MyAcademicID
Blueprint Architecture

Co-financed by the Connecting Europe Facility of the European Union

Table of contents

Introduction **2**

Landscape **2**

Seamless electronic access across borders **3**

Architecture **4**

eduGAIN - eIDAS Bridge 5

European Student Identifier 5

MyAcademicID Service Provider Proxy **7**

Next steps **8**

Annex I – e-services in MyAcademicID **9**

Annex II – eIDAS - eduGAIN comparison **10**

Introduction

The goal of the MyAcademicID project is to enable secure and seamless electronic interactions between Higher Education Institutions (HEIs) with the aim of reinforcing the European student status and enabling seamless mobility of students across borders.

The project is implemented in the broader context of the European Student Card Initiative[1] of the European Commission which aims on the one hand to "enable every student to easily and safely identify and register themselves electronically at higher education institutions within Europe when moving abroad for studies, eliminating the need to complete onsite registration procedures and paperwork", and on the other hand to enable the access to services for students in mobility.

This document draws the technical blueprint for a European eID for higher education creating the digital environment for the 'once only principle' and taking into account existing deployed services and solutions for the research and education community, namely eduGAIN, eduroam, InAcademia, the European Student Identifier along with eIDAS. The technical specifications formulated in this document are the result of numerous consultations with the academic and the eIDAS community. Discussions will continue to be organised with stakeholders and European authorities to define the process leading to the adoption of these new standards.

The scope of the current work involves enabling access to highly relevant existing e-services: the Online Learning Agreement, the Erasmus Dashboard, the Erasmus+ Mobile App, the European PhD Hub, the European Student Card interface and the Erasmus Without Paper Network [Annex I - e-services in MyAcademicID].

Landscape

eIDAS[2] is currently being rolled-out in the European Member States (MS). There is a steady increase in the number of notified countries[3] and the expectation is that in a few years the majority of the European citizens will have access to eIDAS-enabled eIDs.

Currently, the authoritative source in most MS about the academic / student status of the European students are the HEIs, which are also the sending and receiving points in the student mobility process. In Europe, the majority of HEIs participate in the eduroam and eduGAIN inter-federations, through their National Research and Education Networks (NRENs). With **eduroam**[4] and **eduGAIN**[5], students (and also researchers, faculty and staff working in the academic environment) can use the local account provided by their HEI to access the Internet through academic eduroam wireless networks in more

[1] https://ec.europa.eu/education/education-in-the-eu/european-student-card-initiative_en
[2] https://ec.europa.eu/digital-single-market/en/trust-services-and-eid
[3] https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS
[4] https://www.eduroam.org
[5] https://www.edugain.org

than 100 countries around the world[6] and via eduGAIN access more than 2500 online services[7] worldwide.

With the **European Student Card project**[8], a growing number of HEIs can offer their students the possibility to use their home student card in other European campuses, which can be used to assert their student status when travelling abroad as part of the mobility process and access to academic and non-academic services, on and off campus. **InAcademia**[9] is "the real-time, digital equivalent of asking a student to show their student card in order to access or buy services and products". With InAcademia, students validate their affiliation to an HEI institution during a standard process of login to online services.

In addition, there are other national initiatives that are being deployed to facilitate access to student services in and outside of academia. An example of this is the eIDAS-compatible **French initiative**, **Supdata**, that also provides relevant student attributes such as affiliation, status and others, to enable access to public or private service providers, etc. These initiatives are meant to provide identification and authentication solutions in their respective country, while MyAcademicID seeks to identify a solution for service providers at the European level.

Seamless electronic access across borders

In order to provide seamless electronic access across borders, we need to take advantage of the complementarity of the existing deployed services and solutions based on what is available today but also taking into account how the ecosystem is expected to change within the next 2 - 5 years.

Today, the majority of European students have access to federated identities provided by their HEIs, with which they can, via eduGAIN, access more than 2500 online services worldwide. As the availability of eIDAS-enabled eIDs will grow, the expectation is that within the next few years, the majority of European citizens will have a national eIDAS-enabled eID before they enrol in a HEI. Enabling HEIs to use the eIDAS-enabled eIDs during the enrolment process is one of the initial goals of the MyAcademicID architecture. This architecture builds on top of national eIDAS-related initiatives that aim at providing students with access to (e-)services like transport, banking, accommodation, etc.

Taking into account that the majority of HEIs in Europe already support eduroam and eduGAIN, we can enable all European HEIs in eduGAIN to use eIDAS-enabled eIDs, by enabling interoperability between the technical infrastructures of eduGAIN and eIDAS. The alternatives would be that either each MS should enable interoperability between the national academic federation and the national eID services or that each HEI would have to implement its own connection to the national eID services. Both alternatives would require a significant amount of time and a lot of resources to not only implement, but also sustain such solutions. By taking advantage of eduGAIN, we can enable all HEIs at once to use eIDAS-enabled eIDs. On top of this, as an added value, more than 2500 online services will become

