Experiment driven and user eXPerience oriented

Analytics for eXtremely Precise outcomes and decisions

Digital Identity and Distributed Access Control: Bridging Privacy and Transparency in Cross-Organizational Data Sharing

Dr. ir. Marcela Tuler de Oliveira
Assistant Professor in Trustworthy Data Systems
Dept. of Engineering Systems and Services – ICT Section
Faculty of Technology, Policy and Management

ExtremeXP

TU Delft

Funded by the European Union

Co-funded by the European Union Horizon Programme Call HORIZON-CL4-2022-DATA-01-01, under Grant Agreement No. 101093164

About Me

Marcela Tuler
Assistant professor
Trustworthy data systems

M.TulerdeOliveira@TUDelft.nl

https://www.linkedin.com/in/marcelatuler/

- ✓ BSc and MSc in Telecommunications Engineering – University Federal Fluminense, RJ, Brazil.
- ✓ Ph.D. in Digital solutions for cross-organization data sharing and cybersecurity in healthcare from the Amsterdam University Medical Center, University of Amsterdam.
- ✓ My research focuses on
  - Distributed Ledger Technology
  - Privacy-Preserving Data Sharing
  - New-Generation Networks.
- ✓ Lecture of the BSc. course I&C Risk and Control

Funded by
the European Union

About you

Please, tell me about you:

- write down their primary expertise area on a Post-it note
- jot down a few key skills or experiences

Ops… don’t forget to add a unique identification,
your name works ;)

Funded by
the European Union

Sorting Hat

Funded by
the European Union

Gryffindor: The Privacy Law Experts

Gryffindor is known for bravery and determination, much like our Privacy Law Experts, who stand on the front lines, **safeguarding individuals' data rights**. They dive into **legal complexities** and ensure operations adhere to regulations like **GDPR** and **eIDAS**.

Funded by
the European Union

Hufflepuff: The DLT Specialists

Hufflepuff house values hard work, patience, and loyalty. Similarly, our DLT Specialists are the **backbone of digital identity infrastructure**, working diligently behind the scenes to ensure **secure**, **transparent**, and **decentralized data sharing**. Their patience and dedication bring **robustness** and **reliability** to **complex systems**.

Funded by
the European Union

Ravenclaw: The Data Science Enthusiasts

Ravenclaw house prizes learning, wisdom, and wit. These traits are well mirrored in our Data Science Enthusiasts who use their **analytical skills** and curiosity to derive **meaningful insights from data**, **ask the right questions**, and **continuously learn** and adapt to **new methodologies and technologies**.

Funded by
the European Union

Slytherin: The Digital Identity Professionals

Slytherin house is known for ambition, **leadership**, and resourcefulness. Our Digital Identity Professionals show the same characteristics as they **lead the way in implementing effective digital identity solutions**. Their ambition drives them to **create systems** that balance **security**, **usability**, and **privacy**.

Funded by
the European Union

Groups Formation

- ✓ Each group should have a member from every "house"
- ✓ Depending on the total number of participants, each group can have more than one participant from the same house
- ✓ Every group has a diverse set of expertise

Funded by
the European Union

Workshop agenda

Solving the contradictions and finding solutions to integrate the eIDAS (digital wallet solutions) with the use of Smart Access

1. Blockchain distributed access control based on attributes, and discussion of the privacy challenges of authentication — 50 min
2. Assignment Session — 30 min
3. Presentations and Conclusion — 20 min
4. Winners' prizes

Funded by the European Union

Why do we need distributed access control?

1. Motivation → Electronic Medical Records sharing across organizations
   Multiples silo with parts of your history data

2. Data breaches → Healthcare is the industry most plagued
   How much your medical records leakage can affect your life?
   How to protect data confidentiality against a curious cloud provider?

3. Very dynamic → Data availability comes first → Break-the-glass
   How to validate a legitimate request?
   How to enforce Data Processing Agreements after sharing?
   Joint controllers define access control policies together
   Needs for audit trails and data provenance
   Data processing responsibility and non-repudiation

Funded by
the European Union

Why do we need distributed access control?

1. Motivation → Electronic Medical Records sharing across organizations
   Multiples silo with parts of your history data

2. Data breaches → Healthcare is the industry most plagued
   How much your medical records leakage can affect your life?
   How to protect data confidentiality against a curious cloud provider?

3. Very dynamic → Data availability comes first → Break-the-glass
   How to validate a legitimate request?
   How to enforce Data Processing Agreements after sharing?
   Joint controllers define access control policies together
   Needs for audit trails and data provenance
   Data processing responsibility and non-repudiation

Funded by
the European Union

Acute Stroke Care

independent.co.uk

News > Health

Google makes bid to throw out High Court claim over NHS medical record transfer

Lawyers for Google and DeepMind have said the claim is 'bound to fail'.

openDemocracy
free thinking for the world

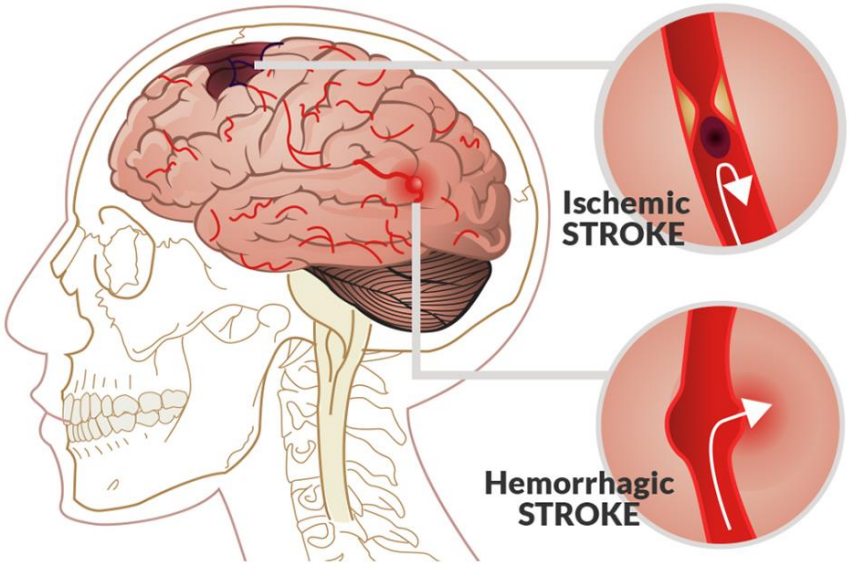
All Themes Projects Regions About

HOME: INVESTIGATION

Exclusive: NHS hospitals told to share patient data with US 'spy-tech' firm

Palantir, whose owner claimed the NHS 'makes people sick', will 'collect and process confidential patient information'

Case study



Acute Stroke Care

Stroke is a condition where poor blood flow to the brain results in cell death

45.000 stroke patients per year in The Netherlands

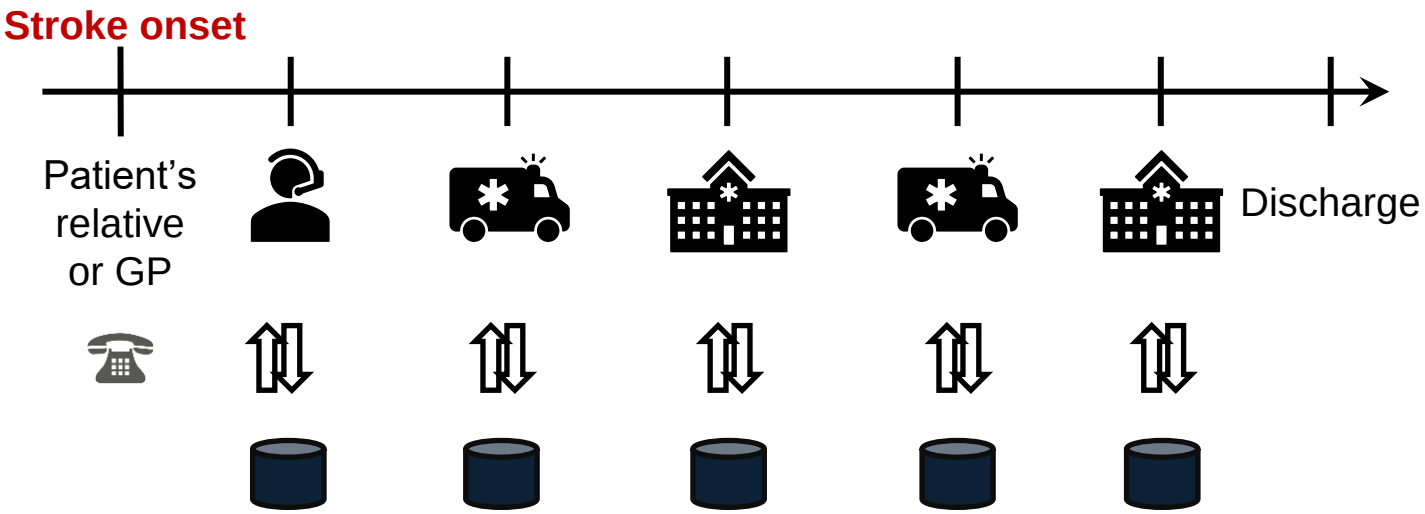
Funded by
the European Union

Data Sharing Challange

https://thesocialmedic.net/2017/07/ready-glove-designed-for-documentation/

https://www.brother.co.uk/labelling-and-receipts/a4-to-a5-mobile-printers

Stroke care ‘takes a village’



