AARC-I085
eID assurance model suitability assessment

Last updated:	17-12-2025
Due Date:	30-10-2025
Authors:	Niels van Dijk (SURF), Martin Kuba (CESNET), V. Ardizzone (EGI), Peter Bolha (CESNET), David Groep (Nikhef)
Document Code:	AARC-I085
DOI:	https://doi.org/10.5281/zenodo.17349747

Abstract

This document investigates capabilities for leveraging national eID, both eIDAS 1.0 and 2.0, for increased identity assurance for the benefit of research services. The document is an AARC TREE Milestone (M2.1) but it is also published as an AARC Community Information document.

Copyright

© Members of the AARC community.
This work is licensed under a Creative Commons Attribution CC-BY 3.0 Licence

Table of Content

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 requirements voiced by research communities and their services when dealing with identity assurance.

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.

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.

- **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. Federated identity (e.g., InCommon, eduGAIN) is used, 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 typically comply with FERPA (student records), GDPR (for EU data), HIPAA (for health-related research data), etc. depending on local legislation.

- **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 like for example banks. 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.

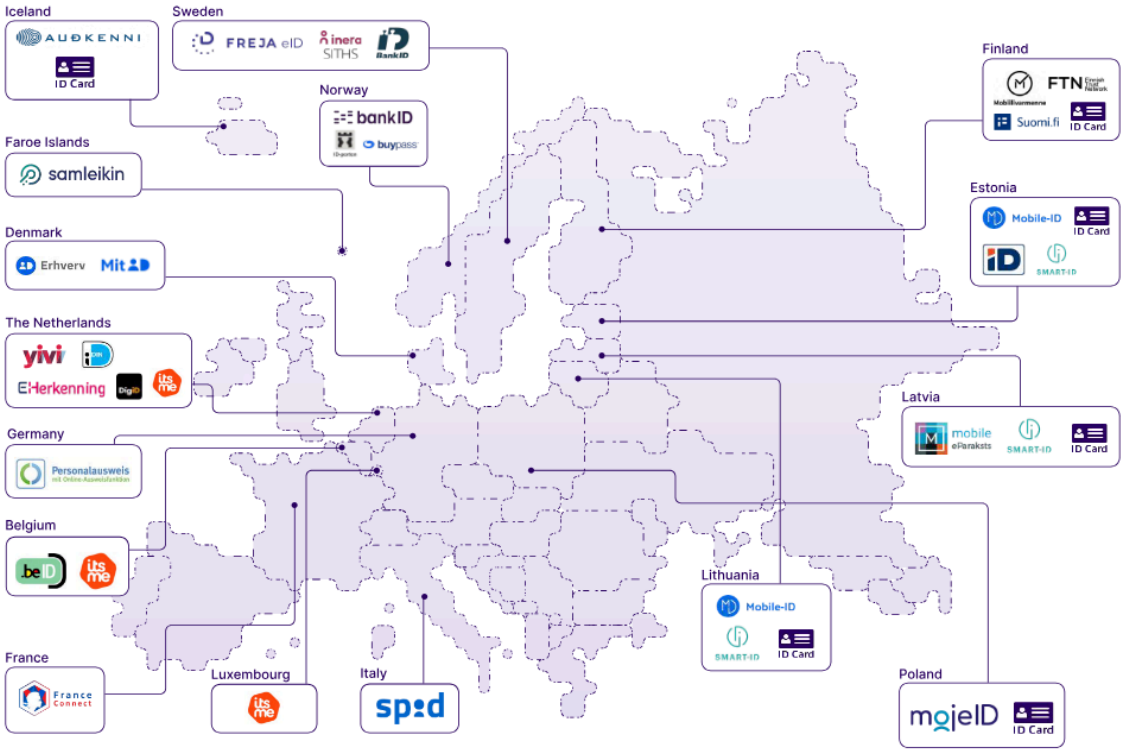

Figure 1: An overview of various eID systems in use throughout Europe [SIG-1]

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.

3.1. National eID Uptake

As shown in Table 1, the uptake of eID on a national level varies greatly between EU countries, ranging from for example 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 not for education or private sector. 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 and usage for various EU countries [SIG-1]

3.2. 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.

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.

