InteropEHRate

EHR in people's hands across Europe

INTEROPEHRATE HR SECURITY AND PRIVACY PROTOCOLS

IEHR 1ST ESB MEETING – NOVEMBER 7TH 2019, BERLIN

Sofianna Menesidou

UBITECH ubiquitous solutions

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826106

PRESENTATION OUTLINE

- Terminologies
- Problem Statement
- State of the Art
- Solutions Implemented
- Conclusions & Next Steps

TERMINOLOGIES

- **Identity Management:**
  Identity management (IDM) is the mechanism or objects used by entities to manage the claims about their digital identities.
- **Identification:**
  Is the act of indicating a person or a thing's identity.
- **Authentication:**
  Is a security mechanism that allows systems to identify a user as a registered user by providing information to prove the user is who he/she claims to be.
- **Consent Management:**
  Consent management (CM) is a system, process or set of policies for allowing consumers and patients to determine what health information they are willing to permit their various care providers to access.

PROBLEM STATEMENT

- Health data are **sensitive data** and **security** is necessary.
- Citizens want to have **control** of their data. Consent Management
- Healthcare Professionals want to **access** citizen's data. Cross-country Identification, Secure Transfer (Integrity check)
- Hospitals want to know whether the patient is **who he claims to be**. Cross-country Identification

"I want to have control of my own data."
"I want my data to be disclosed only to authorized users upon my signed consent.

"I want to access citizens' data"
"I want the data not to be altered"

"Data origin and citizens' identification is necessary"

Missing

Integrated approach for securing healthcare data, including:

- **Cross-border identification and authentication in health sector**
- **Identification without Internet**
- **Consent management in a standard way**

STATE OF THE ART

Security of Health Information

- Identity management, authentication and consent management are crucial parts of security.

Current Status

Identity Management & Authentication

- **usernames/passwords,**
- **certificates,**
- **tokens,**
- **SAML**
- **OpenID**
- **OpenID Connect**
- **OAuth**
- **Mobile Connect**
- **FIDO**

Consent Management

- **Blockchain**
- **XML-based**
  - *Advanced Patient Privacy Consents (APPC)*
  - *Basic Patient Privacy Consents (BPPC)*

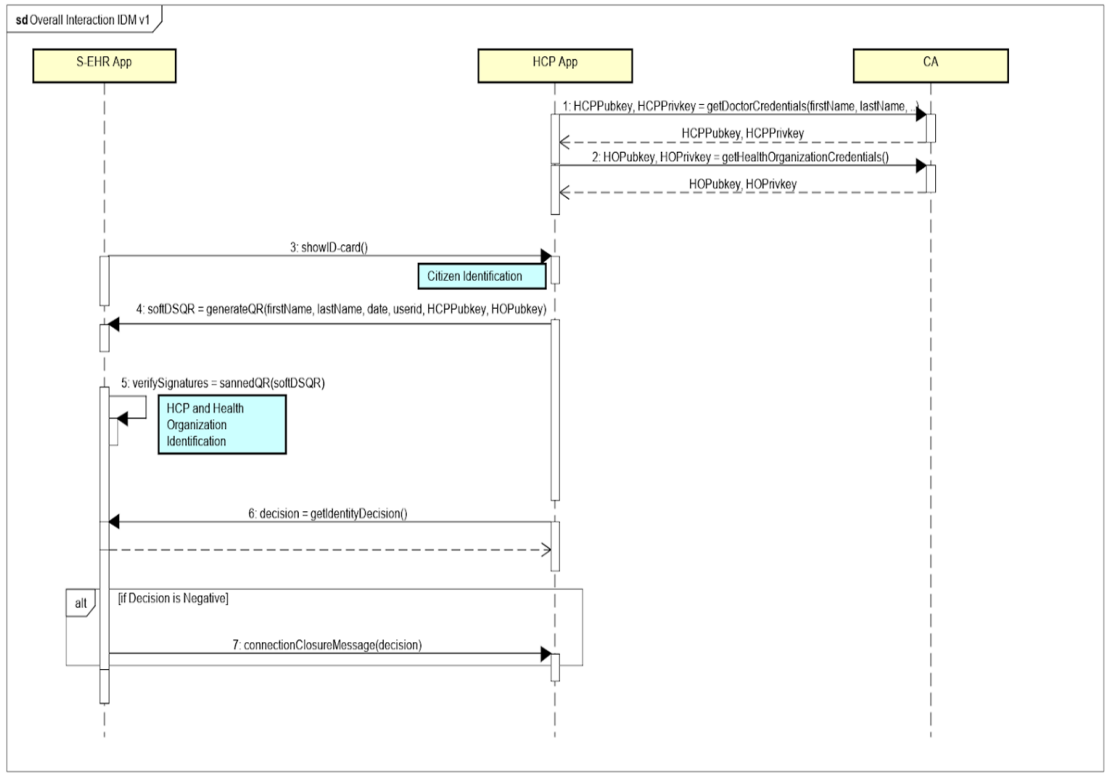
Missing

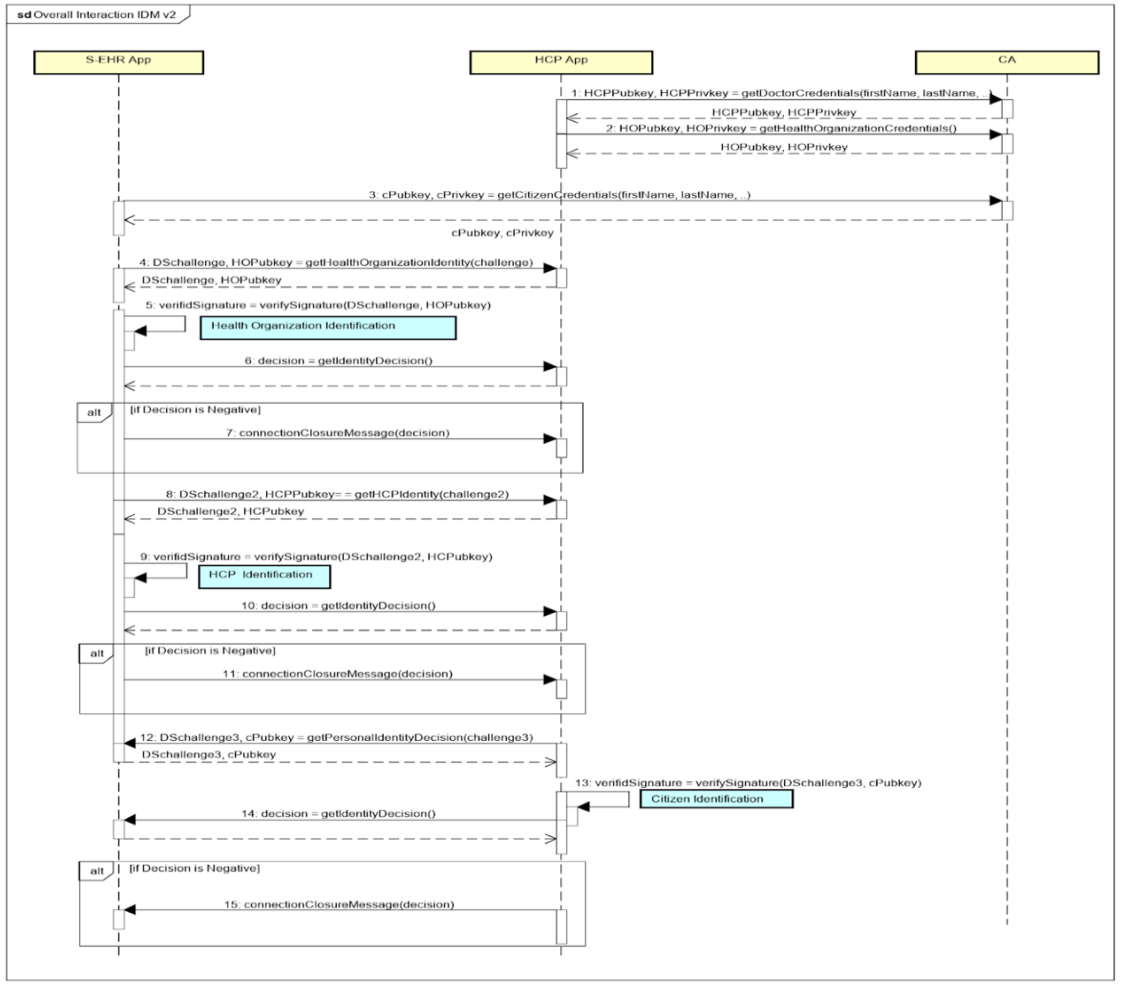
- Cross-border Identity Management and authentication (with or **without Internet** connection)
- Cross-border Consent Management (with or **without Internet** connection)

SOLUTIONS IMPLEMENTED

Identity Management & Authentication in D2D

Variant 1: ID-Card of the citizen identification & QR code generated by the hospital that includes software signature of the HCP
Variant 2: Hardware signatures (qualified) signatures for eIDAS regulation compliance on both parties





Novelties:

- **Identification without Internet Connection**

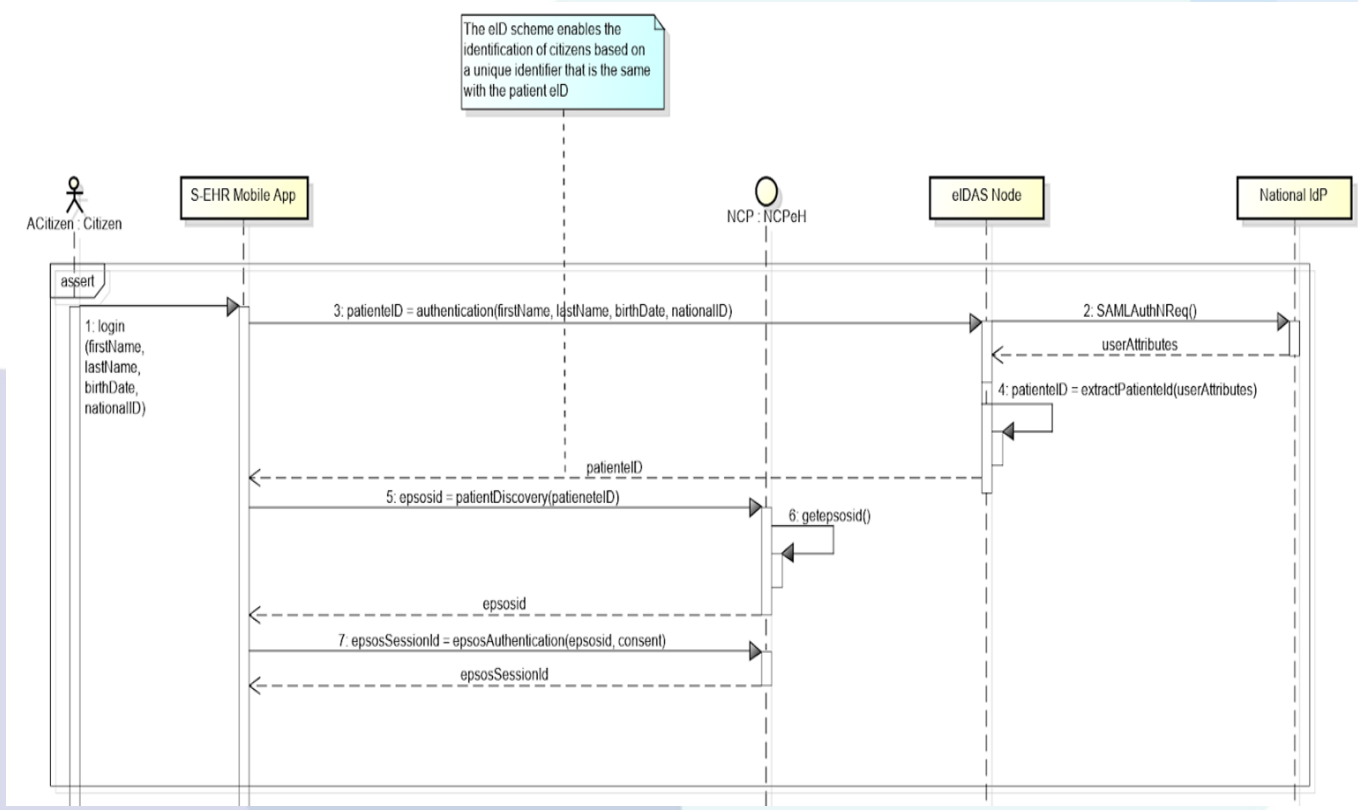
SOLUTIONS IMPLEMENTED

Identity Management & Authentication in R2D

- **Import data from National Contact Point (NCP) by extending EPSOS project**
- **Usage of an Authentication Proxy to support multiple authentication mechanisms implemented per country.**

Novelties:

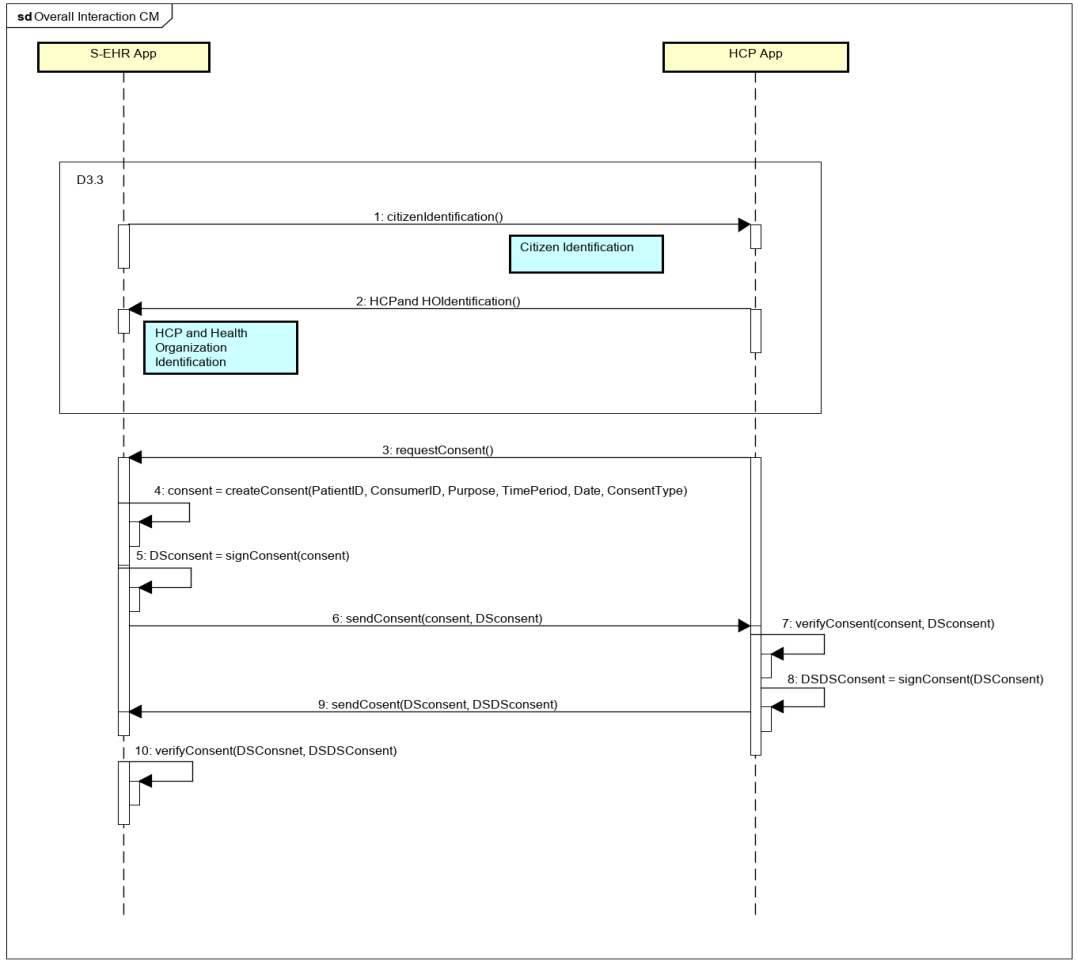
- **eIDAS compliance**
- **FIDO 2FA support**
- **eHDSI extension**



SOLUTIONS IMPLEMENTED

Consent Management & Authentication in D2D

- **APPC Consent – XML-based Consent**
- **Digitally Signed**



IMPLEMENTATION STATUS

User Requirement	Main Actor	SW Application	Implementation
Enabling of HCP and healthcare identification from HCP app	HCP	HCP App	fetchCertificate, createPayload, signPayload
Consent to S-EHR data management	Citizen	S-EHR Mobile App	verifyAPPCConsent, signAPPCConsent
Enabling of Citizen identification from S-EHR	Citizen	S-EHR Mobile App	fetchCertificate, fetchHCPCertificate, verifySignature
D2D authorization to download and upload S-EHR data from HCP App	HCP	HCP App	getAuthenticationMeans, getAuthattributes, get2FAmeans, authenticate, bindUserWith2FA, authenticate2FA
Consent to store Citizen's data	HCP	HCP App	generateAPPCConsent, signAPPCConsent, verifyAPPCConsent
Data provenance tracking	Data user	S-EHR Mobile & HCP App	Focus on the next year
Integrity of medical information	Data user	S-EHR Mobile & HCP App	Focus on the next year
Confidentiality of medical information	Data user	S-EHR Mobile & HCP App	Focus on the next year

NEXT STEPS

- **Qualified certificates for D2D and why**
- **Encryption during storage / Cloud storage – S-HER app**
- **Encryption in transit / Communication**

Thank you!

Q&A time.

InteropEHRate

EHR in people's hands across Europe

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826106