



Connecting services, building trust, empowering students

Christos Kanellopoulos, GÉANT
christos.kanellopoulos@geant.org

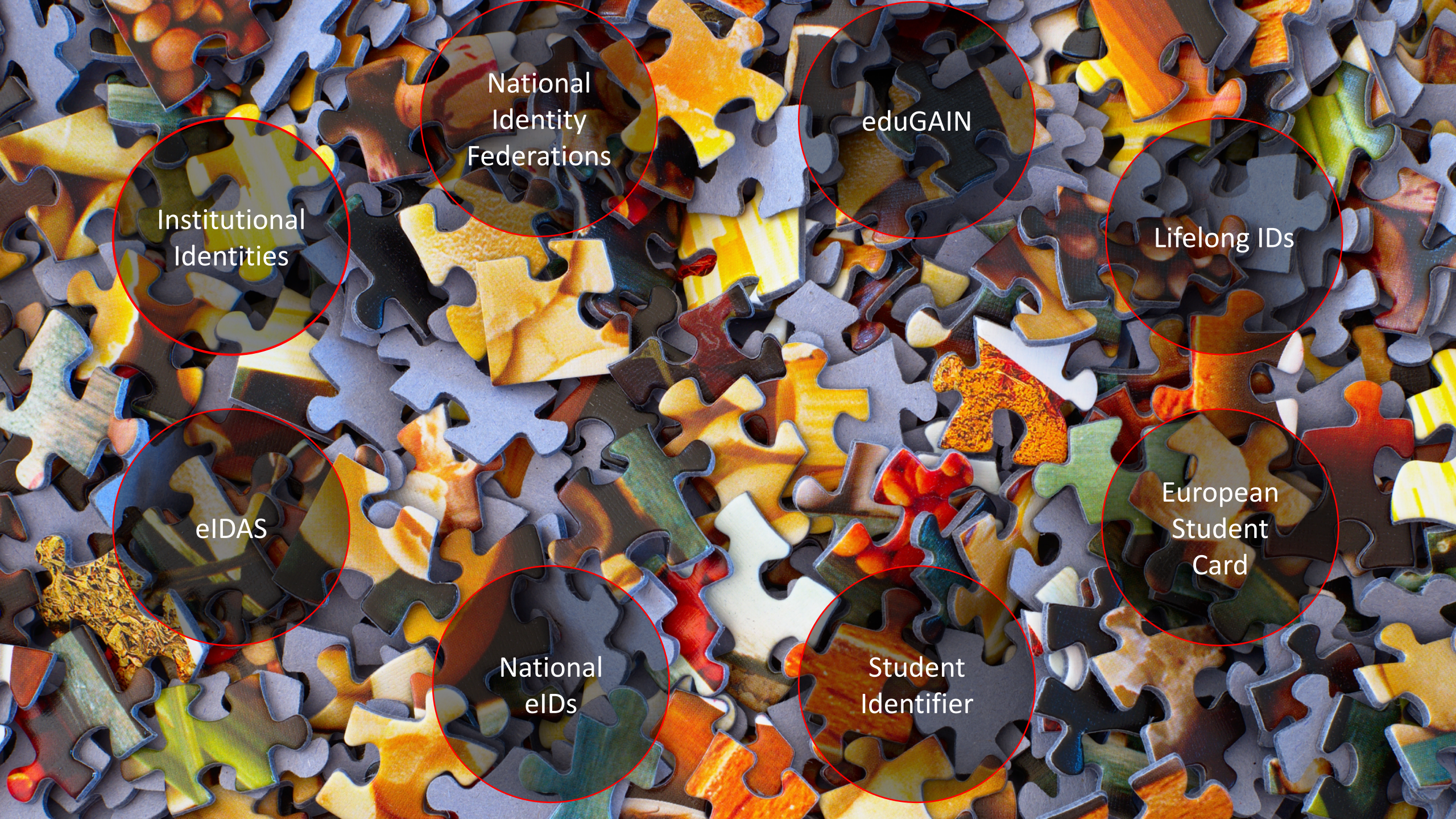


Co-financed by the Connecting Europe
Facility of the European Union

MyAcademicID is/has been all about

- Outlining mobility related use cases
- Agreeing on the specifications of the ESI
- Defining how the ESI can be best transported from A to B
- Building a first bridge with the citizen eID eIDAS
- Designing a single interface for authenticating students
- Implementing the authentication interface on some of the use cases

After numerous
technical meetings on...



