eID assurance model suitability assessment

Publication Date [2025-mm-dd]

Authors: Niels van Dijk (SURF), Martin Kuba (CESNET), V. Ardizzone (EGI)

Document Code: AARC-I085

DOI: *10.5281/zenodo.xyz*

Community:

Abstract

This document investigates capabilities for leveraging national eID for increased identity assurance for the benefit of research services

1 Introduction

Identity assurance in higher education is about verifying that students, faculty, staff, and sometimes external collaborators are who they claim to be, and then managing their access to digital and physical resources. It ensures trust in academic records, research systems, and campus services. Generally speaking, it is the user home institution which is primarily responsible for identity assurance.

To authenticate into remote services, Federated Identity Management (FIM) is heavily used. This allows users to use their home institution account to login to services. For services this means they can rely on the identities provided by the institutions and do not have to do all the heavy lifting of identity and account management themselves.

In chapter 2 we will describe the current practices related to identity vetting and management at institutions, and the role Identity Federations play in establishing trust.

National Identity federations and the eduGAIN interfederation lay out policy which helps establish trust in the identities provided by the institutions. Significant parts of this trust can be expressed by using the REFEDs Assurance Framework (RAF) which lays out a standardised way for expressing identity assurance. Chapter 3 describes the elements of this standard.

When dealing with sensitive research data, sufficient identity assurance is required to allow users to access relevant services. Historically it has been hard to obtain such assurance in a consistent and scalable way from home identity providers in the R&E sector. In addition many research communities have collaborations with contributing parties outside of the R&E sector. In chapter 4 we identify several of the challenges faced by research services when dealing with identity assurance from home institutions.

For any research related service, the affiliation of the user with the home institution is a vital piece of information. One way of improving the identity assurance might be to leverage national government eID systems. In chapter 5 we evaluate leveraging the use of national eID, eIDAS 1.0 and the future eIDAS 2.0 (EUDI Wallet) systems for providing a step-up model to at least a substantial level that could then be done at “home” through the user’s national eID scheme. If suitability is confirmed, [also] guidelines will be provided via AEGIS.

1.1 Notational Conventions

The key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'NOT RECOMMENDED', 'MAY', and 'OPTIONAL' in this document are to be interpreted as described in [RFC2119].

Unless otherwise noted, all the protocol parameter names and values are case sensitive.

1.2 Terminology

This section defines the terminology used by this specification. This section is a normative portion of this specification, imposing requirements upon implementations.

This specification uses the terms “infrastructure proxy”, “SP-IdP-Proxy” defined by the AARC Blueprint Architecture 2019 [AARC-G045].

2. Identity assurance in Higher Education

Identity assurance is typically managed at the institutions, and is generally well managed and professional. Part of this is because researchers are typically employees at the institutions and hence due to EU labor laws these need to be identity vetted by the HR departments based on national ID.

A breakdown of the various aspects of identity assurance managed at an R&E institution encompasses the following:

- **Identity Proofing (Enrollment and Onboarding)**
  When enrolling, students and employees submit official documents (passports, government IDs, transcripts) to admissions. Employment verification usually includes background checks and ID verification through HR. Increasingly, institutions use third-party services for remote identity proofing, especially for online programs.

- **Credential Issuance**
  Once verified, users are issued a unique digital identity (username/email) in the institution's identity management system. Physical cards or mobile credentials serve as proof of identity on campus for accessing buildings, libraries, and labs.
  Institutions implement SSO platforms (like Shibboleth) to provide a unified, federated login across campus systems.

- **Authentication and Access Control**
  Most institutions now require multi-factor authentication (MFA), often using mobile apps or hardware tokens. Access rights are granted depending on whether the person is a student, faculty, staff, alumni, or visitor.
  Higher ed relies heavily on federated identity (e.g., InCommon, eduGAIN) so that users can access resources across institutions (like library databases, research collaborations) using their home credentials.

- **Ongoing Identity Assurance**
  Identity assurance is maintained throughout the person's affiliation, for Faculty/Staff this includes hired, active, retired, departed. As roles change, access rights are automatically adjusted or revoked. Some systems require re-verification (e.g., MFA device re-registration, password resets). Security teams monitor for suspicious access patterns to detect compromised accounts.

