Identity and Privacy

helping us demolish the paper jail

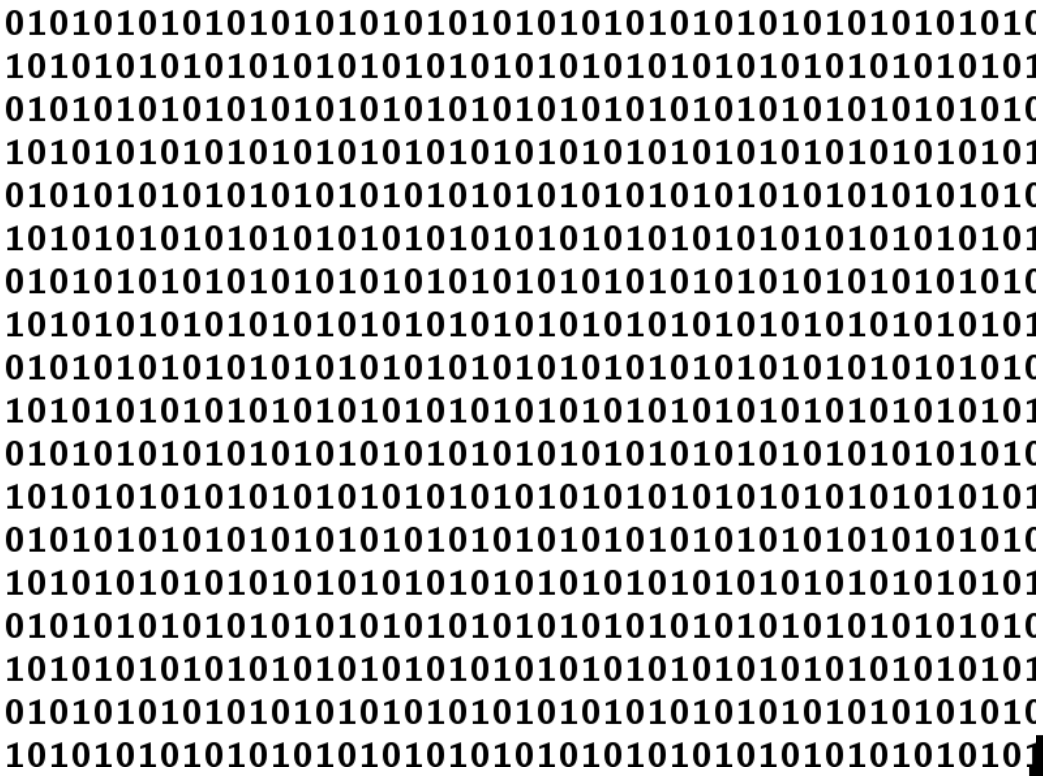
Victoriano Giralt

Central ICT Services
University of Málaga
co-chair of TERENA TF-EMC^2
member of RS^{3}G steering committee

Global Founding Seminar on
Digital Student Data Depositories
Worldwide
Groningen
April 16th, 2012

Information

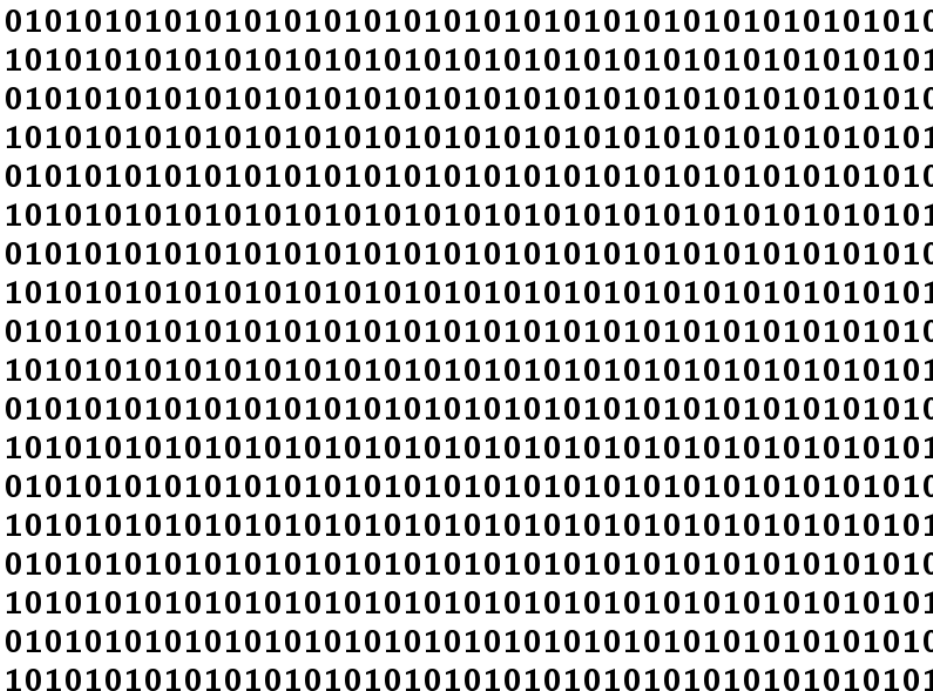
in electronic form, our main character



SSEDIC Programme Partner

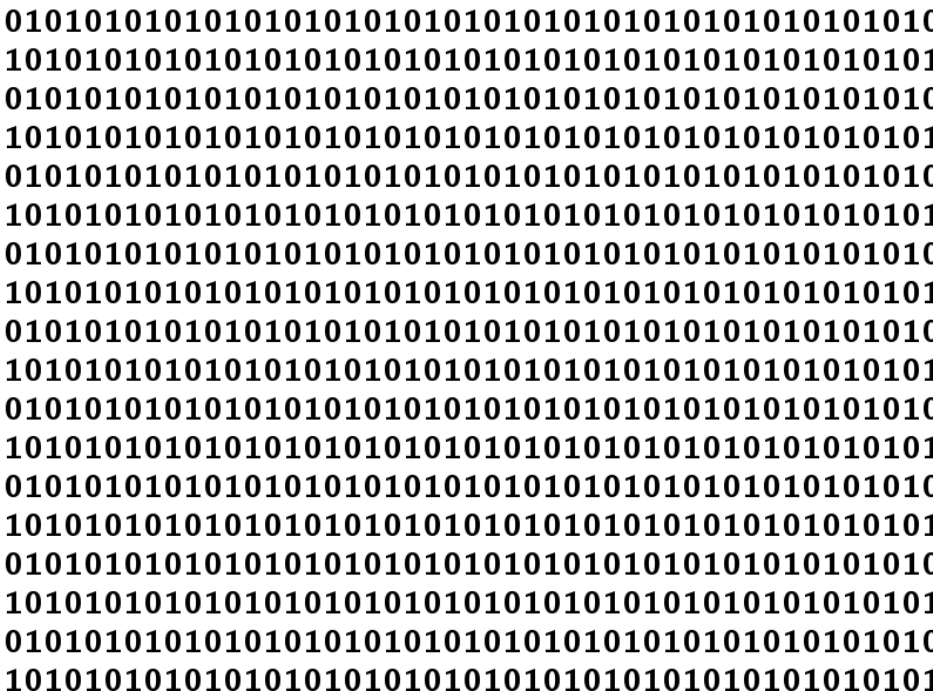
Information

in electronic form, our main character



Information

in electronic form, our main character

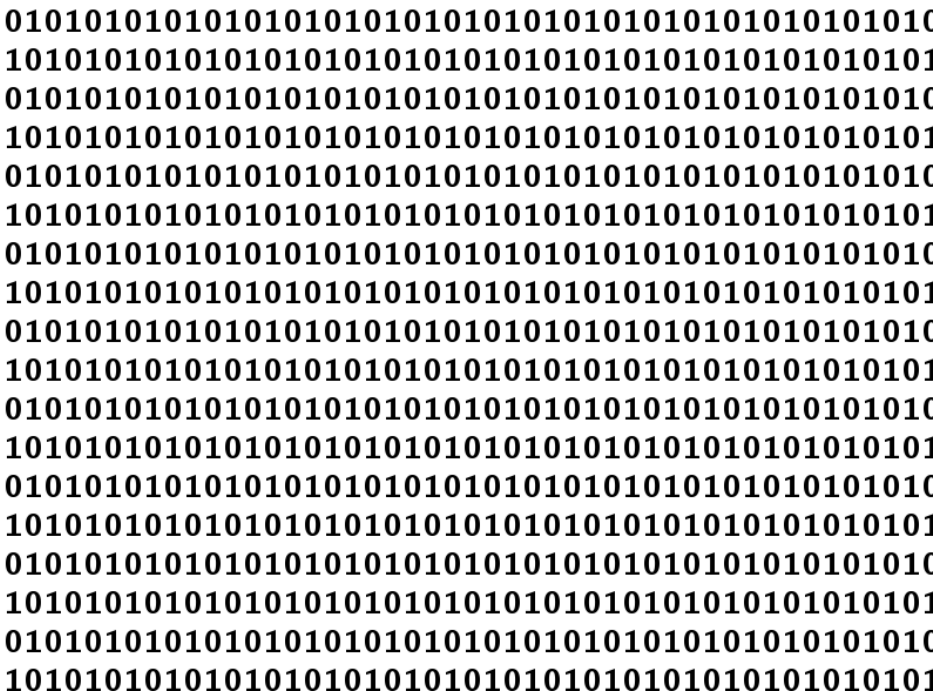


+ Easy to transport

SSEDIC Programme Partner

Information

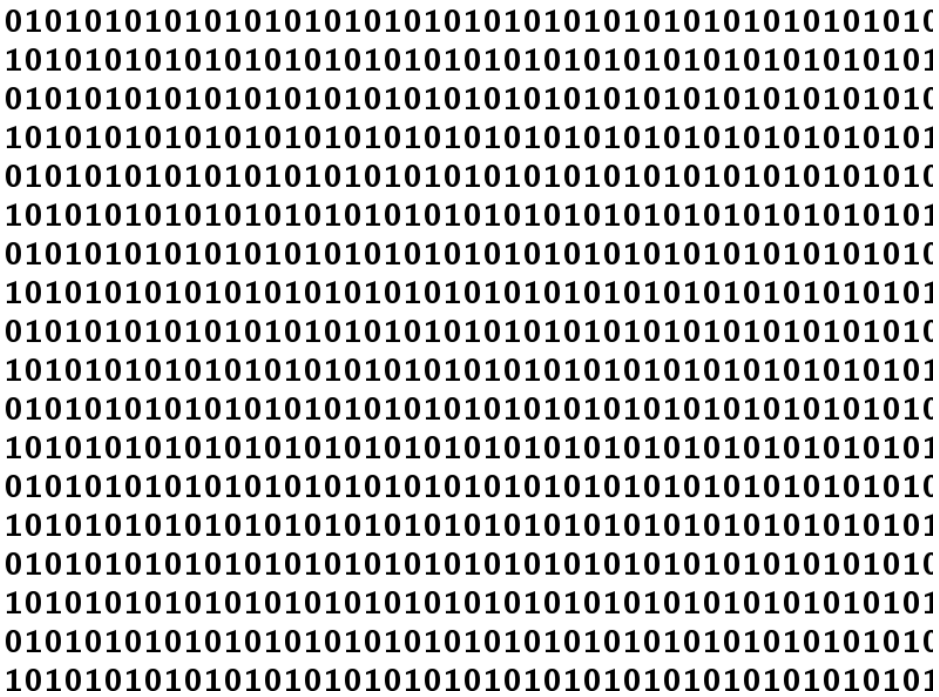
in electronic form, our main character



+ Easy to transport
+ Easy to store

Information

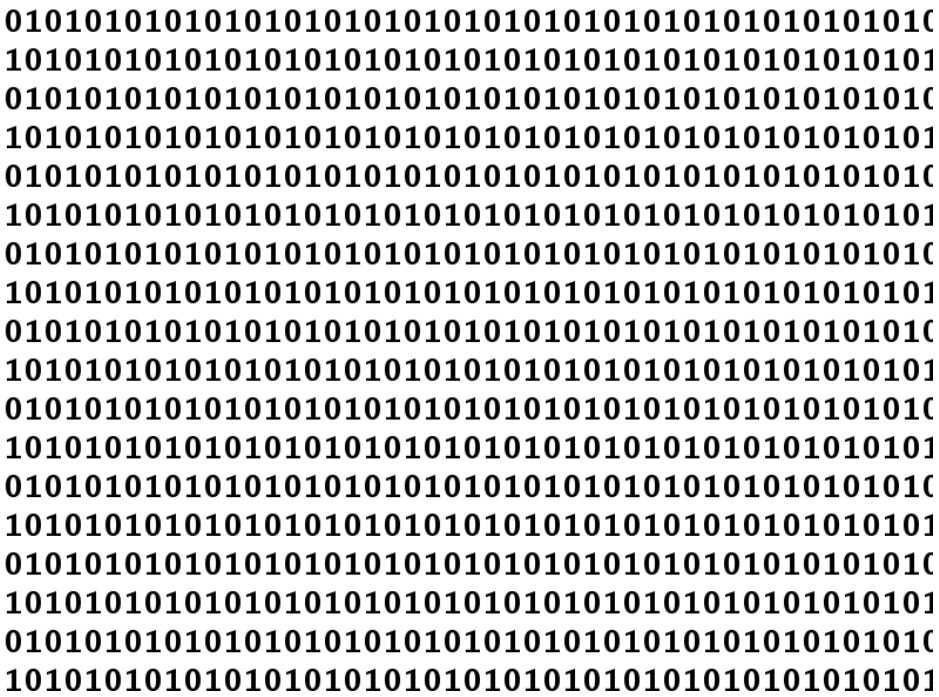
in electronic form, our main character



+ Easy to transport
+ Easy to store
+ Easy to process

Information

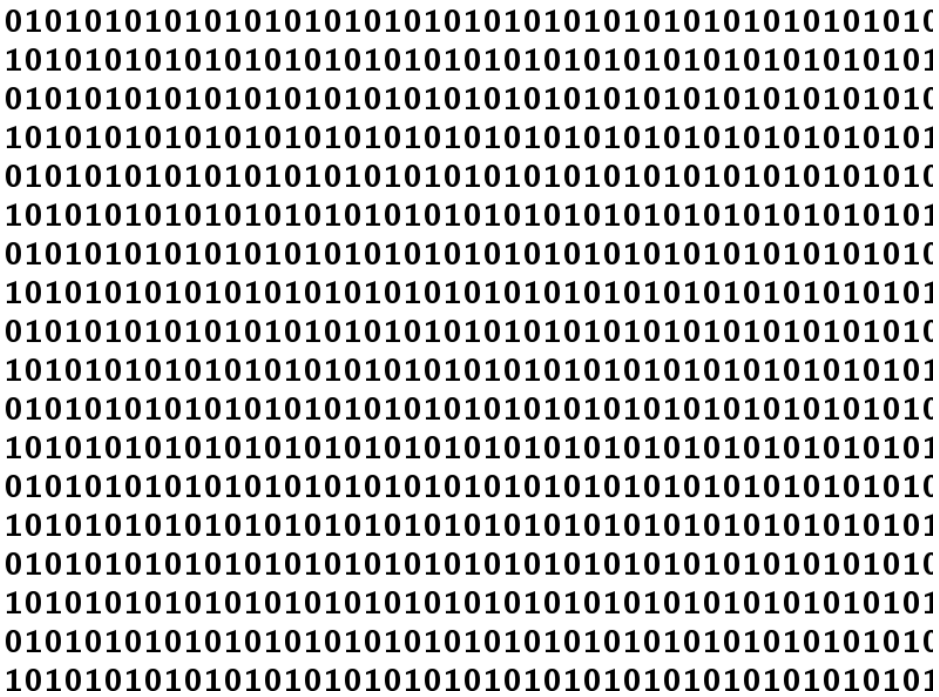
in electronic form, our main character



+ Easy to transport
+ Easy to store
+ Easy to process
+ Easy to retrieve

Information

in electronic form, our main character

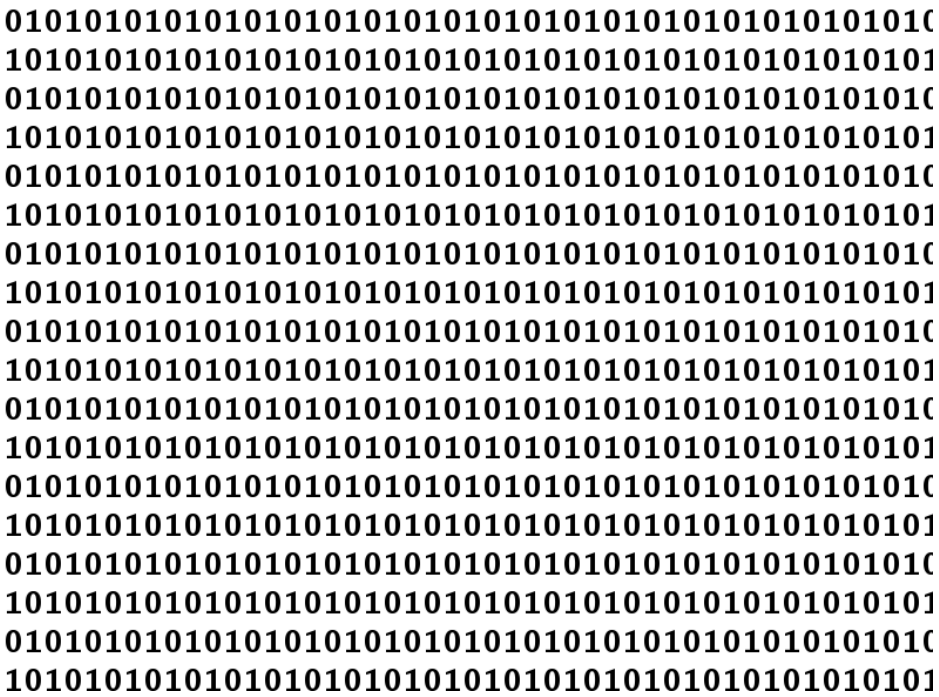


+ Easy to transport
+ Easy to store
+ Easy to process
+ Easy to retrieve
+ Easy to create