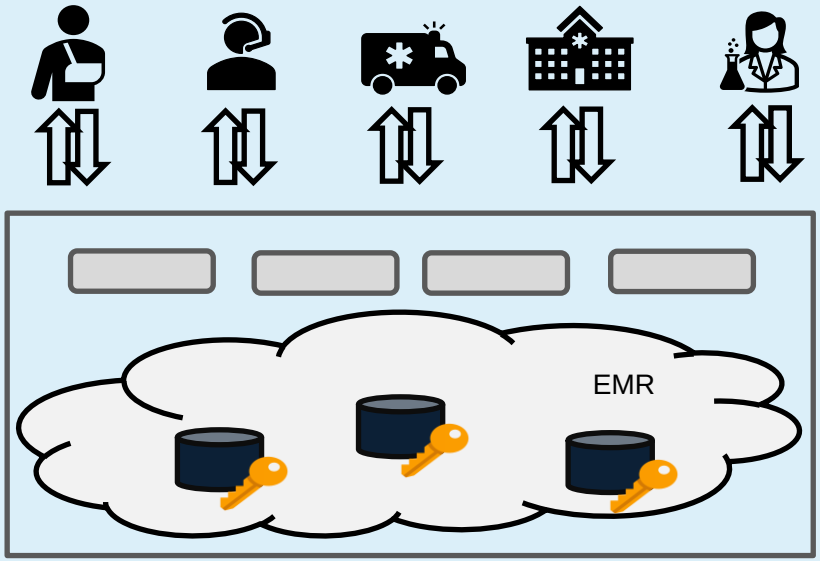

FIRE
BREAK GLASS
PRESS HERE

Electronic Medical Records

Availability of EMR reduce unnecessary investigation and improve communication

Cloud solution offers:

→ remote and available EMR access
→ security and privacy concerns



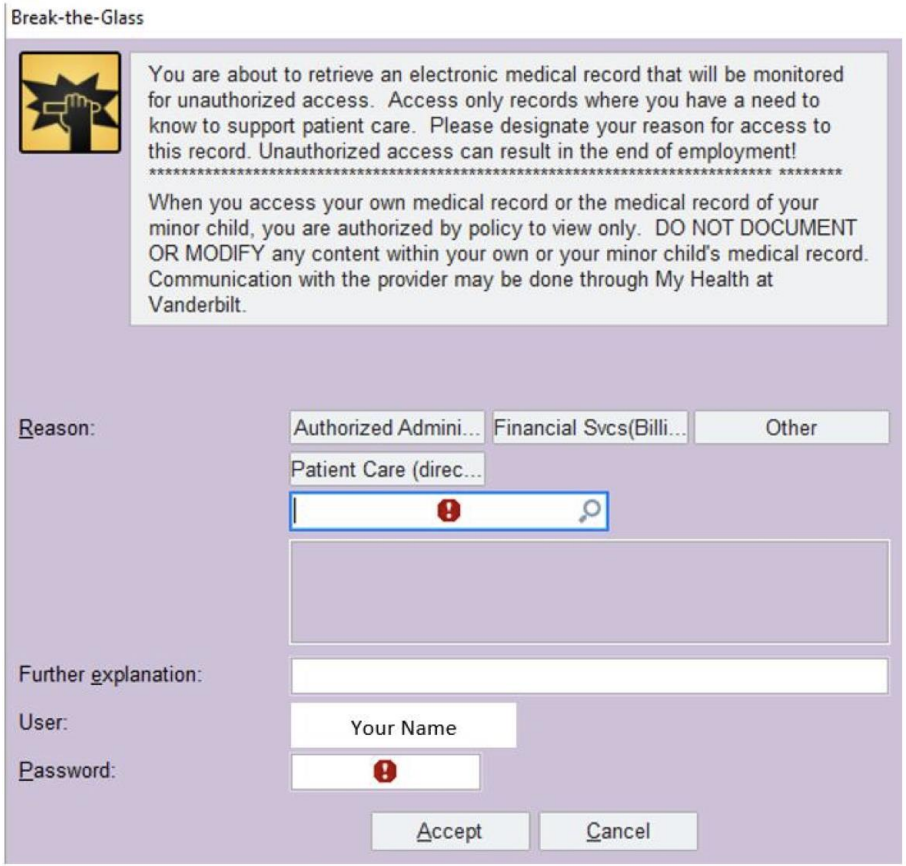
Funded by the European Union

Break-Glass Procedure

Quick means for a person **who does not have access privileges** to certain information to gain access **when necessary**

General Data Protection Regulation (GDPR)

→ Vital interest of the patient



Why do we need distributed access control?

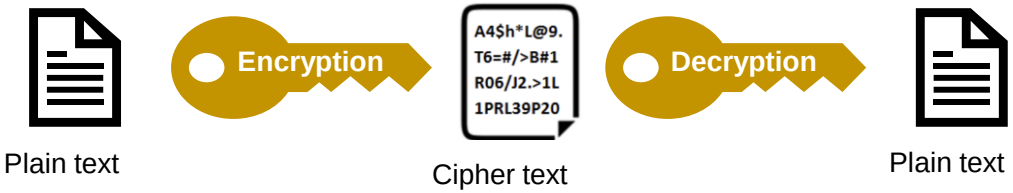
1. Motivation → Electronic Medical Records sharing across organizations
   Multiples silo with parts of your history data

2. Data breaches → Healthcare is the industry most plagued
   How much your medical records leakage can affect your life?
   How to protect data confidentiality against a curious cloud provider?

3. Very dynamic → Data availability comes first → Break-the-glass
   How to validate a legitimate request?
   How to enforce Data Processing Agreements after sharing?
   Joint controllers define access control policies together
   Needs for audit trails and data provenance
   Data processing responsibility and non-repudiation

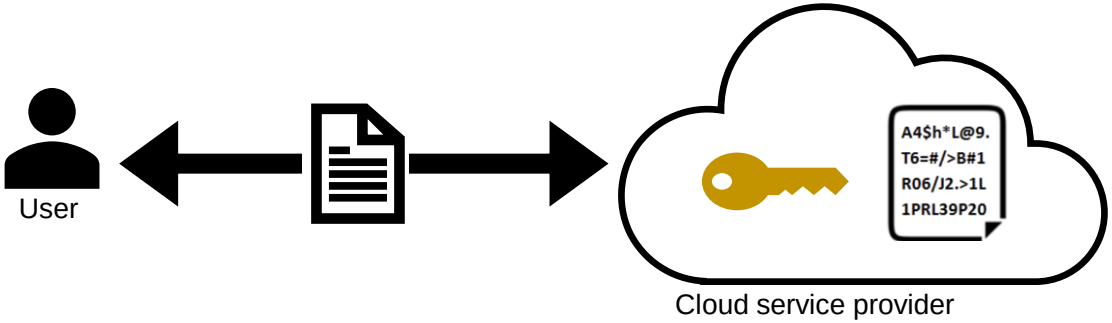
Funded by
the European Union

How to protect data confidentiality?