- **Compliance and Standards**
  Universities must comply with FERPA (student records), GDPR (for EU data), HIPAA (for health-related research data), etc. Many follow NIST 800-63 or eIDAS guidelines on digital identity assurance, especially when federal research data is involved.
  Regular audits ensure proper handling of identity data and assurance practices.

- **Emerging Trends**
  Some institutions are piloting fingerprint or facial recognition for exam proctoring and

physical access. Some are moving toward FIDO2/WebAuthn for stronger and more user-friendly authentication.

3. National eID

Electronic ID (eID) is a digital representation of an individual's or entity's identity. eID serves the triple purpose of identification, authentication and signing in the digital sphere, akin to traditional, physical identification forms, such as passports or identity cards. [Sig-1]

This enables individuals to assert their identity online securely to access various services and execute transactions. eIDs can be issued by governments, private sector institutions or schemes and have been pioneered in the Nordics by Norwegian and Swedish BankID since the early 2000s. Today, there are 60+ eIDs across Europe with varying levels of assurance under eIDAS1, but factoring in all identity providers, the number is likely 150+, with varying use cases and levels of take-up. [Sig-1]

Figure 1 shows a subset of the various eID systems in use throughout Europe.

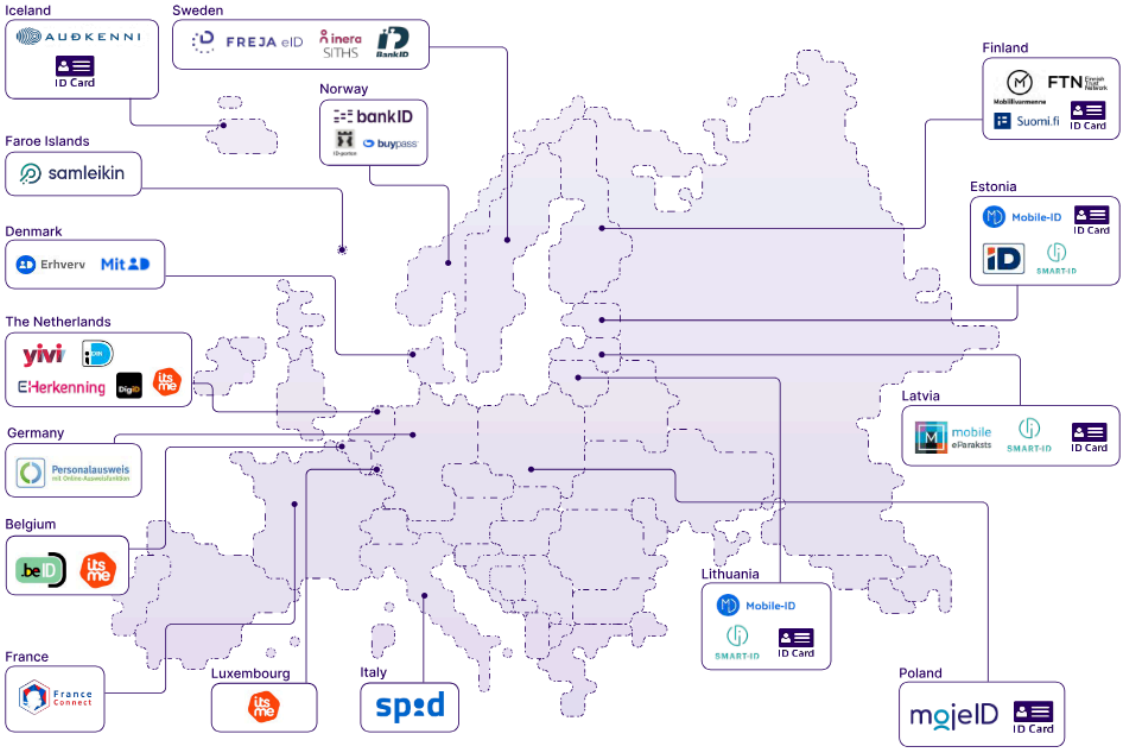


Figure 1: An overview of various eID systems in use throughout Europe [SIG-1]

eID Usability

While many eID systems exist, unfortunately the usability in the context of research is challenging. This is influenced by two factors, the uptake of the eID system per country and the (in)ability to use an eID across borders, which was envisioned in eIDAS 1.0

National eID

As shown in Table 1, the uptake of eID on a national level varies greatly between EU countries, ranging from over 90% in The Netherlands and several of the Scandinavian countries to about 22% in Germany. Next to this, in many cases the eIDs are only used for interaction with government and/or healthcare services, but use for education or private sector is uncommon. Using the national eID for other purposes is uncommon and many users are not accustomed to this.