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

At the time of writing (summer 2025), the eIDAS network indicates that 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, and usability unreliable when wanting to engage with users from all of europe

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.

Furthermore, due to SAML protocol limitations, a user’s identity can only be checked during 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.

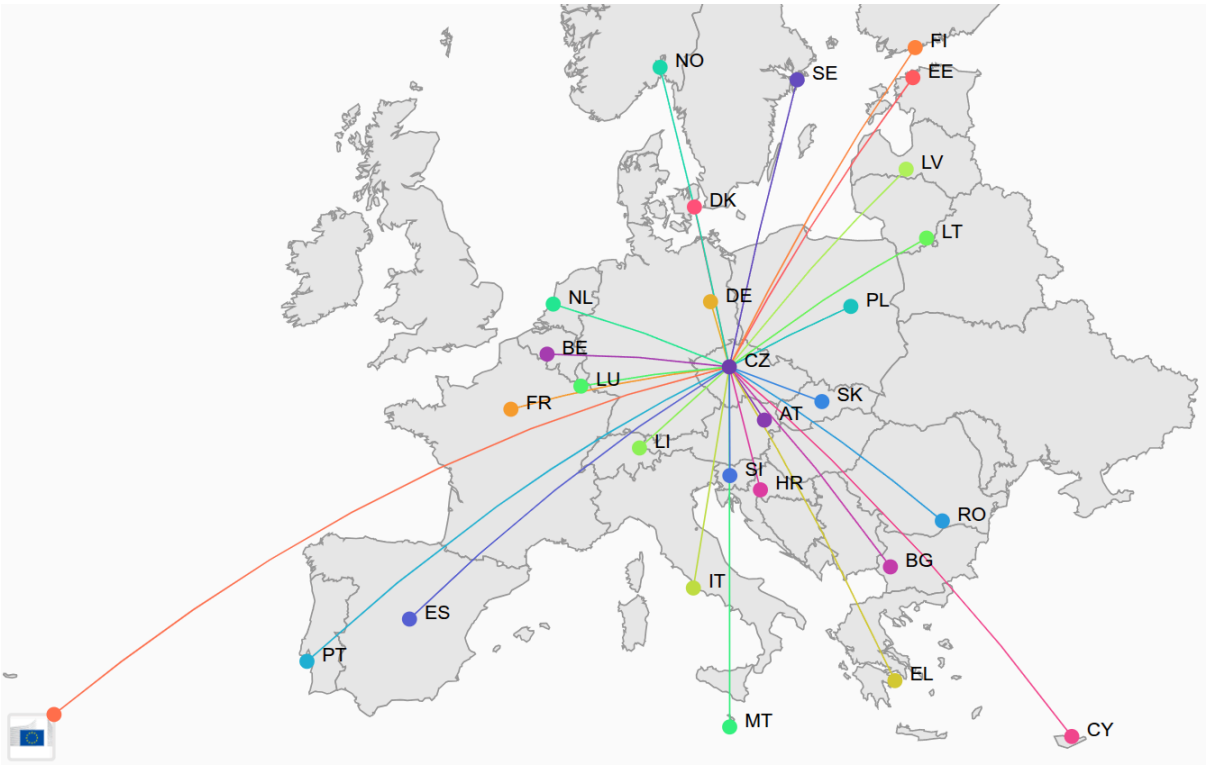

Figure 2: eIDAS interconnections with Czech republic. Note the missing links for Ireland and Hungary **[eIDAS Dashboard]**

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.

3.3. 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.