National
Identity
Federations

eduGAIN

Lifelong IDs

Institutional
Identities

European
Student
Card

eIDAS

National
eIDs

Student
Identifier



30 May 2017

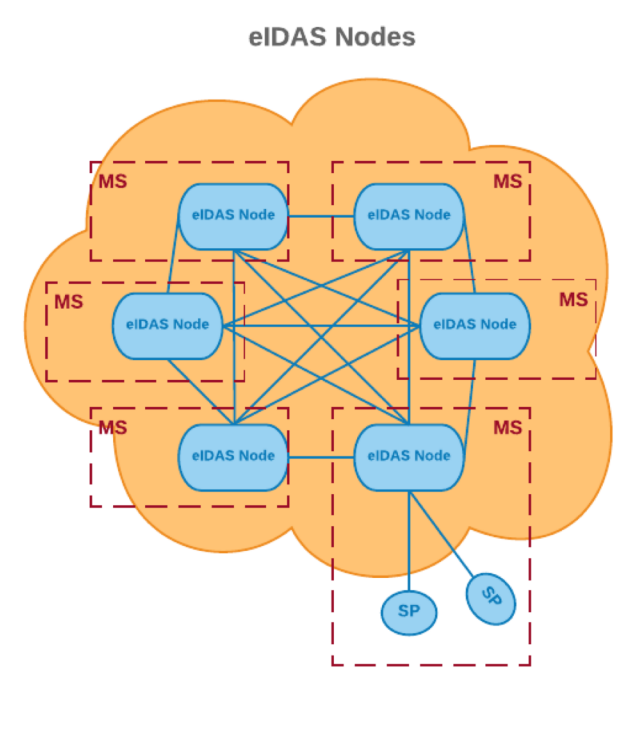
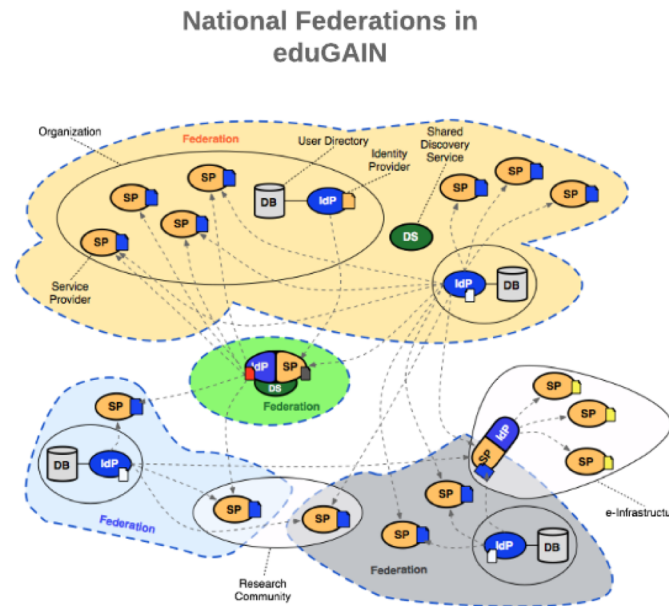
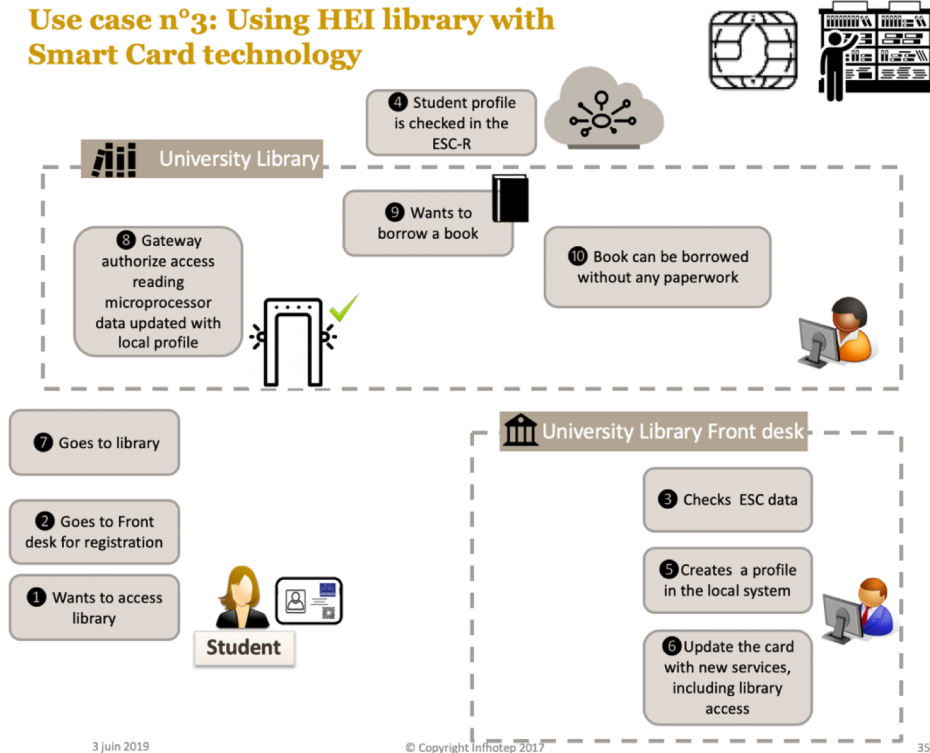
eduGAIN - eIDAS Comparison