Furthermore, to leverage the national eID, a service would have to be registered in the national eID system as a recipient. This does not scale and is practically unachievable for most research services. To support cross border scenarios, eIDAS 1.0 was introduced

Country		eID user rate (as % of total population)	Digital Economy and Society Index (DESI) Score (2022)	E-government users, DESI (2024)	Access to e-health records, DESI score (2024) (0 to 100)	Digital public services for citizens, DESI score (2024) (0 to 100)	Digital public services businesses, DESI score (2024) (0 to 100)	Population, mio (2023)	Population 15+, mio (2023)
Austria		49% (2023)	54.7 (No.10)	79%	88.17	80.72	82.86	9.1	7.8
The Baltics	Estonia	84% (2024)	56.5 (no. 9)	95%	97.5	95.83	98.75	1.4	1.1
	Latvia	70% (2024)	49.7 (No. 17)	79%	84.82	88.22	87.22	1.9	1.6
	Lithuania	60% (2022)	52.7 (No. 14)	81%	95.42	86.7	95.94	2.9	2.4
Belgium		77% (2023)	50.3 (No. 16)	86%	100	82.33	91.59	11.7	9.8
Denmark		90% (2024)	69.3 (no.2)	99%	97.92	82.24	88.69	5.9	5.0
Finland		98% (2023)	69.6 (no.1)	98%	82.62	90.61	100	5.6	4.7
France		79% (2024)	53.3 (No. 12)	91%	79.27	72.09	79.31	66.5	55.2
Germany		22% (2024)	52.9 (No. 13)	62%	86.96	75.83	78.58	84.5	72.0
Italy		56% (2023)	49.3 (No. 18)	69%	82.69	68.28	76.26	59.4	52.2
The Netherlands		94% (2021)	67.4 (no. 3)	95%	72.47	85.87	86.65	18	15.3
Norway		97% (2024)	64.3 (No.5)	92%	-	-	-	5.5	4.6
Poland		67 % (2024)	40.6 (No. 24)	66%	90.03	63.73	72.88	38.7	32.9
Spain		54% (2023)	60.8 (No. 7)	83%	84.58	84.18	91	47.9	41.5
Sweden		90% (2023)	65.2 (no.4)	96%	77.94	93.28	95.97	10.6	8.7
UK		Not applicable	60.4 (2020 data)	-	-	-	-	68.6	56.7

Table 1: eID Uptake end usage for various EU countries [SIG-1]

eIDAS 1.0

The eIDAS Regulation (EU 910/2014), often referred to as eIDAS 1.0, came into effect in July 2016 to create a unified legal framework for electronic identification and trust services across the European Union. Its goal was to ensure that people and businesses could use their national electronic IDs (eIDs) to access public services in other EU countries, supporting the vision of a seamless digital single market. The regulation also provided a legal basis for trust services, such as electronic signatures, electronic seals, time stamps, electronic delivery services, and website authentication, ensuring they were recognized across all member states.