SSEDIC Programme Partner

Information

in electronic form, our main character



+ Easy to transport
+ Easy to store
+ Easy to process
+ Easy to retrieve
+ Easy to create
+ Easy for the environment

SSEDIC Programme Partner

The big tree killer

bad for the environment

CC-BY-SA 2.0 M J Richardson <http://www.geograph.org.uk/photo/510110>

SSEDIC Programme Partner

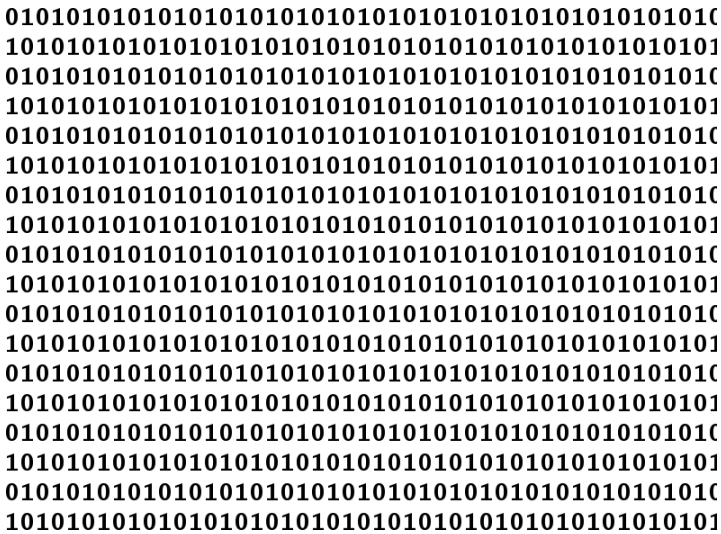
The big tree killer

bad for the environment

The big tree killer

bad for information freedom

+



SSEDIC Programme Partner

Information caught in the paper jail

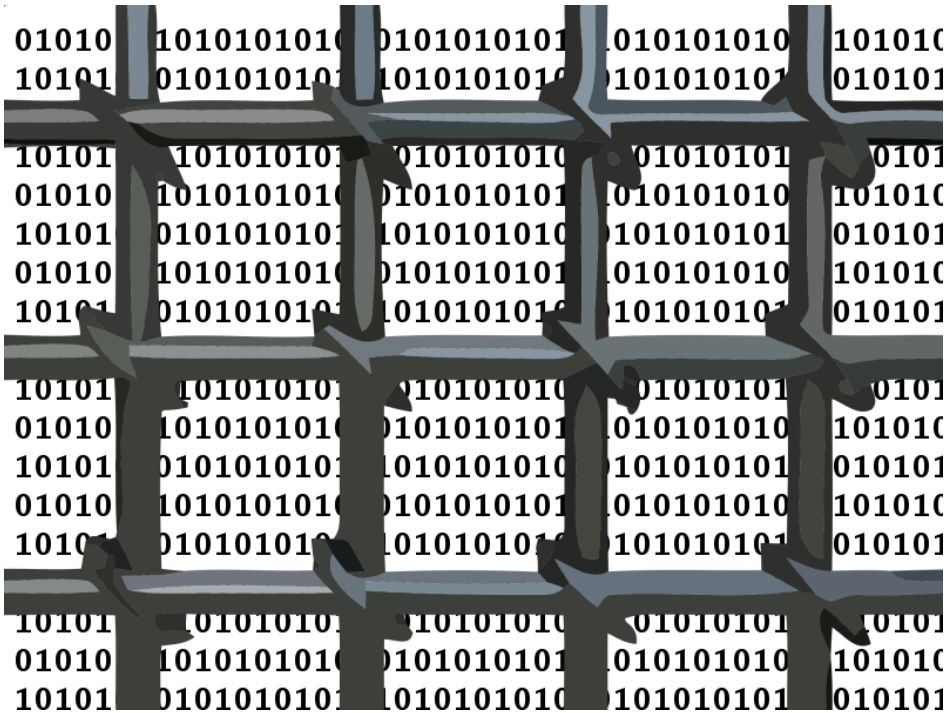
as soon as it gets printed

Scoping the Single European Digital Identity Community

SSEDIC Programme Partner

Printed Information

freedom lost in the paper jail



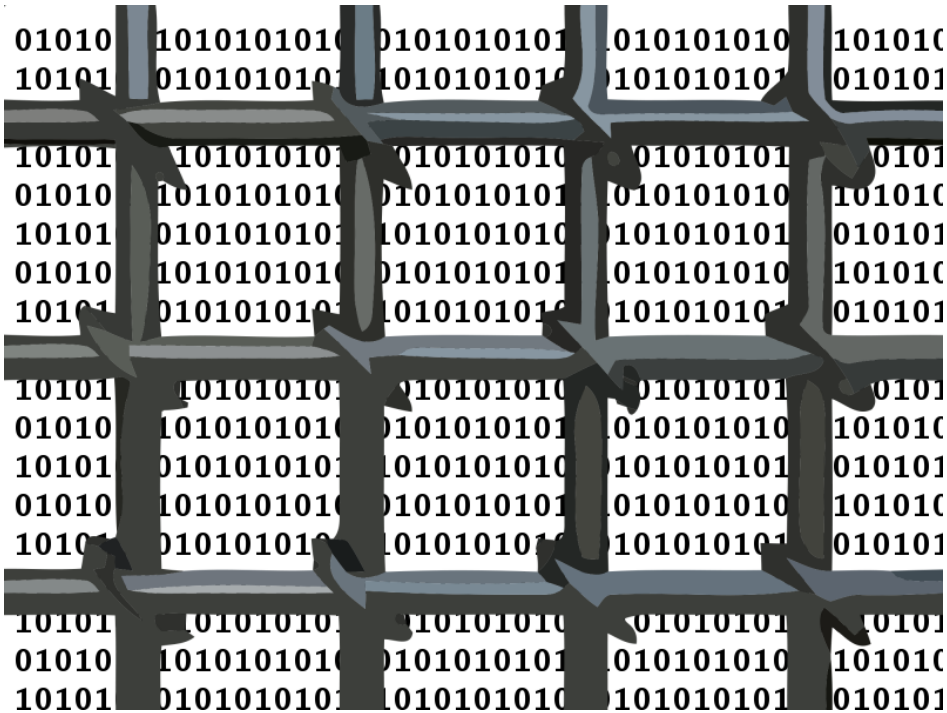
Scoping the Single European Digital Identity Community

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Printed Information

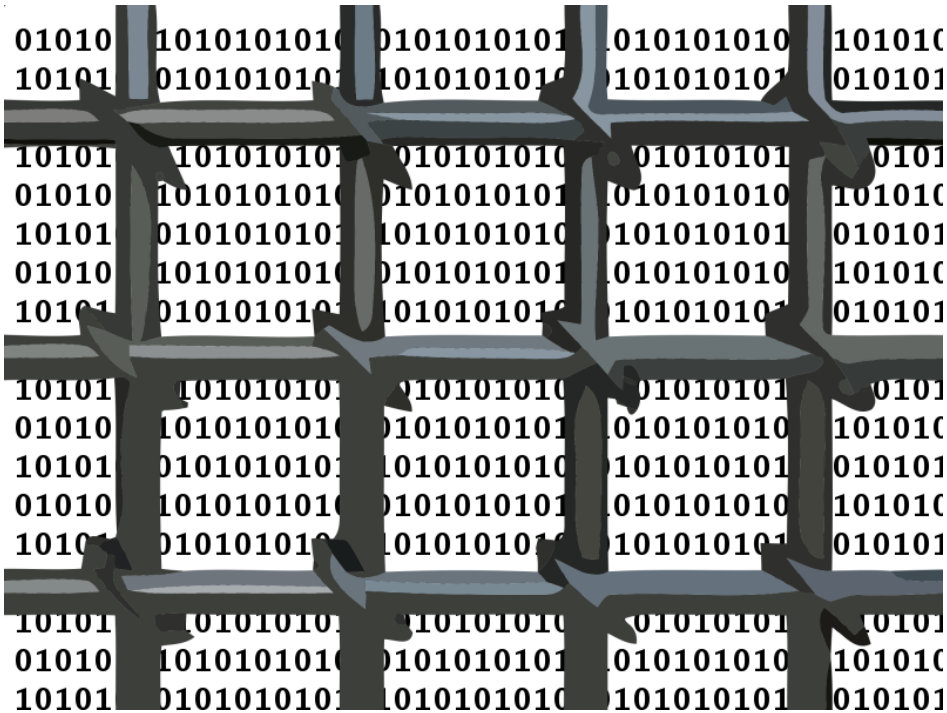
freedom lost in the paper jail



- Difficult to transport

Printed Information

freedom lost in the paper jail

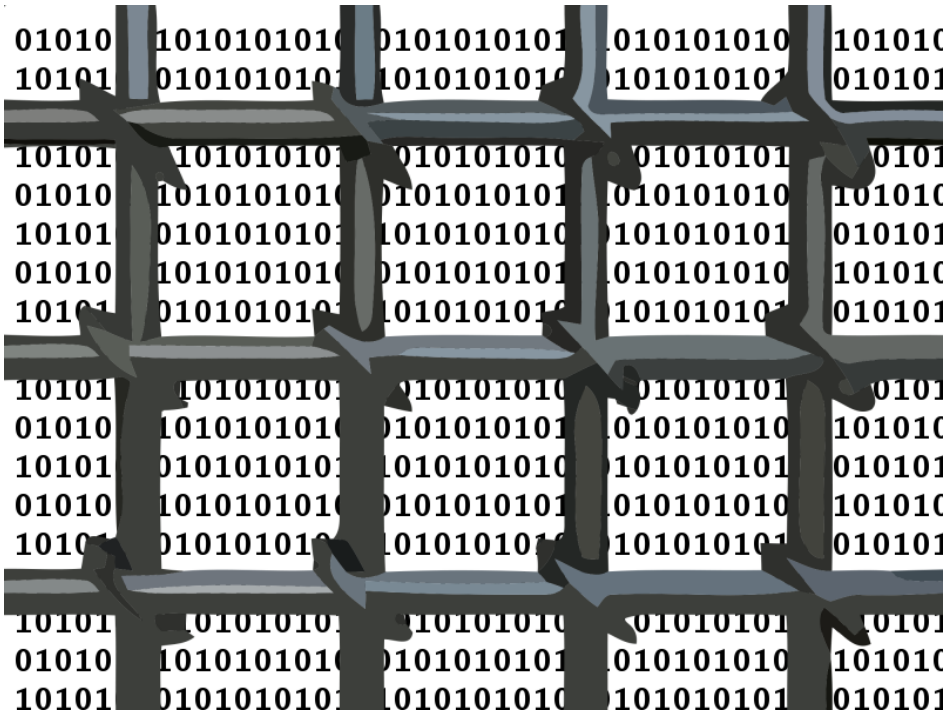


- Difficult to transport
- Difficult to preserve

SSEDIC Programme Partner

Printed Information

freedom lost in the paper jail

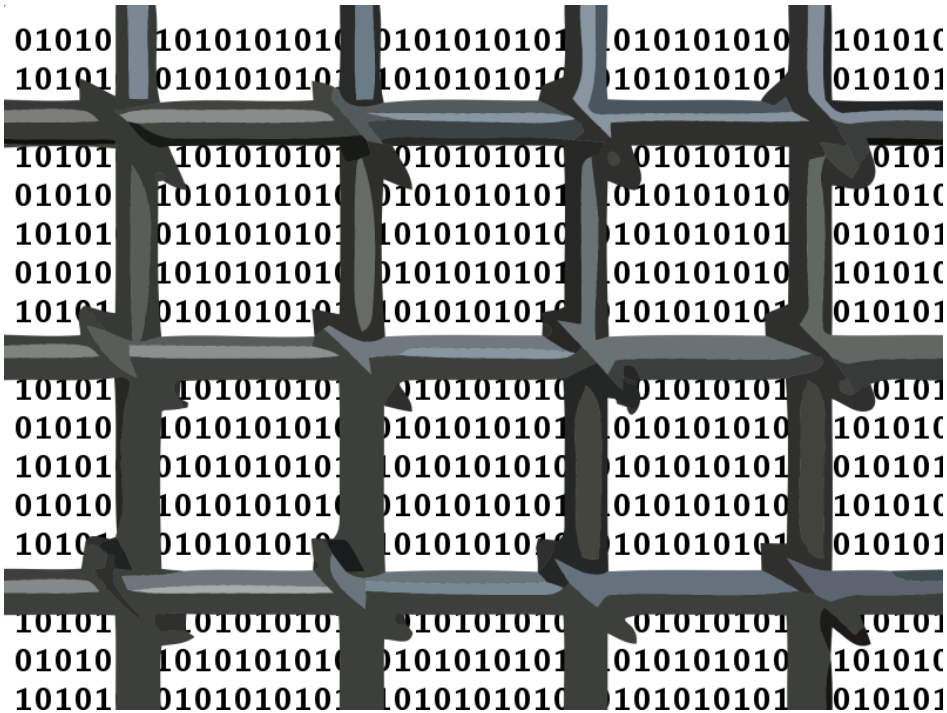


- Difficult to transport
- Difficult to preserve
- Difficult to retrieve

SSEDIC Programme Partner

Printed Information

freedom lost in the paper jail

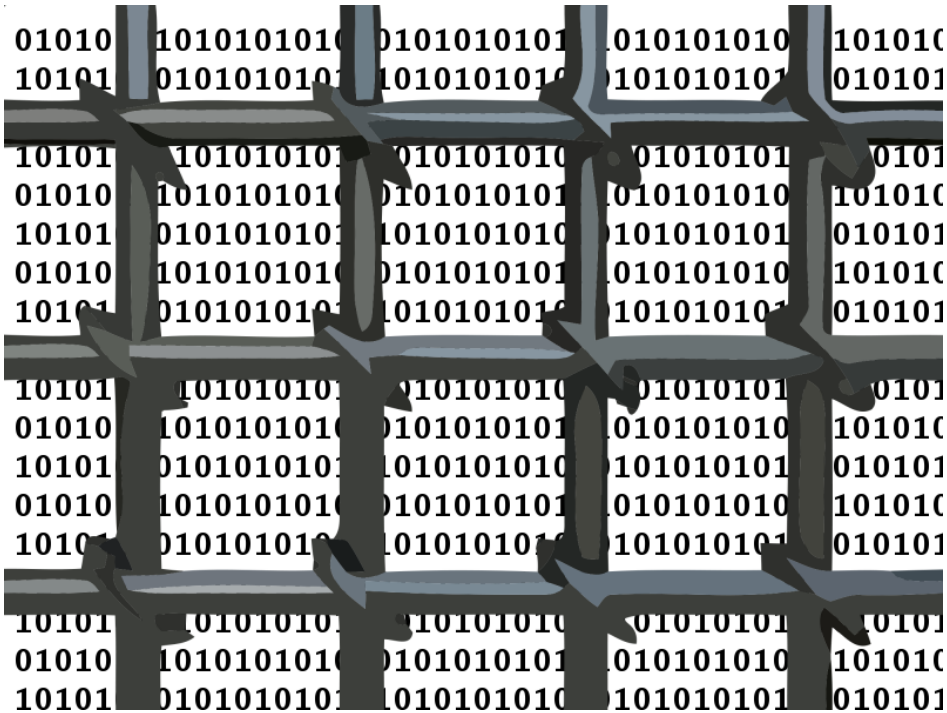


- Difficult to transport
- Difficult to preserve
- Difficult to retrieve
- Too easy to create