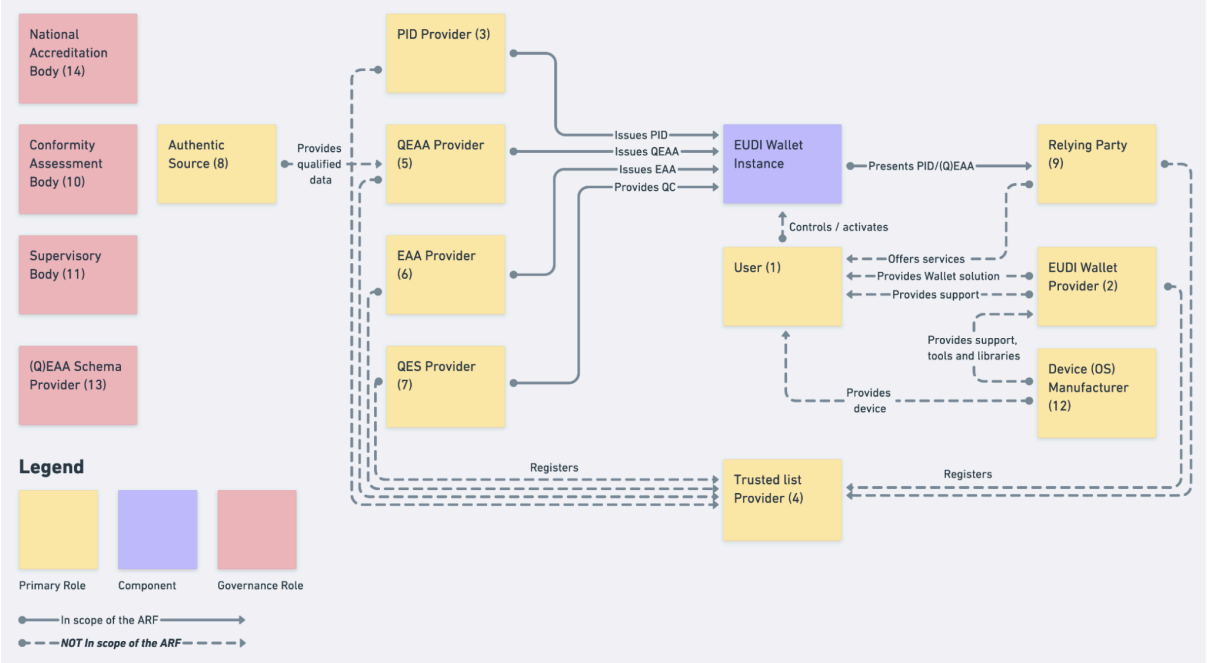

Figure 3: *Overview of the EUDI Wallet roles [ARF]*

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 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.

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.

4.1. Core Concepts

RAF 2.0 is built around three main elements:

1. **5Identity 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 were defined and are 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*

4.2. 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.

4.3. RAF Uptake

Generally speaking, support for RAF is, at the time of writing, poor, meaning few Identity providers publish information in the eduPersonAssurance attribute. Reason for this is both technical as well as organisational: the institutions' internal identity management systems may predate the definition of RAF, and they rarely store the information needed for releasing RAF attributes, and as institutions themselves often do not act as relaying parties receiving identity information from external sources, they awareness for the need for assurance information is low.
The poor support for RAF is an ongoing 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 unfortunate, as generally speaking, the users at the institutions, specifically researchers, have been properly vetted.

As RAF expresses all of the LoA properties of the identity at transaction time, it is also very suitable for usage in Verifiable Credential scenarios. RAF may already be expressed via OIDC claims, and this model can be easily adopted also for VC as shown in the example in figure 6.

```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2"
  ],
  "type": [
    "VerifiableCredential",
    "AcademicBaseCredential"
  ],
  "credentialSubject": {
    "sub": "f2cb63a9-e044-4ce4-88d1-43202214d915",
    "eduperson_unique_id": "1a799b89ebb579f5d0b567dbf34bcc103d2195309518c3931c2e0e3c28c8d2fe@hbot.nl",
    "given_name": "Dinanda",
    "family_name": "Haagen",
    "name": "Dinanda Haagen",
    "schac_home_organisation": "hbot.nl",
    "email": "dhaagen@dev.eduwallet.nl",
    "eduperson_affiliation": ["student","member"],
    "eduperson_scoped_affiliation": ["student@hbot.nl","member@hbot.nl"],
    "eduperson_entitlement": ["urn:mace:dir:entitlement:common-lib-terms-example"],
    "eduperson_assurance": ["https://refeds.org/assurance",
                            "https://refeds.org/assurance/profile/cappuccino",
                            "https://refeds.org/assurance/ID/unique",
                            "https://refeds.org/assurance/IAP/medium",
                            "https://refeds.org/assurance/IAP/local-enterprise",
                            "https://refeds.org/assurance/ATP/ePA-1m"],
    "id": "did:jwk:eyJrdHkiOiJFQyIs.....bFRXYks2eGJRIn0"
  },
  "issuer": {
    "id": "did:web:epi.playground.eduwallet.nl",
    "name": "eduWallet Proeftuin Issuer",
    "description": "eduWallet Proeftuin credential issuer"
  },
  "name": "Academic Base Credential",
  "description": "Basic  Identity credential for use in Research and Education",
  "validFrom": "2025-11-07T13:55:40+00:00",
  "iat": 1762523740,
  "nbf": 1762523740,
  "sub": "did:jwk:eyJrdHkiOiJFQyIs.....bFRXYks2eGJRIn0",
  "iss": "did:web:epi.playground.eduwallet.nl"
}
```


Figure 4: Example of showcasing eduperson_assurance claim and RAF in a hypothetical Verifiable Credential

5. Verifiable Credentials and Wallets

5.1. Verifiable Credentials

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.

It is worth mentioning that the Verifiable Credential Data Model as defined in [VCDM 2.0] has substantially more expressive power than SAML or OIDC protocols. Its semantic model is based on Linked Data that allows making references to dictionaries or ontologies. For example, using the established ontologies [Mondo] and [DUO], it is possible to express complex access requirements like "doing cancer research in a non-profit setting" which may be automatically processed using [OWL] reasoners to make decisions based on complex access policies. It is an opportunity to get past simple access policies like "employee of an academic institution" or "member of a group".

Importantly, some of the VCs types, like SD-JWT 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 userholder to reveal only what is strictly necessary for a transaction.

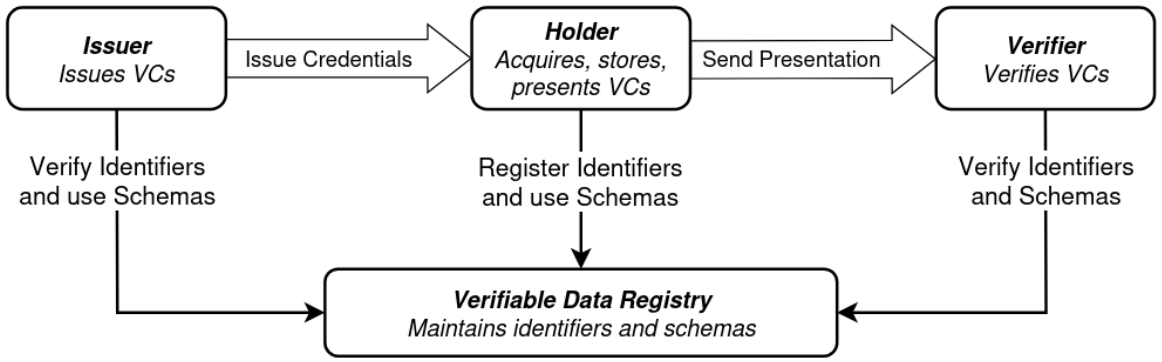

Figure X: The roles and information flows forming the basis for the Verifiable Credential Data model [VCDM2.0]

5.2. (EUDI) Wallets

Although not required, one of the envisioned and probably default transportation mechanisms for VCs is a wallet. The wallet is an end user controlled software component that would e.g. live as an app on a mobile device, which can be used to collect VCs from authoritative sources, the issuers, and present such VCs towards service (verifiers in the VC data model) to prove some part of the users

identity.

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. Moreover, the alignment of VCs with both REFEDS RAF and NIST 800-63-3 may provide a path towards cross-Atlantic interoperability and support the broader adoption of government-backed eIDs in research services.

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.

6. Community Requirements

The requirements for identity assurance differ greatly across research fields. Where some want to make use of citizen scientists and a so-called 'social login' suffices to be allowed to contribute to a data set, working with medical data often comes with all kinds of legal requirements and such communities have very stringent requirements on who is allowed to gain access, as for example shown in the "Bona fide researcher" definition of the Elixir AAI. [ELIXIR]

Furthermore, the role of the institution is different. In the area of high energy physics, where the effort of electronic identification has the longest tradition, the access management is usually based on the user's affiliation to a research institution, and their citizen identity is not important. In the field of genomics, which is the newest and has the most legal restrictions, the access management is usually based on user membership in projects with signed legal agreements with data providers, and their citizen identity is at least as important as their affiliation to institutions. In some other scenarios like EuroHPC, the eligible scientists must be from certain specific countries due to export control regulations, and hence their identity vetting to a higher standard is required.

6.1. Requirements on Identity

When reviewing various resources, the following requirements are noted as relevant when it comes to the assurance of the identity itself:

- **Unique, non-shared individual accounts**
  Each user must have their own account tied to a real individual. Shared logins (e.g. generic accounts) are unacceptable for accountability, provenance, and security. [Pöhn]
- **Persistent, non-reassigned identifiers**
  If someone leaves or there's a change (e.g. affiliation), that identity or identifier is not "re-used" for someone else. Helps with auditing, tracing, historical data. [Pöhn]
- **Identity proofing**
  Verifying that the claimed identity matches real-world identity, usually via documents or authoritative sources. The rigor depends on the level of risk (low-risk vs high-risk data, sensitive data, controlled access). May be remote, in-person, or partly remote with controls [NIST]
- **Affiliation assertion**
  The identity system must assert the researcher's organization/institution affiliation (current), since many access rights or legal responsibilities depend on institutional context. [e.g. ELIXIR]
- **Strong authentication / Multi-factor authentication (MFA)**
  To reduce the risk of compromised credentials, elevated access (especially to controlled, sensitive or private data) usually requires multiple factors. [NIH]
- **Support for different assurance levels**
  Not all data or services require the same level of identity assurance; there should be

flexibility (e.g. low risk vs high risk). The identity system or federation should be able to work with multiple levels [Ziegler]

- **Timely updating of identity**
  If someone changes institution, leaves, or their status changes, the identity records (including affiliation) must be updated promptly. Ensures that access revocation or privilege changes happen when needed. [Pöhn]

Most of the above points refer to the requirements on the identity (and associated processes) itself. It is worth noticing all of the above requirements, except for “Strong authentication” are directly in scope for RAF 2.0 and can be expressed with RAF 2.0 in a standardised way.

6.2. Outsourcing Identity Assurance

With the introduction of identity federation, and potentially wallet technologies, research communities have the possibility of ‘outsourcing’ the identity assurance challenges to the user's home institution or some other authoritative source like a bank ID or government ID.
However, to be *truly* usable several additional requirements need to be fulfilled :

- **Technical scalability**
  Only when the technical exchange of identities is based on open standards, and profiles have been defined to guarantee interoperability, identities may be used at scale. The cost for implementing and maintaining multiple standards and profiles is very high.

  For example, national identity federations evolved using different identifiers, with different properties with respect to persistence, reassigability etc. When the various federations joined eduGAIN, these differences became a challenge to the services consuming these identifiers. In addition, new identifiers were introduced to mitigate shortcoming of existing identifiers, leading to even more requirements for services [eduGAIN]. REFEDs has developed profiles and guidance to streamline the exchange of attributes and identifiers in response to these challenges, for example with the “Personalized Access Entity Category” REFEDs PAEC]

- **Adoption**
  The level of adoption of a certain identity scheme is defined in multiple ways. The ability to adopt a certain system may be limited by policy, cost or the (absence of) governance over a certain standard. Furthermore, some use cases may be easier to implement using certain technologies, like e.g. mobile scenarios. If an identity scheme is effectively a niche product, technical tooling may not be available to implement the identity solution, and developers might not be familiar with the implementation of the identity.

  SAML 2.0 and the saml2int profile has been and still are the “lingua franca” for authentication in the R&E ecosystem,. However the dominant use of OIDC by parties like Google and Facebook, combined with the poor support of SAML for mobile scenarios has led to a steep increase in OIDC uptake and supporting implementations. SAML is now often viewed as “enterprise” and “cumbersome”, whereas OIDC is seen as a better fit for “modern

authentication" [OIDC vs. SAML]

- **Policy reach**
  The identities of the user population of the research community have to live in authentic sources, which must be part of trust frameworks the research community can actually use. As research communities are often pan-European or even global, this may mean having to deal with trust frameworks with very different legal and policy requirements, as these are typically bound to all kinds of local regulations. This may heavily influence the ability to use a certain identity resource.

  As shown in Chapter 3 already, Ireland is currently not available within eIDAS 1.0 ecosystem, making it impossible to engage with Irish researchers via eIDAS 1.0.
  A similar example exists in The Netherlands where by law the social security number may not be used beyond government related use cases. Unfortunately however, there is no other suitable identifier in the government identity.

- **Machine-readable transparency**
  Identity proofing steps, required attributes, levels of assurance, what evidence is required, etc., should be documented and made public. Also clear policies about who is responsible for what [Ziegler]. It is however impossible to (manually) read and evaluate all policies. Therefore the aforementioned processes should be not just transparency expressed but also in a machine readable format, allowing for automated perhaps even real-time evaluation and processing.

  A good example of such an approach may be found in in R&E Identity federations: where all publish a "Metadata Registration Practice Statement" to help understand the Metadata Registration Practices of a federation [REFEDs MRPS]

- **User perception**
  Researchers have a certain perception of which identity they will want to use to conduct their engagements with the research communities. Often, that perception of what is acceptable and usable is based on local and cultural practices. This may lead to very different preferences across communities or countries.

  Often the issuer of the identity may have certain use cases defined, as can be seen here for the Dutch DigiD system: "In the Netherlands the DigiD (digital identity) system is used by citizens in dealings with Dutch government bodies like the Tax and Customs Administration." [DigiD]. As such Dutch citizens will be very surprised to be asked to use their DigiD for login to a work related research service.

- **Sustainability**
  Many factors influence the (long term) availability of the system one may outsource to. The identity sources should at least in part align with the primary business of the research communities. Using sources like e.g. the end-user oriented identity systems provided by Big Tech, may look very appealing because of scale and usability. However the very different business drivers of these parties pose a significant risk to the long term usability of such

identities as policy and technical specification may change at any time in accordance with Big tech business drivers. [For example: FACEBOOK]
On the other hand, using a startup company to provide identity may be risky in terms of future sustainability in case the startup would no longer be able to further support and develop their service.

7. Assessing eIDAS 1.0 and eIDAS 2.0

With the above requirements in mind, it is now possible to assess and compare various aspects of the eIDAS 1.0 and the upcoming eIDAS 2.0.

Requirement	eIDAS 1.0	eIDAS 2.0
Unique, non-shared individual accounts	Government ID	PID is based on government ID
Persistent, non-reassigned identifiers	Yes	Yes
Identity proofing	Local procedures are in place	Local procedures are in place
Affiliation assertion	Does not exist in eID, but eID could be used to identify a person upon employment and henceforward the affiliation may be linked to that identity	Does not exist in eID, but eID could used to identify a person upon employment and henceforward the affiliation may be linked to that identity
Strong authentication / Multi-factor authentication (MFA)	Strong authN is used when onboarding	Strong authN is used when onboarding, fairly strong auth use for access to wallet, optional authN requested upon release. Liveliness checks could be included upon credential release
Support for different assurance levels	Yes, to match look at RAF A.2	Yes, to match look at RAF A.2
Timely updating of identity	Local procedures are in place	Local procedures will have to be in place, which should incorporate the nature of wallets and VCs. Currently no dynamic updating of credentials exists.
Technical scalability	Works, sort of, see chapter 3	At this point the scalability of the ecosystem is untested. Next to technical scalability of the systems also the trust

		framework needs to scale
Adoption	See chapter 3	Unknown. Currently most focus is on governmental use cases and PID release
Policy scalability	Targeted at government and optionally healthcare	Unknown. The intent is to have use across the public and private sector. Organisational aspects like policy requirements for issuers and verifiers, even so called non-qualified, appear stringent and may hinder adoption
Machine-readable transparency	Harmonized at high level, hard to discover at country level, also different at country level.	Policy and registration requirements are left to nation states which may lead to significant differences. No clear strategy yet for cross border use.
User perception	Not used for non-gov. Also see adoption rate in chapter 3	Unknown. Although the intent is to have use across the public and private sector.
Fit for purpose	Again chapter 3 Lack of broad adoption User perception Lack of eID availability per country.	Unknown. Usability for R&E sector will remain unclear until many of the above issues are resolved.

8. Conclusions and Recommendations

This assessment investigates the usability of Government eID for improving the assurance in digital identities in Research. It looks at eIDAS 1 and the upcoming eIDAS 2, and proposes that next to existing evaluation criteria as mostly reflected already in the REFEDs Assurance Framework, additional criteria need to be considered to properly evaluate the usability of a given framework in the research context. When trying to “outsource” the level of assurance to external sources like Government eID, additional factors come into play like Technical scalability, Adoption, Policy scalability, Machine-readable transparency, User perception and if the framework is Fit for purpose.

When taking these additional factors into account, this paper highlights that while both eIDAS 1.0 and the emerging eIDAS 2.0 frameworks offer strong and well-established identity proofing mechanisms, their applicability to research and education use cases remains limited. eIDAS 1.0 suffers from inconsistent national uptake, asymmetrical cross-border connectivity, and protocol incompatibilities that prevent large-scale adoption by research services. Although eIDAS 2.0 promises a more user-centric and interoperable ecosystem, at this point in time, its rollout is incomplete, national implementations vary widely, and support for non-governmental use cases remains immature.

At the same time, research communities express clear yet diverse requirements for identity assurance, from unique personal identifiers and timely updates to robust affiliation assertions and multi-factor authentication. The REFEDS Assurance Framework (RAF) already provides a structured, interoperable way to express many of these requirements, but uptake from institutional identity providers is still insufficient. As a result, high-assurance identities from R&E institutions cannot be communicated reliably to service providers, forcing communities toward costly workarounds or manual vetting processes.

Emerging technologies such as Verifiable Credentials and digital wallets offer a complementary path forward. They can anchor high-assurance identity proofing in authoritative sources and transport these assertions in privacy-preserving, machine-readable formats aligned or compatible with RAF, eIDAS LoA, or NIST 800-63-3. However, their practical usability depends on ecosystem maturity, common standards, cross-border policies, and broad adoption by both issuers and verifiers. These conditions are not yet fully met, and are particularly challenging for global research collaborations involving non-EU participants.

In conclusion, national eID systems, eIDAS 1.0, and eIDAS 2.0 should not be viewed as standalone solutions for achieving identity assurance in the R&E sector. Instead, they may form part of a future hybrid model, where institutional identity management, REFEDS RAF, and verifiable-credential-based mechanisms work together. For this to succeed, research communities should continue to articulate their requirements clearly, identity federations must improve the adoption of RAF and machine-readable assurance declarations, and policymakers should consider R&E use cases in the development of trust frameworks and digital wallet ecosystems. Until then, the reliability of national eID as a scalable assurance mechanism for research services remains unproven.

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/

[Pöhn] Harmonisation: Assurance
https://refeds.org/a/1273

[NIST] Digital Identity Guidelines
https://pages.nist.gov/800-63-3/sp800-63a.html

[ELIXIR] Bona fide researcher service
https://elixir-europe.org/services/compute/aai/bonafide

[NIH] Researcher Auth Service Initiative
https://datascience.nih.gov/researcher-auth-service-initiative

[Ziegler] Improving Identity and Authentication Assurance in Research & Education Federations
https://link.springer.com/chapter/10.1007/978-3-030-31511-5_1

[Facebook] Facebook Changes Displayed Email Addresses To @facebook.com Versions
https://martech.org/facebook-changes-displayed-email-addresses-to-facebook-com-versions/

[ARF] EUDI Wallet Architecture and reference framework
https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.1.0/ar

[eduGAIN] Identifier Attributes
https://wiki.geant.org/spaces/eduGAIN/pages/121348100/Identifier+Attributes

[REFEDs PAEC] Personalized Access Entity Category
https://refeds.org/category/personalized

[OIDC vs. SAML] OIDC vs. SAML: Understanding the Differences and Upgrading to Modern Authentication
https://www.beyondidentity.com/resource/oidc-vs-saml-understanding-the-differences

[REFEDS MRPS] REFEDS Metadata Registration Practice Statement
https://github.com/REFEDS/MRPS/blob/master/mrps.md

[DigiD] What do I need to arrange if I'm moving to the Netherlands?
https://www.government.nl/topics/immigration-to-the-netherlands/question-and-answer/what-do-i-need-to-arrange-if-i%E2%80%99m-moving-to-the-netherlands