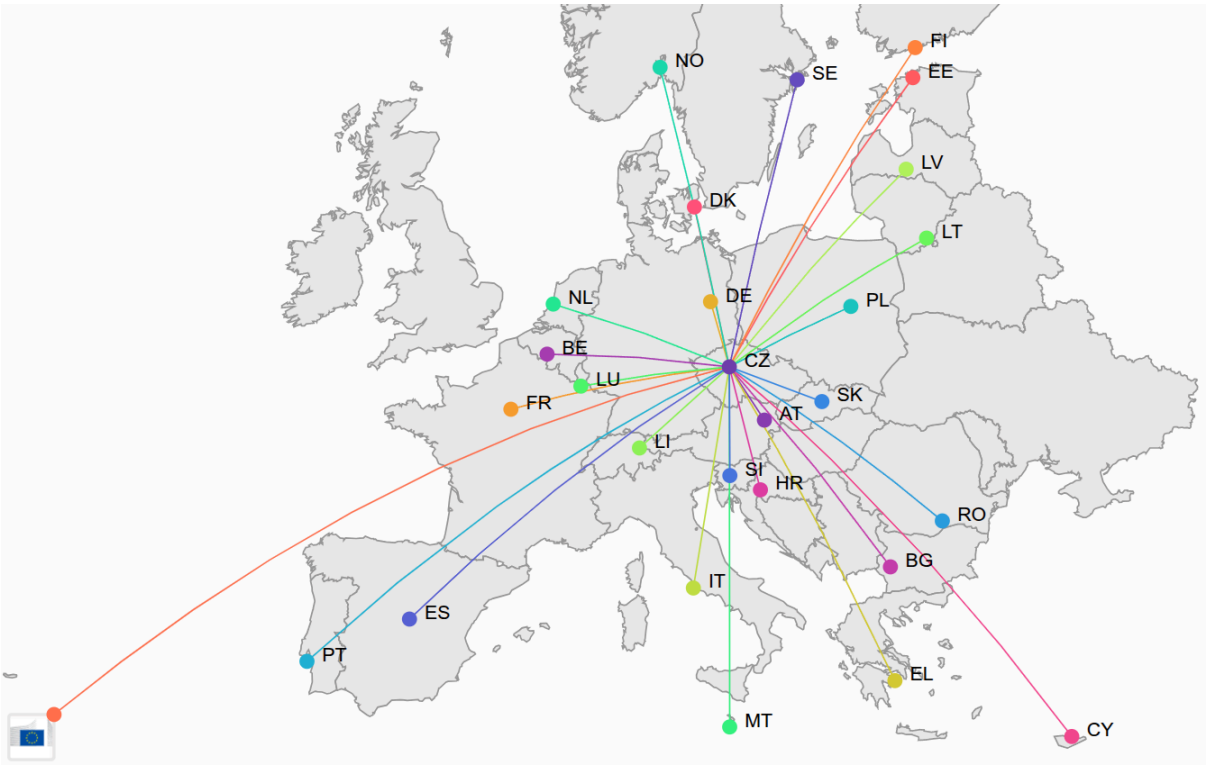
A key feature of eIDAS 1.0 was that it introduced mutual recognition of notified national eID schemes, which allowed cross-border authentication. It also established legal equivalence between qualified electronic signatures and handwritten signatures, giving them full evidentiary value in court.

However, while it laid an important foundation, adoption of eIDAS 1.0 was slow and uneven: not all member states, even today, have notified their eID schemes, and the regulation was seen as more focused on the public sector rather than private sector.

Also for education and research, eIDAS 1.0 is not providing sufficient capabilities. The lack of availability, combined with the great variance in eID uptake across EU countries means it cannot be leveraged as the sole means to reliably establish or improve user identity.

Technically, the eIDAS network is based on the SAML (Security Assertion Markup Language) protocol, the same protocol used in the eduGAIN interfederation, whose properties are well understood thanks to long experience in using it in European research infrastructures enabling cross-border access. Unfortunately, the eIDAS SAML profile is not compatible with the SAML2INT profile commonly used in R&E. Furthermore,, due to SAML protocol limitations, a user's identity can only be checked in the moments of interactive user authentication, and cannot be re-checked during long-running computations, so revocation of access based on changes of user's attributes is not possible until the user re-authenticates.

The current state of the eIDAS network can be seen at [eIDAS Dashboard], where at the time of writing (summer 2025), Ireland, Iceland and Hungary have no interconnections at all, Norway and Finland have no outgoing connections, Bulgaria has a single outgoing connection, Greece has only two outgoing connections, and overall the number of incoming and outgoing connections is different for most countries, making the interconnections asymmetrical.