SSEDIC Programme Partner

Printed Information

freedom lost in the paper jail



- Difficult to transport
- Difficult to preserve
- Difficult to retrieve
- Too easy to create
- Bad for the environment

Use case

Jail demolition in medical practice

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Use case

Jail demolition in medical practice

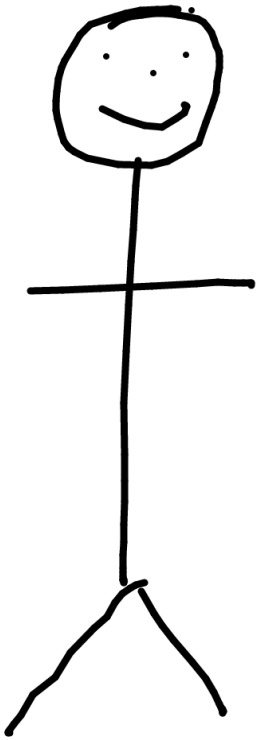
Introducing some characters

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Patient

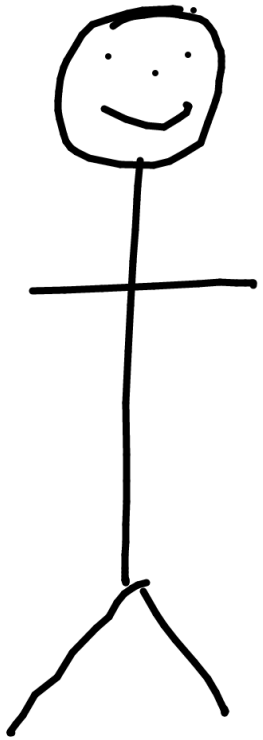
a.k.a. *you or me*



Hi! I'm the patient

Patient

a.k.a. *you or me*



i.e. *you*

SSEDIC Programme Partner

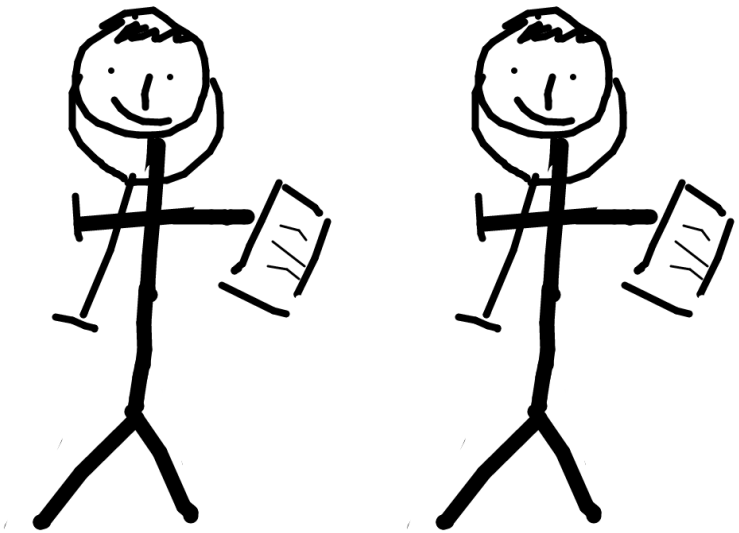
Practitioner

a.k.a. *The* Doctor

Hi! I'm your doctor

Practitioner

a.k.a. *The* Doctor



Hi! I'm also your doctor

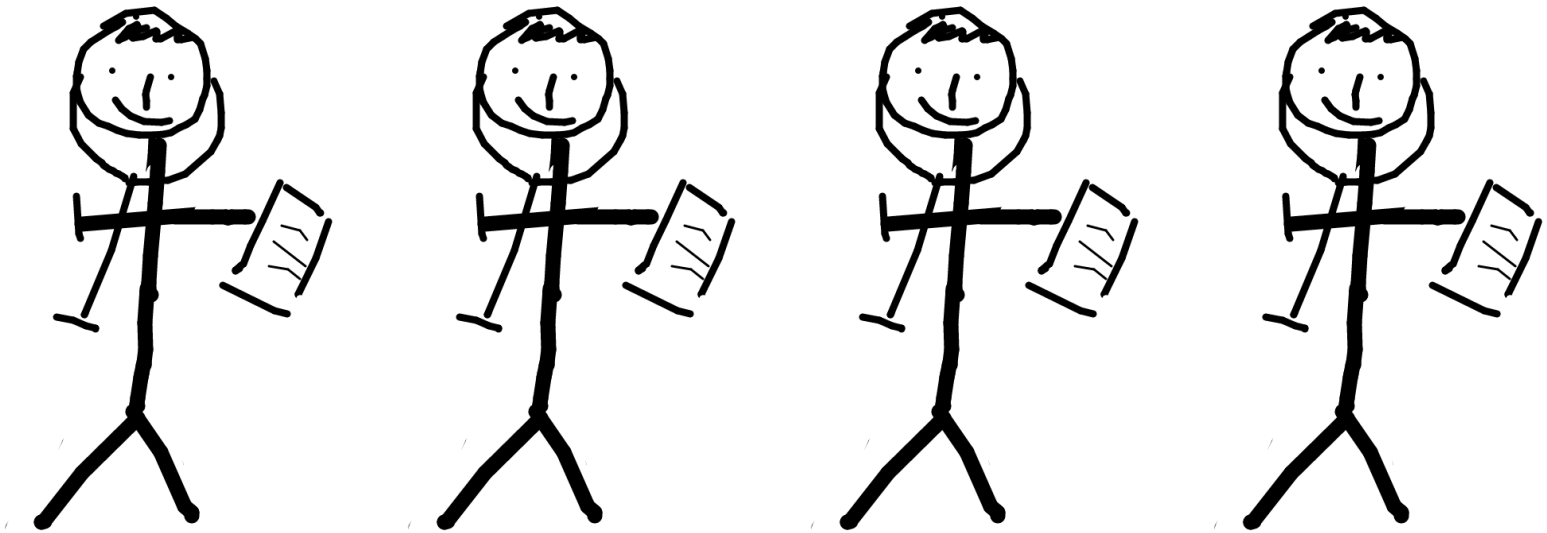
Practitioner

a.k.a. *The* Doctor

Me too!

Practitioner

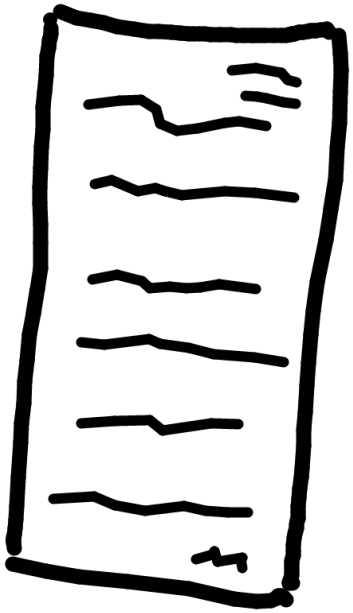
a.k.a. *The* Doctor



we all are your doctors

Health Record

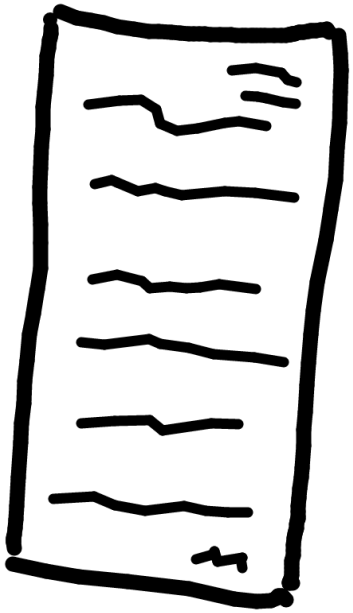
a.k.a. *lots of data about me*



Hi! I'm your Health Record

Health Record

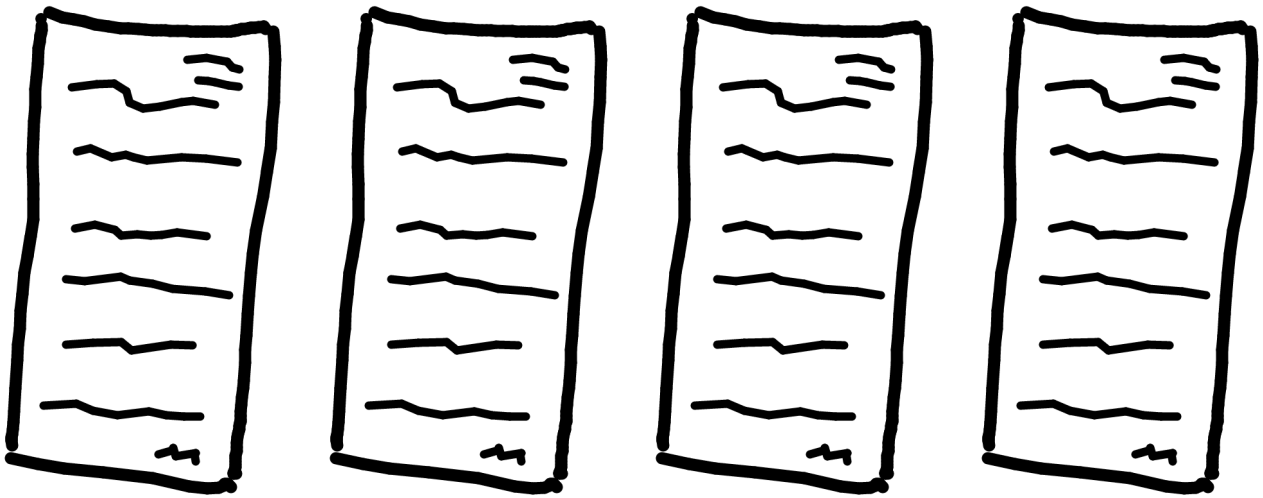
a.k.a. *lots of data about me*



Only me?

Health Record

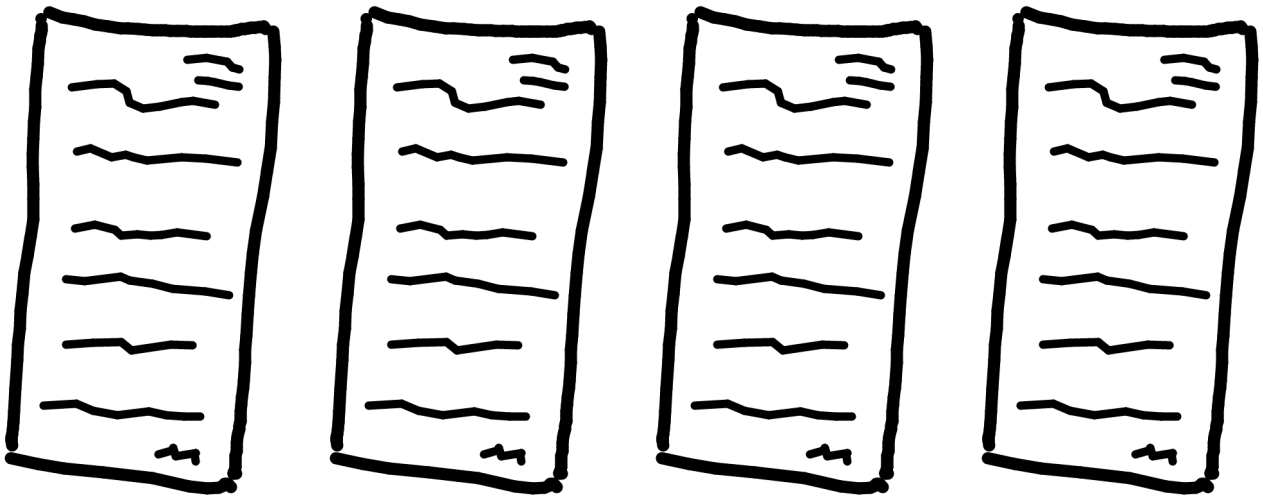
a.k.a. *lots of data about me*



Or us?

Health Record

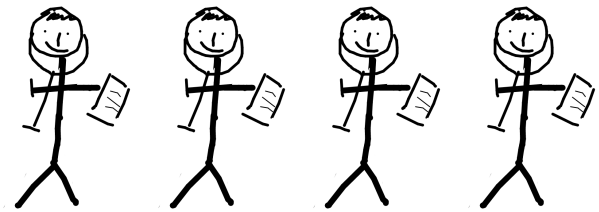
a.k.a. *lots of data about me*

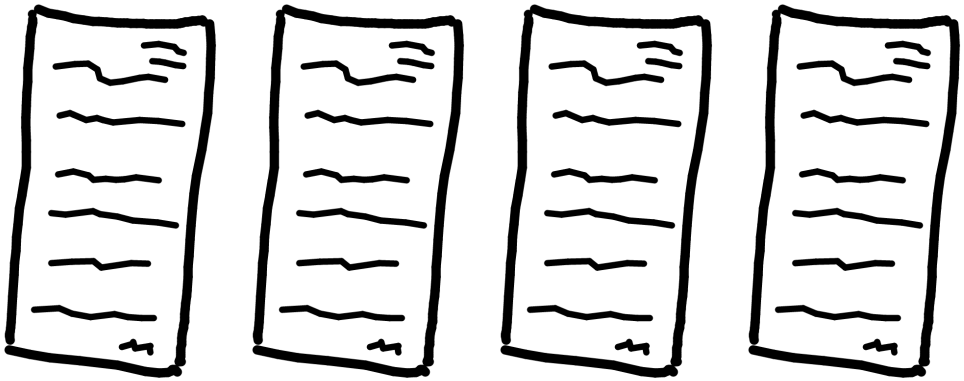


Really yours?

