LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

European Student Card & eID
legal and technical considerations

Alexander Loechel
Referent IT-Projekte
Ludwig Maximilians-Universität München

ECCA Meeting 03.11.2020

ECCA
Student eID Framework

Base for my analysis / Sources

- European Commission > Education & Training > European Education Area (https://ec.europa.eu/education/education-in-the-eu/european-education-area_en)
- European Commission > Education & Training > European Student Card Initiative (https://ec.europa.eu/education/education-in-the-eu/european-student-card-initiative_en)
- General and Technical specifications for implementing the ESC (http://europeanstudentcard.eu/wp-content/uploads/2017/02/2017_03_21_European-student-card-Specifications-v1.pdf)
- ESC Handbook for intitution: Users's Guide to connect to the Platform (http://europeanstudentcard.eu/wp-content/uploads/2017/02/ESC-User-Guide-def.pdf)
- Regulation (EU) 2016/679 of the European Parliament and of the Concil of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e40-1-1)
- Regulation (EU) No 910/2014 of the European Parliament and of the Concil of 23. July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS-Regulation) (https://eur-lex.europa.eu/eli/reg/2014/910/oj?locale=en)
- ECCA – Student eID Framework 2020 Final Report (https://ecca.eu/index.php/members-area/docs/news/283-student-eid-framework-2020-final-report-1)
- ECCA - Student eID Framework Newsletter June 2020 (https://ecca.eu/index.php/members-area/docs/news/282-student-eid-framework-newsletter-june-2020)

Only public information has been used for this analysis

The Vision towards an „European Education Area“:

- spending **time abroad** to **study** and **learn** should become the norm
- school and higher education qualifications should be recognised across the EU
- knowing **two languages** in addition to one's mother tongue should be standard
- everyone should be able to access high-quality education, irrespective of their socio-economic background
- people should have a strong sense of their identity as a European, of Europe's cultural heritage and its diversity

  Source: https://ec.europa.eu/education/education-in-the-eu/european-education-area_en
- „Student and Staff mobility“ as key contribution to that strategy

  Source: https://ec.europa.eu/research/participants/data/ref/other_eu_prog/other/eplus/guide/gfa_eacea-03-2020_en.pdf

Fantastic Idea – that we should support as good as we can!

The Programs:

- THE EUROPEAN STUDENT CARD
- MyAcademicID

} Identity documents (physical and virtual medium; eID, card)

First Question should always be:

Which Problem did we try to solve?

Second Question:

On which foundation can we build?

Last Question:

Are there any hidden agendas linked with the project?

Which Problem did we try to solve?

- Strengthen the **European Identity**

→ European Student Card (common design and holographic logo) ✔

- Enable and support **Student and Staff mobility**
  - short-term & long-term mobility
  - Access to services on and off campus
  - Support digital mobility management
  - Student application, nominations, acceptances and transcript of record
    → Administrative processes

→ **eID** – secure and trusted data flow between Higher Education Institutions
→ common data schema – necessary personal data

→ Electronic Signature (eIDAS)

European Student Card Sample

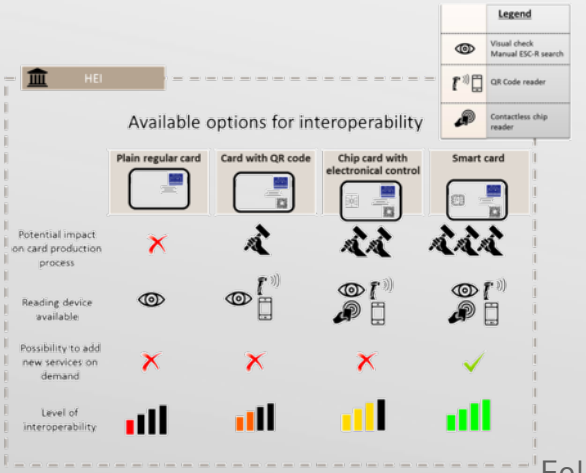
Visual Data on Card

- European Student Card Identifier:
  1. Country Code (ISO 3166-1 norm)
  2. Region code (NUTS; optional)
  3. HEI PIC (Erasmus code)
  4. Student unique code
- Name
- Photo

European Student Card holographic logo

Certification QR code on the front or the back

https://api.esc.eu/card/573ad632-0009-11e7-bc64-92361f002671
URI – based on RFC-4122 (https://tools.ietf.org/html/rfc4122)
unique universal identifier (UUID) 16-byte



The ISIC+ITIC Cards (International Student / Teacher Identity Card)

Both

- physical medium (card)
- virtual medium (native Smartphone App)

available

Provided Data:

- Higher Education Institution (Name)
- Name
- Photo
- Date of birth
- Signature (backside)
- Validity

Accepted by **service providers**

→ Question which of those data are necessary?
→ No ESC equivalent for a StaffID

person data

ESC as a ID Medium → personal data → legal aspects

As an ID document the European Student Card will work on personal data.

