D51.5 – Legal aspects and evaluation of implemented citizen services

Document Identification	
Date	30/10/2015
Status	Final
Version	Version 1.1

Related SP / WP	SP 5/WP 51	**Document Reference**	D51.5
Related Deliverable(s)	D51.4	**Dissemination Level**	PU
Lead Participant	ULD	**Lead Author**	Hannah Obersteller
Contributors	Jessica Schroers (KUL)	**Reviewers**	Colette Cuijpers (RU) Kovila Coopamootoo (UNEW)

Abstract: This deliverable is dedicated to legal issues arising from the implementation of the pilot applications within the "Citizen Services Pilot". It focusses on the use cases that were practically implemented.

This document is issued within the frame and for the purpose of the *FutureID* project. This project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement no. 318424.

1. Executive Summary

In this deliverable, the project's "Citizen Services" pilot is described, and legal data protection obstacles are highlighted. As the goal of the task was to support the run of the pilot application(s) developed in work package 51 and not the run of a respective application in real life, the deliverable focuses on project-specific aspects. Furthermore, it only takes into account the use cases practically implemented within the project runtime.

The pilot builds on the pre-existing epSOS network, a system for cross-border eHealth services. Legal questions arising from this network are described to the extent necessary to draw a full picture in this deliverable in section 5.1.1. In section 5.1.2 the developments of FutureID are considered in relation to epSOS.

Section 5.2 is dealing with general legal data protection challenges and technical standards with respect to health data.

Section 6 provides a conclusion on the legal issues of the pilot applications.

2. Document Information

2.1 Contributors

Name	Partner
Hannah Obersteller	ULD
Jessica Schroers	KUL

2.2 History

Version	Date	Author	Changes
0.1	11/09/2015	Hannah Obersteller	First draft
0.2	19/10/2015	Hannah Obersteller	Full draft
0.3	20/10/2015	Hannah Obersteller	Extended draft
1.0	21/10/2015	Hannah Obersteller	Final review version
1.1	30/10/2015	Hannah Obersteller	Integrating review recommendations

2.3 Table of Figures

2.4 Table of Acronyms

ABC	Attribute Based Credential
AIS	Application Integration Service
ASN.1	Abstract Syntax Notation One
BCD	Binary Coded Decimal
BS	Broker Service
BPMN	Business Process Model and Notation
BPPC	Basic Patient Privacy Consents
CAS	Custom Authentication System
CDA	Clinical Document Architecture
CIP	Competiveness and Innovation Programme
DF	Directory File
ECCF	Enterprise Consistency and Conformity Framework
EF	Elementary File
EHC	Electronic Healthcare Card
eGK	elektronische Gesundheitskarte (EHC in Germany)
EU	European Union
epSOS	European Patients Smart Open Services
ESS	Extended Security Safeguards
FAR	FutureID Authentication Request

FC	FutureID Client
HCP	Healthcare Professional
HCPO	Healthcare Professional Organization
HL7	Health Level Seven
HL7 CDA	Health Level Seven Clinical Document Architecture
HPC	Health Professional Card
HTTP	Hypertext Transfer Protocol
ICC	Integrated Circuit Card
ICT	Information and Communication Technologies
IdP	Identity Provider
IHE	Integrating the Healthcare Enterprise
IHE ITI	Integrating the Healthcare Enterprise IT Infrastructure
IHE XDS	Integrating the Healthcare Enterprise Cross-Enterprise Document Sharing
ISO	International Organization for Standardization
IT	Information Technology
JSON	Java Script Object Notation
JWT	JSON Web Token
LARM	Local Attribute Retrieval and Mapping
LARMS	Local Attribute Retrieval and Mapping Service
LAS	Local Authentication Service
LIS	Legacy Integration Provider
LSS	Local Signature Service
MDA	Model Driven Architecture
MDO	Medical Data Object

MF	Master File
mTAN	mobile Transaction Number
MTOM	Message Transmission Optimization Mechanism
MTOM/XOP	Message Transmission Optimization Mechanism XML-binary Optimized Package
NCP	National Contact Point
nPA	neuer Personalausweis (identity card in Germany)
OASIS	Organization for the Advancement of Structure Information
OASIS DSS	Organization for the Advancement of Structure Information Digital Signature Service
OMG	Object Management Group
PAC	Patient Access
PACE	Password Authentication Connection Establishment
PAKE	Password Authenticated Key Exchange
PIN	Person Identification Number
PKCS	Public Key Cryptography Standard
PN	Participating Nation
PoC	Point of Care
PoS	Point of Service
RM-ODP	Reference Model for Open Distributed Process
SAIF	Service-Aware Interoperability Framework
SAML	Security Assertion Markup Language
SAML HoK	Security Assertion Markup Language Holder of Key
SOAP	formerly Simple Object Access Protocol
SSO	Single Sign On
STORK	Secure Identity Across Borders Linked

TAN	Transaction Number
URI	Uniform Resource Identifier
XAdES	XML Advanced Electronic Signature
XCPD	Cross Community Patient Discovery
XML	Extensible Markup Language