Health Record

a.k.a. *lots of data about me*

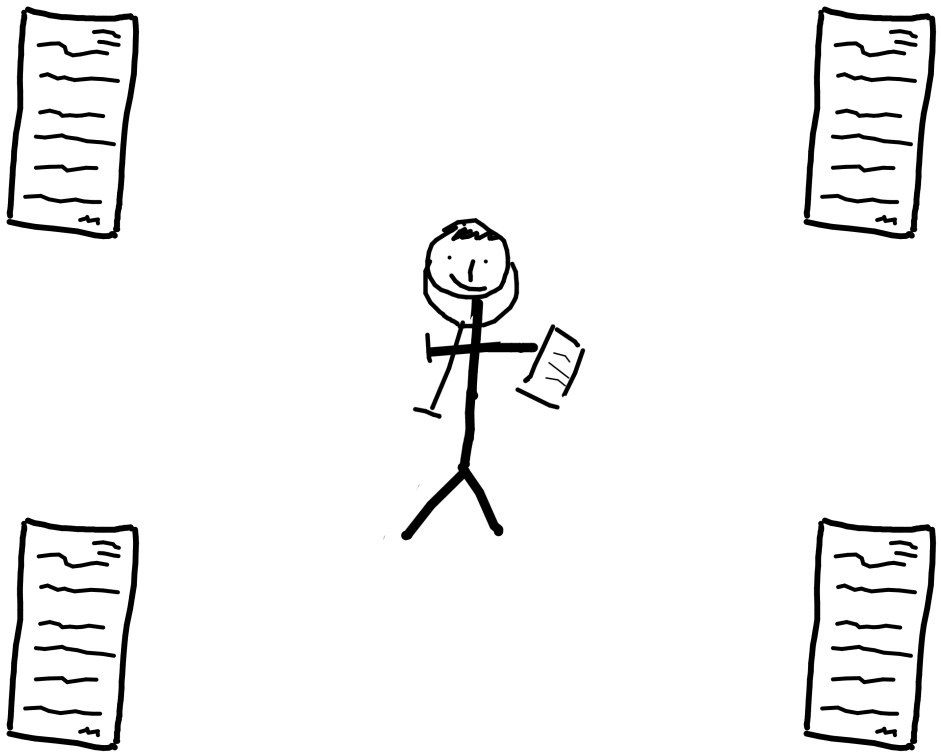




Or theirs?

Present situation

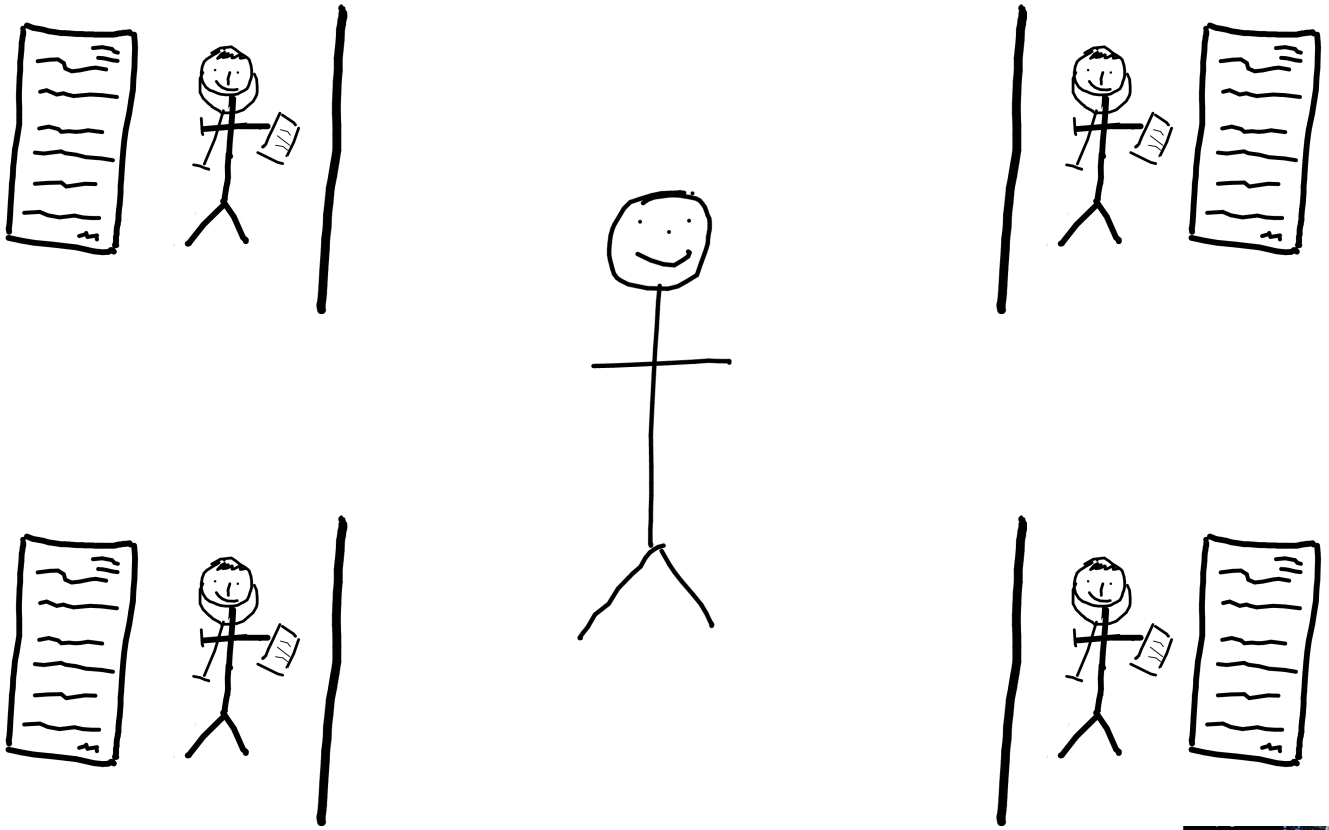
someone controls *my* data



Someone owns *my* HRs

Present situation

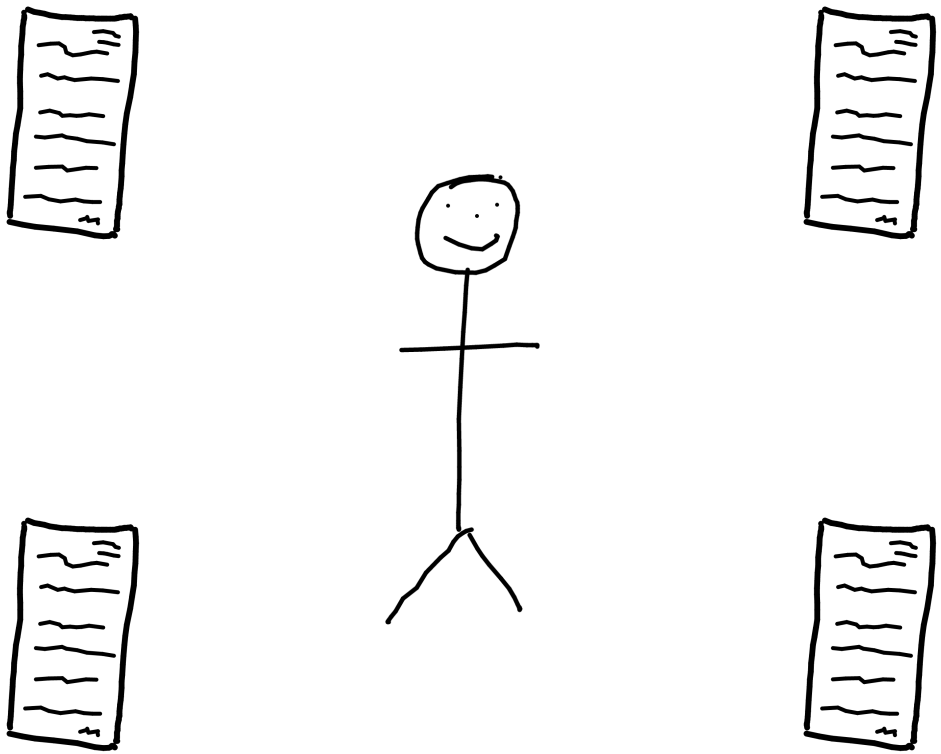
someone controls *my* data



my HRs are in silos

Proposed situation

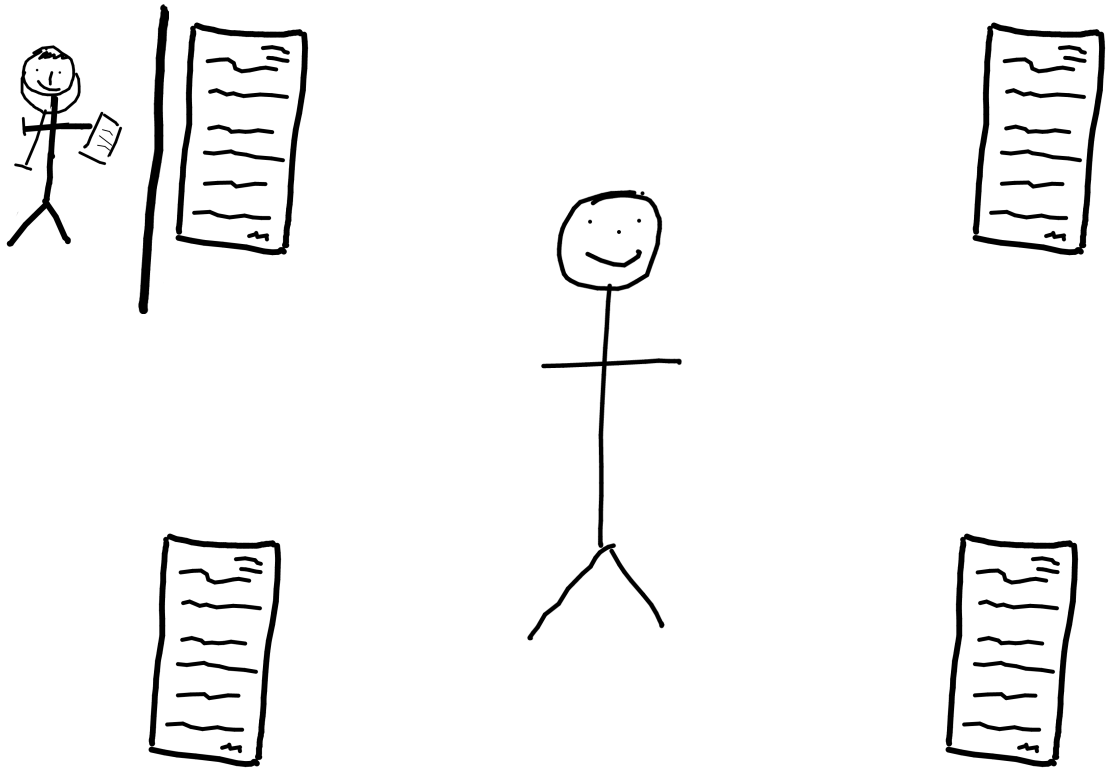
I control *my* data



I own my Heatlh Records

Proposed situation

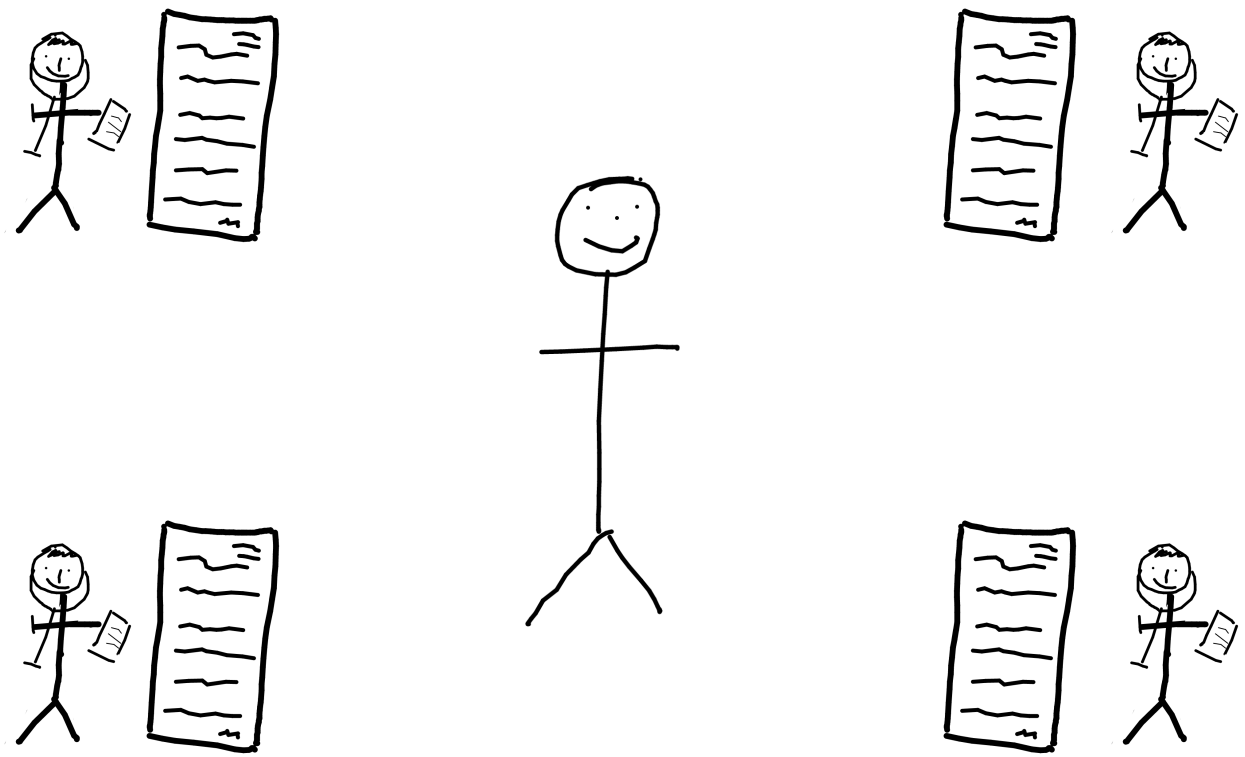
I control *my* data



I *control* access to my HRs

Proposed situation

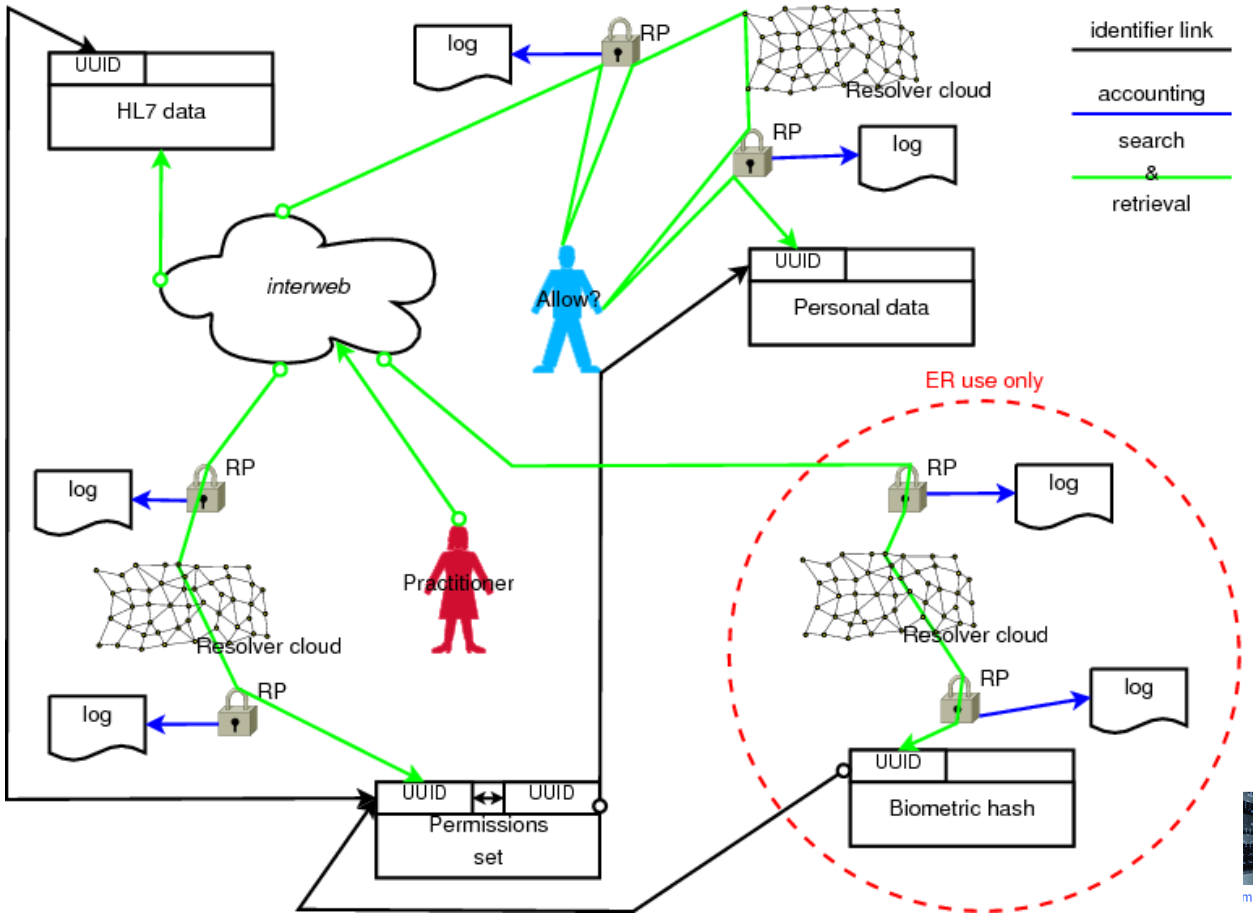
I control *my* data



I *know* **who** is using my HRs

System map

a.k.a. the big picture



User stories

explaining the big picture

1. Individual enrolment
2. Creation of health record in clinical practice
3. Access to health records in clinical practice
4. Access to health records from the emergency room
5. Access to health information for research purposes
6. Access to personal identity information

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Actors

for the user story plays

SSEDIC Programme Partner

Actors

for the user story plays

- Patient

Patient

A person that is the subject of a medical act.

