for binding by requiring that proofing of natural persons acting on behalf of legal persons be verified as having been performed at level substantial or high; that binding has been established on the basis of nationally recognised procedures, which resulted in the registration of the binding in an authoritative source; and that the binding has been verified on the basis of information from an authoritative source.

Similarities between NIST SP 800-63-3 and EU Regulation 910/2014 at LOA2/AAL2

- Both mid-tier authentication assurance levels, LOA2 and AAL2, are designed to address guessing, eavesdropping, and replay attacks, and both require multi-factor authentication (MFA).
- Requirements for suspension and revocation for LOA1/AAL1 are the same for LOA2/AAL2.

Differences between NIST SP 800-63-3 and EU Regulation 910/2014 at LOA2/AAL2

- AAL2 requires the implementation of information security controls at the moderate baseline or equivalent from the security and privacy controls for information systems listed in NIST SP 800-53, and while LOA2 acknowledges the need for an information security management system that adheres to proven standards or principles for the management and control of information security risks, it does not prescribe an approach or offer explicit guidance.
- The NIST guidance establishes a minimum requirement for cryptographic validation while EU Regulation 910/2014 does not.

3.2.3 Summary of LOA3 (IAL3/AAL3) mapping

The highest level of assurance for identity proofing and enrolment (LOA3/IAL3) across NIST SP 800-63-3 and EU Regulation 910/2014 incorporates similar requirements for evidence, validation, and verification, with some differences.

Similarities between NIST SP 800-63-3 and EU Regulation 910/2014 at LOA3/IAL3

- Validation requirements, while semantically different, are functionally similar and focus on the checking of evidence against authoritative sources to determine genuineness and that the identity to which the evidence pertains exists and relates to a real person.

Differences between NIST SP 800-63-3 and EU Regulation 910/2014 at LOA3/IAL3

- **Evidence requirements and verification**
  - Evidence requirements centre on the availability of documentation that includes a photo or biometric, though the NIST guidance allows for various combinations of types and strengths of evidence when evidence of a 'superior' strength is unavailable, whereas EU LOA3 defers to Member State-recognised evidence and processes.
  - Similarly, verification according to IAL3 must follow a process capable of achieving a strength of 'superior', meaning biometric comparison leveraging the strongest piece of evidence offered. EU LOA2 requires comparison of one or more physical characteristics of the person with an authoritative source.
- **Address confirmation**
  - EU LOA3 enumerates binding requirements that build on EU LOA2's requirement that the natural person being identity-proofed is not known by an authoritative source to be in a status that would prevent that person from acting on behalf of the legal person *and* that the binding has been established based on nationally recognised procedures which resulted in the registration of the binding in an authoritative source. LOA3 increases the burden for binding by requiring that proofing of natural persons acting on behalf of legal persons be verified as having been performed at level high; and that binding has been verified based on a unique identifier representing the legal person used in the national context and on the basis of information uniquely representing the natural person from an authoritative source. LOA3 also requires that the activation process verifies that electronic identification means are delivered only into the possession of the person to whom it belongs.
  - NIST IAL3 requires address confirmation, specifies that valid records to confirm the address must originate from the issuing source or an authoritative source, and requires that notification of proofing be sent to the confirmed address of record.

Similarities between NIST SP 800-63-3 and EU Regulation 910/2014 at LOA3/AAL3

- Both high-confidence authentication assurance levels, LOA3 and AAL3, are designed to address guessing, eavesdropping, and replay attacks, and both require MFA.
- Both LOA3 and AAL3 require the implementation of information security management controls enumerated at the lower level of assurance (LOA2/AAL2). NIST AAL3 renewal and replacement requirements are the same as AAL2. However, LOA3 adds to LOA1 (repeated at LOA2),

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

Differences between NIST SP 800-63-3 and EU Regulation 910/2014 at LOA3/AAL3

- NIST AAL3 is also designed to address verifier impersonation (phishing resistance). Authentication at AAL3 is based on proof of possession of a key through an approved cryptographic protocol; control of two distinct authentication factors bound to a subscriber account through secure authentication protocols; and MFA leveraging a hardware-based authenticator and an authenticator that provides verifier impersonation resistance.
- The NIST guidance calls out a minimum requirement for cryptographic validation while EU Regulation 910/2014 does not.

3.3 International standards references

The list of international standards referenced by each authoritative document is an important part of the mapping exercise. The results of the comparison show evident differences that can be linked to each document's nature (regulatory text in the EU versus technical guidelines in the US) and scope (focus on digital identity management practices versus integration of trust services alongside documentation of practices).

Specifically, the EU framework, eIDAS, contains several international standards references that relate to electronic signatures, which are a fundamental part of the regulatory framework and are enabled through corresponding trust services. In contrast, while the NIST Digital Identity Guidelines do not touch on electronic signatures in depth, they do refer to international standards focused on security techniques that are not covered by the eIDAS regulation.

While over two dozen international standards are referenced across the two documents, the mapping exercise shows overlap in only two areas:

- ISO/IEC 29115:2013 for identity assurance of persons and non-person entities
- RFC 5280 describing Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

The first, ISO 29115, is used as a reference by the EU implementing act, Commission Implementing Regulation (EU) 2015/1502, Assurance levels for electronic identification means. The standard is considered for the specifications and procedures set out in this implementing act as the main international standard available in the domain of assurance levels for electronic identification means. However, the content of Regulation (EU) No 910/2014 differs from the international standard in relation to identity proofing and verification requirements, as well as to the way in which the differences between Member State identity arrangements and the existing tools in the EU for the same purpose are taken into account.