Feasibility Study on Cross-border Use of eID and Authentication Services (eIDAS compliant) to support Student Mobility and Access to Student Services in Europe



Use case n°3: Using HEI library with Smart Card technology

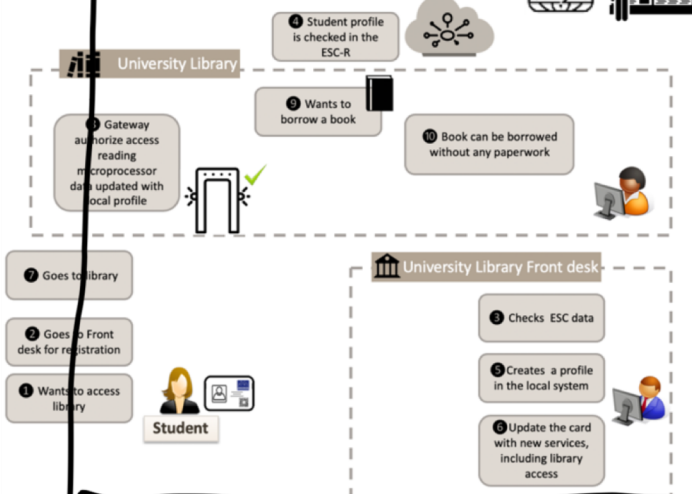


Assurance

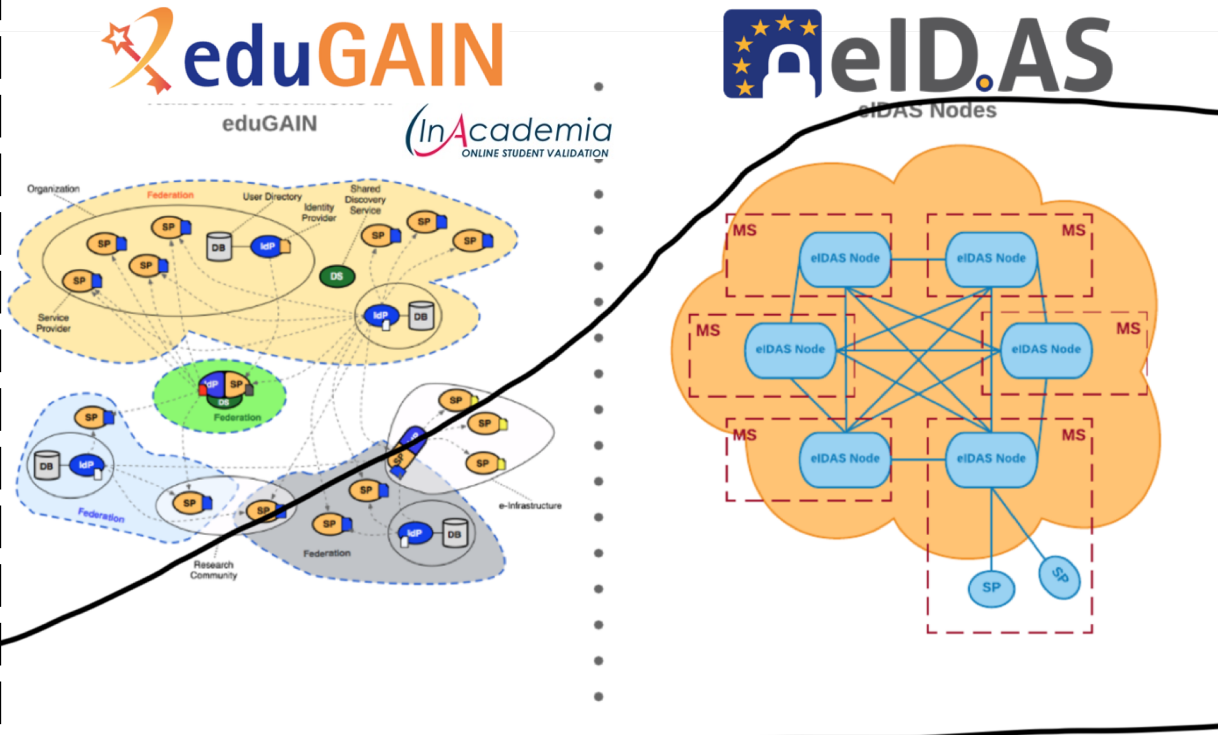
Complementarity



Use case n°3: Using HEI library with Smart Card technology



Identification