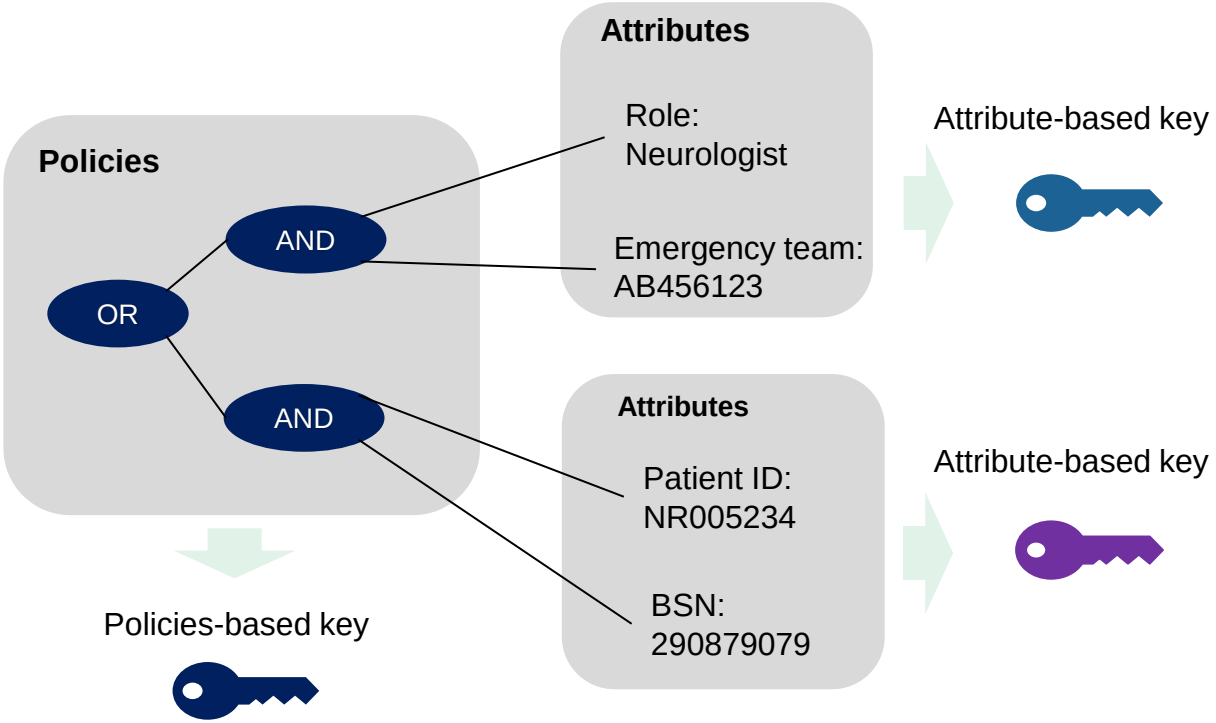


Symmetric encryption scheme

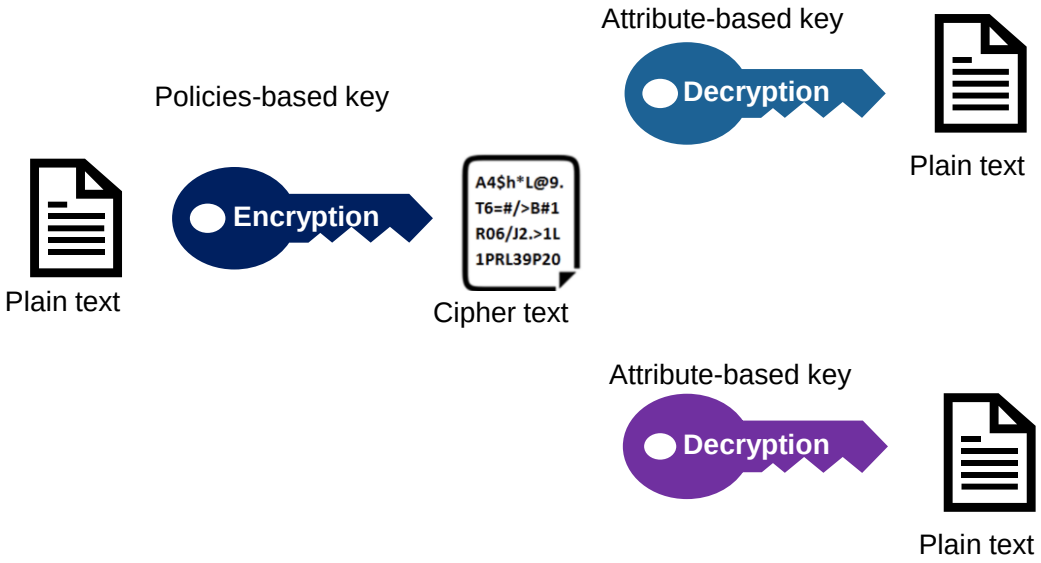
Data encryption on the Cloud



Alternatives: Polices and Attributes



Attribute-based encryption



Hybrid-encryption scheme

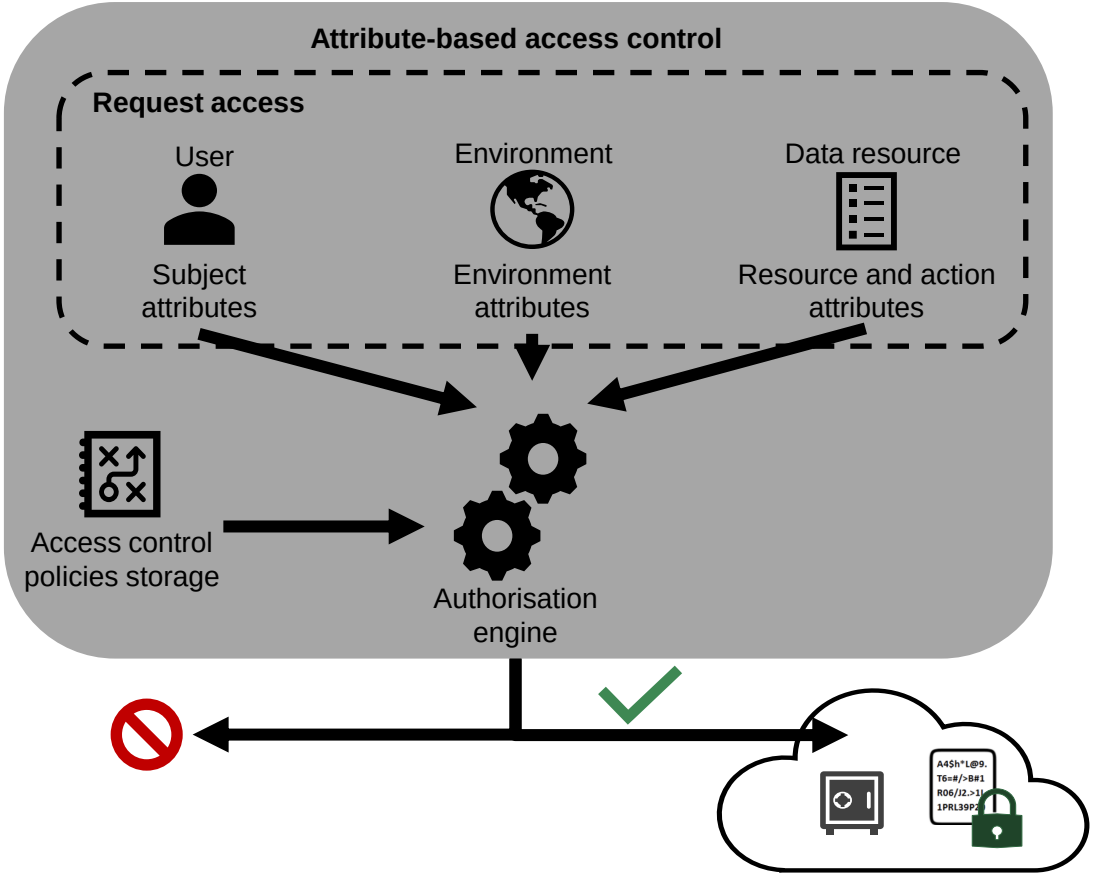
Data confidentiality:
Local symmetric encryption