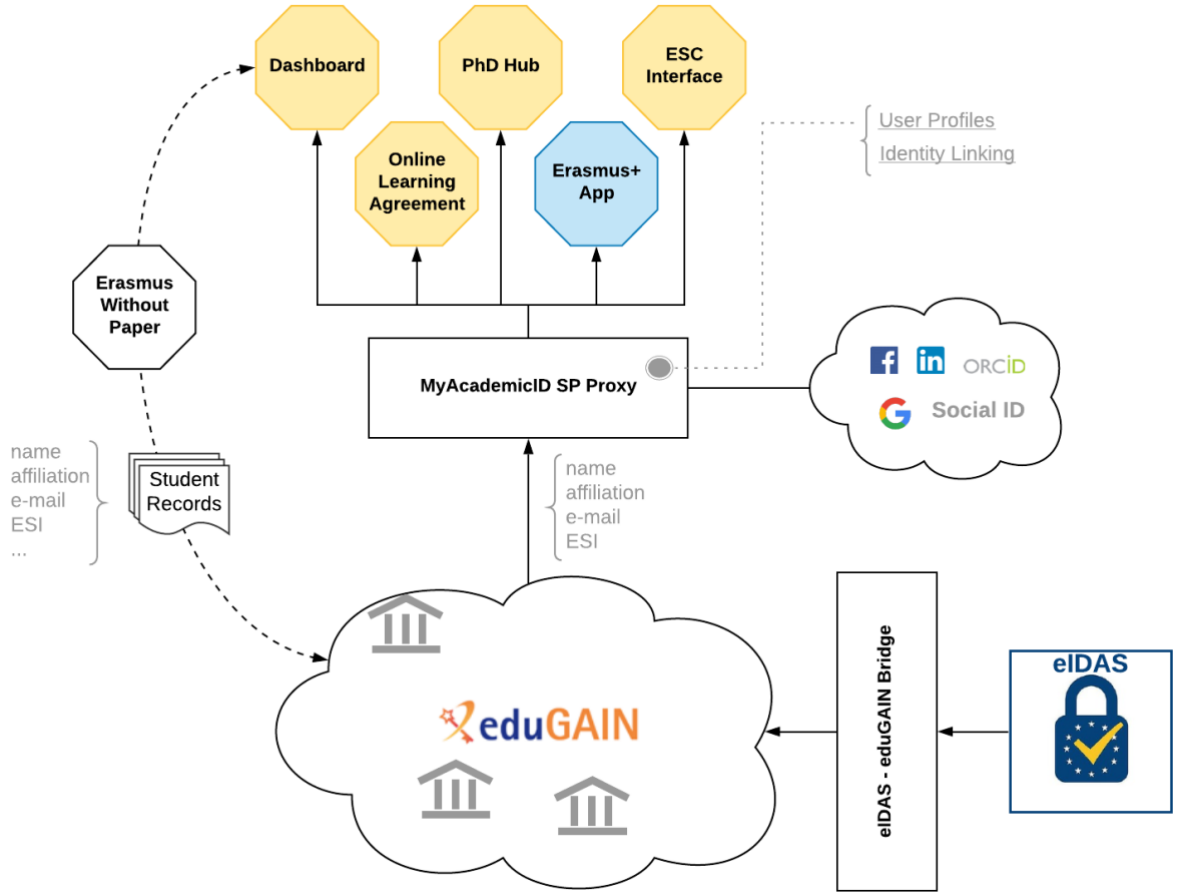
6 https://www.eduroam.org/where/
7 https://technical.edugain.org/entities
8 https://europeanstudentcard.eu/
9 https://www.inacademia.org

instantly available to European students using their eIDAS-enabled eIDs, potentially allowing students to use them as well when going on exchange to countries outside of the EU.

Authentication via national eIDs will not replace the federated identities provided by HEIs to their students, at least not in the near future. HEIs will still have to provide and manage accounts for their students in order to provide them with access to services such as eduroam, the institutional e-mail, the learning management systems and the growing number of e-services that are used in the daily academic life of the students. By enabling HEIs to use the eIDAS-enabled eIDs in the enrolment process, not only will enrolment itself become much easier and intuitive for future students, avoiding unnecessary paperwork, but also enable HEIs to link their students/user records with their national eID. Identity Linking is a key characteristic of the MyAcademicID solution that can enable the consolidation of multiple identities / accounts and enable the user to be able to choose the most appropriate and convenient method of proving his/her identity.

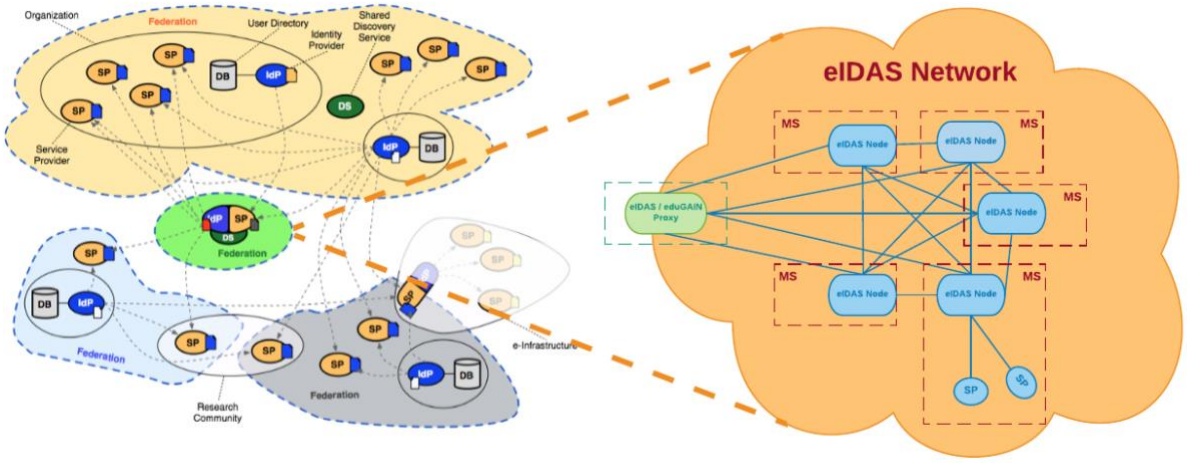
The student mobility process requires the use of a number of services, all of which are involved in different stages of the pipeline and which will need to be able to exchange data about the students who are in mobility. In order to enable these processes, a European Student Identifier is required that can be made available by the institutions and which can be used by all services directly involved in the student mobility process to uniquely identify the user.

Architecture



eduGAIN - eIDAS Bridge

The comparison between the architecture and the SAML deployment profiles in eduGAIN and eIDAS [Annex II - eIDAS - eduGAIN comparison], shows that although there are many similarities, there are also a number of differences that would prevent their seamless integration without a component to bridge these gaps.



In the proposed solution, a SAML-to-SAML protocol proxy acts as a bridge between the eIDAS Nodes and the Identity Federations in eduGAIN. In the identity federations in eduGAIN the proxy appears as an Identity Provider, while in the eIDAS Network, the service participates as an eIDAS Connector. While a technical solution for interoperability between eIDAS and eduGAIN is already being implemented, solutions for an efficient roll-out of the architecture are being discussed with the relevant eduGAIN and eIDAS stakeholders, who will provide input on the best way forward.

European Student Identifier

The student mobility processes require the use of a number of services, all of which are involved in different stages of the pipeline and which will need to be able to exchange data about the students who are in mobility.

The initial European Student Identifier[10] (ESI) was designed in the European Student Card project. At the time of writing this report this implementation is already being used in twelve countries by more than one hundred institutions, while a similar number of institutions is looking into activating the connection.

The consortium has decided to revisit that structure to make it more future proof, due to the expected changes in some of the fields that constitute the original ESI (namely the PIC number, which as of 2019 is no longer issued/maintained by the European Commission for the purpose of Erasmus+

10 http://www.europeanstudentcard.eu/wp-content/uploads/2017/02/2017_03_21_European-student-card-Specifications-v1.pdf

decentralised actions). Note that in the context of the ESC project the PIC will continue to be used and a transition phase is being planned. The outline of the new format does not immediately impact present infrastructure with regards to student card systems.