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Actors

for the user story plays

- Patient
- Practitioner

Practitioner

Any health care professional of any kind that interacts with patients in medical acts.

SSEDIC Programme Partner

Actors

for the user story plays

- Patient
- Practitioner
- ERP

Emergency Room Practitioner

A practitioner assigned to an Emergency Room that will have special access in the stories.

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Actors

for the user story plays

- Patient
- Practitioner
- ERP
- Staff

Staff member

Non medical professionals that have a role in medical acts that require access to partial content of the HRs or to personal data of the patients.

SSEDIC Programme Partner

Actors

for the user story plays

- Patient
- Practitioner
- ERP
- Staff
- Relative

Patient Relative

A person with a family or other kind of social relationship to a patient that might play a role in authorising access to HR or provide personal information about the patient.

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Actors

for the user story plays

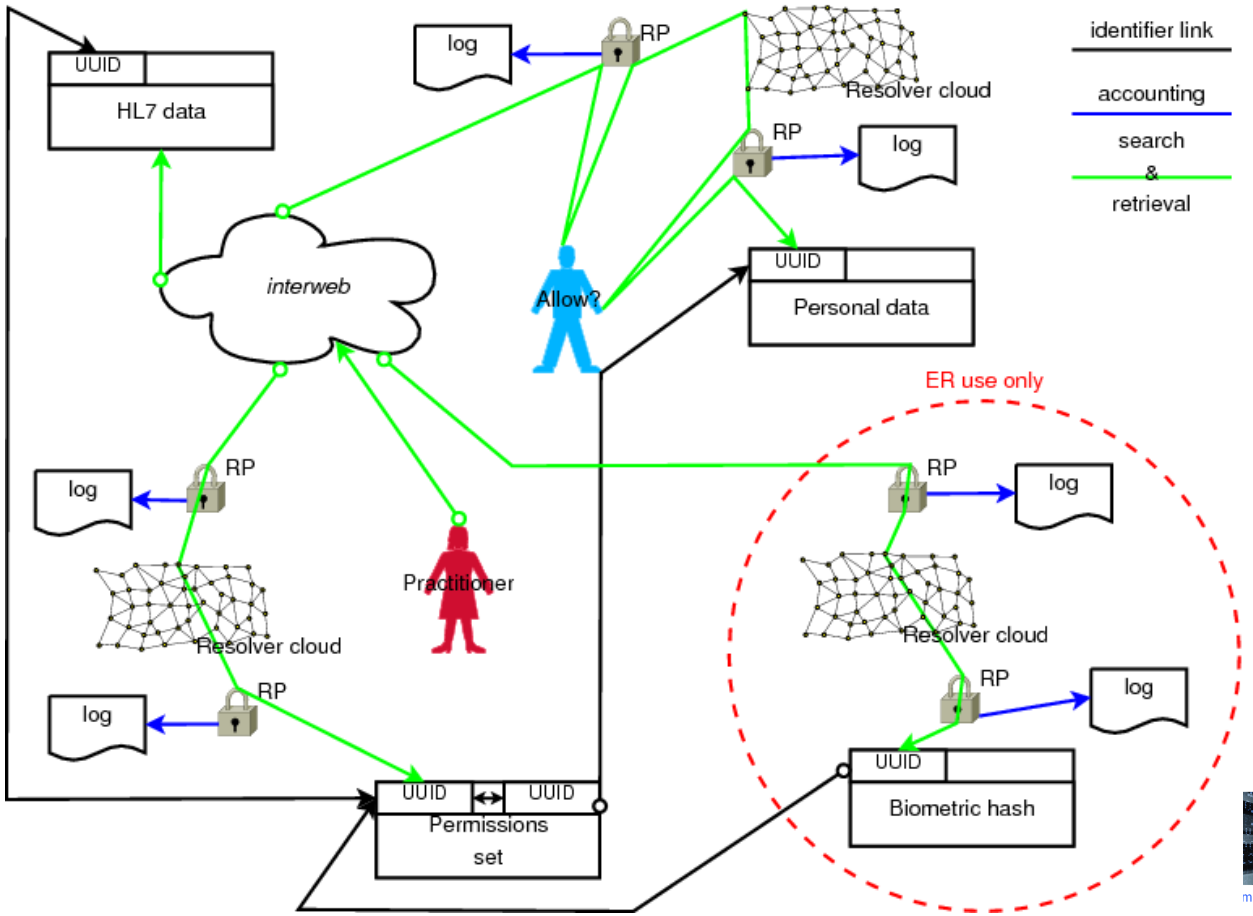
- Patient
- Practitioner
- ERP
- Staff
- Relative
- Researcher

Researcher

A person that requires anonymous, or, at most, pseudonymous access to HRs for scientific research work.

System map

a.k.a. the big picture



Individual enrolment

I'm a patient and want to publish my HR

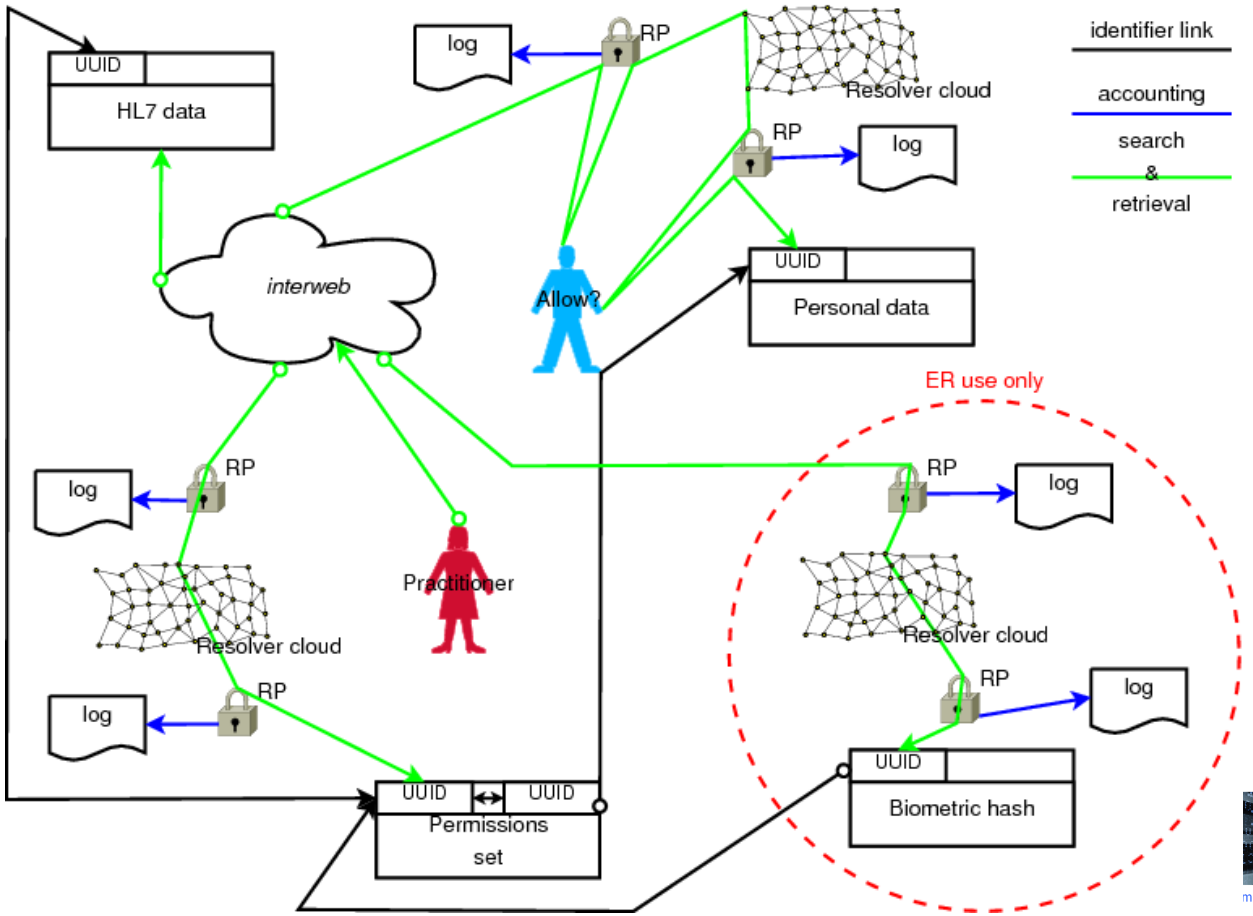
1. I select an IdP or
   the national health system provides me one.
2. I identify to the IdP using documents to
   achieve the required LoA and provide
   contact information for me and my closest relative.
3. I get the UUID that identifies my personal data.
4. My UUID is published by the IdP resolver.
5. My biometric hash is published in the resolver cloud.
6. I get my biometric hash UUID and link it to my UUID.

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

System map

a.k.a. the big picture



Creation of health record in clinical practice

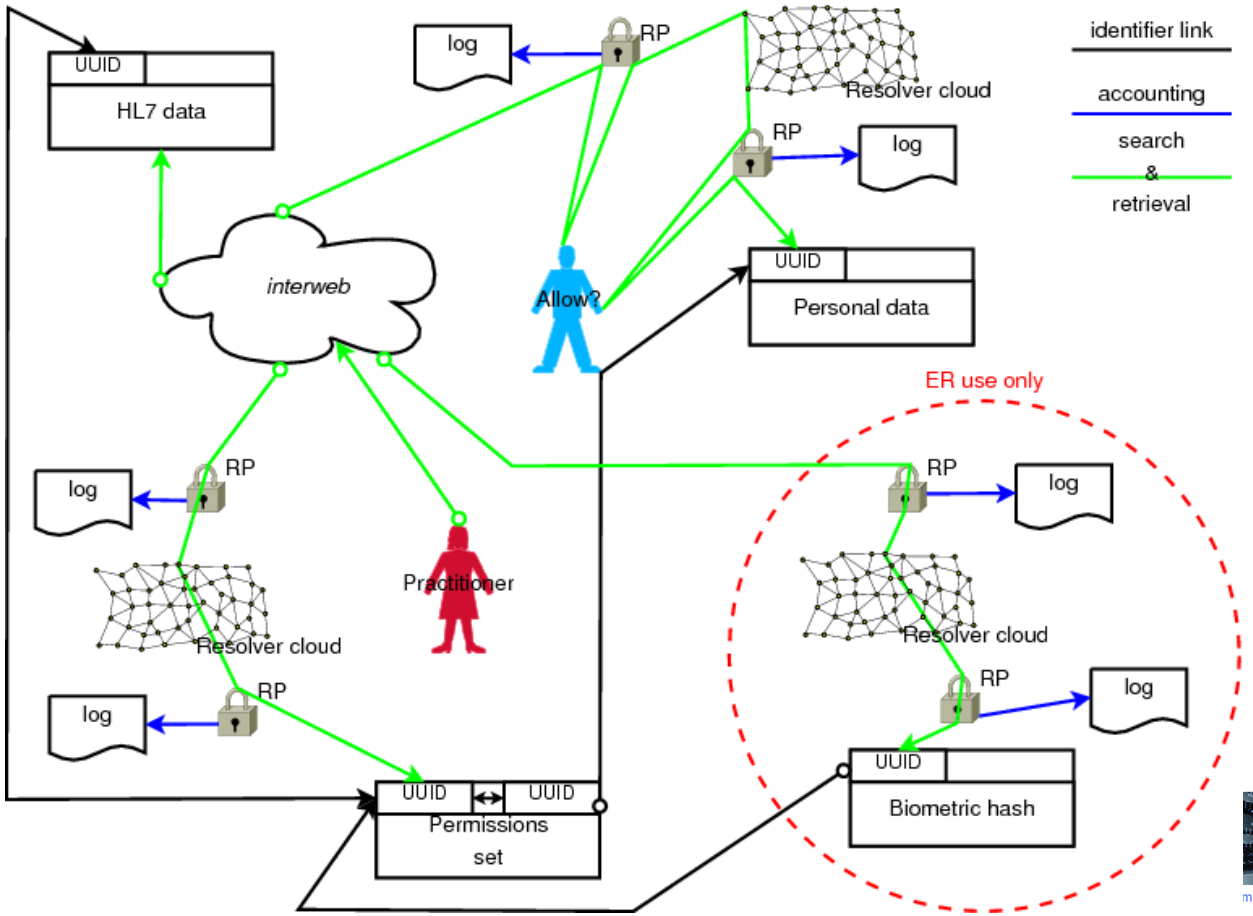
1. I as a patient go visit a practitioner.
2. All acts are compiled into HR documents.
3. The HR are dated and get UUIDs.
4. The HR UUIDs and my UUID are inserted in my IdP resolver.
5. The HR UUIDs and pointers are sent to the resolver finder cloud from the resolver.