These issues eventually led to the development of eIDAS 2.0, which aims to expand the scope and usability of trusted digital identities across Europe.

eIDAS 2.0 (EUDIW)

eIDAS 2.0 (proposed in 2021, entering force gradually from 2024) builds on the eIDAS 1.0 foundation by introducing a European Digital Identity Wallet available to all EU citizens, residents, and businesses. Unlike eIDAS 1.0, it explicitly targets both public and private sector use, enabling secure access to services like banking, health, education, and e-commerce.

eIDAS 2.0 aims to facilitate interoperability, allow for higher levels of assurance, and promotes broader cross-border adoption. In short, where eIDAS 1.0 created the legal scaffolding, eIDAS 2.0 aims to deliver a practical, universal, and user-centric digital identity ecosystem across the EU.

At the time of writing (summer 2025) the eIDAS 2.0 implementing acts are being issued and policy, standards and technical requirements are being finalized. While the aim is to have an ecosystem available by 2026, it seems more likely a first version of this ecosystem will become available by 2027. Even though several EU countries are progressing well in a trajectory toward national rollout, others have not engaged in any activity yet. [SOURCE]

Furthermore, while the initial set of scenarios where this ecosystem could be used include all sectors, it has increasingly become clear that the initial focus is on national eID scenarios, as e.g. policies for cross border use have not been laid out yet. Also wallet use cases beyond eID will require significant sectorial effort as technical and semantic standardisation will be needed to ensure interoperability. Finally, the eIDAS 2.0 effort is an EU project, which will not satisfy the needs of research services for users outside of the EU.

4. REFEDs Assurance Framework

The REFEDS Assurance Framework (RAF) 2.0 is a standard developed by REFEDS (Research and Education Federations) that defines how to express identity assurance -how confidently a digital identity can be trusted- across research and education identity federations. It helps identity providers (IdPs) and service providers (SPs) to communicate about the reliability of user identities in a consistent and standardised way.

What the Framework Covers

RAF 2.0 defines specific requirements across several areas of identity lifecycle and management, including:

- Identity proofing: How the user's identity was initially verified (e.g., in-person check, government-issued ID, etc.)
- Credential binding: How the verified identity is linked to login credentials (e.g., password, certificate, MFA)
- Credential management: How securely credentials are stored, updated, and revoked
- Operational practices: How identity systems are maintained and monitored

These requirements are grouped and described for each assurance level, allowing institutions to assess and declare the appropriate level for their users.

Core Concepts

RAF 2.0 is built around three main elements:

1. **Identity Assurance Profiles** (IAPs)
   These define the level of confidence that a user's identity is accurate and trustworthy, based on how it was verified during registration, bound to authentication credentials and managed over time. For each of these aspects, a set of criteria allows an identity provider to assert how their processes have been defined and were executed. For example, an institution may use RAF to express the way they vet the identity of the user, the properties of the identifiers they are using, or the 'freshness' of the affiliation attribute.
   The IdP may express the profiles individually, but for convenience some specific sets have been bundled into a single expression ("Cappuccino" and "Espresso").

2. **eduPersonAssurance**
   Identity assurance is communicated through the eduPersonAssurance [eduPerson] attribute in SAML assertions, or by using an eduperson_assurance claim in OIDC and other claim based protocols such as Verifiable Credentials.

   This attribute contains URIs that indicate the assurance profile and version, for example: *https://refeds.org/assurance/IAP/high* or *https://refeds.org/assurance/ID/eppn-unique-no-reassign*

3. **Versioning**
   RAF 2.0 introduces explicit versioning so that service providers can reliably interpret what the assurance claim means. The version URI must be included alongside any assurance claims: *https://refeds.org/assurance/version/2*

RAF Interoperability

The REFEDS RAF is aligned with international frameworks such as eIDAS LoA and can also be mapped to the assurance levels defined in NIST 800-63-3. For example, REFEDS IAP "High" is broadly comparable to NIST IAL2-IAL3 in terms of identity proofing, while authentication requirements can be mapped to NIST AAL2 or AAL3. This interoperability facilitates cross-Atlantic collaborations, where research services may need to express assurance in terms understandable to both European and U.S. partners.