2.5 Referenced Documents

Literature

Art. 29 Working Party, “Working Document on the processing of personal data relating to health in electronic health records (EHR) (WP 131)”, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf

Art. 29 Working Party, “Working Document 01/2012 on epSOS (WP 189)”, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp189_en.pdf

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail, http://www.bfdi.bund.de/SharedDocs/Publikationen/Sachthemen/DEMail/DeMailHand-reichung.pdf?__blob=publicationFile

epSOS project, “D2.1 – Legal and Regulatory Constraints on epSOS Design-Participating Member States; epSOS Key Task 2.1.1 – Legal and Regulatory Requirements at EU level”

epSOS project, “D.2.1.2. Legal and Regulatory Constraints on epSOS Design-Participating Member States. Standard contract terms for MS Document for Engagement of Pilot Sites”

FutureID project, “D33.6 – Legal analysis of eSignature services”; http://futureid.eu/deliverables

FutureID project, “D41.6 – Legal analysis of the FutureID Broker”, http://futureid.eu/deliverables

FutureID project, “D51.2 – Technical Module and Interface Specification”, http://futureid.eu/data/deliverables/year2/Public/FutureID_D51.02_WP51_v1.2_Technical_Module_and_Interface_Specification.pdf

Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit, Hinweise zur Risikoanalyse und Vorabkontrolle nach dem Hamburgischen Datenschutzgesetz, https://www.datenschutz-hamburg.de/uploads/media/Hinweise_zur_Risikoanalyse_und_Vorabkontrolle.pdf

Legislation

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

German Criminal Code (StGB), in der Fassung geändert durch Artikel 6 Abs. 18 des Gesetzes vom 10.10.2013 (BGBl. I S. 3799), http://www.gesetze-im-internet.de/englisch_stgb/

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS)

Commission implementing regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

3. Table of Contents

4. Project Description

The *FutureID* project builds a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe, which integrates existing eID technology and trust infrastructures, emerging federated identity management services and modern credential technologies to provide a user-centric system for the trustworthy and accountable management of identity claims.

The *FutureID* infrastructure will provide great benefits to all stakeholders involved in the eID value chain. Users will benefit from the availability of a ubiquitously usable open source eID client that is capable of running on arbitrary desktop PCs, tablets and modern smart phones. *FutureID* will allow application and service providers to easily integrate their existing services with the *FutureID* infrastructure, providing them with the benefits from the strong security offered by eIDs without requiring them to make substantial investments.

This will enable service providers to offer this technology to users as an alternative to username/password based systems, providing them with a choice for a more trustworthy, usable and innovative technology. For existing and emerging trust service providers and card issuers *FutureID* will provide an integrative framework, which eases using their authentication and signature related products across Europe and beyond.

To demonstrate the applicability of the developed technologies and the feasibility of the overall approach *FutureID* will develop two pilot applications and is open for additional application services who want to use the innovative *FutureID* technology

Future ID is a three-year duration project funded by the European Commission Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318424

5. Legal Support

This deliverable is dedicated to the legal support given to the technical partners who were developing the pilot application(s) "Citizen Services". As the pilot was developed building on and extending a pre-existing system – namely the epSOS network – it is of utmost importance to note that the legal observations laid down in this deliverable solely focus on the additional FutureID-specific aspects of the pilot application. The legality of the epSOS system itself, including the consent-based processing of the patients' personal data within the epSOS network and the privacy policy of the epSOS network, were not to be reviewed but their existence and legal correctness assumed as given facts. Rather, we are focussing on legal aspects arising especially from the integration of the FutureID components. Therefore, in the following a short description of epSOS and the additional benefit through FutureID is provided, before legal questions arising from it are discussed. The legal support and evaluation is mainly based on face-to-face-meetings and conference calls with the developers. Also, the technical deliverables on the pilot implementation (WP 51) and screencasts of the pilot application were taken into account. Apart from that, all legal assessments in this deliverable take into account the general legal assessments of the FutureID components and the framework provided in earlier deliverables. It focuses on legal data protection aspects.

5.1 Use Cases

FutureID builds on the results of another European research project named „epSOS". One of its goals is to integrate its own infrastructure with the epSOS infrastructure, in order to extend the patient identification and authentication functionality of the epSOS network. Furthermore, FutureID provides an additional functionality by implementing electronic signing of the patient consent forms as they were developed by epSOS.

5.1.1 epSOS

A short description of the epSOS project and its outcomes has already been provided in the internal FutureID deliverable D51.1, and the publicly available D51.2.[1] Legal aspects of epSOS itself have been discussed within the epSOS project[2] and by the Art. 29 Working Party.[3] Some of

[1] D51.2 – Technical Module and Interface Specification, par. 9.2.
[2] Cf. epSOS, D2.1 – Legal and Regulatory Constraints on epSOS Design-Participating Member States; epSOS Key Task 2.1.1 – Legal and Regulatory Requirements at EU level; epSOS, D.2.1.2. Legal and Regulatory Constraints on epSOS Design-Participating Member States.
Standard contract terms for MS Document for Engagement of Pilot Sites",
[3] Art. 29 Working Party, "WP 189 – Working Document 01/2012 on epSOS";
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp189_en.pdf.

those findings are summarized or referenced in this deliverable. A revision of them is not envisaged.

However, for a better understanding a summary of the epSOS network is to be given first. The epSOS project developed a practical eHealth framework and ICT infrastructure that allows to access health records of registered patients cross-border from several European Member States and healthcare systems.[4] The following entities are relevant for the functionalities of epSOS which were extended by FutureID:

- NCP-A: National Contact Point in the country of affiliation (A) of the patient registered with epSOS; accesses the patient data ("health record") stored in country A and transmits it to NCP-B
- NCP-B: National Contact Point in the country of treatment (B)
- PoC: Point of care where the health care professional (HCP) the patient sees in country B is working at
- Patient: Lives in country A and has a health insurance in country A; is registered to epSOS and has his epSOS health record stored at country A; is visiting country B

The steps in the general epSOS process (as described in the epSOS deliverable D2.1.2) are the following[5]:

1. HCP at country B at a PoC accepts patient ID which may identify the patient as being eligible to take part in the epSOS trial.
2. HCP in country B at a PoC confirms patient consent to access data in country A; or HCP ticks the override box in cases where consent cannot be obtained because of patient incapacity. HCP query can be processed only with consent or override duly confirmed.
3. HCP in country B sends query to NCP in country B.
4. NCP in country B authenticates the HCP and PoC.
5. The NCP in country B queries NCP in country A for the requested patient data.
6. NCP-A authenticates NCP-B.
7. NCP-A validates patient ID and local prior consent (if applicable).
8. NCP-A transmits the requested data to NCP-B.
9. NCP-B authenticates NCP-A.
10. NCP-B provides the requested data to HCP requestor.

Processing of personal data is based on contractual agreements between NCPs and HCP resp. PoC.[6] The processing of the patients' personal data is principally to be regulated by consent

[4] http://www.epsos.eu/home/about-epsos.html.
[5] epSOS: "D.2.1.2. Legal and Regulatory Constraints on epSOS Design-Participating Member States. Standard contract terms for MS Document for Engagement of Pilot Sites", p. 31.

forms. The first consent must be obtained before any participation in epSOS happens, i.e. when the patient generally agrees that his health record is stored at the HCP-A etc. An additional consent from the patient – to the concrete encounter taking place – has to be obtained in case of medical treatment at the respective PoC in country B before the treatment begins.[7] In cases of emergency the data processing of the personal data of a registered epSOS participant can be based on art. 8 (2) Dir. 95/46/EC instead of a second consent.[8]

While epSOS developed two cross-border patient services – Patient Summary and ePrescription – FutureID focused on the Patient Summaries and how to ease the access to them for HCP, in particular how to improve the consent-based workflow that grants access to authorised people only. Therefore, two use cases were developed and implemented.

5.1.2 FutureID Development

In this section, we focus on the additional functionalities developed within FutureID.

5.1.2.1 Use case 1: access to the epSOS system using a smart card

This use case concerns a step which is not explicitly mentioned in the description of the general epSOS process described above. The HCP will not be able to print out a consent form (as needed in step 2) without having authenticated to the HCP portal of the epSOS system, as the system provides the consent form in an individually appropriate language to the HCP.[9] In this use case (as far as it concerns FutureID) only personal data of the HCP is processed, as he is the one who needs to authenticate to the system (in order to be allowed to access the personal data of the patient at a later stage).

In order to start the accessing process to the Patient Summary with epSOS, a HCP first has to access the HCP portal. In epSOS, a HCP in country B could do so, by opening the HCP online portal on his computer and typing in his username and password. FutureID developed an additional way to log in to the epSOS online portal for HCPs by using a smart card and a PIN. For testing reasons several smart cards available were supported.

---

[6] epSOS, "D.2.1.2. Legal and Regulatory Constraints on epSOS Design-Participating Member States. Standard contract terms for MS Document for Engagement of Pilot Sites", p. 19.
[7] Art. 29 WP 189, p. 7. Consent in case of processing of medical data is regulated in art. 8 (1) Dir. 95/46/EC.
[8] Art. 8 (2c) Dir. 95/46/EC: "processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent".
[9] epSO,S "D.2.1.2. Legal and Regulatory Constraints on epSOS Design-Participating Member States. Standard contract terms for MS Document for Engagement of Pilot Sites", p. 35.

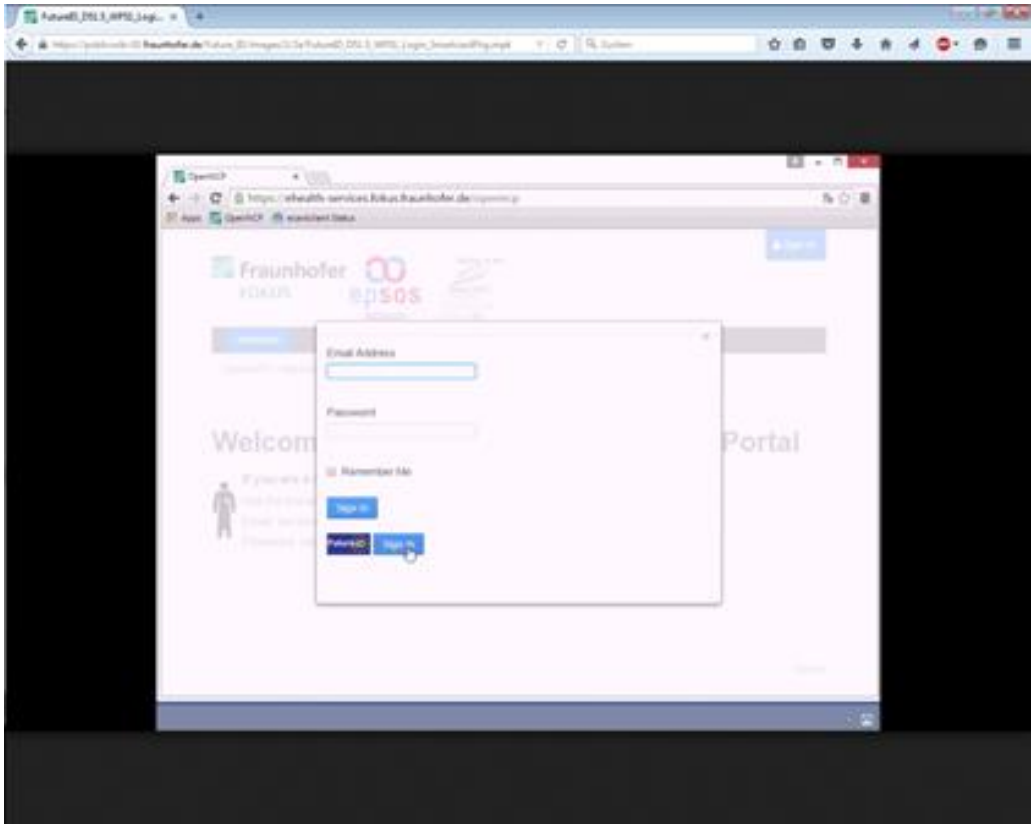

Figure 1 Log in with FutureID

The HCP chooses to log in to the HCP portal with FutureID. In this step, the first actual FutureID component comes into play. The FutureID button directs the user to the component “Broker Service”. In the pilot application, this component is run by the partner who developed it. In practice, it most likely would be run by the HCP portal or an external entity.[10] If it was run by the HCP portal (assumed that it is a separate entity) or the NCP-B, this would not change the legal responsibility with respect to data protection law, as no further legal entities would become part of the data processing. However, the personal data of the HCP the FutureID components are obtaining from the smart card and are working with, as far as it is not covered by the epSOS contracts, would have to be made part of the contract.

[10] For a general assessment of possible roles of the component Broker Service please refer to D41.6, pp. 9.

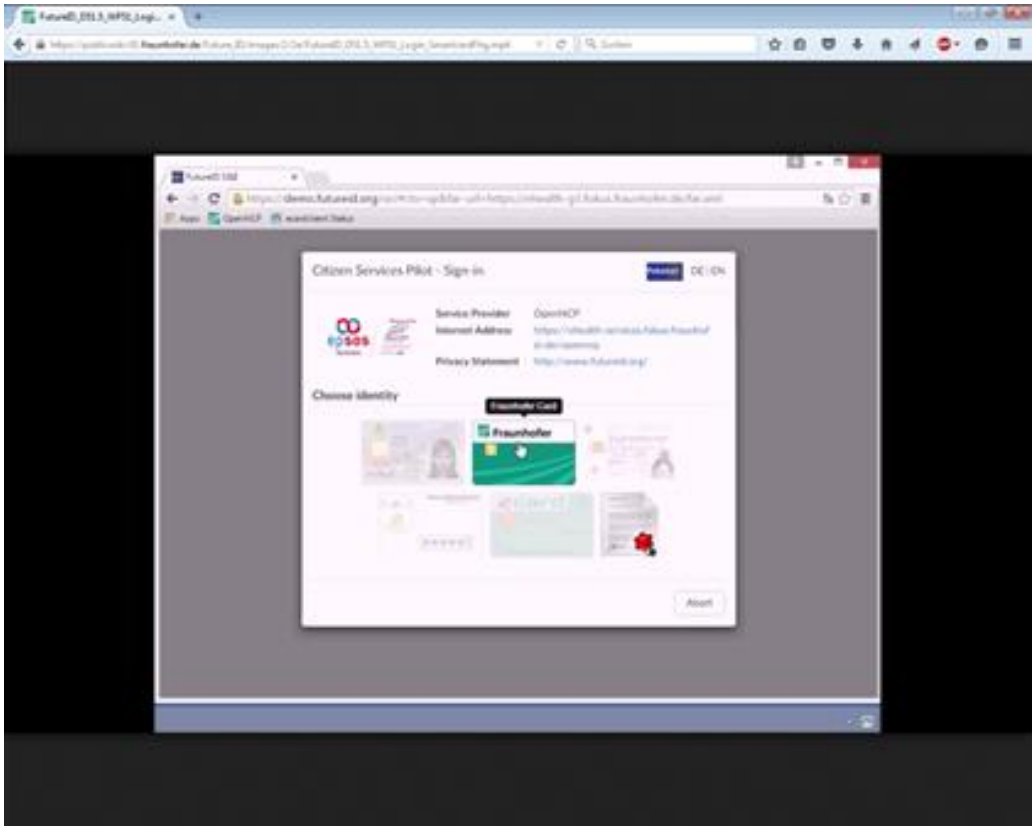

Figure 2 Choose smart card

The smart cards supported by the system are presented to the HCP. In a system like epSOS which is dealing with medical data and therefore needs a strict access control, only eIDs with an appropriate level of security should be supported in practice. As already suggested in earlier deliverables, it would be useful to take the assurance levels of electronic identification schemes as defined in the eIDAS Regulation[11] into account. For the purpose of accessing medical data, the assurance level "high" (art. 8 (2c) eIDAS Regulation) should be met by any eID supported. This means, it needs to provide a high degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto. This includes technical controls. Unlike the assurance levels "low" or

[11] Art. 8 eIDAS Regulation.

"substantial" it does not only have to be capable to decrease the risk of misuse or alteration (substantially), but to prevent misuse or alteration of an identity. This was also demanded by the Art. 29 Working Party, as it stated that "[s]pecial attention must be paid to adopting a reliable and effective electronic identification system that provides strong authentication. This applies equally to both participating staff members and patients."[12].

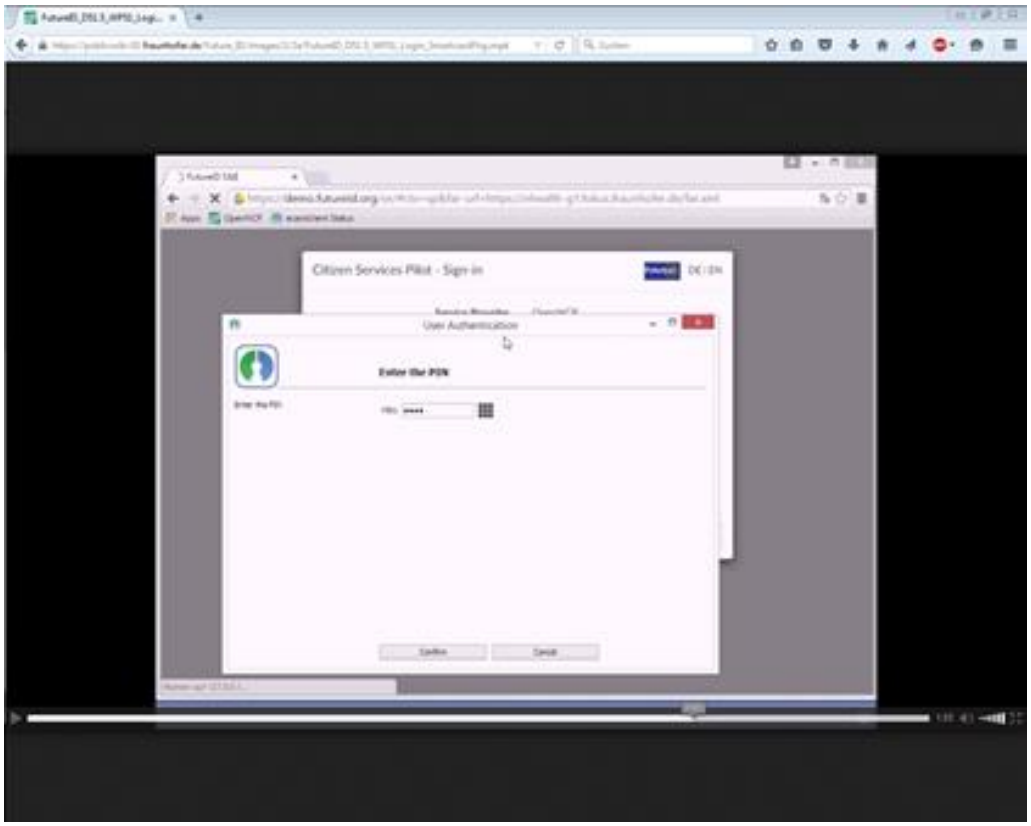

Figure 3 Entering PIN

After having been informed about the data that will be transferred, the HCP is asked to provide a PIN. This means, the authentication to the epSOS system with FutureID can be considered as more secure than the original authentication method (username/password). Also, the Art. 29 Working Party explicitly recommended the employment of smart cards as authentication

[12] Art. 29 WP, WP 189, p. 17.

means.[13] This is understandable, as the Working Party considers health data as highly vulnerable. Unlike a username/password authentication, which is only knowledge-based, FutureID introduces a two-factor-authentication. Authentication is based on possession (smart card) and knowledge (PIN). While one-factor authentication in any case only can meet the security level "low" in terms of Art. 8 eIDAS Regulation, two-factor-authentication can meet "substantial" or "high", given that the other requirements are fulfilled.[14]

[13] Art. 29 WP, WP 181, p. 15.
[14] For technical specifications of the levels of assurance please refer to the annex to the Commission's implementing regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. More detailed considerations on the levels of assurance can be found in D41.6, pp. 25.

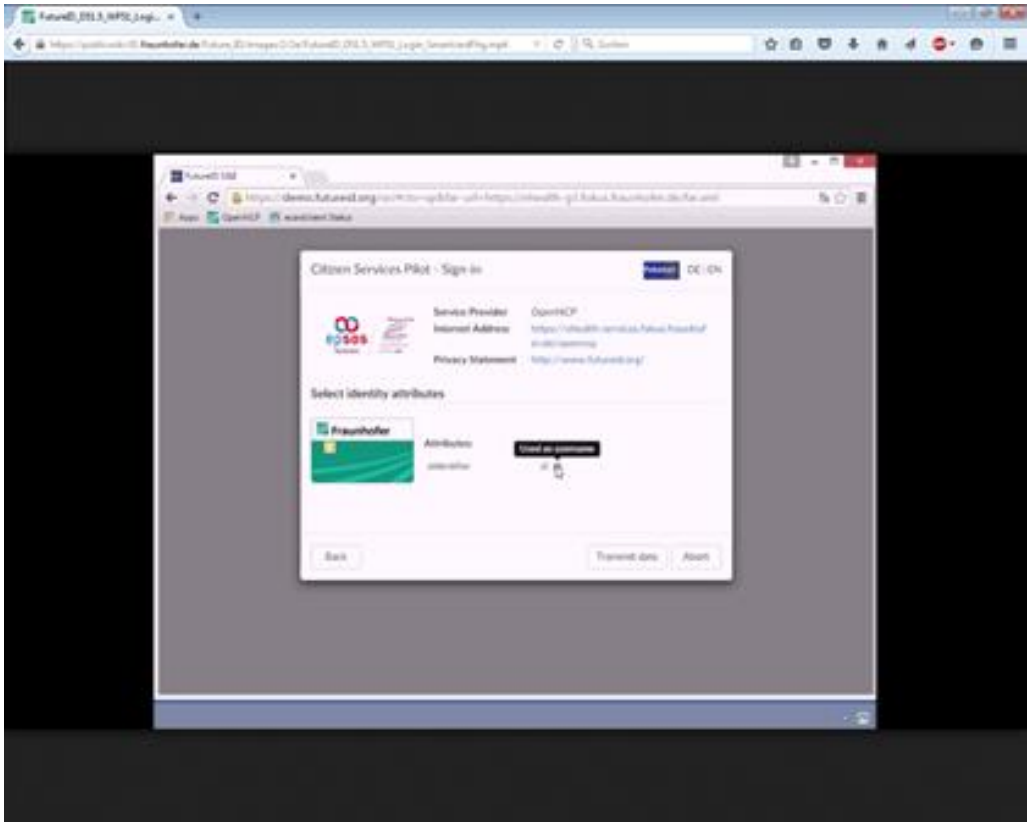

Figure 4 Transmit data

The HCP again is informed about the kind of data that is transferred to the epSOS portal. In case of the test card it is an “eIdentifer”. He actively must choose to transmit the data. Alternately he can stop the session and prevent any data transfer to the Broker Service.

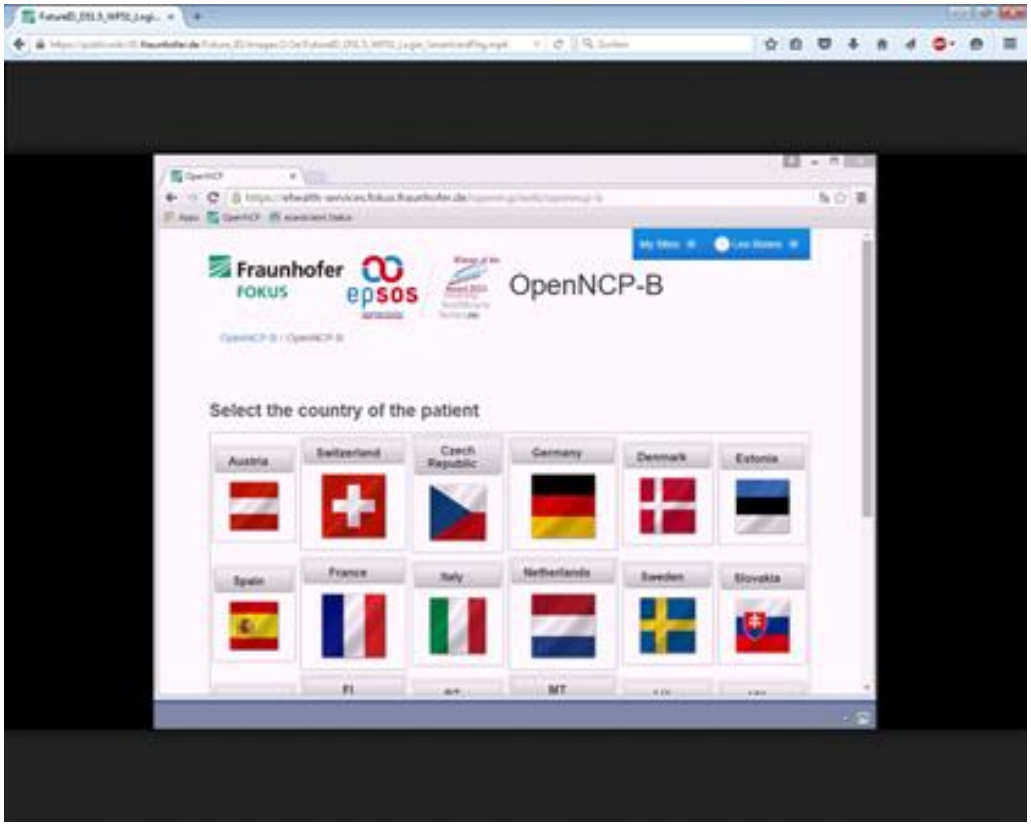

Figure 5 Access granted

After the HCP has successfully accessed the epSOS portal, he can go ahead with the actual epSOS process; i.e. step 2, obtaining the consent form in order to obtain consent from the patient in front of him. Here, the epSOS system provides the HCP with a consent form in a language the patient understands. (Cf. figure 5 above: The HCP is asked to select the patient's country of origin.)

Formatiert: Block

5.1.2.2 Use Case 2: Consent Signing

In epSOS step 2, the HCP in country B at a PoC has to obtain consent from the patient in order to be allowed to access the patient's health record. In epSOS, the only way to obtain legally binding consent from the patient at the PoC was to having the patient sign the printed form manually. Qualified electronic signatures, which have to be granted the same legal effect as handwritten signatures,[15] were not implemented. FutureID developed and implemented the "electronic signature service" (eSign service).

The legally relevant steps of the process will be described in the following.[16]

The HCP completes the patient consent form as it is provided by the epSOS system. Then he presses the "Sign with FutureID" button. Another FutureID component comes into play here: The patient consent form is shown as electronically signable document in the FutureID client, resp. its sub-component "trusted viewer". As the FutureID client is a component exclusively run on the local machine of the HCP, no legally relevant data transfer is happening at this stage.

Now, the patient can insert his card to the card reader of the HCP. The patient must be given enough time to check whether the form is filled in correctly, before he follows the instructions on the screen by entering his PIN and pressing the "sign" button. By doing so, he creates an electronic signature. Afterwards, the electronically signed form is transmitted to the HCP portal and onwards to the NCP-B. Here, only an authentication of the HCP and the PoC takes place (cf. epSOS step 4 above). In epSOS step 7, after the NCP-A has authenticated NCP-B, NCP-A validates the patient ID and the locally given consent. The NCP-A has to validate the electronic signature of the patient. In case of a successful validation, the following epSOS steps can be taken.

According to art. 25 (2) eIDAS Regulation only qualified electronic signatures shall have the same legal effect of a handwritten signature. Qualified electronic signatures are advanced electronic signatures that are created by a qualified electronic signature creation device, and are based on a qualified certificate for electronic signatures (art. 3 (12) eIDAS Regulation). However, in principle FutureID is considered as being capable to create qualified signatures.[17]

If the eSign service became part of the epSOS system, the epSOS NCPs would have to be enabled to validate qualified electronic signatures.

Therefore, they could be enabled to validate the eSignatures they receive themselves.

---

[15] For a detailed explanation of legal effects of qualified electronic signatures, please refer to D33.6, section 6.
[16] A technical description of the process can be found in D51.2, p. 20.
[17] Cf. D33.6, p.33.

Another option would be to have a qualified validation service for qualified electronic signatures validating the electronic signatures they receive. A qualified trust service provider must be able to validate qualified electronic signatures according to art. 32 (1) eIDAS Regulation,[18] and allow relying parties – in this case the NCP – to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service (art. 33 (1) eIDAS Regulation).

5.2 Legal Data Protection Obstacles

In section 5.1 it was stated repeatedly, that health data require a high level of protection. In this section, this will be explained in more detail and the major consequences for automated data processing, arising from this high need for protection, will be summarized.

5.2.1 Health data as such

"All data contained in medical documentation, in electronic health records and in EHR [electronic health care] systems are "sensitive personal data" and therefore subject to Article 8 of the Directive."[19] Medical data – in other words, personal data that "have a clear and close link with the description of the health status of a person"[20] – are sensitive data in terms of art. 8 Dir. 95/46/EC. The same holds for any other data, such as administrative data, which is relevant for documentation of the treatment of the patient.[21] This is comprehensible, as the damage caused for an individual if his health data falls in the wrong hands can be severe. The general confidentiality of health related aspects is also traditionally preserved by the professional medical secrecy of HCP.[22] In most countries it is a criminal offence to expose health data as a HCP. However, this means that appropriate security measures need to be implemented in case of automated processing of health data in order to allow HCP to obey the law.

One obvious consequence from the fact that health data is considered as sensitive can be found in the Directive 95/46/EC itself: In contrast to processing of "normal" personal data, the consent to be obtained from the data subject in case of health data must be explicit.[23] This means, for instance, a strict exclusion of opt-out solutions.[24]

[18] The requirements have been described in more detail in D33.6.
[19] Art. 29 WP, WP 189, p. 17.
[20] Art. 29 WP, WP 131, p. 7.
[21] Art. 29 WP, WP 131, p.7.
[22] Art. 29 WP, WP 131, p.10.
[23] Cf. art. 8 Dir. 95/46/EC.
[24] Art. 29 WP, WP 131, p. 9.

5.2.2 End-to-end-encryption

As far as a test of the pilot applications with real user involvement was considered, real users' health data – of course – would have to be processed in a lawful way.

Which national law applies to a data processing operation in principle depends on the establishment of the data controller, art. 4 (1a) Dir. 95/46/EC. The data controller is the central entity with respect to legal data protection responsibility. It is defined as the entity "which alone or jointly with others determines the purposes and means of the processing of personal data".[25] To carry out specific data processing operations, the controller can employ a data processor, who is defined as an entity which processes personal data on behalf of the controller.[26] Details on the definitions and the responsibilities of both data controller and data processor can be found in the FutureID deliverable D22.6.

Within the FutureID infrastructure many constellations of legal responsibility are possible. Depending on which component is run at which entity and the corresponding contractual agreements between these entities the legal situation is very different. Also the amount of entities involved in a data processing operation is of matter. This has been discussed in detail in the FutureID deliverable D41.6[27], focussing on liability aspects, and also holds for an integration of FutureID components to the epSOS system.

The partners (developing and) running the FutureID components relevant for the Citizen Services pilot both are located in Germany. As the components developed within FutureID do not have any functionality if they are not integrated into the epSOS network and consequently cannot be seen, and legally assessed, individually without having regard to the epSOS system they are meant to be integrated to, a "test NCP-A" at e.g. the developers' premises could have been built up in order to conduct tests with real user involvement.[28]

However, tests involving real users were excluded at an early stage. If the pilot application would have processed real users' health data (as it is done in epSOS), this would have happened illegally: A "test NCP-A" would have turned the partner running this component into a data controller.[29] A potential processing contract[30] – with the partners who have developed and run

[25] Art. 2 (d) Dir. 95/46/EC.
[26] Art. 2 (e) Dir. 95/46/EC.
[27] D41.6, section 7.2.
[28] An official German NCP does not exist. An implementation had been provided within epSOS, but was not accessible for the FutureID project. This means, German citizens (patients) and HCPs could not have been chosen as test users. But for practical reasons, tests with real users necessarily would have to be conducted in Germany.
[29] According to the Art. 29 WP's legal assessment of epSOS, the NCPs are to be considered as data controllers. Cf. Art. 29 WP, WP 189, p. 12.
[30] The same holds for a controller-to-controller contract, as both partners fall under German law.

the Broker Service – consequently would have fallen under German data protection law. A real-life employment of epSOS in Germany had been denied due to the fact that the epSOS system does not provide end-to-end-encryption when transmitting data from one epSOS component to another.

In accordance with the findings of the Art. 29 Working Party, which stated, that for data exchange in a system processing health data, secure communication protocols and end-to-end-encryption must be adopted, German law considers as "adequate security measures"[31] in case of transmission of health data measures which offer the security level "high" or even "very high" because health data in general have a high protection requirement.[32] This means, end-to-end-encryption with respect to data transfer is principally mandatory.[33]

Implementing end-to-end-encryption was envisaged as one use case in FutureID,[34] but was not chosen in the end. From a legal perspective, this was the main reason for advising against testing the pilot with real users' health data.

[31] In terms of art. 17 Dir. 95/46/EC.
[32] Hamburger Beauftragter für Datenschutz, Hinweise zur Risikoanalyse und Vorabkontrolle nach dem Hamburgischen Datenschutzgesetz, p. 5. https://www.datenschutz-hamburg.de/uploads/media/Hinweise_zur_Risikoanalyse_und_Vorabkontrolle.pdf
[33] BfDI, Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail, p. 6.
Also from a criminal law point of view end-to-end-encryption must be recommended, as the disclosure of information that is subject to the professional medical secrecy of HCP is a criminal offence (section 203 German Criminal Code – Violation of private secrets). End-to-end-encryption is the only reliable way to make sure that no unauthorised person gets to know the content that is exchanged via the epSOS network.
[34] Cf. D51.2.

6. Conclusion

FutureID potentially adds additional data processing to the epSOS network by involving new authentication means and components. However, at the same time it provides a higher level of assurance to the participants and therefore fosters the recognition of electronic health care systems as a feasible and legally possible solution.

Although for the concrete deployment remaining questions like the actual integration of the FutureID components into the epSOS network would have to be answered, the results allow to presume that for the aspects addressed and implemented in the pilots, a solution compliant to the law is possible. With regard to the assessment and the recommendations of the Art. 29 Working Party, it can be concluded that two shortcomings of epSOS could be addressed and partially solved: The pilot applications allow a two-factor-authentication and a more reliable way of verifying the patient's explicit consent to the access of an HCP to his health record by having him sign the consent electronically.