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

System map

a.k.a. the big picture



Access to health records in clinical practice

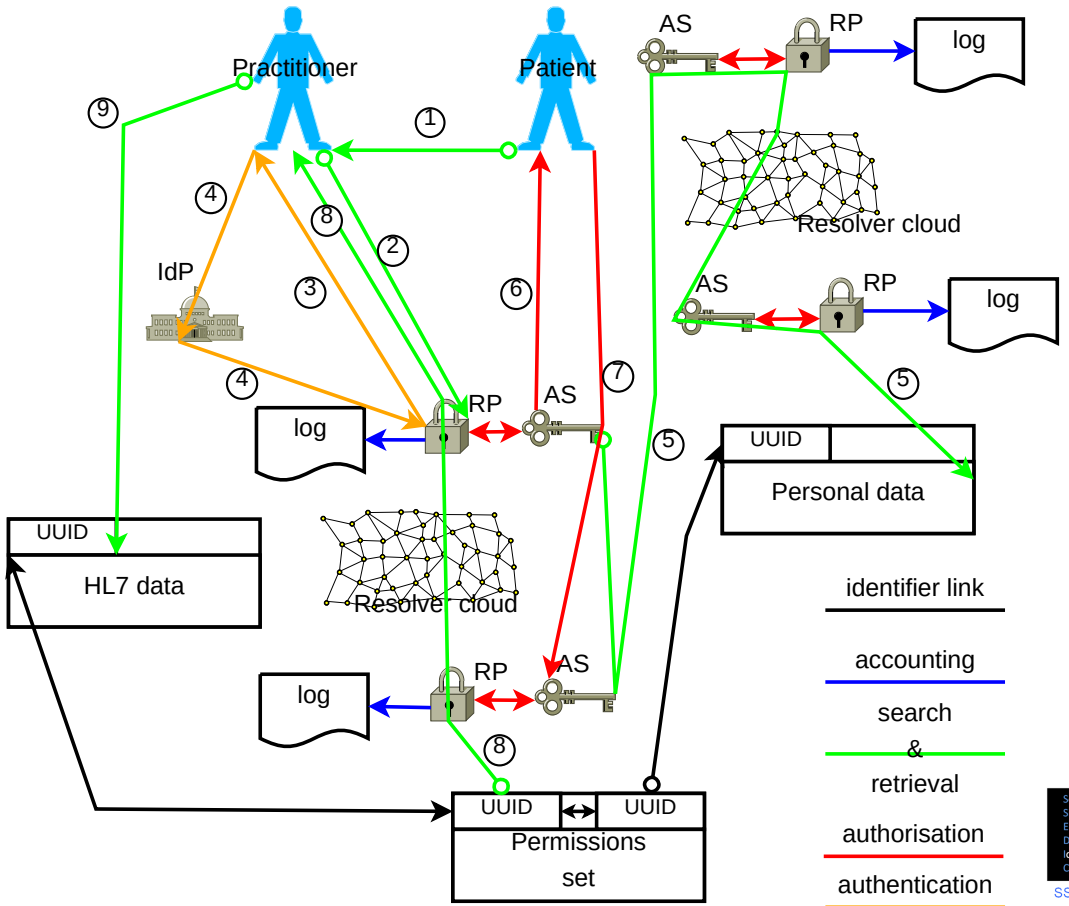
1. I as a patient go visit a practitioner.
2. The practitioner requests historic HR information.
3. I provide the practitioner with my UUID.
4. The practitioner identifies to the pertinent IdP and queries the resolver finder cloud and then, the appropriate resolver.
5. The resolver AS sends me a message indicating the practitioner identity, information about the requested data and a request for granting authorisation.
6. I grant the access and set a time limit.
7. The practitioner can access the data.

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Access to health records in clinical practice

a *smaller* picture



SSEDIC Programme Partner

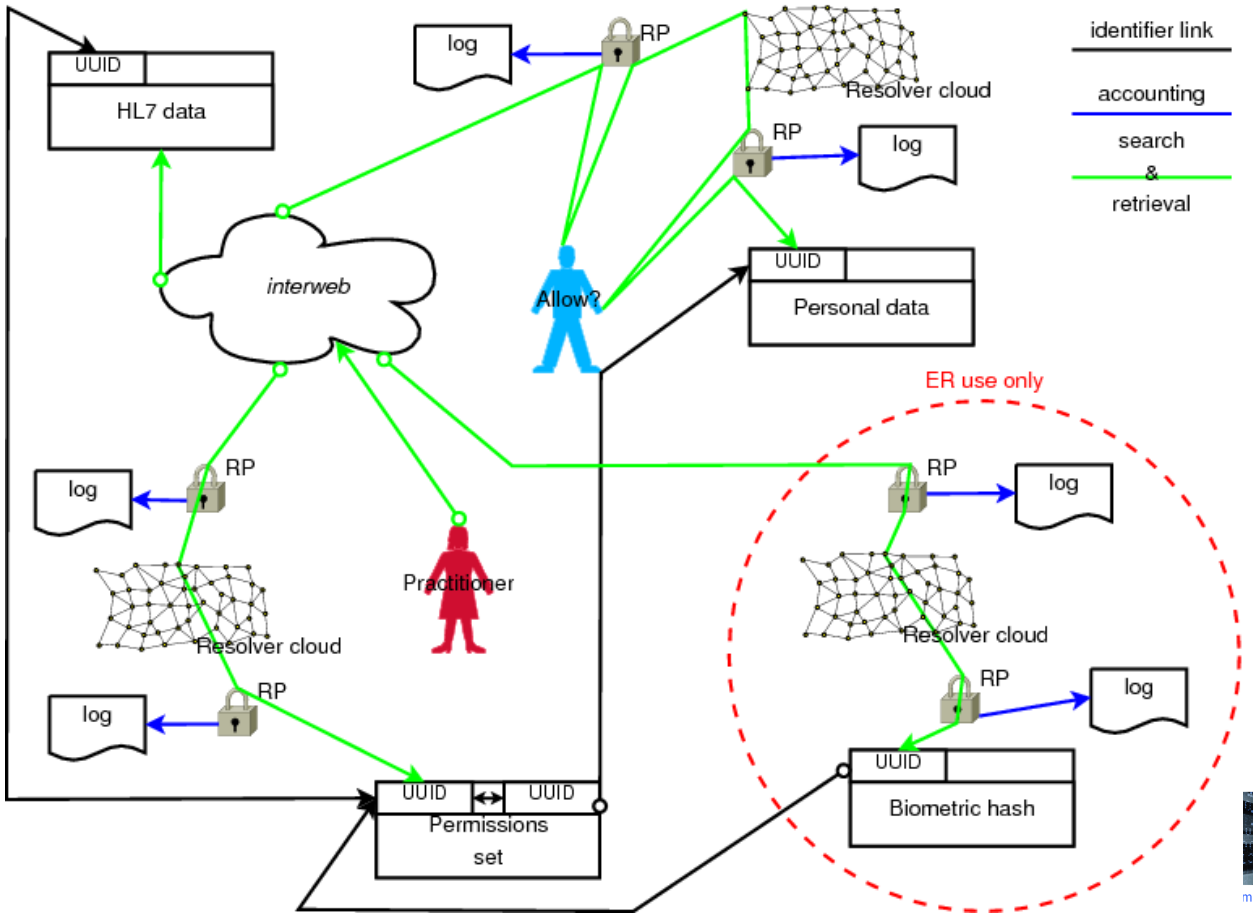
Access to health information for research purposes

1. I am a researcher working on a certain disease.
2. I search the web an collect all pertinent HRs.
3. I need to know about historic HR data about the same individuals that form the population under study.
4. I identify to my IdP that has an AA that asserts attributes to prove my researcher condition.
5. I query the resolvers for other HR UUIDs that belong to the same individuals as the HR UUIDs in the collection under study.
6. Depending on user preferences, data sensitivity or other parameters, patients get a request for granting access to the HR.

SSEDIC Programme Partner

System map

a.k.a. the big picture



Access to personal identity information

1. I am a hospital staff member.
2. I need to know a patient identity for billing purposes.
3. I identify to the hospital IdP and the hospital AA asserts attributes to prove my administration staff status.
4. I query the resolver finder cloud to find the resolver for the patient UUID.
5. I query the patient resolver.
6. I get back the data needed to bill the patient.
7. The patient is notified of the personal data request.

SSEDIC Programme Partner

Steps in the right direction

<http://www.va.gov/bluebutton/>

<http://www.whitehouse.gov/blog/2011/11/21/empowering-customers-green-button>

Scoping the Single European Digital Identity Community

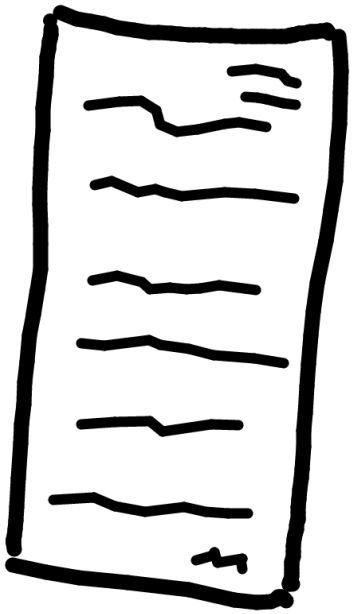
SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Steps in the right direction

Tarvi Martens' "Inimitable identity"

Educational sector



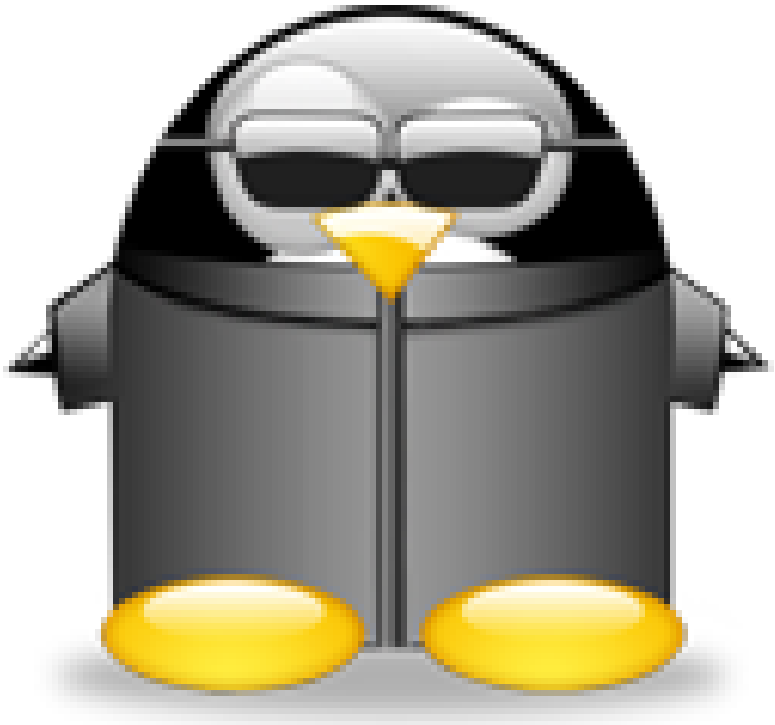
HR = Educational achievements

Challenges

Urbanidades #51 by Nana Sousa Dias <http://photo.net/photodb/photo?photo_id=4169934>