Key management:
Attribute-based encryption

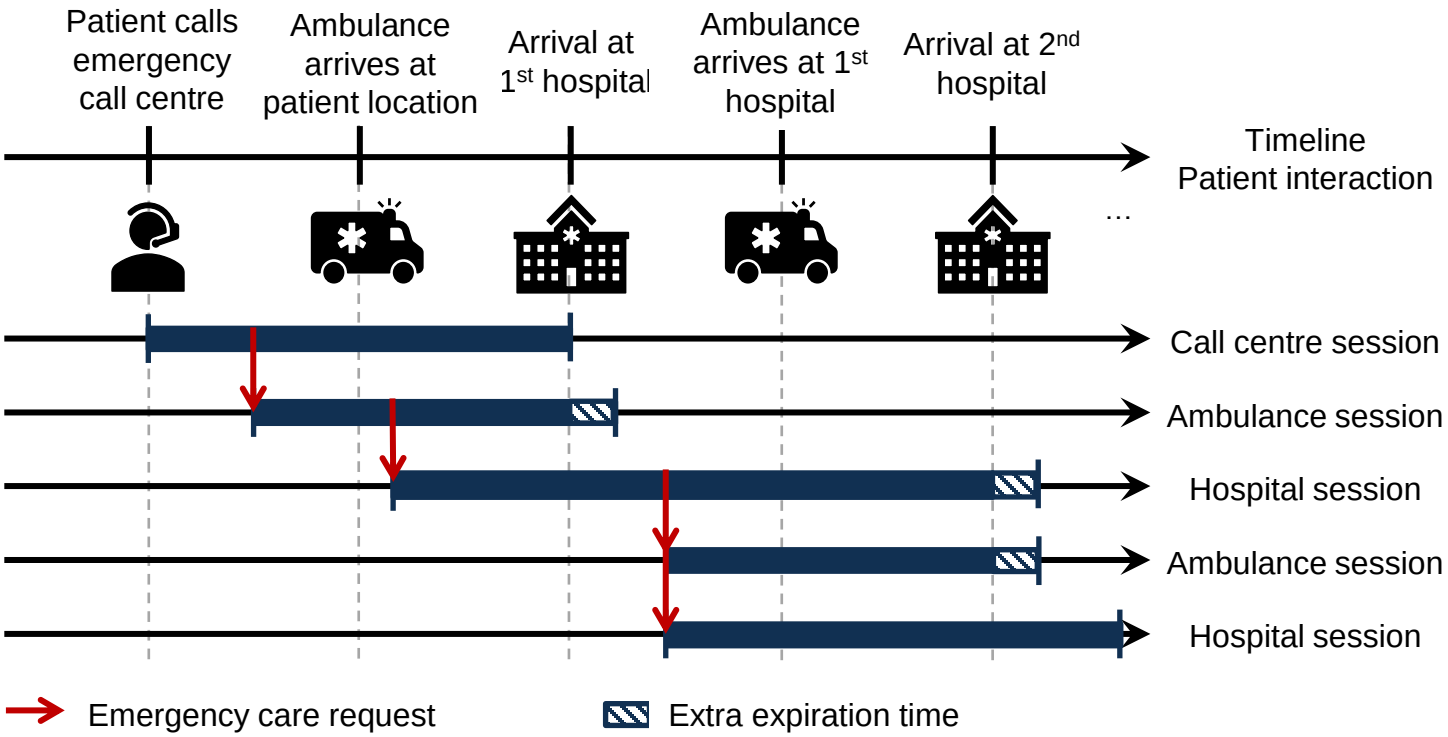
Attribute-based access control

Emergency access policies

Dynamic access control: grant and revoke



Stroke care and data access timeline



Why do we need distributed access control?

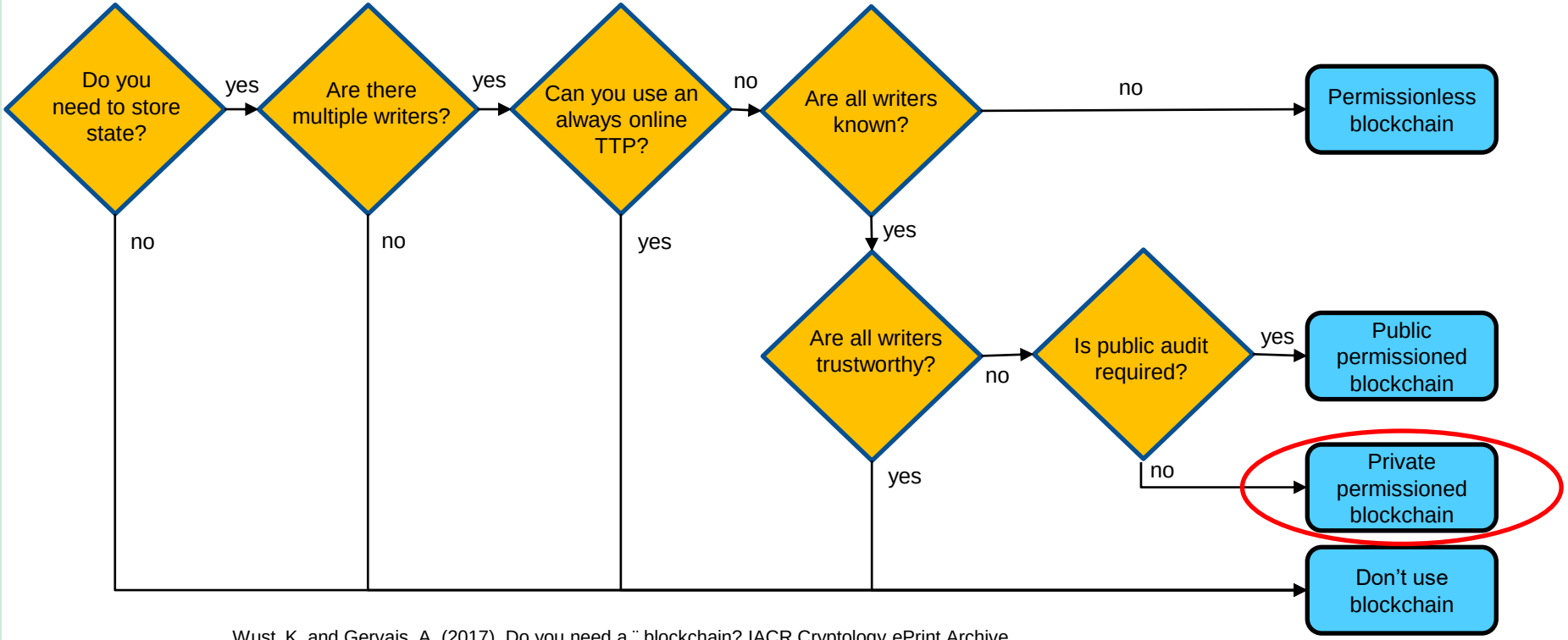
1. Motivation → Electronic Medical Records sharing across organizations
   Multiples silo with parts of your history data

2. Data breaches → Healthcare is the industry most plagued
   How to protect data confidentiality against a curious cloud provider?
   How much your medical records leakage can affect your life?

3. Very dynamic → Data availability comes first
   How to validate a legitimate request?
   How to enforce Data Processing Agreements after sharing?
   Joint controllers define access control policies together
   Needs for audit trails and data provenance
   Data processing responsibility and non-repudiation

Funded by
the European Union

When to consider using blockchain?



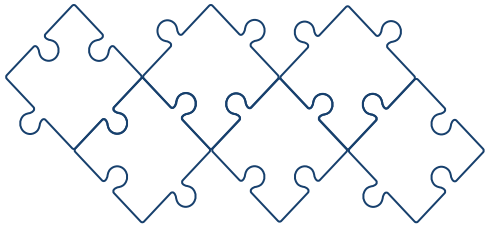
Wust, K. and Gervais, A. (2017). Do you need a ¨ blockchain? IACR Cryptology ePrint Archive, 2017:375.https://eprint.iacr.org/2017/375.pdf

Funded by the European Union

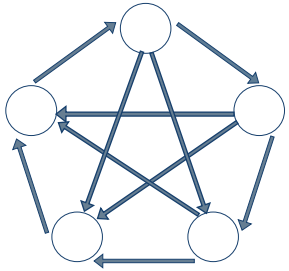
Blockchain Technology

TECHNOLOGY

Block Chaining
Data Structure



Peer-to-Peer Network



Funded by
the European Union

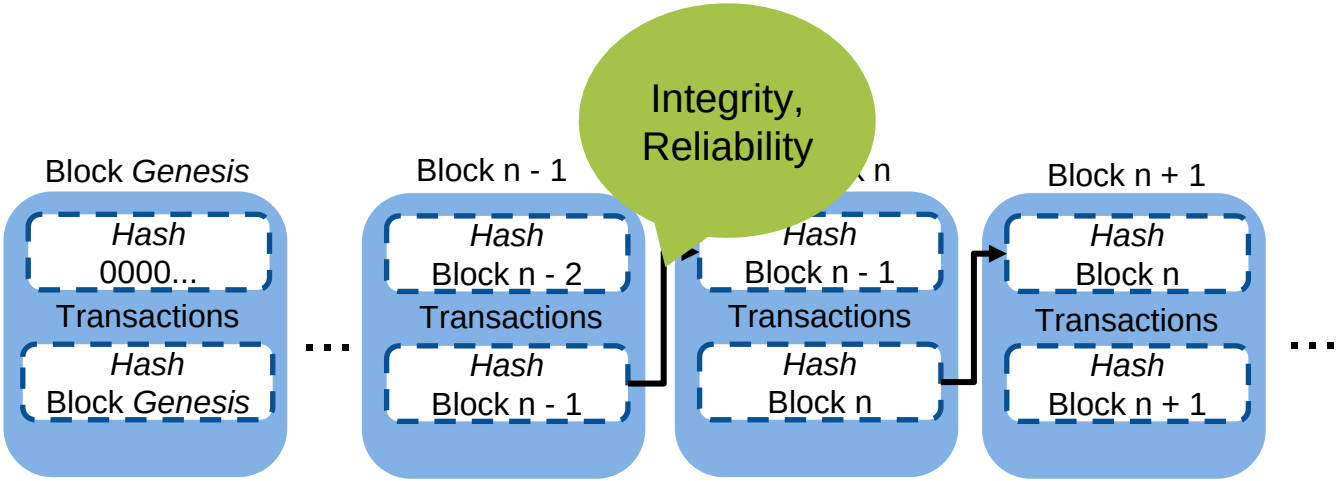
Hash function

Hash function generates the finger print of a data.