Authentication

So after numerous
meetings...

A blueprint architecture was approved and released for the higher education community

A bridge between the Swedish eIDAS node and eduGAIN was established and moved into production

An authentication proxy linking to eduGAIN, eIDAS (and other OIDC IdPs) was created

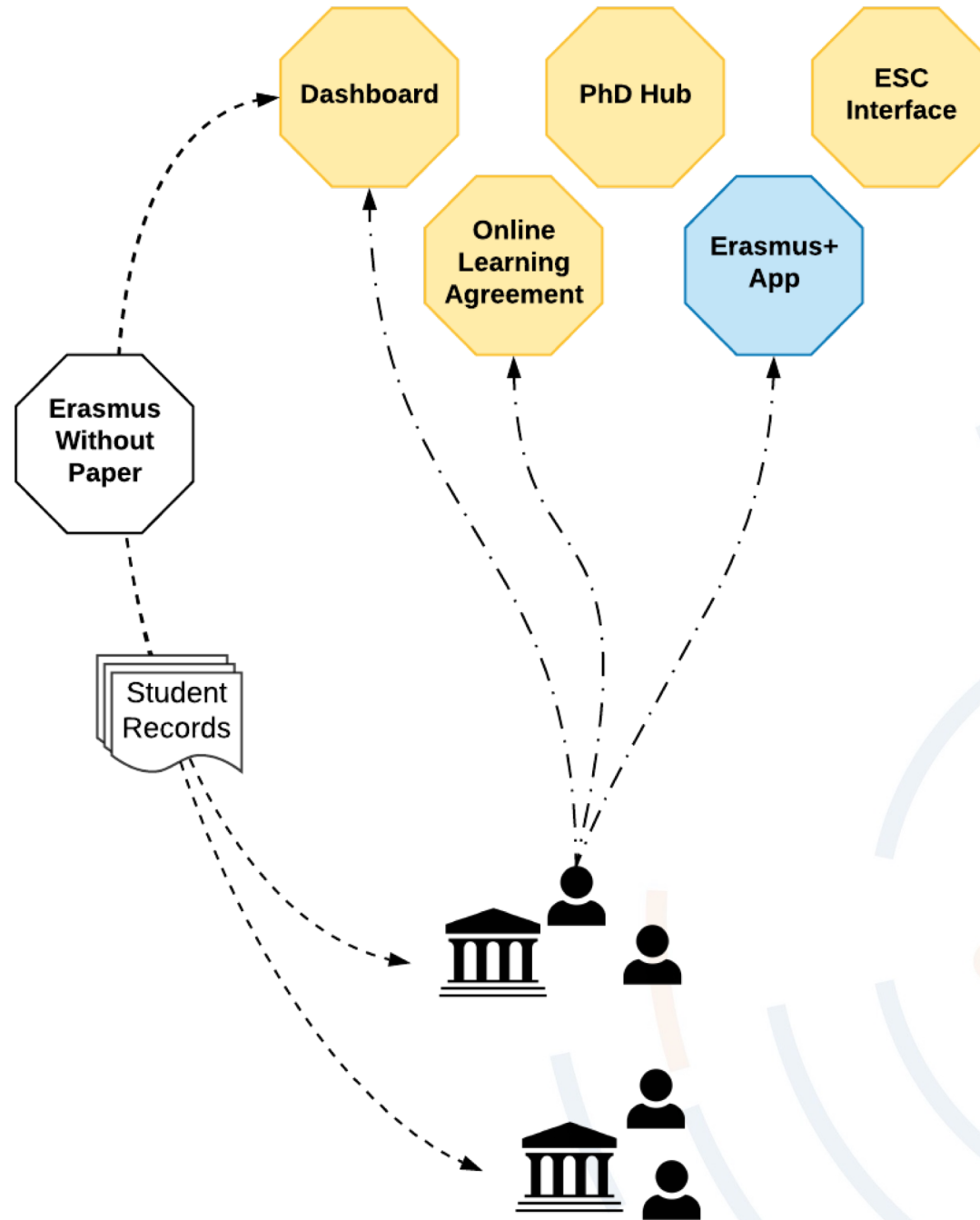
That's all very well, but how does it work?