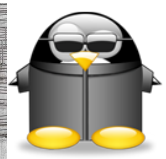
Identity and privacy

Challenges



Standards

Challenges



SECURE
IDENTITY
ACROSS
BORDERS
LINKED

Scoping the Single European Digital Identity Community

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Privacy

there are many ways to look at privacy in education

European Digital Identity Community

SSEDIC Programme Partner

Privacy

with increased knowledge of the subject

Full anonymity

SSEDIC Programme Partner

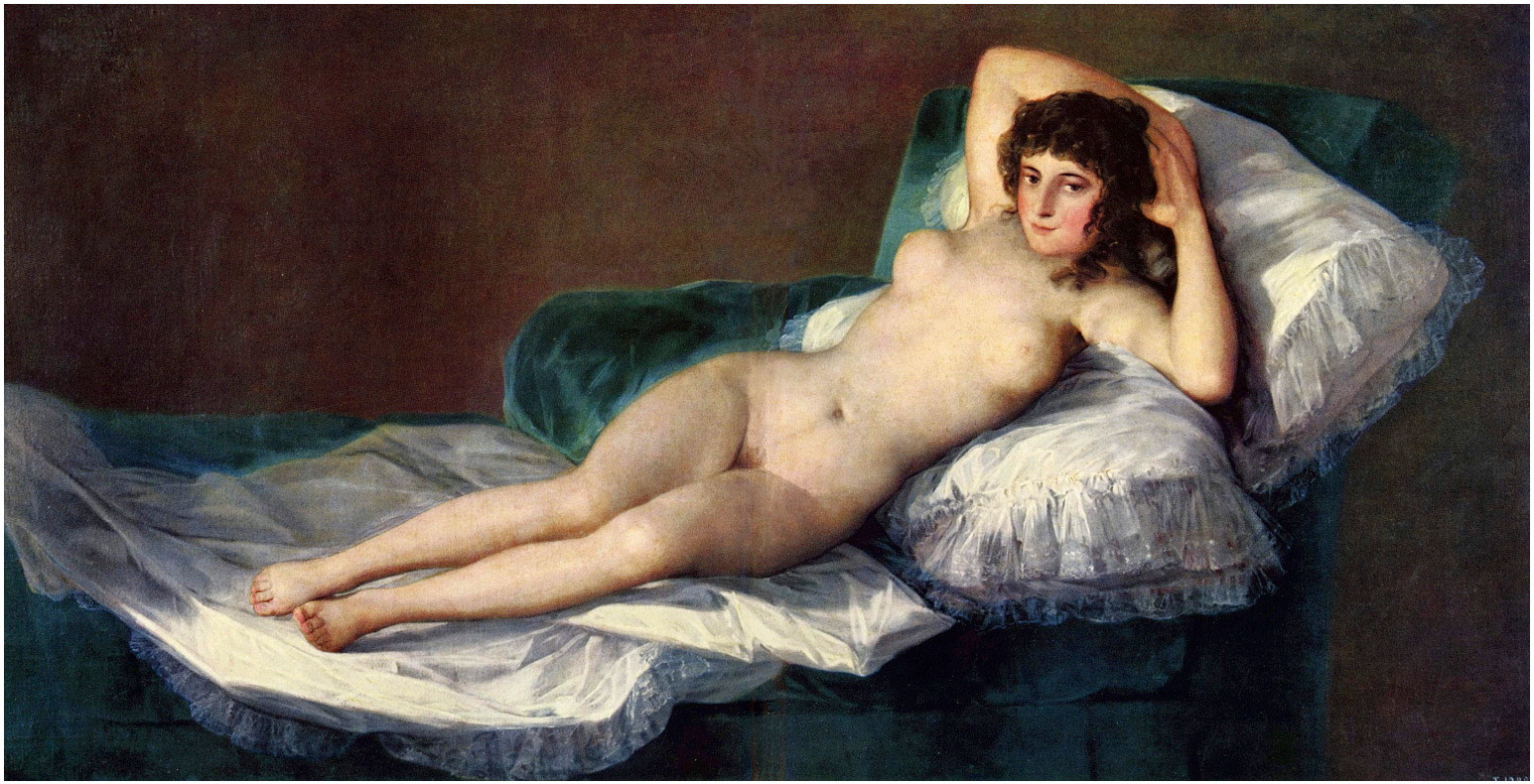
Privacy

with increased knowledge of the subject

Pseudonymous identity

Privacy

with increased knowledge of the subject

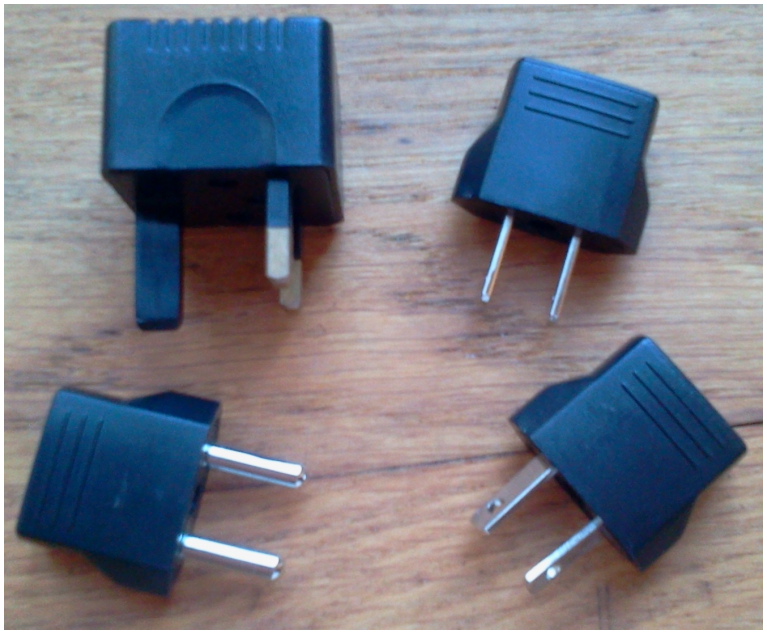


Full disclosure

Goya's Nude Maja <http://commons.wikimedia.org/wiki/File:Goya_Maja_naga2.jpg>

Standards

Challenges

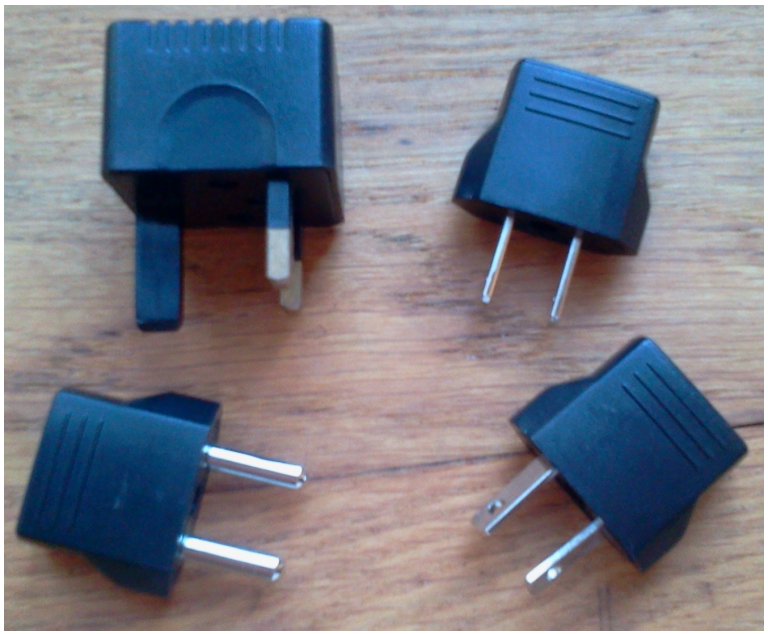


There are never enough

SSEDIC Programme Partner

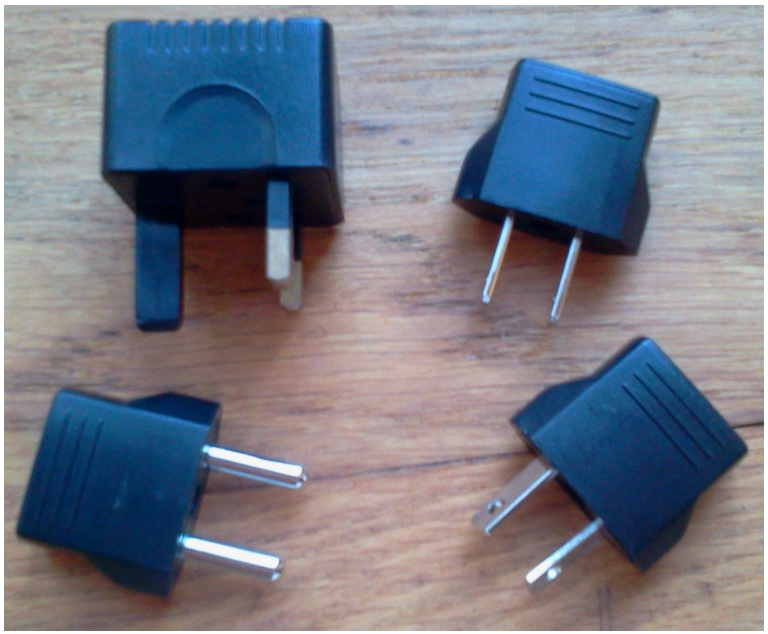
Standards

Challenges



Standards

Challenges

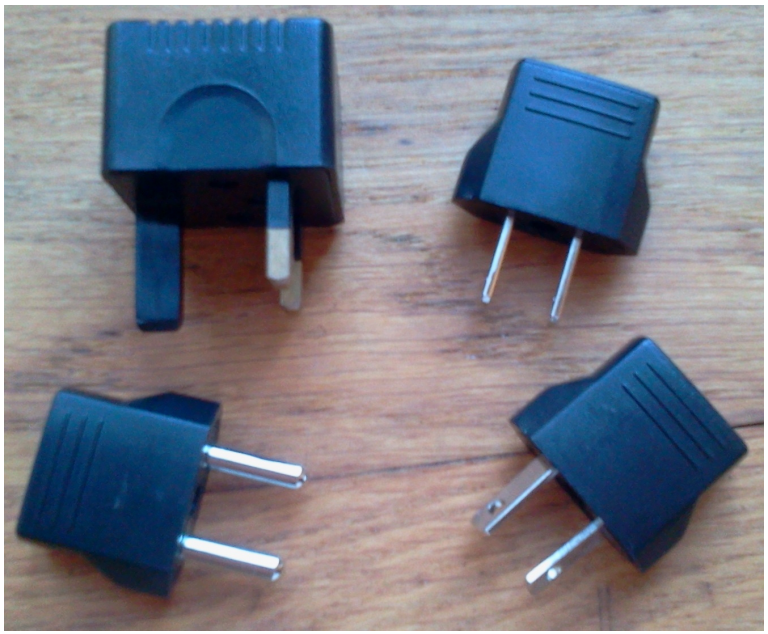


- SAML

SSEDIC Programme Partner

Standards

Challenges

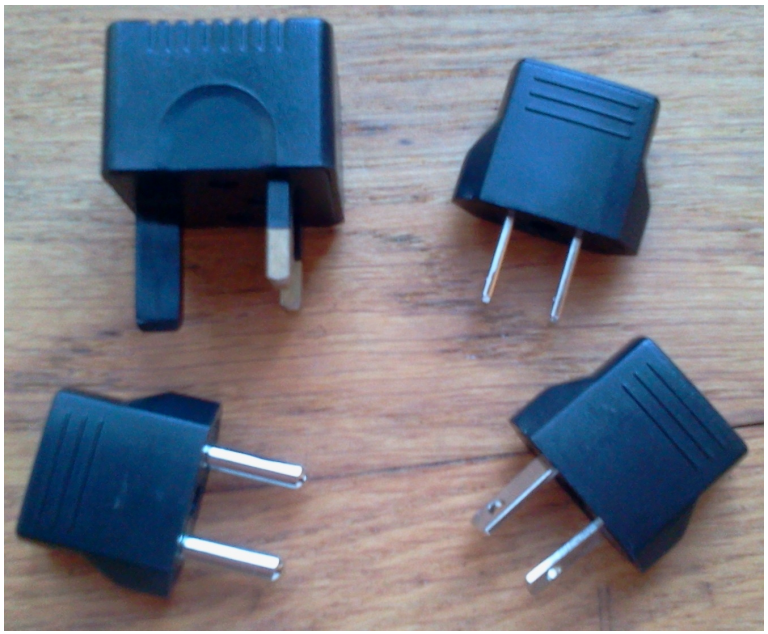


- SAML
- OAuth

SSEDIC Programme Partner

Standards

Challenges

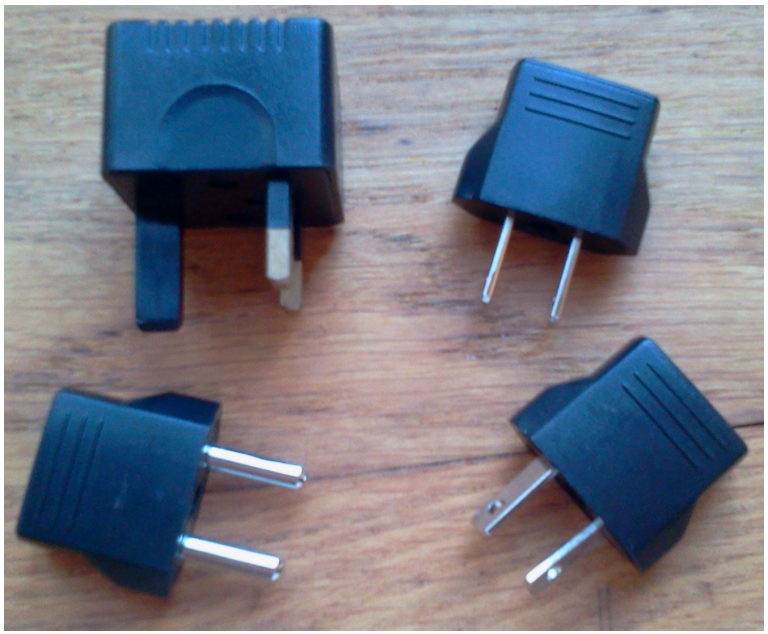


- SAML
- OAuth
- eduPerson

SSEDIC Programme Partner

Standards

Challenges

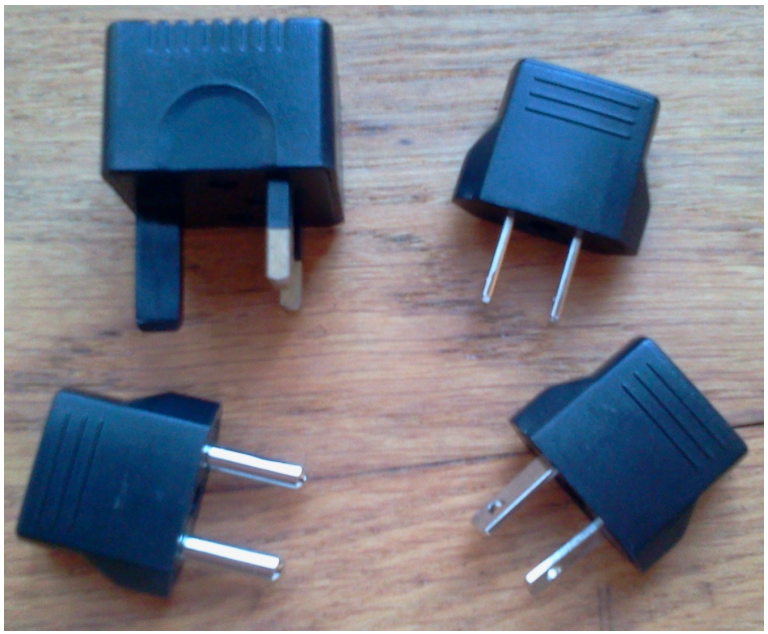


- SAML
- OAuth
- eduPerson
- SCHAC

SSEDIC Programme Partner

Standards

Challenges

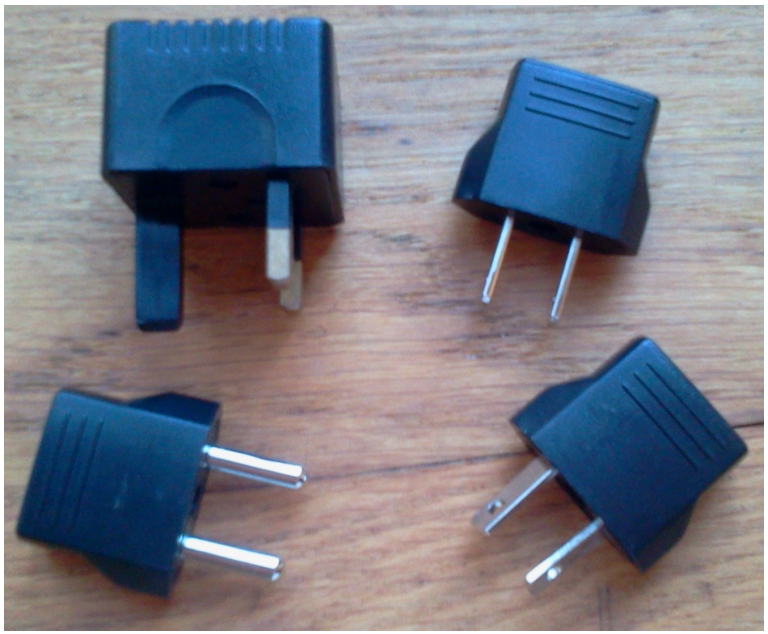


- SAML
- OAuth
- eduPerson
- SCHAC
- MLO

SSEDIC Programme Partner

Standards

Challenges

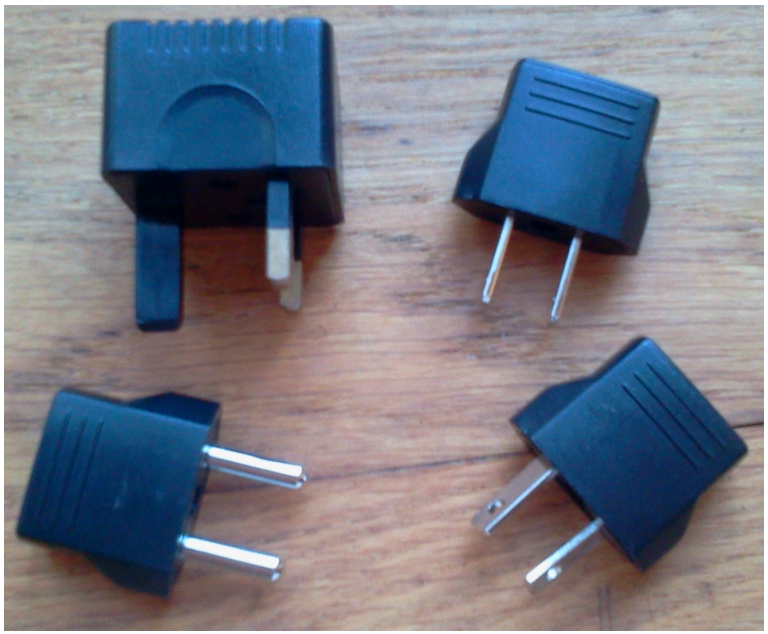


- SAML
- OAuth
- eduPerson
- SCHAC
- MLO
- Europass

SSEDIC Programme Partner

Standards

Challenges



- SAML
- OAuth
- eduPerson
- SCHAC
- MLO
- Europass
- ...

SSEDIC Programme Partner

Security

Challenges



SSEDIC Programme Partner

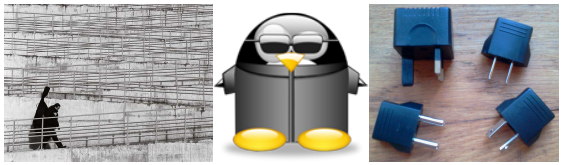
Security

Challenges




Security

Challenges



- TCS

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Security

Challenges




- TCS
- STORK2

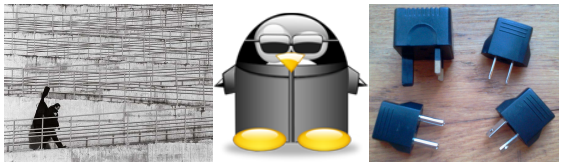
Scoping the Single European Digital Identity Community

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Security

Challenges

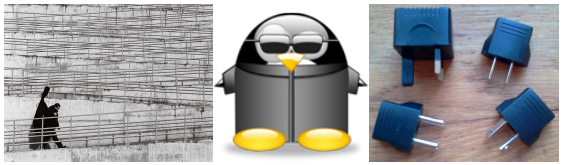


- TCS
- STORK2
- TF-CSIRT

SSEDIC Programme Partner

Security

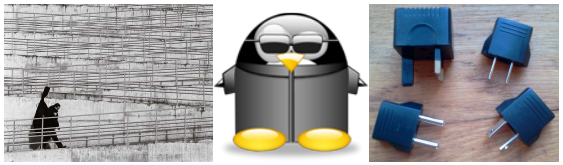
Challenges



- TCS
- STORK2
- TF-CSIRT
- Trusted Introducer

Security

Challenges



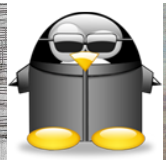
- TCS
- STORK2
- TF-CSIRT
- Trusted Introducer
- ...