One way encryption →
Is infeasible to convert hash to data

Funded by
the European Union

Block Chaining Data Structure



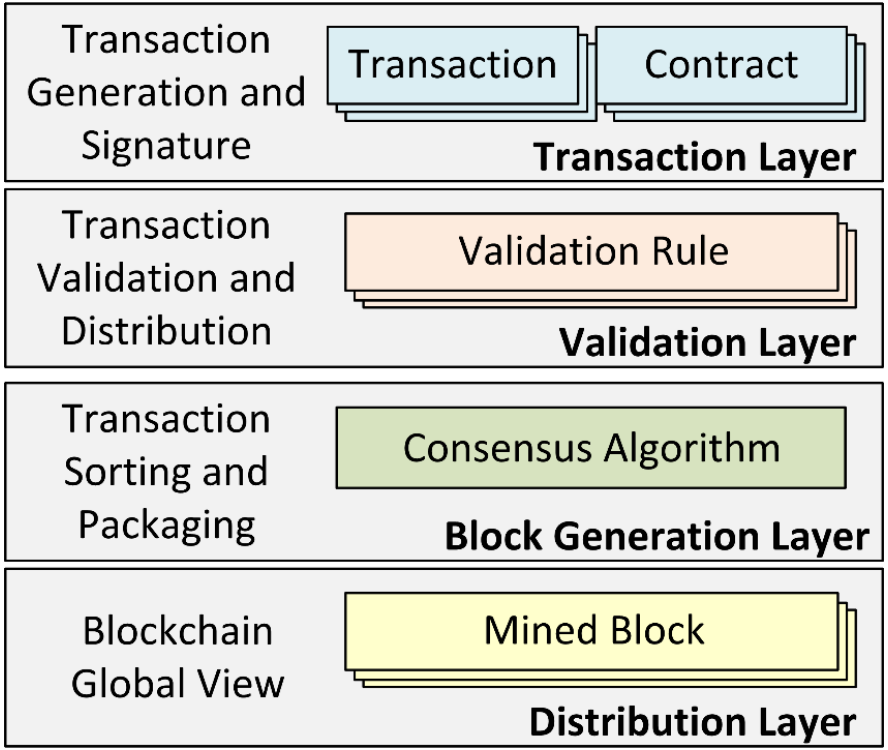
Funded by
the European Union

Peer-to-Peer Blockchain Network

Distributed Execution of Transaction

Validation and Consensus Algorithm

- → Each node keeps a replica of the chain.
- → Agreement on the most updated version of the chain



Funded by the European Union

SmartAccess: Proposal

- Exploit the technology of **Blockchain** and **Smart Contracts**
  - Decentralised access control mechanism based on Attribute-based Access Control (ABAC) for healthcare
  - Collaboration among healthcare organisations
    - Compliance with GPDR
- SmartAccess
  - An access control mechanism based on **smart contracts** for distributed systems

Smart contract is a computer program or a transaction protocol that is intended to automatically execute, control or document legally-relevant events and actions according to the terms of a contract or an agreement

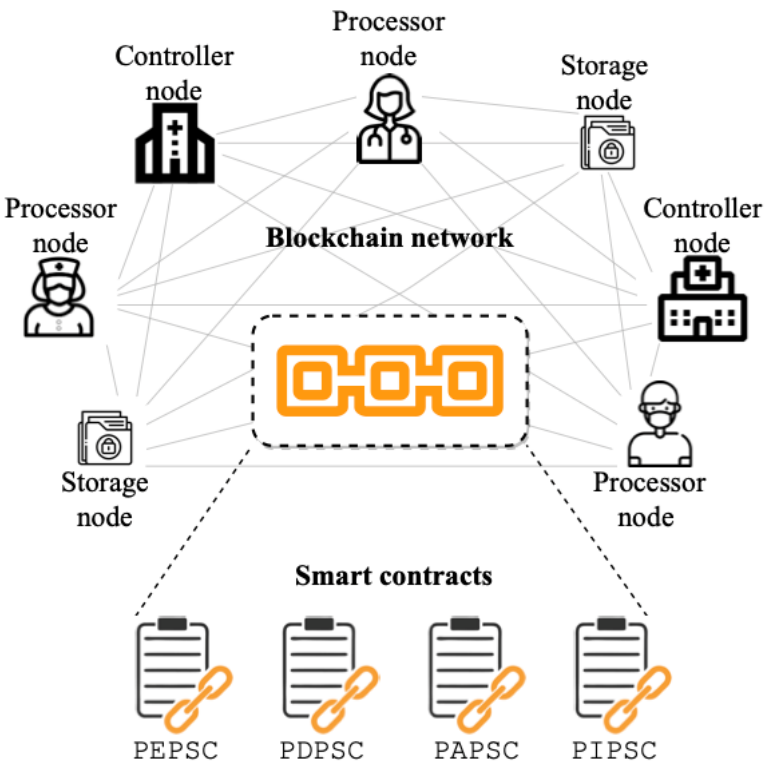
Funded by the European Union

SmartAccess: Architecture

Network nodes → GDPR

- Storages: Organizations that store the patient data
- Controllers: Healthcare organizations
- Processors: Healthcare professionals and patients

Each node has its own copy of the blockchain, and the SmartAccess contracts



Funded by the European Union

Attributes-Based Access Control

PAP (Policy Administration Point)

- Authorisation policy management

PDP (Policy Decis

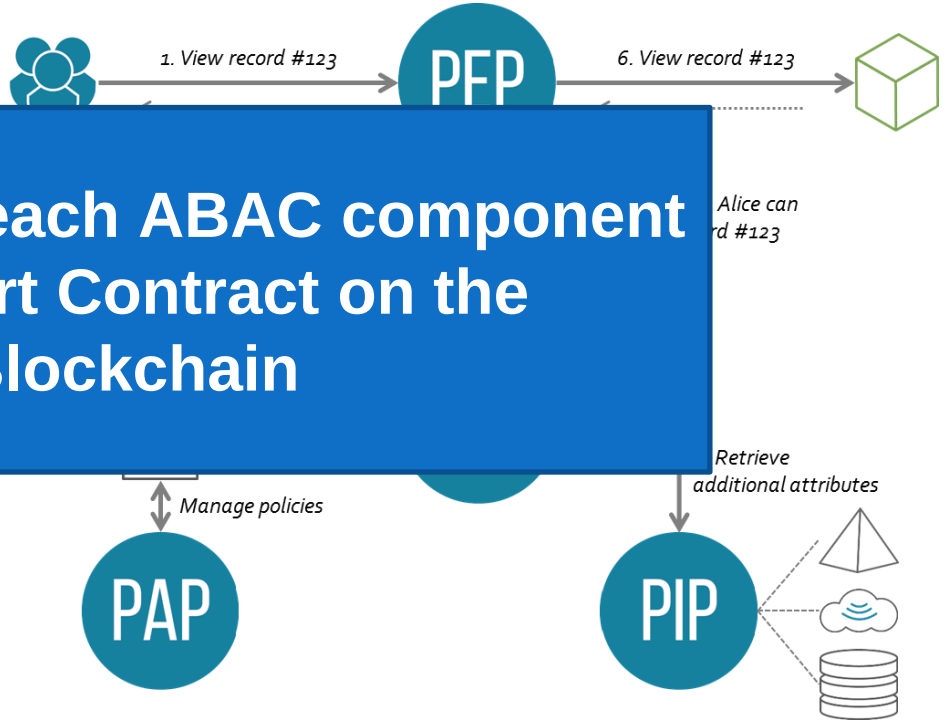
- Evaluation c
  according to
  before defin

PEP (Policy Enfor

- Intercept ac
  user, make
  access decisions and act on the
  decision

PIP (Policy Information Point)