Using RAF

Generally speaking, support for RAF is poor, meaning few Identity providers publish information in the eduPersonAssurance attribute. This is a challenge for the research services as they now have no way to establish the assurance of the incoming identity, in effect reducing it to 'junk', and forcing them to take alternative and often expensive measures to compensate for this lack of information.

This is sad, as generally speaking, the users at the institutions, specifically researchers, have been properly vetted.

5. Glueing it all together

In this chapter we can describe how we glue together all of the above? However, what do we want to describe?

- eID as mitigation to id vetting seems not usefull/possible and
- Home IdP identity vetting is already ok, just need to publish RAF
- Force RAF for IdPs in eduGAIN?
- Force use of RAF for VCs in EUDI and eduWallets to mitigate this issue in the future?

7. Implementation Considerations

Verifiable Credentials as an implementation pathway

An important consideration for future implementations is the potential role of Verifiable Credentials (VC) in strengthening both identity and authentication assurance. VCs, issued by trusted authorities such as governments, universities or funding agencies, can provide cryptographically verifiable attestations of identity attributes and affiliations.

From an identity assurance perspective, VCs can encapsulate strong proofing events (e.g. government-issued eIDs or institutional HR-based vetting), corresponding to eIDAS Substantial/High and NIST IAL2-IAL3. From an authentication assurance perspective, VCs presented through secure wallets and bound to strong authenticators (such as FIDO2, smartcards, or mobile ID) can satisfy requirements equivalent to NIST AAL2 or higher.

In practice, this would allow proxy-based architectures (such as the AARC BPA) to consume VCs as trusted inputs, enabling scalable “step-up” assurance across borders and sectors. Moreover, the alignment of VCs with both REFEDS RAF and NIST 800-63-3 provides a path towards cross-Atlantic interoperability and support the broader adoption of government-backed eIDs in research services. Importantly, VCs are designed with privacy-preserving features. Because digital information is persistent and easily aggregated across different domains, uncontrolled sharing would increase privacy risks. The VC model addresses this through mechanisms such as selective disclosure and zero-knowledge proofs, allowing the holder to reveal only what is strictly necessary for a transaction.

From an implementation perspective, there is a growing convergence between VCs and government-issued electronic identities (eIDs), especially within Europe under eIDAS 2.0 and the European Digital Identity Wallet (EUDI Wallet) initiative.

(Issuance) National eID systems can serve as high-assurance identity proofing mechanisms. These can be used as the basis for issuing a VC that represents a person’s legally verified identity attributes.

(Binding) The VC can then be cryptographically bound to the holder’s wallet (EUDI Wallet or another SSI-compatible wallet). This ensures continuity between the strong identity proofing (eID) and the ongoing use of credentials (VC/VP).

(Authentication) When a VC is presented through a wallet, authentication can be enforced using strong factors (e.g. FIDO2 tokens, biometrics, device PIN). This creates equivalence with NIST AAL2-3 or eIDAS Substantial/High authentication levels.

(Federation and Interoperability) Proxies in the AARC BPA model can consume VC or their presentations as assurance artifacts, aligning them with REFEDS RAF, eIDAS LoA, or NIST 800-63-3 assurance requirements.

In short, VC can act as the technical bridge between the identity proofing carried out in government eID ecosystems and the authentication and authorization needs of research services, providing interoperability and future-proof alignment across assurance frameworks.

8. Security Considerations

References

[SIG-1] Signicat - The State of Digital Identity in Europe 2024 – 2025
https://www.signicat.com/the-state-of-digital-identity-in-europe-2024-2025

[eIDAS Dashboard] eIDAS Dashboard
https://eidas.ec.europa.eu/efda/browse/notification/eid-chapter-contacts

[VCDM 2.0] Verifiable Credentials Data Model 2.0, W3C Recommendation

https://www.w3.org/TR/vc-data-model-2.0/

[Mondo] Mondo Disease Ontology

https://www.ebi.ac.uk/ols4/ontologies/mondo

[DUO] GA4GH Data Use Ontology

https://www.ga4gh.org/product/data-use-ontology-duo/

[OWL] OWL 2 Web Ontology Language Document Overview

https://www.w3.org/TR/owl2-overview/