4. Next steps

TTC Working Group 1 invites feedback on this report and is kicking off an engagement process intended to contribute to shaping the direction of future initiatives. The aim is to ensure this mapping exercise provides the most value and captures the perspectives of the wide global audience that relies not only on the EU and US documents included in this exercise but also on future transatlantic cooperation efforts.

The contributions and feedback received through previous stakeholder engagement will help complete the mapping exercise in the coming months with at least two additional elements, including:

- open questions across the ecosystem affecting use and interoperability of digital identity systems that will need to be addressed in the future through cooperative transatlantic effort
- a selection of potential use cases for transatlantic cooperation that highlight the need for and value of enabling the cross-border use of digital identities.

The identification of open questions will follow a structured and systematic approach based on information obtained from stakeholders and specific discussions within the TTC on the subject. The aim of this exercise is to understand the current state of knowledge on the topic and identify trends, common findings and areas where there may be inconsistency or lack of consensus specific to the technical, international and cross-border scope of the current exercise.

Expert and stakeholder contributions will also support the identification and definition of applicable transatlantic use cases. This topic is of paramount relevance as it can pave the way for future cooperation in specific aspects of interoperability of digital identities.

4.1 Use cases

Feedback is requested on the cross-border use cases that should be investigated by TTC WG1. Although subject to the feedback received, areas for potential use cases and/or that are already underway at the local or regional level on both sides of the Atlantic include:

- **Travel**
  - Travel documents, such as passports and visas, play a fundamental role in facilitating global movement of people. Transatlantic collaboration in this area is vital for enhancing security, streamlining processes, and ensuring the rights of travellers, including those representing vulnerable populations (e.g. stateless persons).
- **Finance**
  - Technological innovation is driving a rapid evolution in this area and digital identities have a relevant role to play.
  - Digital identities offer numerous benefits to companies in international trade (increased efficiency, reduced environmental impact, enhanced transparency, etc.).
- **Healthcare**
  - Cross-border use of digital identities for access to health records can be a critical step towards enhancing healthcare delivery and achieving equitable health outcomes

across populations so that they and their data are enabled through greater mobility and options to obtain care.

- **Education and professional credentials**
  - Interoperable academic credentials could be essential in facilitating research collaboration opportunities across borders.
  - Providing the mechanisms for university diplomas and similar professional credentials to be recognised across borders could be a catalyst for reciprocity efforts across various occupations.

4.2 Standards coordination and pre-standardisation research

To ensure sustained focus and collaboration between the EU and US on this topic, feedback is requested on the gaps, barriers, challenges and risks that are actively hindering adoption of digital identity technologies and standards. Beyond general challenges to adoption, feedback is requested specifically on barriers and gaps affecting cross-border interoperability, as well as possible actions that the EU and US governments could take through the TTC to address these challenges, including opportunities to collaborate with academia, civil society, industry, not-for-profit organisations, and other public sector organisations.

By identifying these ecosystem-wide challenges and opportunities, our goal is to create a backlog of potential transatlantic cooperative efforts that centre on questions such as:

- How do we ensure that the systems we are building work for everyone and respond to the needs of vulnerable populations?
- How might we maximise the use of privacy-enhancing technologies in identity systems, for instance, selective disclosure and federated learning?
- What common trust models should we leverage or build?
- What approaches to certification should we consider?
- How do we build the necessary expertise and capacity to facilitate next-gen credential provisioning?
- How should we design and architect mobile (smartphone) security features, including where to store credentials, how to determine which wallets to trust and which systems get to access them?
- How should digital credentials like mobile driving licences (mDLs) work for online interactions?

5. Call for feedback

To inform and improve this mapping, the TTC invites input from subject matter experts and others with equities related to the topic of digital identity.

The Digital Identity Subgroup is particularly interested in feedback on the following topics:

1. **Definitions**
    a. Additional definitions that could be added to the existing mapping exercise
    b. Any additional context that could be incorporated in the current mapping to clarify when and how certain definitions apply
2. **Levels of assurance**
    a. Feedback on the extent to which the mapping reflects the experiences of individuals and organisations that have overseen or been the subject of real-world implementation
    b. Additional components that could be added to the mapping (i.e., categories in the leftmost column of the IAL and AAL summary tabs within the linked mapping exercise spreadsheet, for instance, evidence requirements and allowed authenticators)
3. **International standards references**
    a. Additional references that could be added
    b. Which standards individuals and/or their organisations rely on most often, and for what sectors and scenarios
4. **Ecosystem gaps and questions**
    a. If/what gaps exist in technical guidance and standards
    b. If/what gaps exist in the body of knowledge and research related to identity verification; open questions that could be addressed through dedicated joint EU-US research efforts
    c. If/what gaps exist in the market of available identity verification services and technologies
    d. Barriers to cross-border interoperability of identity solutions and processes, such as policies, practical challenges and other factors
5. **Use cases**
    a. Input on the most critical use cases that would benefit from transatlantic pre-standardisation research cooperation on remote identification, e.g.:
        i. transportation/travel (digital travel credentials, mobile driving licences)
        ii. financial services (retail payment, eInvoicing)
        iii. health (health records)
        iv. education/professional credentials (diplomas, certifications)

Appendix

Reference documents

- NIST Special Publication 800-63-3: Digital Identity Guidelines
- 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) 2015/1502 of 8 September 2015 on setting 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 (text with EEA relevance).