- System entity that acts as a source of attribute values

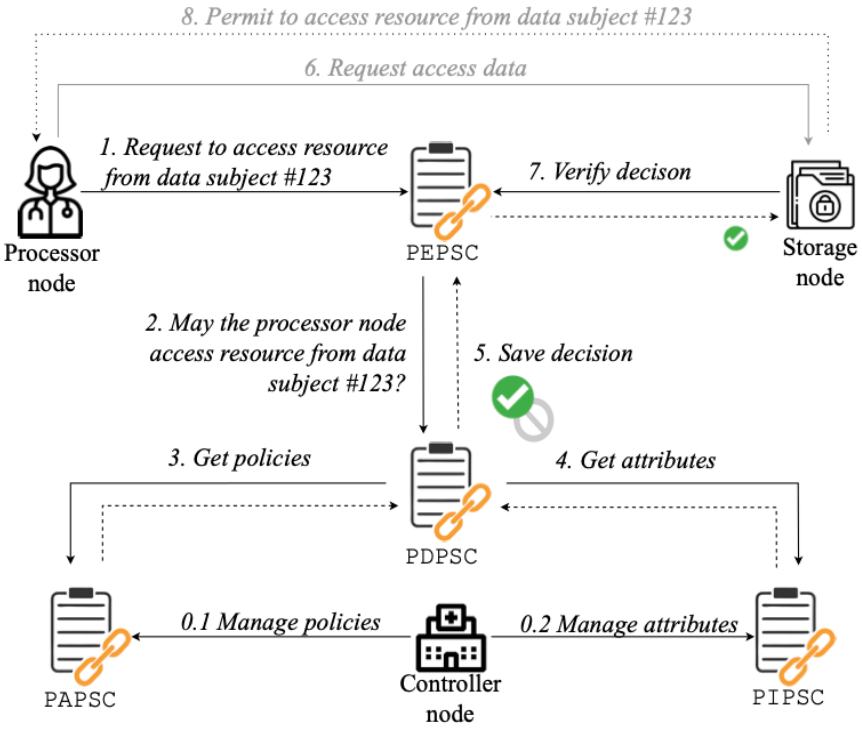


Execution of each ABAC component in a Smart Contract on the Blockchain

Funded by
the European Union

SmartAccess: ABAC

- SmartAccess contracts communication flow
  - Each contract represents a component of the Attribute-based Access Control (ABAC) mechanism
- Access control is performed on-chain (steps 1-5 and 7)
- Data access is performed off-chain (steps 6 and 8)



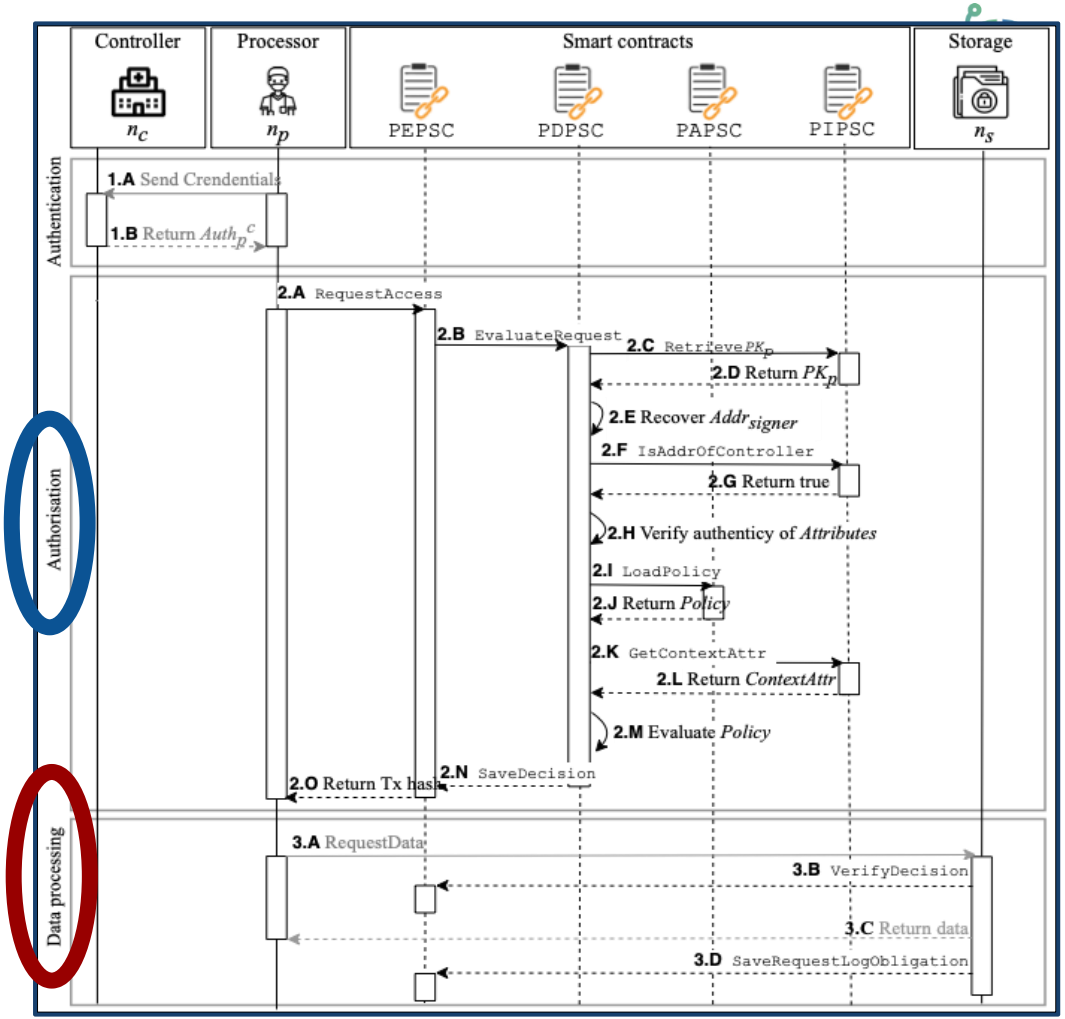
Funded by the European Union

Access control flow

Three major steps

- Authentication
- Authorisation
- Data Processing

SmartAccess play its role in the authorisation step and data processing



Funded by the European Union

Policy evaluation

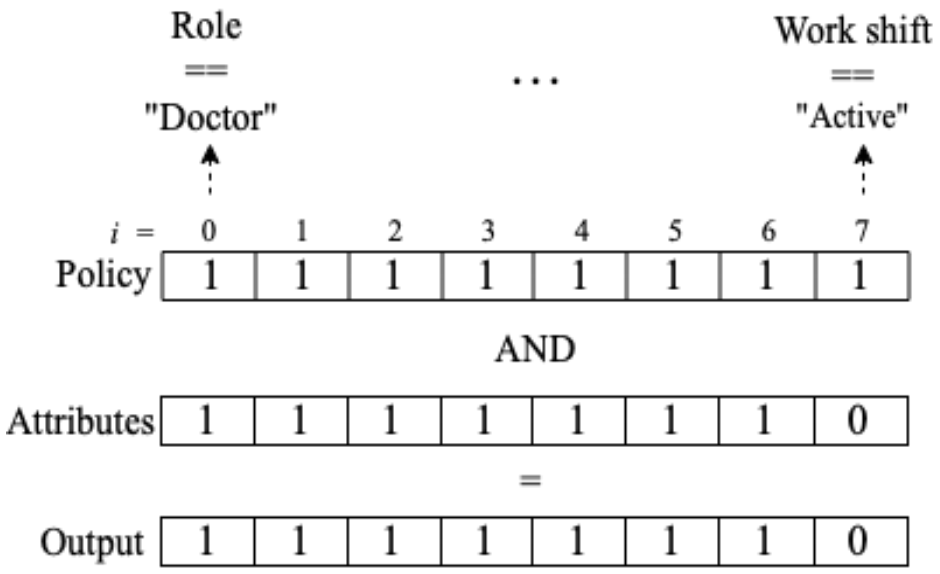
The definition and evaluation of a policy is done with an array of bits

Bit 0 - Processor does not have a specific attribute

Bit 1 - Processor has a specific attribute

The attributes (auth token) of a processor is generated by its controller (e.g. hospital generates doctor attributes).