The new version of European Student Identifier is globally unique, persistent, non-targeted, protocol neutral and data transport neutral. The implementation of the new proposed ESI will be done in a privacy-preserving manner.

- Globally Unique: Each student should be uniquely identified across organizational and national boundaries.
- Persistent: The identifier should follow the student during her/his time of studies.
- Non-targeted: The identifier should be the same for all services involved in the student mobility processes.
- Protocol neutral: The identifier should not change value depending on the protocol used. For example, it should be the same regardless of whether SAML or OpenID Connect is used.
- Data transport neutral: The identifier should not change value depending on how it is transported. For example, the students should be identified by the same identifier, be it through a federated authentication flow or a back-channel transfer of records.

The proposed format of the updated ESI is the following:

urn:schac:personalUniqueCode:<country-code>:<eNS>:<sHO>:<code>

- <country-code> is a valid two letter ISO 3166 country code identifier or the string “int” and assigned by the SCHAC URN Registry.
- <eNS> is the string “ESI” or a string from a nationally controlled vocabulary that denotes that this is a European Student Identifier and which is published in the SCHAC URN Registry.
- <sHO> OPTIONAL – This is the schacHomeOrganization. Required if the student code is provided by the Home Organization of the student and there can be no guarantees that it uniquely identifies the student within the member state. Making this element of the identifier optional is meant to ensure that the ESI does not release any more information than is actually required.
- <code>: The code of the student that uniquely identifies the student within the scope that has been issued. <code> has to be a URN string following the requirements of RFC 2141[11]

Examples of the new ESI:

- Student codes issued and managed centrally at the Member State level

[11] https://tools.ietf.org/html/rfc2141

urn:schac:PersonalUniqueCode:hr:ESI:xxxxxxxxxx

- Student codes are issued and managed by the HEI

  urn:schac:PersonalUniqueCode:es:ESI:uma.es:xxxxxxxxxx

- Student codes are issued by sub-units of the HEI

  urn:schac:PersonalUniqueCode:es:ESI:yyy.uma.es:xxxxxxxxxx

In SAML implementations the ESI is transported as shacPersonalUniqueCode (1.3.6.1.4.1.25178.1.2.14). In OIDC implementations the ESI will be transported as shac_personal_unique_code.

MyAcademicID Service Provider Proxy

In the MyAcademicID project we have identified a set of representative services that are used for enabling student mobility and promoting the internationalisation of higher education in Europe. These services include:

- the Erasmus Dashboard;
- the Erasmus Mobile App;
- Erasmus Without Paper;
- the Online Learning Agreement;
- the PhD Hub[12];
- and the European Student Card interface

These services have some common characteristics, but also important differences. The Erasmus Dashboard, the Online Learning Agreement, the PhD Hub and the ESC interface are web-based applications, which offer personalised services to users. In the case of the Erasmus Dashboard, students are identified in the system, which is accessible to higher education (HE) staff that manage the student mobilities. The other services are directly accessible by the students. In all cases, the users, being students or HE staff, need to authenticate themselves in order to access those services and at the same time the services need to know which institution the user is coming from. The Erasmus Mobile App is very similar in requirements to the previous set of services, in regard to requiring students to authenticate themselves, but it is a mobile application.

Erasmus Without Paper is another service involved in the enablement of student mobility. The main difference with the previous services, is that Erasmus Without Paper is not a user facing service, but rather a service that connects directly to the IT backends of institutions and can be used to transfer

[12] Although not directly related to student mobility, the PhD Hub is a platform that fosters business-driven research by connecting PhD candidates, universities and businesses at European level.

student records to other Erasmus services, including the ESI that will be transported through a back-channel flow. As this service is not user facing, it does not require student authentication.

In order to enable access to the mobile app and the web-based services, we are going to make them available to the National Federation through eduGAIN. This will allow (a) the users to authenticate at their home institutions and (b) the services to receive information such as the European Student Identifier, the users' affiliation and contact information from the home institutions. The services are going to be connected through a multi-protocol SP Proxy (Service Provider Proxy) provided by GÉANT, which will allow the services to use the OpenID Connect protocol in order to authenticate users in eduGAIN, which uses the SAML protocol.

Next steps

The MyAcademicID partners will run the test implementation of the proposed architecture on the e-services outlined above and discuss with European and national authorities how this will further impact digital development in the context of the European Education Area and the eIDAS framework. This also means that the consortium will seek to implement bridge solutions that will allow for current implementations of the European Student Identifier to continue to exist as long as it is technically possible.

The consortium partners will also discuss both internally and with European authorities how education institutions that currently do not participate in eduGAIN can be involved in the digital roadmap by providing them with an alternative solution.

This technical blueprint is a living document and, if required, more information will be added to it as more experience is gained by the consortium in deploying it; national activities related to the deployment of eIDAS in the countries covered by the consortium will also inform the future of the MyAcademicID infrastructure.

Annex I – e-services in MyAcademicID

- The Online Learning Agreement[13] is digitising the process of students preparing, signing and updating their Learning Agreement (LA), the key document for students to go on Erasmus+ mobility and get their studies recognised. The platform is intended to become an integral part of the next Erasmus programme from 2021 onwards. This e-service is connected with the Erasmus+ Dashboard allowing HEIs to manage, approve or reject students' LAs, thus creating an integrated and streamlined process for mobile students.

- Erasmus Without Paper[14] is enabling the electronic exchange of data between HEIs, and more specifically between their existing student information systems. The network caters for all use cases for exchanging data in the field of student mobility - Inter-institutional Agreements (between HEIs), students' nominations, arrival/departure information, Learning Agreements, Transcript of Records.

- The European Student Card[15] is enabling the student status at transnational level to provide students access to campus services (canteen, library, e-payment, etc.) and off-campus services without having to undergo a manual verification process of their student status.

- The Erasmus+ Mobile App[16] is becoming the single point of access for the students intending to study abroad with the Erasmus+ programme. It allows students to already interact with their HEIs as it is connected with the Online Learning Agreement platform and the Erasmus+ Dashboard.

- The European PhD Hub[17] provides PhD students the opportunity to conduct joint research activities with their peers or a company at local and transnational and interdisciplinary levels through an online platform used by companies, HEIs and the PhD students.

- The Erasmus Dashboard[18] is a free, cloud-based tool that supports higher education institutions in managing student mobility under the Erasmus+ programme. Fully integrated with the Online Learning Agreement and the Erasmus+ Mobile App, the Dashboard allows HEIs to communicate with students and initiate, sign or decline learning agreements online.