Which are the legal aspects?

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 27 April 2016
on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
(**G**eneral **D**ata **P**rotection **R**egulation)

Each processing of personal data needs a legal purpose
→ Chapter II - Principles

- Article 5 – Principles relating to processing of personal data
- Article 6 – Lawfulness of Processing
- Article 7 – Condition for consent

Technical and organizational aspects of processing of personal data
→ Chapter IV – Controller and Processor

- Article 24 – Responsibility of the controller
- Article 25 – Data protection by design and by default
- Article 26 – Joint controllers
- Article 28 – Processor
- Article 32 – Security of processing

ESC as a ID Medium → personal data → legal aspects

Core principles

- **Membership with the European card system is freely chosen** by any institution of higher education.
- Membership may be done and withdrawn any time by the institution.
- Each student registered in an HEI participating in the ESC program is **free to opt in or out**.
- Each institution maintains the full control over the process of creating, producing and issuing its student card.

General and Technical specifications for implementing the ESC
(http://europeanstudentcard.eu/wp-content/uploads/2017/02/2017_03_21_European-student-card-Specifications-v1.pdf)

#MRAP.2 (ESC Handbook)

In the context of the implementation of the ESC project, **each HEI is responsible for ensuring full conformity to all aspects of GDPR** (General Data Protection Regulation)

ESC Handbook for intitution: Users's Guide to connect to the Platform
(http://europeanstudentcard.eu/wp-content/uploads/2017/02/ESC-User-Guide-def.pdf)

→ *ESC Handbook recommends applying Article 6 par. 1 lit. (a) given consent for ESC*

Erasmus Charter for Higher Education EACEA/03/2020 2021-2027 Selection year

„Implement the priorities of the Programme:

- By undertaking the necessary steps to implement digital mobility management in line with the technical standards of the **European Student Card Initiative**.
- …"

Erasmus Charter for Higher Education EACEA/03/2020 2021-2027 Selection year 2021 – guidelines for applicants
(https://ec.europa.eu/info/funding-tenders/opportunities/docs/cap/eplus2020/eche-fp-2020/1877638-charter-annotated-guidelines-feb2020_en.pdf)

StaffID – Ludwig-Maximilians-Universität München

Issuing of a StaffID is regulated by law

„Allgemeine Geschäftsordnung für die Behörden des Freistaates Bayern“ (AGO)

§ 35 - Dienstausweise

(1) Beschäftigte, die regelmäßig Außendienst wahrnehmen, sollen einen Dienstausweis erhalten und sich damit erforderlichenfalls im Außendienst unaufgefordert ausweisen.
Sonstige Beschäftigte können einen Dienstausweis erhalten.

(2) Dienstausweise sollen den **Vor- und Zunamen**, die **Beschäftigungsbehörde mit Anschrift**, ein **Lichtbild** und die **Unterschrift** des Beschäftigten enthalten.

(3) Beim Ausscheiden aus der Beschäftigungsbehörde ist der Dienstausweis unaufgefordert der ausstellenden Behörde zurückzugeben. Der Verlust des Dienstausweises ist der ausstellenden Behörde unverzüglich anzuzeigen; er wird nicht veröffentlicht.

(4) Über die ausgegebenen Dienstausweise ist ein Verzeichnis zu führen.

(5) Dienstausweise mit einem **elektronischen Speicher** können für **weitere Funktionen** verwendet werden (z.B. Zugangssysteme, digitale Signatur). Die Beschäftigten sind über die weiteren Funktionen, insbesondere über den Umfang der Datenspeicherung in geeigneter Form **zu informieren**.

Article 6 – Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Source: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e1888-1-1

→ Art. 6 par. 1 lit. a is the strongest?

If someone consent to the processing of their data, everything is allowed?

→ Art. 6 par 1 lit. b-e are the conditions public institutions work based on

GDPR Art. 6 par. 1 lit. (a) has a few Problems:

- It might be the strongest if consent is given
- But consent is limited by Article 7 – Conditions for consent
- Also Recital 42 sentence 5 GDPR – Burden of Proof and Requirements for Consent

"Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."

Article 7 - Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. The data subject shall **have the right to withdraw his or her consent at any time**. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4. When assessing whether **consent is freely given**, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Source: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e1888-1-1

Consent requires a free given choice – the Erasmus Charter eliminates that option

Result on Article 6

If the proposed Article 6 par. 1 lit. (a) will not work for any European Student Card what ware the options:

1. Create a Union Law for Academic ID cards / eIDs
   - Advantage: the same for all member states
   - Mandatory data could be defined, similar to StaffIDs (e.g. AGO §35 Dienstausweis)
   - Data processing based on GDPR Article 6 par. 1 lit. (e)
2. Based on the national law and contracts (Erasmus)
   → GDPR Article 6 par. 1 lit. (e), (c), (b), (d) in combination with the law
   - LMUcard example (https://gitlab.lrz.de/LMU-Dez-VI-public/lmucard.terms-of-use/-/blob/master/StudentID-de.md)

     Article 6 par. 1 lit. (e) GDPR in combination with Art. 42 par. 4 sent. 1 BayHSchG for all personal data, as those data are required to fulfill the public duties of the university – identification and verification of student identity

→ If possible do not rely on consent

central processing of person data
→ ESC-Router

Verification process:

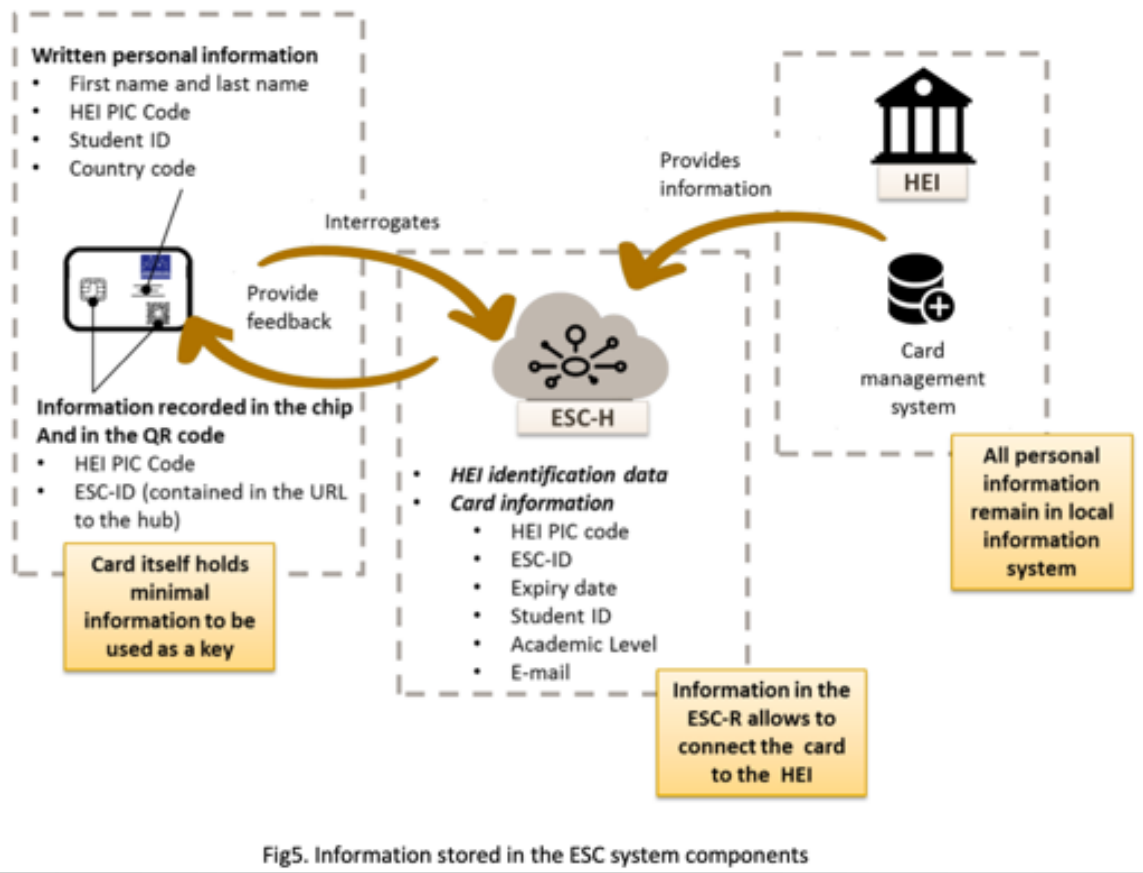
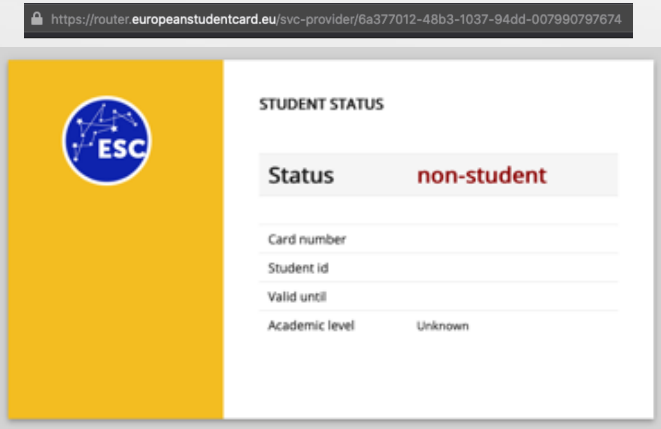


Fig5. Information stored in the ESC system components



General and Technical specifications for implementing the ESC (http://europeanstudentcard.eu/wp-content/uploads/2017/02/2017_03_21_European-student-card-Specifications-v1.pdf)

GDPR Chapter IV Section 1
Controller and Processor – general obligations

Article 24 – Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall **implement appropriate technical and organisational measures** to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the **implementation of appropriate data protection policies** by the controller.
3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 25 – Responsibility of the controller

1. Taking into account the **state of the art**, the cost of implementation and the nature, scope, context and **purposes of processing** as well as the **risks** of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, **implement appropriate technical and organisational measures**, such as pseudonymisation, which are designed to implement data-protection principles, such as **data minimisation**, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, **by default, only personal data which are necessary for each specific purpose of the processing are processed**. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that **by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons**.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Source: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e1888-1-1

Router → Design Pattern – Proxy / Facade

Technological considerations

- As the ESC Specification names a Router, but described a centralized database
- ESC-ID is a scoped identifier → routing information

Consequences of the GDPR requirements:

- implement appropriate technical and organisational measures
- State of the art implementation

→ Micro-Service Architecture and Software Design Patterns
ESC Router is both "Proxy and Facade pattern"

- It is not necessary to have a centralized database, via routing person data could be received by the identity management systems of Students home HEI
- A real data exchange format and specification necessary
  → **OpenAPI** 3 (https://swagger.io/specification/)
  → ESC-Router just a small App without data or as an access provider
- Limit data access (no data enumeration) / authentication & authorization for more data

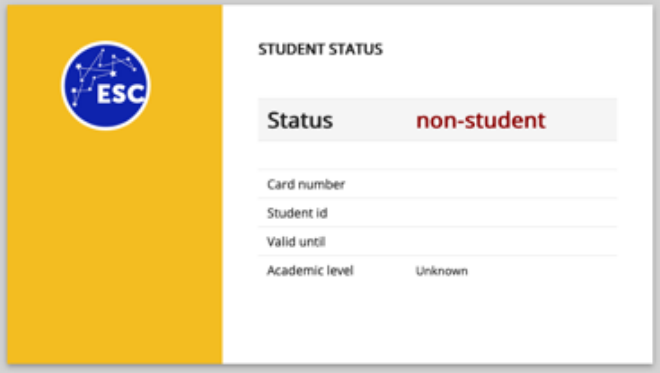
European Student Card verification process - trust

Framework of trust:

- Verification of Student Status online
- Verification by ESC-ID
  - Textual
  - QR-Code
  - Common Data zone on Chip

→ **never include Website / URL**

https://router.europeanstudentcard.eu/svc-provider/6a377012-48b3-1037-94dd-007990797674



Have a dedicated and communicated Website / App to check the status

→ IT-Security considerations
→ similar to phishing sites ← trust worthiness

technical considerations IDM

Reiventing the Wheel?

Do we need to reinvent the wheel?
Aren't there already Systems we could build upon?

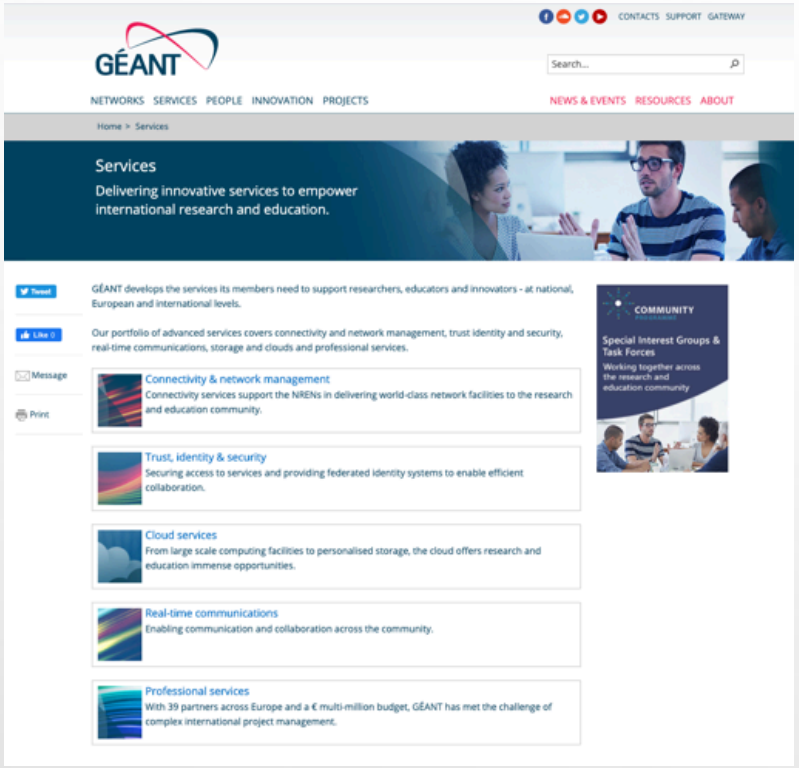
→ *„If I have seen further it is by standing on the shoulders of giants"*

Sir Isaac Newton, 1675 / Bernard of Chartres 12th century

Existing and established standards for IDM in HEI

Federated identity systems

GÉANT



- eduroam

  Seamless Wi-Fi access for resarch and education around the world
- eduGAIN

  Unlocking global research and education collaboration: interconnects research and education identity federation
- InAcademia – ONLINE STUDENT VALIDATION

  Online student validation for retail and online services
- eduPKI – A SERVICE PROVIDED BY GÉANT

  digital certificates
- urn:geant Uniform Resource Name (URN)

  GÉANT administers a Uniform Resource Name (URN) namespace, supporting the assignment of unique, global, persistent names to various kinds of resources by the GÉANT community and its delegates.

Base: LDAP Schema: eduPerson

The European Student Card Initiative seams to have started from scratch,
→ no relations to existing and established standards

LDAP schema for EduPerson (https://wiki.refeds.org/display/STAN/eduPerson+2020-01):

- eduPersonPrinicalName: example@foo.edu
- eduPersonUniqueId: 28c5353b8bb34984a8bd4169ba94c606@foo.edu

→ **Scoped Identifier** → *Routing Information*

Example for myself: 72C918A84D785B9F@lmu.de

- User-identifier: 72C918A84D785B9F (internal UUID)
- @ → Scope indicator
- LMU → HEI Identifier → Ludwig-Maximilians-Universität München
- DE → Country Code

→ Routing is implicit included – no central database necessary
→ delegation of identity proof to home institution

other legal and technical points not mentioned

Other legal and technical points not mentioned

- eIDAS, electronic wallets / payment
  - EU competition Law
  - who and how will “qualified digital certificates” be issued
  - banking license necessary
  - Identity verification process upfront
- Open Source design and implementation of ESC-Router
  - License
  - Hosting and infrastructure costs
- Costs and subsidies
- Legal Requirements for Services
  - Library – verified address
  - Public transport - ticketing
- …