The evaluation of a policy is done using an **AND** logical operator between ***policy*** and ***attributes***



Funded by the European Union

Policy evaluation : Contextual attributes

The policy evaluation also performs a contextual attribute evaluation, which is not part of the policy definition array

```
IF policyCompliant
    IF requiresContextualAttribute
        IF contextualAttributeCompliant
            YIELD decision = permit
        END IF
    END IF
END IF
```

The evaluation of contextual attributes is programmatically defined inside the smart contract

Funded by
the European Union

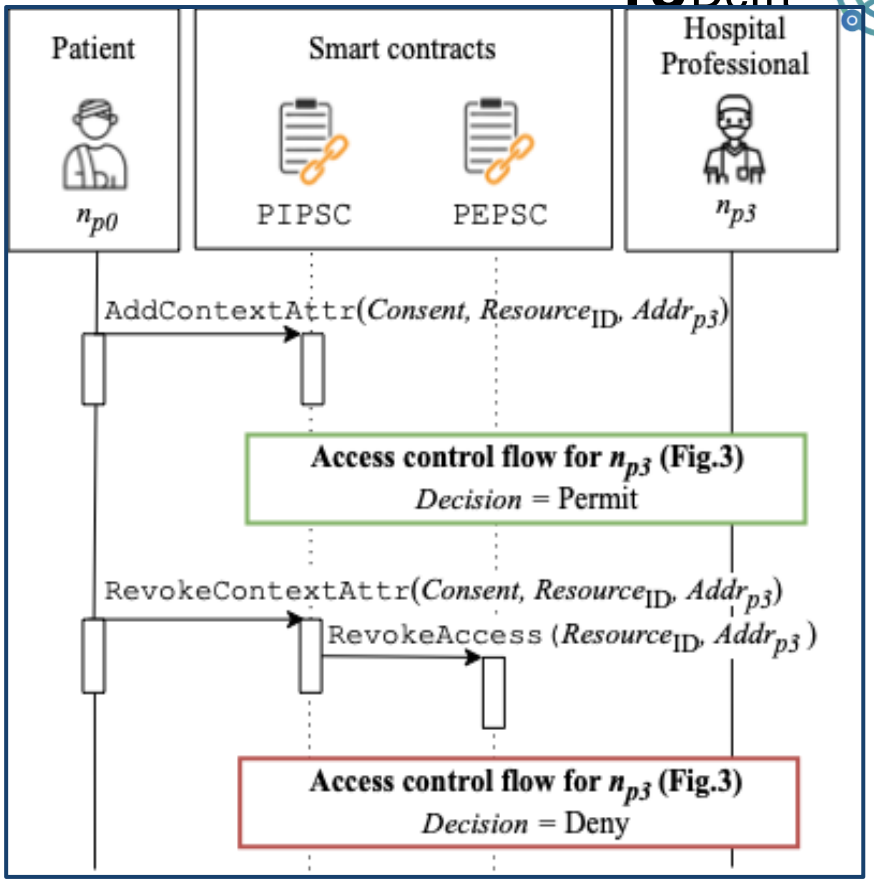
Usage: access with consent

Patient gives consent before professional goes through access control

Professional performs access control

- Including policy and contextual attribute evaluation

Patient retrieves consent after the professional has finished the consultation

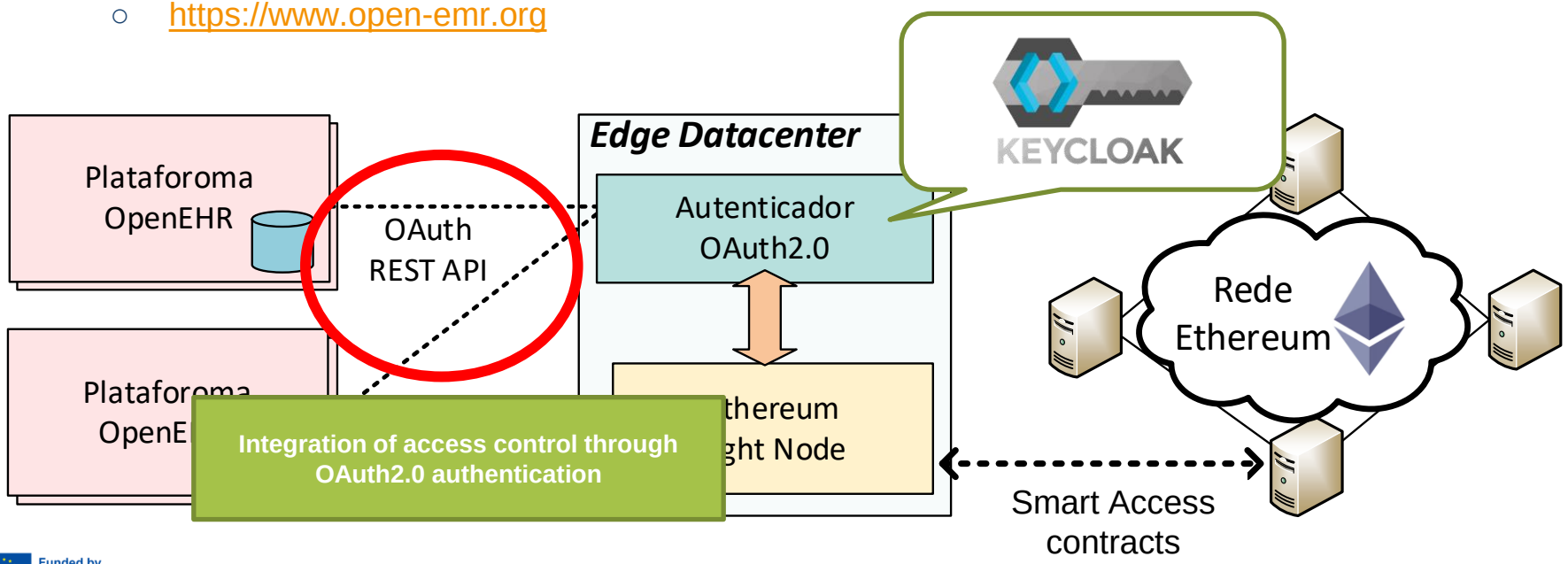


Funded by the European Union

Integration of medical Open Data source with SmartAccess

Cross-platform integration with attribute-based access control (ABAC)

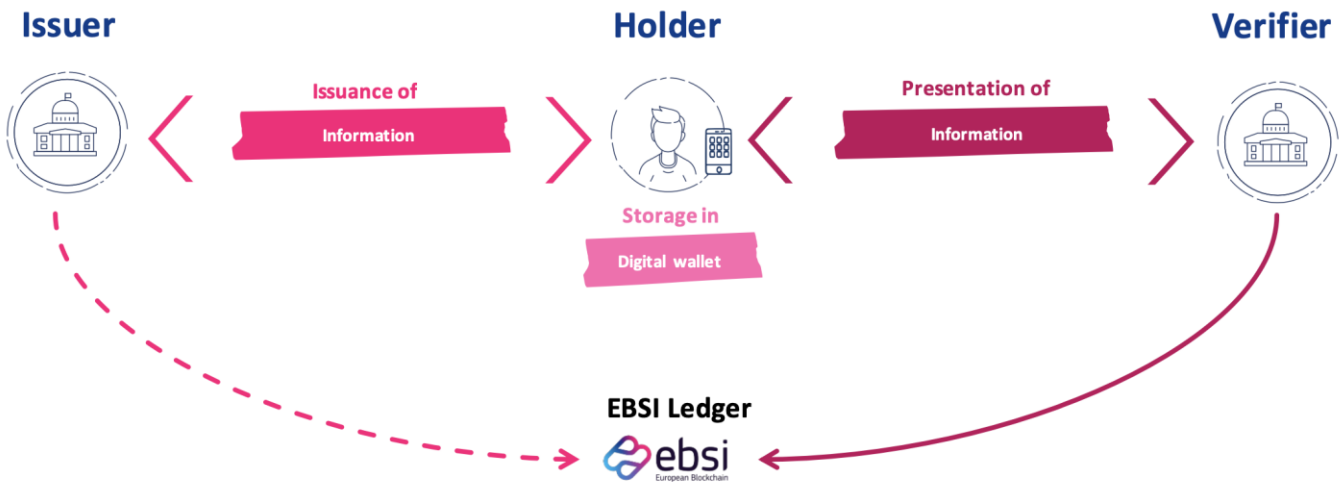
- Execution of ABAC through smart contracts on the Ethereum Network
- https://www.openehr.org
- https://www.open-emr.org



Funded by
the European Union

Direct verification/ self-sovereign scenario.

A new pattern for sharing information



Funded by
the European Union

Challenges associated to the self-sovereign scenario.

Technology can help

We aim at significantly easing the verification of information in a Citizen to Business (C2B) and Citizen to Government (C2G) context. VERIFIABLE CREDENTIALS are an essential but not sufficient element to achieve this objective . There are two other challenges:

Issuer

Verifiable Credentials must be supplemented by a Trust Model for Issuers

Holder

Verifiable Credentials must be supplemented by a trusted (Digital) Identity of Citizens

Verifier

- Business or
- Government

Can I trust the Issuer of the Verifiable Credential?

Can I trust who is presenting the Verifiable Credential?

Funded by the European Union

How does it work?