13 https://www.learning-agreement.eu/start/
14 https://www.erasmuswithoutpaper.eu/
15 https://europeanstudentcard.eu/
16 https://erasmusapp.eu/
17 https://phdhub.eu/
18 https://www.erasmus-dashboard.eu/intro

Annex II – eIDAS - eduGAIN comparison

1. Introduction

This document presents a comparison between the eduGAIN Inter-Federation Service and the eIDAS-Network.

eduGAIN is a service developed within the GÉANT project. eduGAIN interconnects identity federations around the world, simplifying access to content, services and resources for the global research and education community. eduGAIN enables the trustworthy exchange of information related to identity, authentication and authorisation (AAI) by coordinating elements of the technical infrastructure of the federations and providing a policy framework [EDUGAIN-PF] that controls this information exchange. In the eduGAIN model there is usually one Identity Federation per country participating and by 2017 eduGAIN counts 40 Identity Federations as members, while 11 more are in the process of joining.

The eIDAS Interoperability Framework (eIDAS-IF) defines the interoperability components of the eIDAS-Network. These are the necessary components in order to achieve interoperability of notified eIDS schemes according to the eIDAS Regulation.

In this document we are going to compare the two infrastructures and their accompanying services in terms of their architecture and technical implementation.

1.1 Definitions

The following terms[19] and assumptions are used throughout this document:

- ***MS***: Member State that is under eIDAS regulation
- ***Sending MS***: the *MS* whose eID scheme is used in the authentication process
- ***Receiving MS***: the *MS* where the sending *MS* is requesting an authentication of a person
- ***eIDAS-Node***: an operational entity involved in cross-border authentication between *MS*. The *eIDAS-Node* operational entity has two roles:
    - ***eIDAS-Connector***: the SAML SP interface towards the other *MS*
    - ***eIDAS-Service***: the SAML IdP interface towards the other Member States. The *eIDAS-Service* can be further divided in two possible scenarios:
        i. ***eIDAS-Proxy-Service***: an eIDAS-Service operated by the *Sending MS* relaying authentication requests and assertions between the *Sending MS* and the *Receiving MS*

[19] These terms are in accordance to eIDAS spec v1.2 as found in the eIDAS - Interoperability Architecture document [eIDAS-IA] section 1.1

ii. ***eIDAS-Middleware-Service***: an eIDAS-Service running *Middleware* provided by the *Sending MS* which is also operated by the *Receiving MS*

The following namespace prefixes are used:

- ***saml2p***: to denote elements and attributes of the SAML 2.0 Protocol namespace: urn:oasis:names:tc:SAML:2.0:protocol
- ***saml2***: to denote elements and attributes of the SAML 2.0 Core namespace: urn:oasis:names:tc:SAML:2.0:assertion

2. Architecture

From an architectural point of view, the eIDAS Interoperability Framework (eIDAS-IF) shares some of the same principles found in the Federations that participate in eduGAIN, although there are also significant differences. In the diagram below, we present a side by side high-level schematic comparison of what the Federations in eduGAIN and the implementation of the eIDAS-IF look like.

Both services have the same technical goal: *allow users to use their home organization identities in order to access remote services within and across countries*.

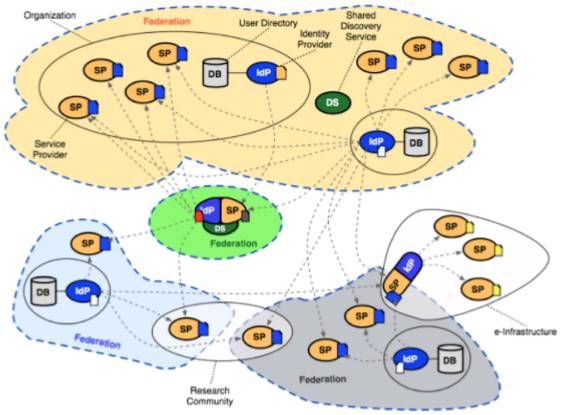
In eduGAIN, the home identities are organization bound and are typically provided by academic institutions and research centers. User credentials are in the form of username and password, although a very small percentage makes use of x509v3 certificates for that purpose. During the last 2 years, there has been significant interest in multi-factor authentication (MFA) support by many organizations.

In eIDAS, the eGOV IDs are provided by the European Member States to their citizens. In many Member States (MS), this function is outsourced to institutional organizations, such as banks, telecom providers and post office services. X509v3 certificates is the prevailing token technology and typically users are provided with smart cards or other forms of hardware tokens.

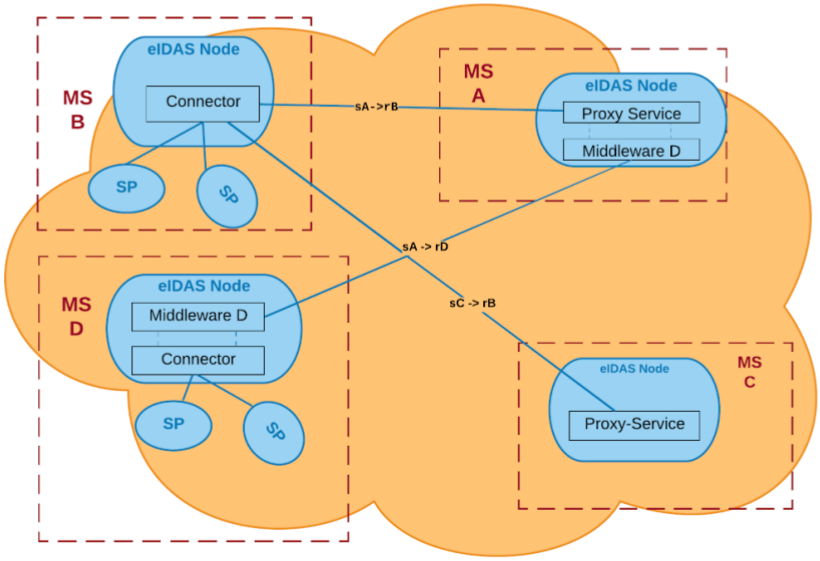
The eIDAS-IF defines two possible schemes that can be employed by a MS. The **proxy based scheme** and the **middleware based scheme.** The former eID scheme, enables cross-border authentication via an eIDAS-Proxy-Service, while the latter, provides cross-border authentication via eIDAS-Middleware-Services. Currently, the proxy based scheme is used by all the MSs except from Germany and Austria.

In cross-border authentication transaction, the eIDAS architecture defines the MS whose eID scheme is used in the authentication process as the **Sending MS**, while the MS where the relying party requesting an authentication of a person is established is called the **Receiving MS**.