E-service providers

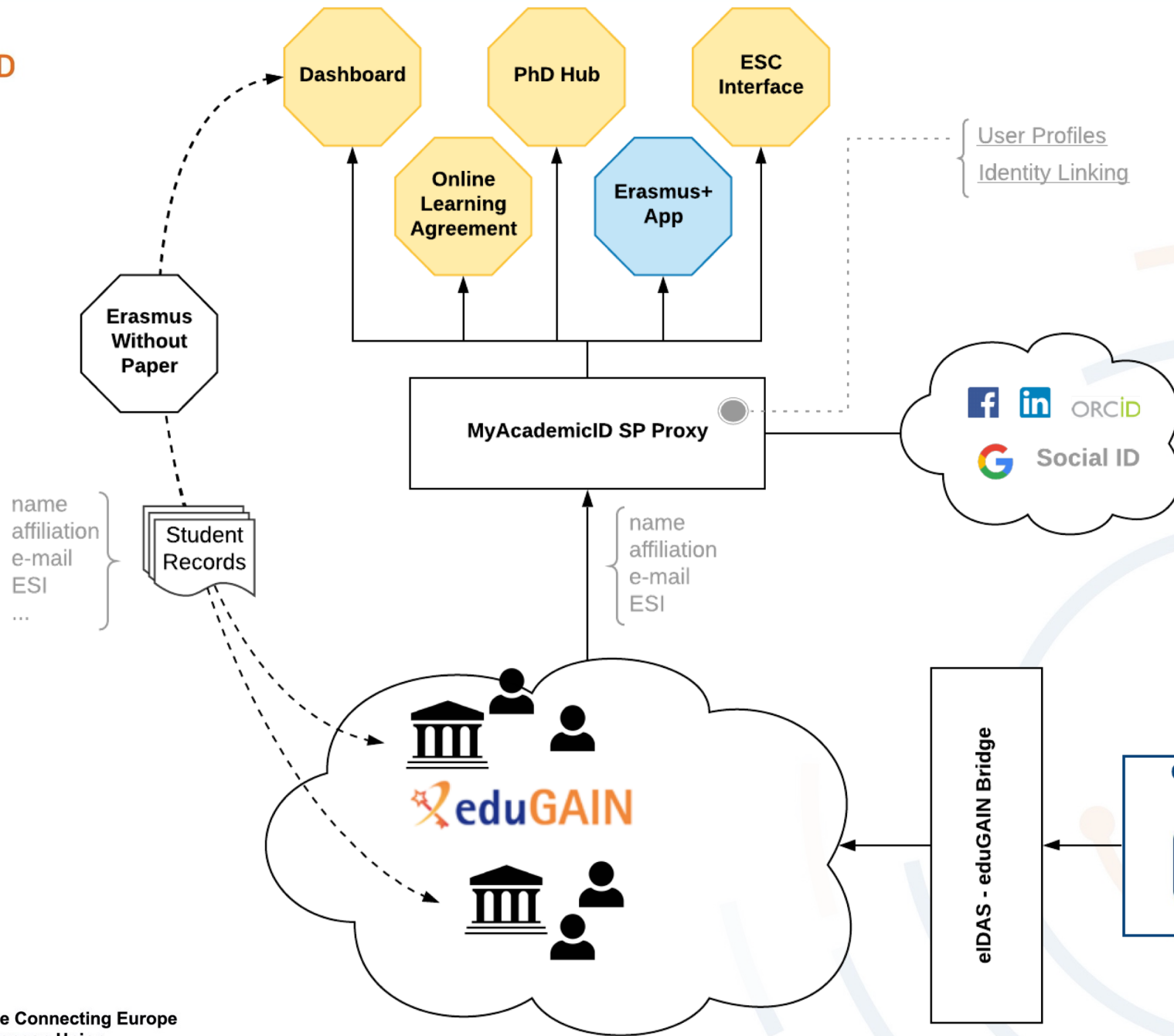
Use cases





European Student Identifier

- **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 if SAML or OpenID Connect is used
- **Data transport neutral:** The identifier should not change value depending on how it is transported.
- **Privacy preserving:** The identifier should not be used to track the students' activities across services



Criteria	European Student Identifier (ESI)	eduPerson Principal Name (ePPN)	eduPerson Targeted ID (ePTID)	schac Personal Unique Code	schac Personal Unique ID	subject ID	ORCID ID
Target audience	Student	R&E Community	R&E Community	R&E Community	R&E Community	Security subjects (generally but not exclusively people)	Researchers
Adoption rate	 limited to ESC pilot institutions	 commonly used in eduGAIN	 commonly used in eduGAIN	 not commonly used in eduGAIN but more within boundaries of federations and/or institutions	 not commonly used in eduGAIN but more within boundaries of federations and/or institutions	 low adoption (new identifier)	 high adoption (7,218,074 ORCID IDs)
Sustainability	 ESI institution part (PIC Code) is about to be replaced	 eduPerson specification (201602)	 eduPerson specification (201602)	 SCHAC specification (version 1.5.0)	 SCHAC specification (version 1.5.0)	 SAML V2.0 Subject Identifier Attributes Profile Version 1.0	 ISO 27729 compatible
Direct link with student unique code in student record	 ESI right part directly matches the student unique code in HEI at enrollment	 Depends on the value used for the user ID in the left part (name-based generally)	 opaque identifier	 Yes if the <INSS> part contains the student unique code in HEI	 Must contain a legal unique identifier	 Depends on the value used for the user ID in the left part	 no reference to student unique code (https URI with 16 digits number)
Globally unique	 Same principle as IBAN banking format (guarantee of uniqueness)	 Globally unique in a federation context	 Globally unique in a federation context	 Yes but the value of the <INSS> part must be defined accordingly	 globally unique by design	 suitable for use as a globally-unique external key	 globally unique by design
Persistent (stable over time)	 institution part potentially subject to change case of student mobility : a student will have as many ESI that he is enrolled to different HEIs	 subject to change or reassignment	 persistent by design but bound to institution (case of student mobility)	 can potentially be bound to institution depending on the value of INSS	 persistent by design	 persistent by design but bound to institution (scope part)	 persistent by design
Non-targeted	 services independent	 services independent	 service specific its value will change from one service to another	 services independent	 services independent	 services independent	 services independent
Protocol neutral	 specification of R&E claims and scope for OIDC needed	 SAML specific (scoped attribute)	 SAML specific	 specification of R&E claims and scope for OIDC needed	 specification of R&E claims and scope for OIDC needed	 SAML specific	 specification of R&E claims and scope for OIDC needed
Data transport neutral	 no tied to a transport mechanism	 Federation specific (not necessarily stored in user directory, can be generated on-the-fly by the IdP)	 Federation specific (generally not stored in user directory and generated directly by the IdP)	 no tied to a transport mechanism	 no tied to a transport mechanism	 Federation specific	 no tied to a transport mechanism

Criteria	European Student Identifier (ESI)	eduPerson Principal Name (ePPN)	eduPerson Targeted ID (ePTID)	schac Personal Unique Code	scnac Personal Unique ID	subject ID	ORCID ID
Target audience	Student	R&E Community	R&E Community	R&E Community	R&E Community	Security subjects (generally but not exclusively people)	Researchers
Adoption rate	limited to ESC pilot institutions	commonly used in eduGAIN	commonly used in eduGAIN	not commonly used in eduGAIN but more within boundaries of federations and/or institutions	not commonly used in eduGAIN but more within boundaries of federations and/or institutions	low adoption (new identifier)	high adoption 7,218,074 ORCID iDs
Sustainability	ESI institution part (PIC Code) is about to be replaced	eduPerson specification (201602)	eduPerson specification (201602)	SCHAC specification (version 1.5.0)	SCHAC specification (version 1.5.0)	SAML V2.0 Subject Identifier Attributes Profile Version 1.0	ISC 27729 compatible
Direct link with student unique code in student record	ESI right part directly matches the student unique code in HEI at enrollment	depends on the value used for the user ID in the left part (name-based generally)	opaque identifier	Yes if the <INSS> part contains the student unique code in HEI	Must contain a legal unique identifier	depends on the value used for the user ID in the left part	no reference to student unique code (http://URI with 15 digit's number)
Globally unique	Same principle as IBAN banking format (guarantee of uniqueness)	Globally unique in a federation context	Globally unique in a federation context	Yes but the value of the <INSS> part must be defined accordingly	globally unique by design	suitable for use as a globally-unique external key	globally unique by design
Persistent (stable over time)	institution part potentially subject to change case of student mobility : a student will have as many ESI that he is enrolled to different HEIs	subject to change or reassignment	persistent by design but bound to institution (case of student mobility)	can potentially be bound to institution depending on the value of INSS	persistent by design	persistent by design but bound to institution (scope part)	persistent by design
Non-targeted	services independent	services independent	service specific its value will change from one service to another	services independent	services independent	services independent	services independent
Protocol neutral	specification of R&E claims and scope for OIDC needed	SAML specific (scoped attribute)	SAML specific	specification of R&E claims and scope for OIDC needed	specification of R&E claims and scope for OIDC needed	SAML specific	specification of R&E claims and scope for OIDC needed
Data transport neutral	no tied to a transport mechanism	Federation specific not necessarily stored in user directory, can be generated on-the-fly by the IdP)	Federation specific generally not stored in user directory and generated directly by the IdP)	no tied to a transport mechanism	no tied to a transport mechanism	Federation specific	no tied to a transport mechanism

European Student Identifier

<https://wiki.geant.org/display/SM/European+Student+Identifier>

urn:schac:personalUniqueCode:int:esi:auth.gr:23456790G

Namespace for the
European Student Identifier

schacHomeOrganization

Student
Identifier

ESI with HEI-wide scope student code

European Student Identifier

<https://wiki.geant.org/display/SM/European+Student+Identifier>

urn:schac:personalUniqueCode:int:esi:hr:23456790G

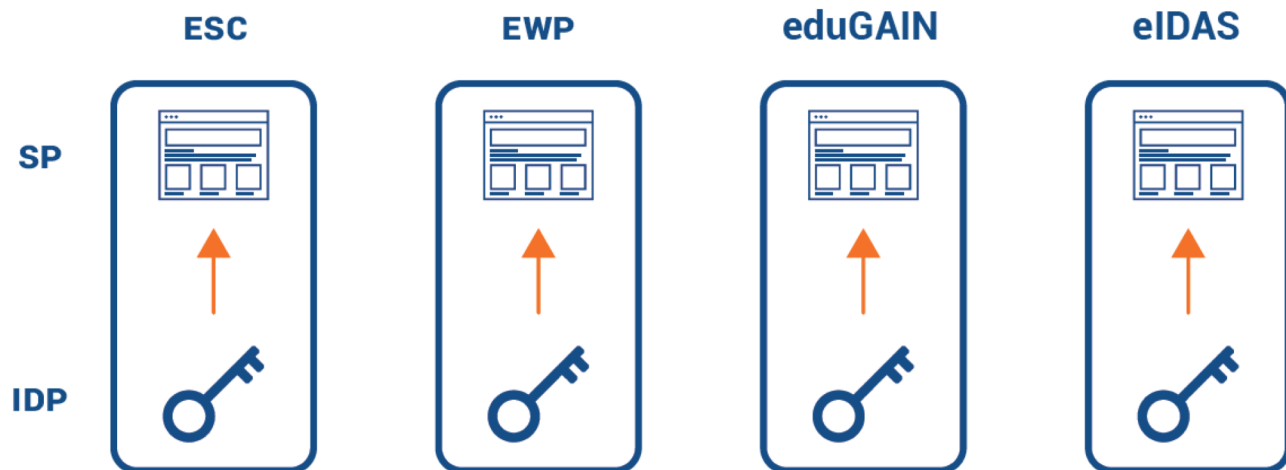
Namespace for the
European Student Identifier

Country code

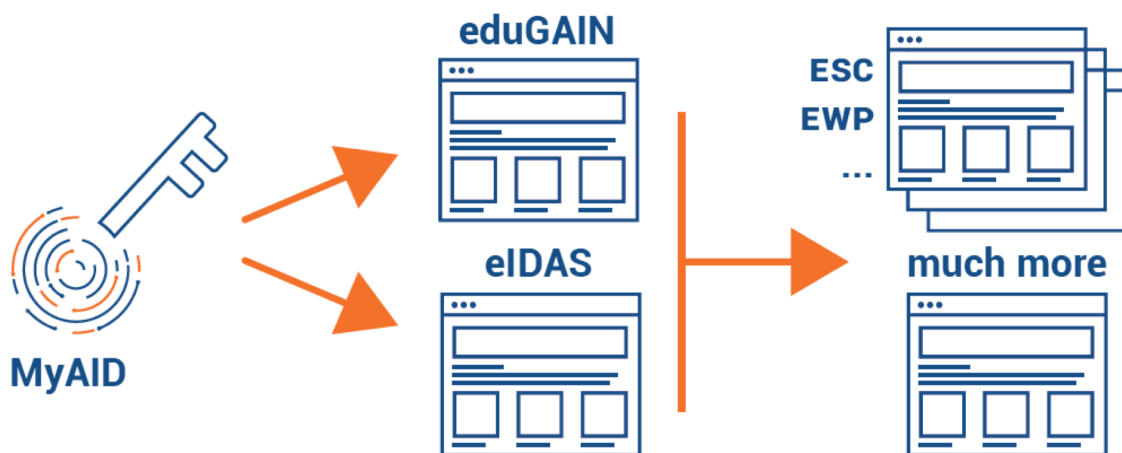
Student
Identifier

ESI with nation-wide (or region-wide) scope student code

CURRENT SITUATION



AFTER MyAcademicID



**FEWER
SILOS, MORE
CONNECTIVITY
AND GLOBAL
ACCESS TO
e-SERVICES
THROUGH A
SINGLE SIGN-ON!**

Integrating multiple eIDs from different existing ecosystems, will enable the possibility to overcome the actual silos architecture. One student eID scheme will give students access to a wide range of different services that currently live in different systems. Moreover, this approach will open the possibility for future integration with more services.

- Secure and seamless exchange of information
- Reliable student identification and authentication
- Reuse of existing digital structures
- Online management of mobility process
- Access to e-services through single sign-on
- Reinforced student status
- Reduced administrative burden



Benefits

Thank you

www.myacademicid.eu

+ contact