Step 1. Issuance of a Verifiable Credential which is then stored on an EBSI conformant wallet

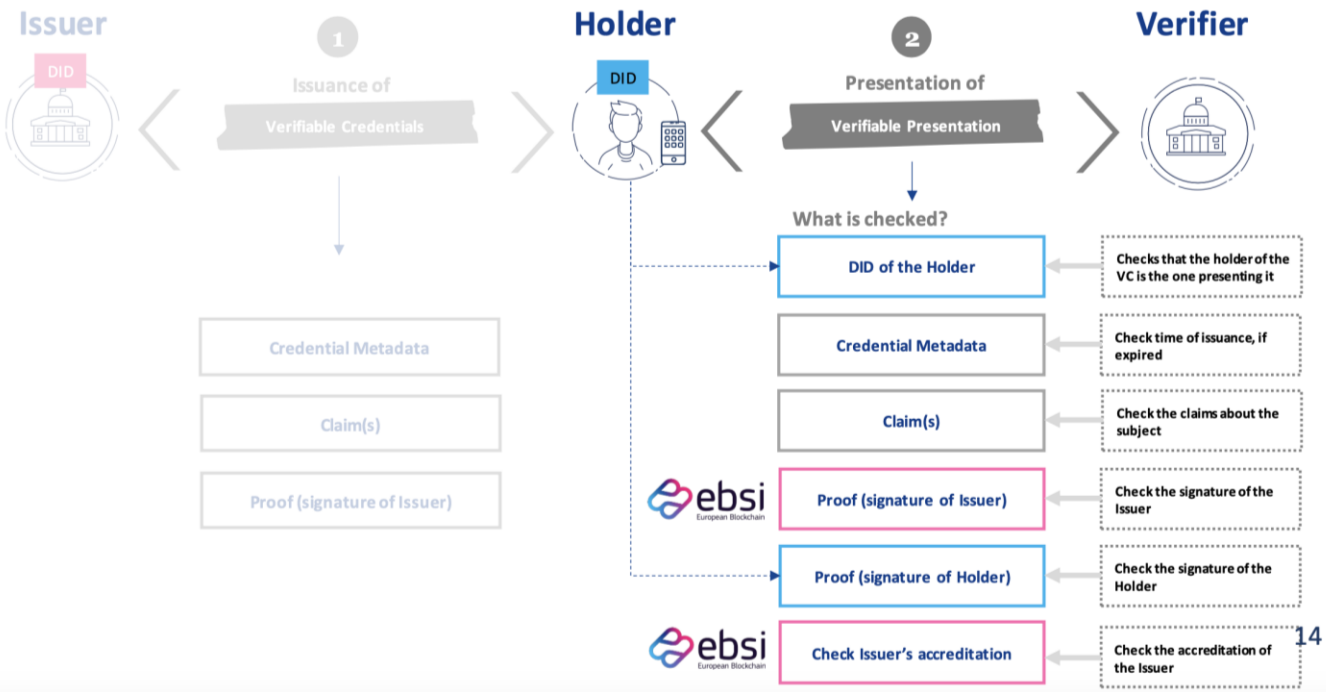
What does it contain?

Credential Metadata	> The DID of the entity that issues the credential > The status of the credential (Issuance Date, Expiry date)
Claim(s)	> The DID of the Holder of the credential > The claims about the subject (What the issuer asserts about the subject)
Proof (signature of Issuer)	> Digital proof to make the credential tamper-evident (One or more cryptographic proofs that can be used to detect tampering and verify the authorship of a credential).

Funded by the European Union

How does it work?

Step 2. Presentation of a Verifiable Credential for verification



14

There are three different approaches to digital identity

The Holder's Digital Identity can be asserted in different ways

My Identity

My Digital Identity

National Approach

Authenticate to national services

eID means

- National
- Sectorial

Federated Approach

Authenticate to services that trust your IDP

Federation within a country

Cross-border authentication such as eIDAS (high LoA use cases)

Social Network login (low LoA use cases)

Self-sovereign Approach

Share credentials and authenticate to services that trust Trusted Issuers

European SSI

Authentication (Verifiable ID - based on the eIDAS common data set)

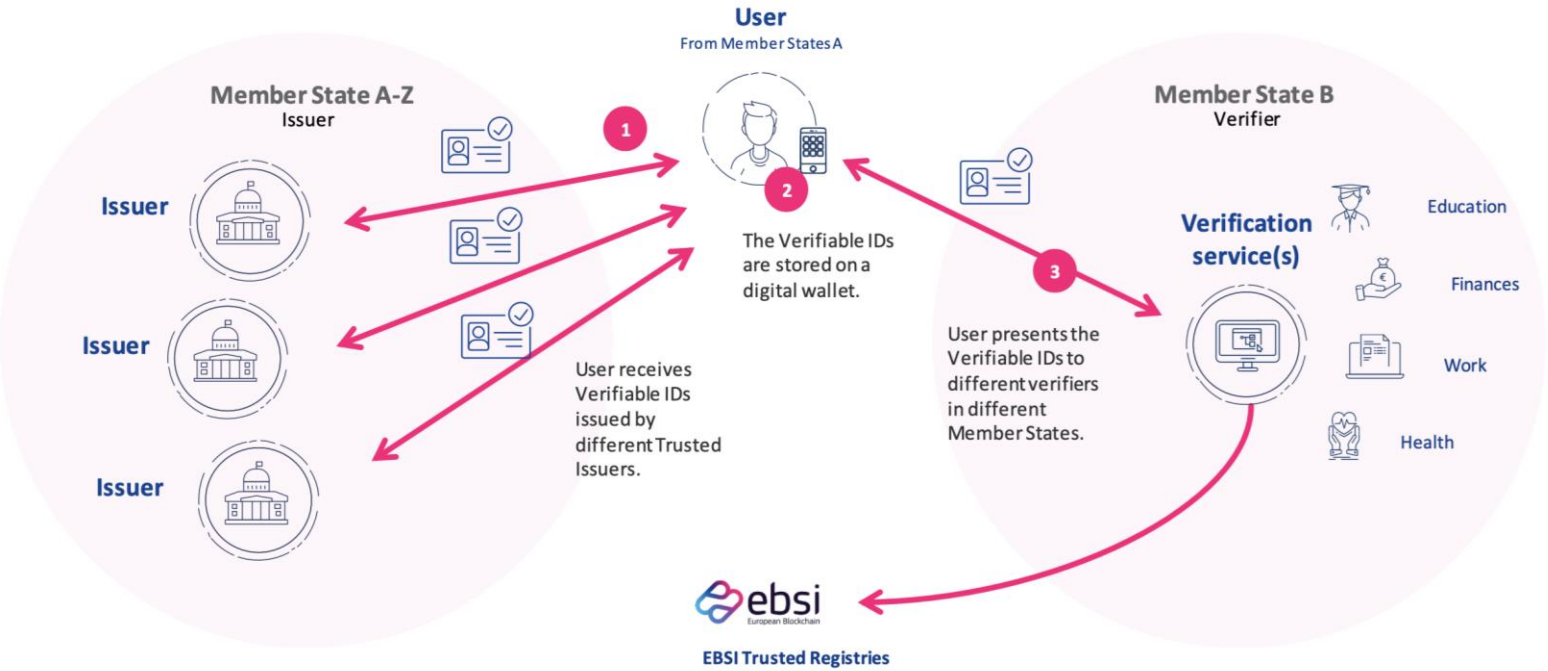
Verifiable Credentials exchange

Funded by the European Union

Based on the work of the European Self Sovereign Identity (ESSIF) initiative part of EBSI

The Self-sovereign Approach – How does it work?

The Self-sovereign Approach – How does it work?



Funded by the European Union

Group Assignment

How to unlock the power of distributed access control using digital identity?

How to overcome the privacy challenges related to authentication with verifiable credentials and DID?

1. What are the main challenges of ensuring privacy during the authorization phase in the SmartAccess with digital identity management?
2. What are some potential solutions to the privacy challenges identified in the workshop?
3. What are the potential advantages and limitations associated with implementing these solutions?
4. What ethical considerations must be considered when designing and integrating digital identity solutions into the SmartAccess?

Funded by the European Union

Guidelines

Participants will work together to propose a solution or set of solutions to the challenge questions.

Each group will have a designated moderator to guide the discussions and ensure the proposed solutions are feasible and practical.

Privacy impact assessment: Participants will be asked to conduct a privacy impact assessment for their proposed solution involving digital identity management systems.

The groups can then present their findings and recommendations to the rest of the groups.

Extra: Should the authentication consider:

- Which type of digital identity?
  - National Approach
  - Federated Approach
  - Self-sovereign Approach
- Verifiable credentials?
  - Decentralized Identifiers (DID) Methods to process the Personal Attributes stored in the Blockchain after the execution of the smart contracts?
  - Could zero-knowledge proof validation work?

Funded by the European Union

Presentations and Conclusion

Winners

Funded by
the European Union

ExtremeXP

Experiment driven and user eXPerience oriented Analytics for eXtremely Precise outcomes and decisions

https://extremexp.eu/