National Federations in eduGAIN



eIDAS Nodes



s<MS>: denotes Sending Member State
r<MS>: denotes Receiving Member State
MS D is receiving (rD) from MS A (sA) an Identity Assertion for user citizens of MS A
MS B is receiving (rB) from MS C (sC) an Identity Assertion for user citizens of MS C
MS B is receiving (rB) from MS A (sA) an Identity Assertion for user citizens of MS A

Receiving MSs MUST ensure that personal identification data received via an eIDAS-Connector is processed according to applicable data protection legislation. This includes that data MUST NOT be

forwarded to unidentified peers.

A Receiving MS that operates just one eIDAS Connector is referred to as Centralised MS, while MSs operating more than one eIDAS Connectors are referred to as Decentralised MSs.

In the proxy based scheme, a MS operates an eIDAS-Node, which basically is a SAML Proxy Service. The eIDAS-Node operational entity has two roles: the eIDAS-Connector, which is the SAML SP interface towards the other Member States; and the eIDAS-Service, which is the SAML IdP interface where the other Member States request identity information.

In the middleware based scheme, software is provided by a MS. This scheme has two scenarios: In the first scenario, the Receiving MS provides middleware software; the Sending MS has to use the middleware software to relay the authentication of persons to relying parties of the Receiving MS from their (Sending MS) Proxy to the middleware the Receiving MS provides. In the second scenario, the Sending MS provides middleware software; the Receiving MS has to relay the authentication from their eID-Connector(s) to the middleware software for the purpose of authentication of persons to relying parties of the Receiving MS.

In the eIDAS architecture there is a clear dissociation between the Service Provider and the eIDAS Connector and in the architecture documents it is *explicitly* stated[20] that the connection between the SPs and the eIDAS Connector is not defined and it is up to the MS to define how these connections should be made. Although technically the same applies for the SPs found in the federations connected via eduGAIN, typically what we see in these implementations is that the SAML SP interface is within the administrative domain of the SP.

Regarding the process flow, a request for authentication must be solicited by an SP. Unsolicited response messages are NOT accepted by the eIDAS Services. **In the eIDAS authentication request, the eIDAS Connector must include the type and the name of the relying party**. If the requesting relying party is a private entity, the Service MAY reject the Request if the terms of access of the eID scheme are not fulfilled. This is an eIDAS proprietary extension and thus not used in eduGAIN.

Another difference between the academic federations in eduGAIN and eIDAS is that in the eIDAS cross-border authentication flows Single Sign On is prohibited.

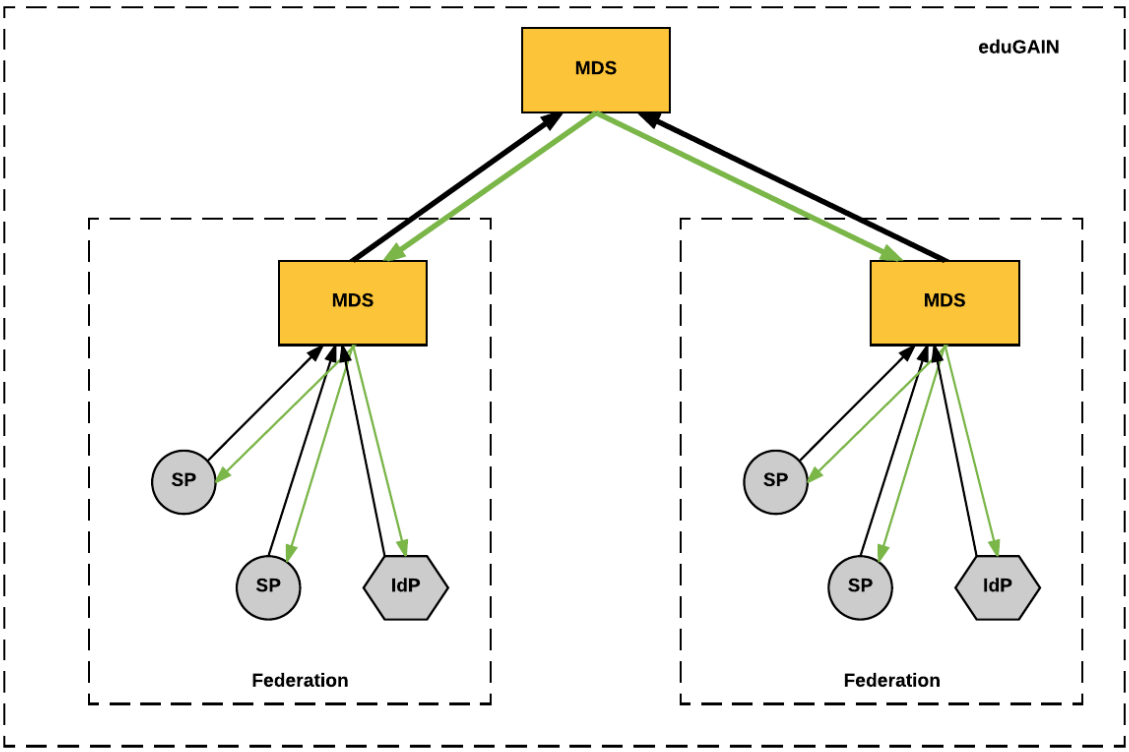
Both in eduGAIN and eIDAS, trust is established by exchanging metadata, which include the public keys for signing and encryption of SAML entities. In eduGAIN, each federation operates a metadata service (MDS), which aggregates metadata from all the SAML entities in the federation. eduGAIN provides a central MDS, which aggregates the exported[21] metadata from the federation MDS and creates one

[20] For more information see [eIDAS-IA] section "3.1. INTERFACE BETWEEN EIDAS-CONNECTOR AND RELYING PARTY". Quoting part of the section:

> This interface is up to the Receiving MS and out of scope of this specification.

[21] It is not mandatory that all entities in a federation are visible to eduGAIN. It is up to the operators of the services to decide whether they want to have their services available in eduGAIN or not. Some federations have an opt-out policy, which means all services are made available to eduGAIN unless their operators explicitly opt-out from eduGAIN, while other federation have an opt-in policy, which means that none of the services are made available to eduGAIN unless their operators explicitly opt-in to eduGAIN.

aggregate feed.



In eduGAIN, an additional trust anchor exists by means of Entity Categories[22]. An Entity Category groups entities (i.e. IdPs, SPs, stand-alone Attribute Authorities) that share common criteria. The intent is that all entities in a given entity category are obliged to conform to the characteristics set out in the definition of that category.

While Entity Categories have multiple potential uses, they were initially conceived as a way to facilitate IdP decisions to release a defined set of attributes to SPs without the need for detailed local review for each SP. The decision by the IdP would instead be based on the criteria detailed in each SP entity category specification. Categories were also conceived for IdPs to indicate support for the SP categories; SPs would use this information to tailor discovery and other aspects of the user experience. Federations make use of both a SAML entity attribute which can be used to assert category membership for an entity (typically by SPs), and a second attribute for use in claiming interoperation with or support for entities in such categories (typically by IdPs).

In eIDAS, there is no central trust anchor (e.g. via the Commission) for metadata exchange. Trust Anchors are exchanged bilaterally between MSs. The EntityIDs must be https URLs, from which the metadata of each entity is publicly accessible.

Regarding the operational and security requirements, according to article 9(3) of [eIDAS-IF], the node operator shall store data which, in the event of an incident, enable reconstruction of the sequence of the message exchange for establishing the place and the nature of the incident. The data shall be

22 https://wiki.refeds.org/display/ENT/Entity-Categories+Home

stored for a period of time in accordance with national requirements and, as a minimum, consist of the following elements: a) node's identification, b) message identification, c) message date and time.

Another interesting aspect is that eIDAS Node operators of nodes providing authentication shall prove that, in respect of the nodes participating in the interoperability framework, the node fulfils the requirements of standard ISO/IEC 27001 by certification, or by equivalent methods of assessment, or by complying with national legislation.

3. Comparison of SAML deployment profiles

Apart from the differences in the architecture of eIDAS and eduGAIN, there are also differences in the SAML deployment profiles that are used in each infrastructure. In eduGAIN, the SAML2Int profile [SAML2INT] is used as the basis upon which eduGAIN adds its own policy framework [EDUGAIN-PF], while eIDAS has defined its own SAML profile. Although there are many commonalities between the two profiles, there are also significant differences. For the purposes of this document we are comparing version 0.2.1 of the SAML2Int profile with version 1.2 of the eIDAS profile.

3.1 Metadata

Service Providers

	eIDAS	**SAML2int v2.0**	**eduGAIN Profile**
<md:SPSSODescriptor>	MUST AuthnRequestsSigned= true	-	-
EntityID	MUST be a HTTPS URL	-	MUST start with either urn: , https:// , or http://
SingleLogoutElementService	SHOULD NOT contain	-	OPTIONAL
ArtifactResolutionService	SHOULD NOT contain	-	OPTIONAL
ManageNameIDService	SHOULD NOT contain	-	OPTIONAL
<md:KeyDescriptor>	MUST declare	OPTIONAL (unset in IdP defaults to signing, unset in SP defaults to encryption)	OPTIONAL
Default AssertionConsumerService index[23]	SHOULD be indicated by the attribute isDefault set to "true"	MUST NOT contain attribute AssertionConsumerSer	OPTIONAL

[23] There are three ways to set the default AssertionConsumerService index; in the metadata by setting the "isDefault" attribute of the AssertionConsumerService element, in the request by setting the AssertionConsumerServiceIndex attribute of the AuthnRequest element, in the request by setting the

	within SAML Metadata AssertionConsumerService element.	viceIndex SHOULD contain an AssertionConsumerServiceURL	
Default AttributeConsumingService index[24]	SHOULD be indicated by the attribute isDefault set to "true" within SAML Metadata AttributeConsumingService element.	-	OPTIONAL
<md:Organization>	SHOULD have	OPTIONAL	MUST contain
<md:OrganizationName> or <md:OrganizationDisplayName> or <md:OrganizationURL>	SHOULD be provided	OPTIONAL	MUST contain all three
<md:ContactPerson> element with a contactType of technical and an <md:EmailAddress> element	SHOULD contain	MUST contain	MUST contain <md:ContactPerson> with contactType="technical" and/or contactType="support"
<md:ContactPerson> element with a contactType of support and an <md:EmailAddress> element	SHOULD contain	OPTIONAL	MUST contain <md:ContactPerson> with contactType="technical" and/or contactType="support"

AssertionConsumerServiceURL attribute of the AuthnRequest element.

[24] There are two ways to set the default AttributeConsumingService index; in the metadata by setting the "isDefault" attribute of the AttributeConsumingService element, and in the request by setting the AttributeConsumingServiceIndex attribute of the AuthnRequest element.

<eidas:SPType>	MUST be present either in the<md:Extensions> element of SAML metadata or in the <saml2p:Extensions> element of a <saml2p:AuthnRequest>. If the SAML metadata of an eIDAS-Connector contains a <eidas:SPType> element, SAML authentication requests originating at that eIDAS-Connector MUST NOT contain a <eidas:SPType> element. The <eidas:SPType> element can contain the values “public” or “private” only.	N/A	N/A
Requested Attributes <eidas:RequestedAttributes>	In AuthN Request[25] as <eidas:RequestedAttributes>[26]	In metadata as <saml2:RequestedAttribute>	In metadata as <saml2:RequestedAttribute>
eIDAS protocol version	eIDAS-Nodes SHOULD publish information about the implemented eIDAS protocol version . MUST be published as entity attribute in the <md:Extension> element	N/A	N/A
eIDAS application identifier	eIDAS-Nodes SHOULD publish information about which product/software and	N/A	N/A

[25] Note that RequestedAttributes is part of the AuthN Request (in the SAML-eIDAS profile) - not the Metadata

[26] For representation cases (e.g. a natural person representing a legal person) the SAML response MAY contain attributes of a representative not requested as <eidas:RequestedAttributes>

	version is used by the node. MUST be published as entity attribute in the <md:Extension> element		
<eidas:NodeCountry>	MUST be present in the <md:Extensions> element of SAML metadata for indicating which Member State or international organisation is responsible for an eIDAS-Node. MUST be the Nationality Code of the SP country or international organization 2 in ISO 3166-1 alpha-2 format.	N/A	N/A
<mdui:DisplayName>	-	MUST contain	SHOULD contain
<mdui:Logo>	-	MUST contain	SHOULD contain MUST be expressed as a Data URI (embedded logo) or an https URL. URLs used for this element MUST be publicly accessible
<mdui:Description>	-		SHOULD contain

Identity Providers

	eIDAS	**SAML2int v2.0**	**eduGAIN Profile**
<md:IDPSSODescriptor>	MUST contain WantAuthnRequestsSigned=true	-	

EntityID	MUST be an HTTPs URL	-	
SingleLogoutElementService	SHOULD NOT contain	-	OPTIONAL
ArtifactResolutionService	SHOULD NOT contain	-	OPTIONAL
ManageNameIDService	SHOULD NOT contain	-	OPTIONAL
<md:KeyDescriptor>	MUST declare	OPTIONAL (unset in IdP defaults to signing, unset in SP defaults to encryption)	OPTIONAL
<md:Organization>	SHOULD have	OPTIONAL	MUST contain
<md:OrganizationName> or <md:OrganizationDisplayName> or <md:OrganizationURL>	SHOULD be provided	OPTIONAL	MUST contain all three
<md:ContactPerson> element with a contactType of technical and an <md:EmailAddress> element	SHOULD contain	MUST contain	MUST contain <md:ContactPerson> with contactType="technical" and/or contactType="support"
<md:ContactPerson> element with a contactType of support and an <md:EmailAddress> element	SHOULD contain	OPTIONAL	MUST contain <md:ContactPerson> with contactType="technical" and/or contactType="support"

LoA	eIDAS-Services MUST publish its highest supported Level of Assurance as entity attribute in the <md:Extension> element. The NameFormat of the including <saml2:AttributeValue> MUST be set to "urn:oasis:names:tc:SAML:2.0:attrname-format:uri" and the Name value MUST be set to “urn:oasis:names:tc:SAML:attribute:assurance-certification”	N/A	N/A
Supported Attributes	MUST be published as <saml2:Attribute> elements in the metadata	-	-
RequesterID	If an eIDAS Service requires the RequesterID for identification of non-public relying parties, it SHALL indicate this via a flag in the SAML metadata. These information MUST be published as entity category attribute according to in the <md:Extension> element	Used only in AuthnRequest	Used only in AuthnRequest
eIDAS protocol version	eIDAS-Nodes SHOULD publish information about the implemented eIDAS protocol version . MUST be published as	N/A	N/A

	entity attribute in the <md:Extension> element		
eIDAS application identifier	eIDAS-Nodes SHOULD publish information about which product/software and version is used by the node. MUST be published as entity attribute in the <md:Extension> element	N/A	N/A
<eidas:NodeCountry>	MUST be present in the <md:Extensions> element of SAML metadata for indicating which Member State or international organisation is responsible for an eIDAS-Node. MUST be the Nationality Code of the SP country or international organization 2 in ISO 3166-1 alpha-2 format.	N/A	N/A
<mdui:DisplayName>	-	MUST contain	SHOULD contain
<mdui:Logo>	-	MUST contain	SHOULD contain MUST be expressed as a Data URI (embedded logo) or an https URL. URLs used for this element MUST be publicly accessible

3.2 Name Identifiers

	eIDAS	**SAML2int/eduGAIN**
NameID formats	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent urn:oasis:names:tc:SAML:2.0:nameid-format:transient urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent urn:oasis:names:tc:SAML:2.0:nameid-format:transient

3.3 Attributes

Natural Person

	eIDAS Attribute Profile	**eduGAIN (eduPerson[27])**
Surname	FamilyName - *mandatory*	sn
Name	FirstName - *mandatory*	givenName
Date of Birth	DateOfBirth - *mandatory*	
Unique Identifier	PersonIdentifier - *mandatory*[28]	eduPersonUniqueId eduPersonPrincipalName[29] subject-id[30]
First Name at Birth	BirthName - *optional*	
Family Name at Birth	BirthName - *optional*	

[27] eduPerson is defined by [I2-EDUP]

[28] For more information see [eIDAS-AP] section "2.2.3. Unique Identifier (mandatory). '' Quoting part of that section:

The unique identifier consists of ():

1. The first part is the Nationality Code of the identifier
   This is one of the ISO 3166-1 alpha-2 codes, followed by a slash ("/"))
2. The second part is the Nationality Code of the destination country or international organization 1
   This is one of the ISO 3166-1 alpha-2 codes, followed by a slash ("/")
3. The third part a combination of readable characters
   This uniquely identifies the identity asserted in the country of origin but does not necessarily reveal any discernible correspondence with the subject's actual identifier (for example, username, fiscal number etc)

[29] When the IdP has a policy not to reassign the eduPersonPrincipalName(s)

[30] subject-id is not part of eduPerson, but defined by [SAML-SUB-ID]

Place of Birth	PlaceOfBirth - *optional*	
Current Address	CurrentAddress - *optional*	
Gender	Gender - *optional*	

Legal Person

Current Legal Name	LegalName - *mandatory*	
Unique Identifier	LegalPersonIdentifier - *mandatory*	
Current Address	LegalAddress - *optional*	
VAT Registration Number	VATRegistration - *optional*	
Tax Reference Number	TaxReference - *optional*	
Directive 2012/17/EU Identifier	BusinessCodes - *optional*	
Legal Entity Identifier (LEI)	LEI - *optional*	
Economic Operator Registration and Identification (EORI)	EORI - *optional*	
System for Exchange of Excise Data (SEED)	SEED - *optional*	
Standard Industrial Classification (SIC)	SIC - *optional*	

3.4 SAML AuthN request

-	**eIDAS**	**SAML2int/eduGAIN**
SAML Request Messages *<saml2p:AuthnRequest>*	MUST be signed	
Binding	HTTP Redirect or HTTP-POST binding (HTTP-Redirect recommended)	MUST be communicated to the Identity Provider using the HTTP-REDIRECT
Verification	eIDAS-Service MUST verify the integrity/authenticity of a	Identity Providers MAY omit the verification of signatures in

	SAML Request Message	conjunction with HTTP-REDIRECT binding
Endpoints		SHOULD be protected by TLS/SSL
Force Authn	MUST be set to true	-
SPType	MUST be set to private or public	-
RequestedAuthnContext	It MUST be set Comparison attribute MAY be provided	MAY be set, but SHOULD do if arrangement exists between the IdP and SP The Comparison attribute SHOULD be omitted or be set to "exact"
AssertionConsumerService	AssertionConsumerServiceURL SHOULD NOT be provided, if provided the eIDAS-Service MUST compare it with the metadata ProtocolBinding SHOULD NOT be used	AssertionConsumerServiceURL MAY be provided indicating preference. ProtocolBinding attribute, if present, MUST be set to urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST.
Service Provider Type <eidas:SPType>	eIDAS proprietary extension. Can be either “public” or “private”	N/A
Requested Attributes <eidas:RequestedAttributes>	MUST be included in the <saml2p:Extensions> element of the SAML AuthnRequest MAY contain attributes published in the SAML metadata of the eIDAS-Service[31]	N/A

[31] For representation cases (e.g. a natural person representing a legal person) the SAML response MAY contain attributes of a representative not requested as <eidas:RequestedAttributes>

<eidas:RequestedAttribute>	MUST have for each requested attribute	N/A
<eidas:RequestedAttribute isRequired>	MUST be set to “true” for mandatory requested attributes MUST be set to “false” for optional attributes	N/A
AssertionConsumerServiceURL	SHOULD NOT have	SHOULD have
ProtocolBinding	SHOULD NOT use	OPTIONAL typically accompanied by the AssertionConsumerServiceURL
ForceAuthn	MUST support ForceAuthn. ForceAuthn MUST be set to “true”.	OPTIONAL
isPassive	MUST support isPassive. isPassive SHOULD be set to “false”.	OPTIONAL
RequesterID	SHOULD use to indicate the actual relying party filing the authentication request. When present, the RequesterID MUST be guaranteed to be unique at least within the Connector of the Member State where the request originates from.	OPTIONAL
NameIDPolicy	<saml2p:NameIDPolicy> SHOULD be used	<saml2p:NameIDPolicy> SHOULD NOT be used
RequestedAuthnContext	SHALL be used to indicate the requested eIDAS Levels of	OPTIONAL

	Assurance[32]	MUST be included iif SP does require a specific <saml2:AuthnContextClassRef>
<eidas:SPType>	MUST be present either in the<md:Extensions> element of SAML metadata or in the <saml2p:Extensions> element of a <saml2p:AuthnRequest>. If the SAML metadata of an eIDAS-Connector contains a <eidas:SPType> element, SAML authentication requests originating at that eIDAS-Connector MUST NOT contain a <eidas:SPType> element. The <eidas:SPType> element can contain the values “public” or “private” only.	N/A
<eidas:NodeCountry>	MUST NOT contain	N/A

3.5 SAML AuthN Response

	eIDAS	**SAML2int/eduGAIN**
SAML Response Messages <saml2p:Response>	MUST be signed	-[33]
Assertion signing/encryption[34]	MAY be signed MUST be encrypted	MUST be signed[35] If endpoint is not TLS/SSL, it SHOULD be encrypted. It is NOT RECOMMENDED to encrypt each attribute, but the entire assertion.

[32] See 3.6 Levels of Assurance for other scenarios
[33] MUST be signed in next version of SAML2int
[34] Shibboleth IdP encrypt by default, SSP sign by default but do not encrypt.
[35] MAY be signed in the next version of SAML2int

Message content	Response MUST contain exactly one EncryptedAssertion-element Assertion MUST contain exactly one AuthnStatement-element and one AttributeStatement-element	Response MUST contain exactly one assertion (either a <saml2:Assertion> or an <saml2:EncryptedAssertion> element) Assertion MUST contain exactly one <saml2:AuthnStatement> element and MAY contain zero or one <saml2:AttributeStatement> elements
Binding	HTTP Post MUST be used *(SHALL in the original doc --- translated to MUST as for RFC2119)*	HTTP Post MUST be used
Unsolicited response	MUST NOT be accepted	MUST be supported *(by Service Providers)*
Verification	eIDAS-Connector MUST verify the authenticity before processing the assertion *(extract, verify the signature of the message, verify the signature of the assertion if signed)*	MUST verify signatures MUST verify Recipient MUST verify NotOnOrAfter MUST verify InResponseTo MAY verify address in SubjectConfirmationData (Defined in SAML V2.0 Web Browser SSO Profile [SAML2-BSSO])
AuthnContext	MUST contain a URI that points to eIDAS LoA	
<saml2:NameID>	MUST be contained in <saml2:Subject>	SHOULD be contained in <saml2:Subject>

3.6 Levels of Assurance

For the assurance of identity and authentication, eIDAS and the implementing regulation 2015/1502 [eIDAS-LoA] introduces three assurance levels; low (limited degree of confidence), substantial (substantial degree of confidence) and high (high degree of confidence in the claimed or asserted identity of the person). The levels cover identity proofing, credential issuance, credential management and authentication. eIDAS further imposes requirements on information security management, record keeping, compliance and audits.

eIDAS allows Member States to support other URIs than the three assurance levels defined by eIDAS. This means that interoperability between systems can be achieved. However, it is noted that "a non-notified eID does not claim any guarantees for assurance or does not claim any sending Member State liability", and that when "requesting a LoA of a non-notified eID, the Comparison attribute of <saml2p:RequestedAuthnContext> MUST be set to "exact" and the eIDAS-Connector MUST include any LoA URI (for notified and non-notified eID) that are acceptable in a response assertion".

eduGAIN does not impose particular requirements for identity providers in its member federations. However, the REFEDS community has developed a REFEDS Assurance Framework [RAF] introducing requirements on identifiers, identity proofing and attribute freshness. Two authentication profiles for single-factor (REFEDS SFA) and multi-factor authentication (REFEDS MFA) are also introduced. Unlike eIDAS, REFEDS does not introduce mandatory layers (combinations of sufficient identity proofing and authentication levels) for identity providers although potentially useful combinations of different assurance components are suggested in the Espresso and Cappuccino profiles.

Where possible, REFEDS Assurance Framework leverages work done in external specifications, including eIDAS. The following table maps eIDAS requirements to REFEDS. Notice that the mapping is unidirectional; a credential service provider's qualification to certain eIDAS level *may* imply certain RAF values, but not vice versa.

Assurance component	eIDAS level	Resulting REFEDS Assurance Framework or authentication profile value
Identity proofing and credential issuance, renewal and replacement	low	IAP/medium
	substantial	IAP/high
Authentication	substantial	REFEDS MFA

Note that there is no mapping between eIDAS and REFEDS-MFA.

4. Software implementations for eIDAS Nodes

1. OpenSAML extensions for the eIDAS Framework -- Java -- extension to OpenSaml
   https://github.com/litsec/eidas-opensaml
2. SwedenConnect; Swedish eIDAS proxy -- Java -- using (1)
   https://github.com/swedenconnect
   https://github.com/swedenconnect/opensaml-bom
3. German eIDAS Middleware -- Java -- using (1)
   https://github.com/Governikus/eidas-middleware
4. UK Proxy node -- Java -- with patched opensaml
   https://github.com/alphagov/verify-proxy-node
5. Esthonian eIDAS node -- Java
   https://github.com/e-gov/eIDAS-Connector
   https://github.com/e-gov/eIDAS-Client
6. CEF Demo implementation -- Java -- unofficial mirror on GitHub
   https://github.com/yuriylesyuk/eidas-x509-for-psd2
7. SATOSA proxy based eIDAS gateway -- Python -- work in progress
   https://github.com/IdentityPython/SATOSA/
8. Spanish eIDAS to National Research and Education Identity Federation bridge
   https://github.com/rediris-es/simplesamlphp-clave2