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

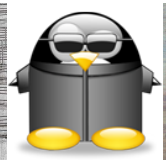
Storage

Challenges

Storage

Challenges







Storage

Challenges





Scoping the Single European Digital Identity Community

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Storage

Challenges





- Grids

Storage

Challenges





- Grids
- Geánt3+

Storage

Challenges





- Grids
- Geánt3+
- TF-Storage

Scoping the Single European Digital Identity Community

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Storage

Challenges





- Grids
- Geánt3+
- TF-Storage
- TF-EMC^2

Scoping the Single European Digital Identity Community

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Storage

Challenges

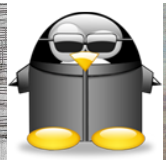


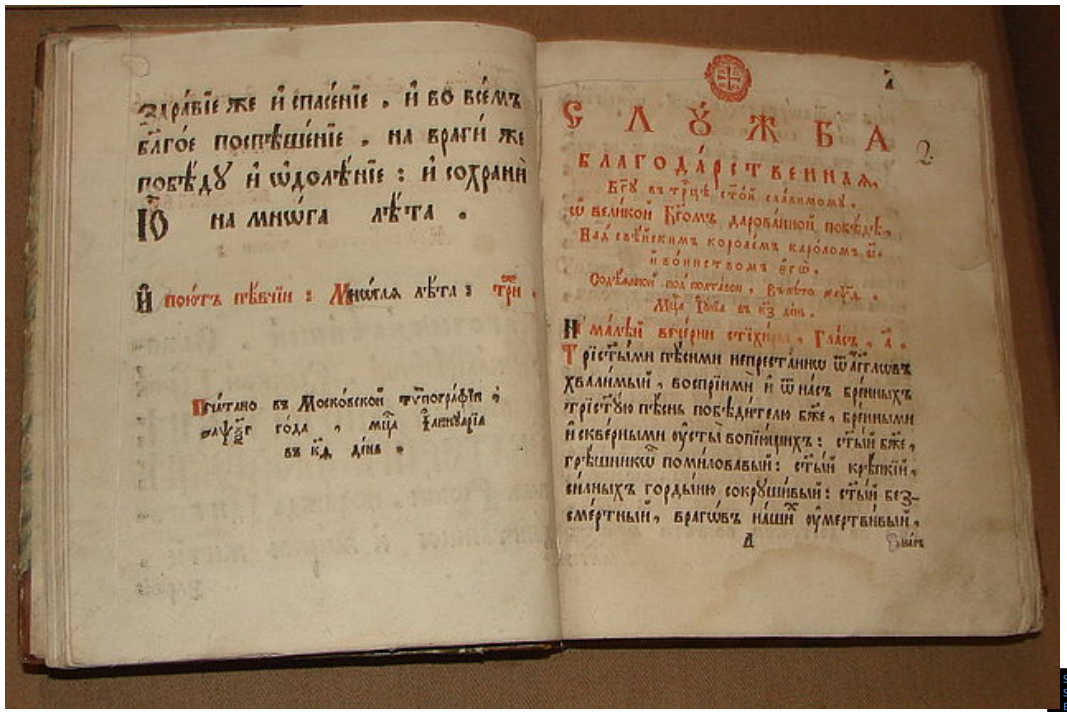


- Grids
- Geánt3+
- TF-Storage
- TF-EMC^2
- ...

Storage

Challenges

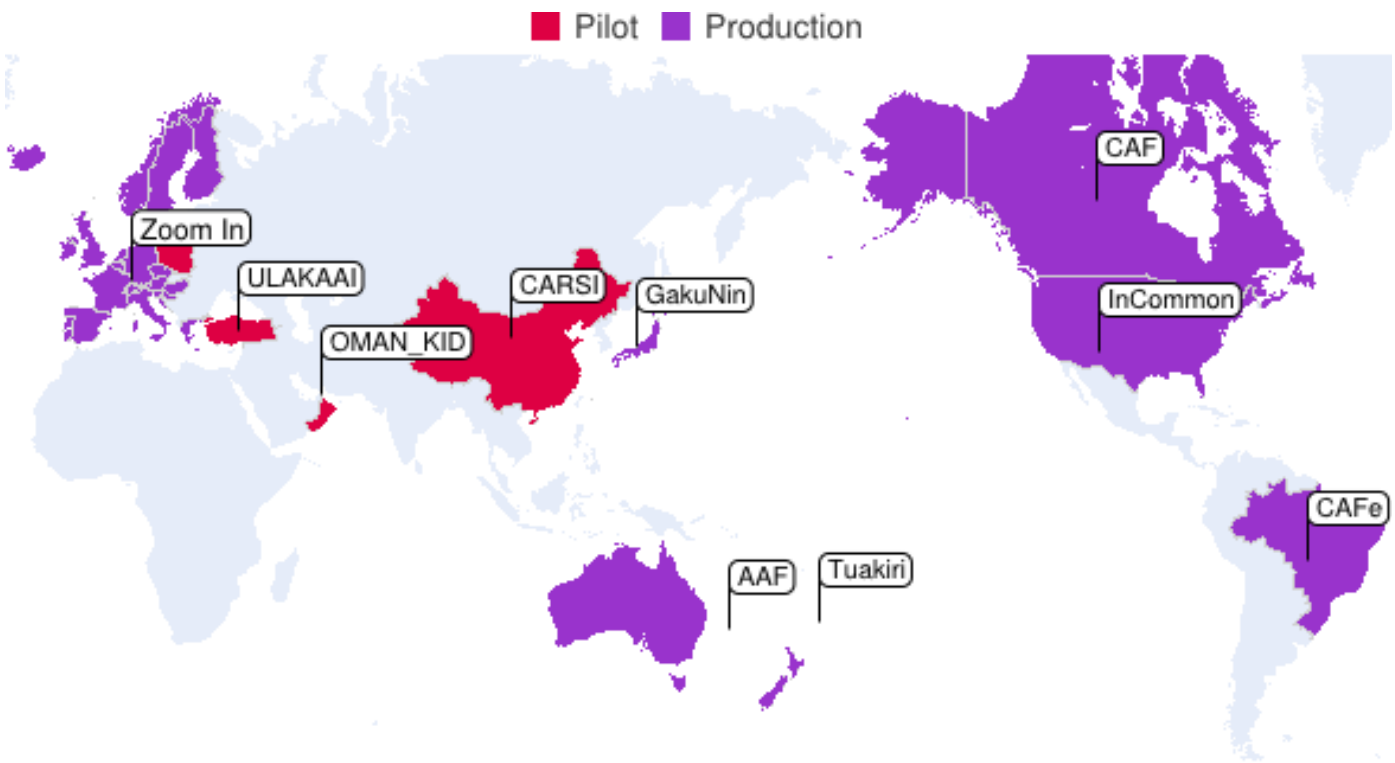



CC-BY-SA Sergeev Pavel <http://commons.wikimedia.org/wiki/File:Slugebnik_93.jpg>

HiEd Federations

spanning the globe

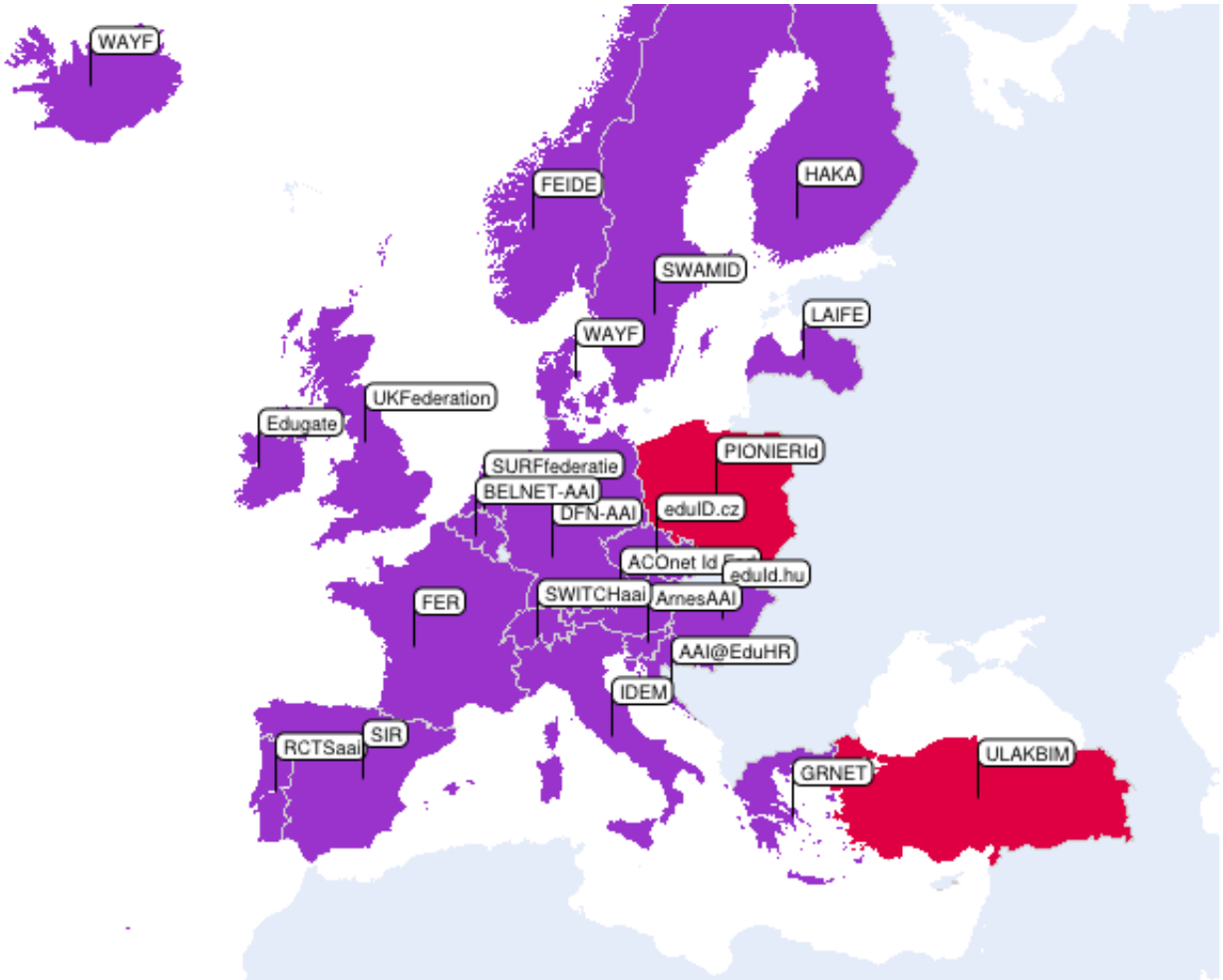


existing intereoperable identity infrastructure

SSEDIC Programme Partner

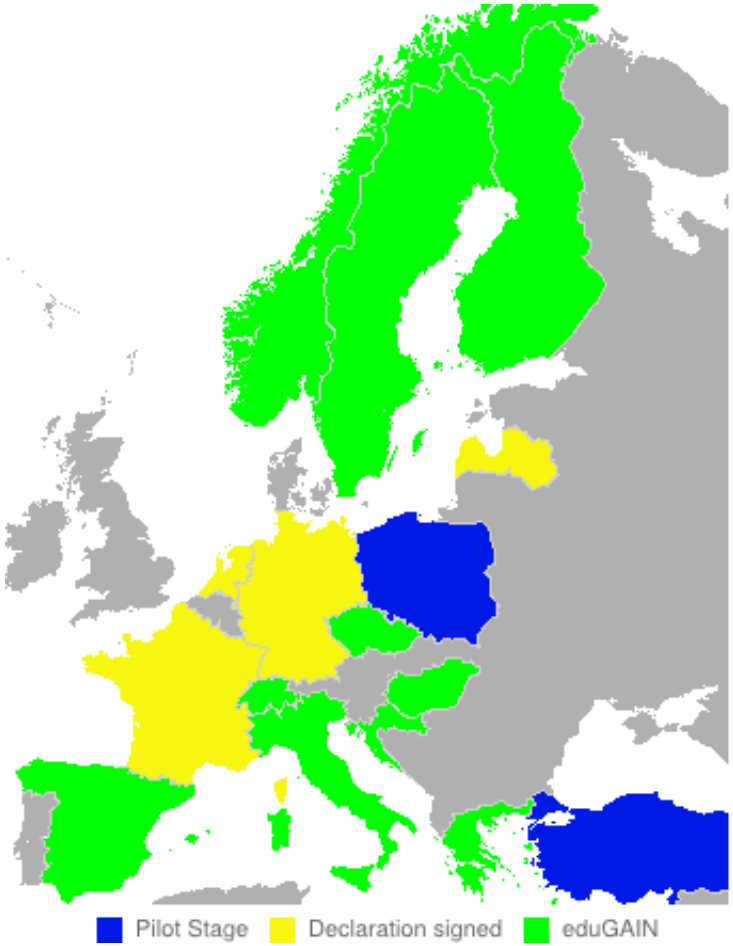
HiEd Federations

covering Europe



Interfederation

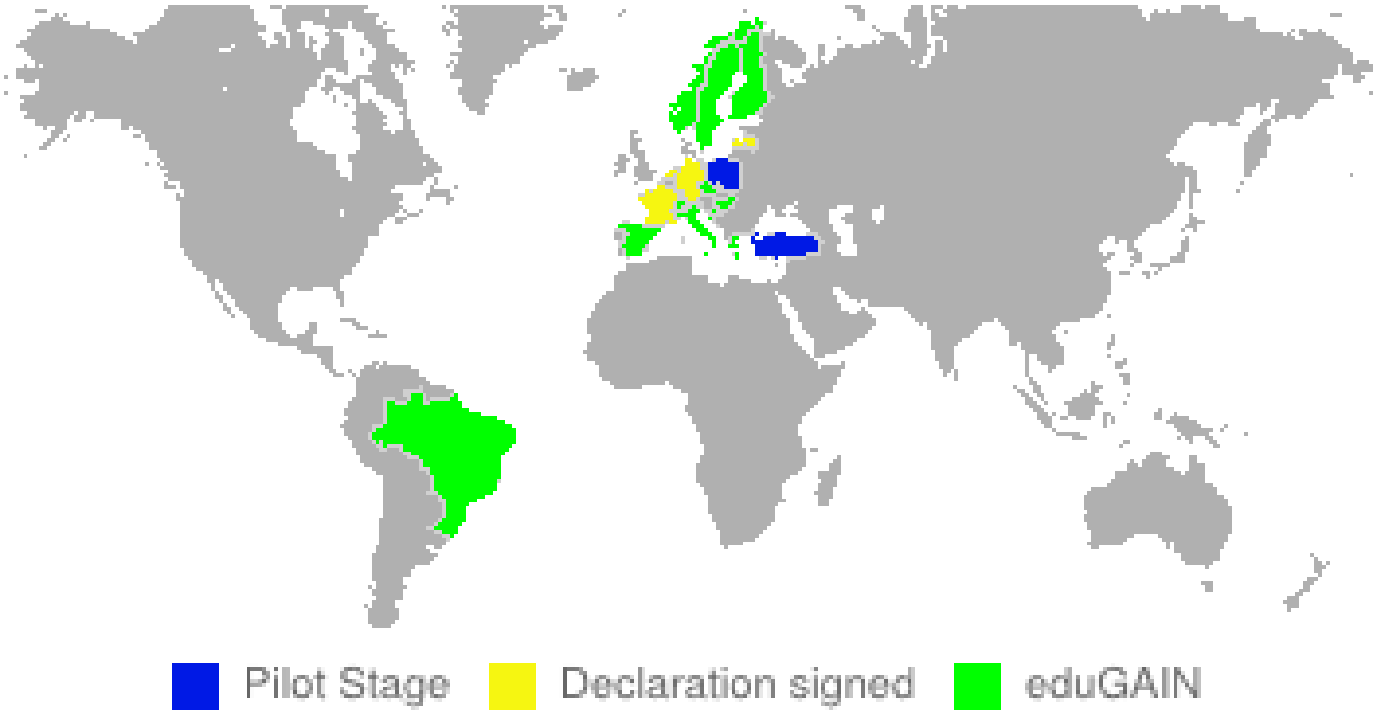
edugain: started in Europe



SSEDIC Programme Partner

Interfederation

edugain: reaching out for the globe



It’s your turn now!
go home
grab your favourite techies
send them to us

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

It’s your turn now!
go home
grab your favourite techies
send them to
your local federation

SSEDIC Programme Partner

It's your turn now!
go home
grab your favourite techies
send them to
TF-EMC^2

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

It's your turn now!
go home
grab your favourite techies
send them to
RS3G[3]

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

It’s your turn now!
go home
grab your favourite techies
send them to
EUNIS

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

It's your turn now!
go home
grab your favourite techies
send them to
TERENA

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Dank u!

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Dank u!

Questions?

answers not assured

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA