Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
Conférence des directrices et directeurs cantonaux de la santé
Conferenza delle direttrici e dei direttori cantonali della sanità

EPR architecture

A detailed description

Contents

SMA
31.01.2024

Schwarzenburgstrasse 157
CH-3003 Bern

www.e-health-suisse.ch

ehealthsuisse
Kompetenz- und Koordinationsstelle
von Bund und Kantonen

1 Introduction

This document provides an overview of the architecture and service landscape of the electronic patient record (EPR) in Switzerland.

From the user's point of view the EPR is a distributed document-management system designed to exchange medical data[1] and documents between healthcare professionals and patients in the context of treatment.

At the start of treatment, healthcare professionals should download a patient's medical history from the EPR and transfer it to their primary system. During treatment, or after treatment has been completed, healthcare professionals should save the data and documents generated in the course of the treatment in the patient's EPR, thus making them available for follow-up treatment or for patients' information. Patients may also record their own data and documents in the EPR.

In particular, the architecture of the EPR reflects the stringent data protection requirements stipulated for the EPR. Patients can stipulate access rights very specifically, even down to the release of documents for individual healthcare professionals. All users must use strong authentication (at least two factors), all instances of access are logged, and all technical systems connected to the EPR must be registered in the EPR and must authenticate themselves in the network layer or by the application of digital signatures to any communications sent.

2 Disclaimer

This document provides an overview of the architecture of the EPR for interested readers seeking to gain an overview of the technical implementation of the EPR. The document concentrates on the most important aspects, makes no claim to considering all aspects of the EPR exhaustively and, in particular, is not normative.

[1] Contrary to what is often claimed, structured data can also be stored in the EPR. (Core) communities must support the exchange formats stipulated in the EPRO-FDHA but may define and use exchange formats as they wish.

3 EPR architecture

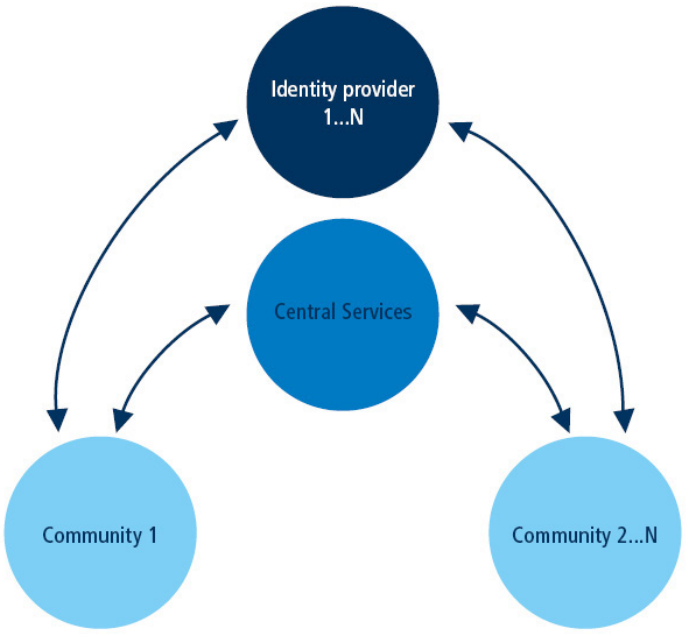

Fig. 1: Overview of the systems involved in the EPR.

EPR is a distributed document-management system comprising the following systems:

- Identity providers: Services that authenticate natural persons in the internet.
- Central Services of the federal government: services that provide data used by all (core) communities, in particular queries for definitions of EPR metadata for use in documents and searches for them, the directory of access points for (core) communities, the directory of healthcare professionals and institutions affiliated to the EPR system and a service to query the patient identification number for the EPR (EPR-SPID).
- (Core) communities: association of institutions and healthcare professionals which provide the EPR platform and the processes for operating the EPR system.
- Connected systems of healthcare professionals and their institutions: in particular, the primary systems, archive systems for documents and pictures (PACS).

3.1 Identity providers

Identity providers provide healthcare professionals and their ancillary staff, patients and their representatives as well as administrators of the (core) communities with the means of authentication required to access the EPR.

The identity providers implement the processes used to issue the means of authentication, legally valid identification, revocation, etc. and provide the interfaces used to authenticate natural persons.

The requirements which identity providers must fulfil are defined in the Electronic Patient Record Act (EPRA) and the associated ordinances (EPRO, EPRO-FDHA). Identity providers must be certified users of the EPR system. The certification criteria are stipulated in Annex 8 of the EPRO-FDHA and cover the requirements for both processes and interfaces.

In order to use the EPR, (core) communities conclude agreements with one or more identity providers which can then be used to authorise users in the portals of the (core) communities and connected systems (primary systems).

The EPR stipulates the interfaces that must be supported but, beyond this, does not set out any requirements for the architecture of the identity providers.

In accordance with Annex 8 of the EPRO-FDHA, certified identity providers must support the interfaces of the following integration profiles:

- SAML 2.0 Artifact Binding with the Artifact Resolution protocol via SOAP backchannel.
- SAML 2.0 Logout Binding via SOAP backchannel.
- Renew Protocol with EPR-specific integration profile (Annex 8 of the EPRO-FDHA) based on the WS-Trust standard.

Certified identity providers may optionally support interfaces of the following integration profiles for use in the EPR, particularly for mobile clients:

- OpenID Connect authorisation code flow with EPR-specific integration profile (Annex 8 of the EPRO-FDHA).
- OpenID Connect logout flow with EPR-specific integration profile (Annex 8 of the EPRO-FDHA).

3.2 Central Services of the federal government

The federal government operates the 'Central Services' which are required for the correct operation of the distributed architecture:

- Service to query the sectoral personal identifier for the EPR (EPR-SPID).
- EPR metadata: catalogue of the value sets of the document metadata and the value sets used to code the structured data of the exchange formats.
- Access points of the (core) communities: catalogue of the information and data required for cross-community communication.
- Directory of the healthcare professionals and institutions affiliated to the EPR: designated compilation of the institutions, healthcare professionals and groups of healthcare professionals which may be authorised by patients to access the EPR.

3.2.1 Service to query the sectoral personal identifier (EPR-SPID)

The service to query the sectoral personal identifier (EPR-SPID) / Unique Person Identification Service (UPI) implements an interface to the database of the federal government's Central Compensation Office, which also issues and manages old-age and survivors' insurance (OASI) numbers (AHVN13).

The interface supports the following functions for the (core) communities in particular:

- Query for the sectoral personal identifier for the EPR (EPR-SPID) on the basis of the patient's demographic data or AHVN13.
- Query to generate a new EPR-SPID, stating the patient's demographic data or AHVN13.
- Cancellation or deactivation of the EPR-SPID.
- Information about the status of an EPR-SPID (active, inactive, cancelled).

Communication with the UPI requires a SEDEX client to be operated in the EPR platform of the (core) communities. The SEDEX client offers the (core) communities the following interfaces:

- SOAP web service based on the eCH-0213 communication standard (query).
- SOAP web service based on the eCH-0213 communication standard (generate, inactivate, cancel).

- File interface based on the eCH-0215 communication standard (broadcast for status change).

3.2.2 EPR metadata

The service implements an interface to query EPR-compliant document metadata and to code the structured data of the exchange formats.

The interface supports the following functions in particular:

- Download of the EPR value sets from the website
- Query of the EPR value sets via an XML SOAP web service in accordance with the IHE integration profile “Sharing Value Sets (SVS)”.

3.2.3 Access points of the (core) communities (CPI)

The (core) communities access point directory service implements interfaces to query the contact data required for communication between the (core) communities. These are, in particular:

- URL and X.509 certificates of the gateways for document exchange.
- URL and X.509 certificates of the endpoint for access control.
- URL and X.509 certificates of the endpoint for access protocols.

The data are sent by the operations managers of the (core) communities to the FOPH by secure e-mail and made available to the certified (core) communities using a proprietary data format (see EPRO-FDHA) based on the LDAP protocol.

3.2.4 Directory of the service providers affiliated to the EPR

The service implements interfaces for the cross-community exchange of data from the healthcare professionals and groups of healthcare professionals whom patients may authorise for access.

The data are designated for this purpose only and contain only the data concerning the healthcare professionals, groups of healthcare professionals and institutions stipulated as a legal requirement in the EPR, in particular:

- GLN number to identify healthcare professionals.
- OID to identify groups of healthcare professionals and institutions.
- BUR (Swiss company and enterprise register) number of institutions.
- Names and addresses of healthcare professionals, groups of healthcare professionals and institutions.
- Relationships between the healthcare professionals, groups of healthcare professionals and institutions.

The data are recorded by the (core) communities. The (core) communities use the service for cross-community data exchange.

For this purpose the service supports the DSML (LDAP) and XML SOAP-based interfaces of the IHE profile Healthcare Provider Directory (HPD) with national modifications of the EPRO-FDHA.

The integrity of the data is the responsibility of the (core) communities that record the data and distribute them to other (core) communities with the aid of the directory.

3.3 (Core) communities

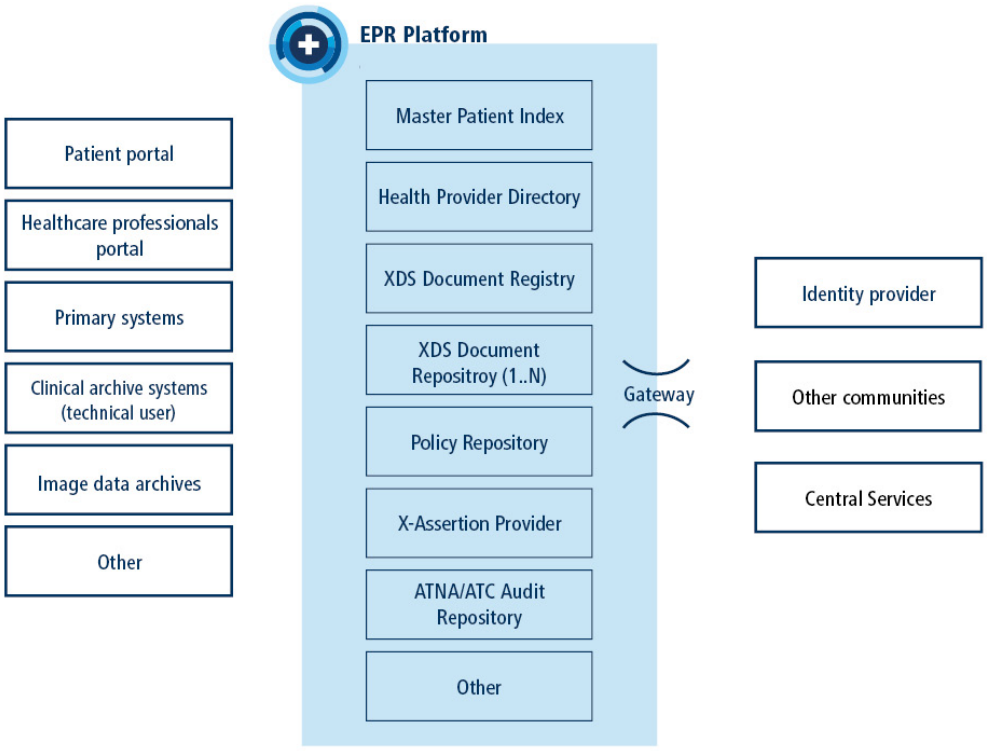

Fig. 2: Overview of the services and applications of a (core) community.

The EPRO-FDHA formulates requirements for the interoperable interfaces and data security of the (core) communities' technical infrastructure but imposes no other requirements on the architecture.

(Core) communities and their platform providers (suppliers and operators of their EPR platform) may therefore allocate the services to apps freely and in line with their own requirements. The (core) communities therefore have both monolithic and distributed service architectures.

In practice, however, an architecture that implements the services described below has become established (see Fig. 2).

3.3.1 Master Patient Index

Service to manage patient identifiers in a (core) community. The Master Patient Index in the EPR is designated for this purpose only and supports all the functions necessary for the cross-system identification of patients in the context of document management, in particular:

- Storage and management of the local identities of patients in connected systems (e.g. primary systems, archives) and associated demographic data.
- Assignment of a Master Patient ID to identify patients in the (core) community.
- Matching of identifiers using demographic data and the EPR-SPID.
- Storage of the EPR-SPID.

The data are recorded by the (core) communities initially when the EPR is opened and by the connected systems while they are in operation when new patients are registered (e.g. in patient data management systems, hospital or practice information systems, portals) and registered in the Master Patient Index.

The Master Patient Index stores all registered identifiers and the associated demographic data and assigns a Master Patient ID which can be used as an identifier in the document repositories. The Master Patient Index also detects which identifiers identify the same patient and contains a reference table with the detected identifiers and the Master Patient ID.

The connected systems of a (core) community query the Master Patient Index for the Master Patient ID of patients, which they need to search for and request documents.

For this purpose the Master Patient Index supports the following interfaces, which comply with international standards, using HL7 V3 and XML SOAP web services with national modifications of the EPRO-FDHA:

- Patient Identifier Cross-Referencing HL7 V3 (PIXV3),
- Patient Demographics Query HL7 V3 (PDQV3),
- Cross-Community Patient Discovery (XCPD).

There are plans to introduce FHIR-based interfaces. Here the intention is to support the following FHIR-based profiles.

- Patient Identifier Cross-Reference for Mobile (PIXm),
- Patient Demographics Query for Mobile (PDQm).

All calls to the service are logged in a standard format in accordance with the requirements of the IHE profiles and the national extensions, and they are stored in the ATNA Audit Record Repositories of the (core) community.

Access to the data is authenticated in the network layer (mTLS). Setting-up of connections and access are only granted to systems which are registered in the (core) communities and have valid X.509 certificates.

The data held in the Master Patient Index are designed to fulfil the minimum requirements for the cross-system exchange of documents in the EPR. The comprehensive revision of the EPR should make the service usable for other purposes as well.

The integrity of the data is the responsibility of the (core) communities and the connected systems (e.g. primary systems) which record the data. The EPRO-FDHA requires the (core) communities and connected systems to take over the trusted demographic data from the service for querying the sectoral unique person register (UPI) and, where necessary, to add contact data or other information required to operate the EPR.

3.3.2 Healthcare Provider Directory (HPD)

The service implements interfaces for the exchange of data from affiliated healthcare professionals, healthcare professionals' ancillary staff, groups of healthcare professionals and institutions and EPR administrators of a (core) community.

The data are designated for this purpose only and contain only the data required by the EPRA, in particular:

- GLN number of the healthcare professionals and their ancillary staff.
- OID of institutions and groups of healthcare professionals.
- BUR (Swiss company and enterprise register) number of institutions.
- Names and addresses of healthcare professionals, groups of healthcare professionals and institutions.
- Relationships between healthcare professionals, groups of healthcare professionals and institutions.
- Relationships between the ancillary staff and the healthcare professionals.

The data are recorded by the (core) communities or taken over from other (core) communities via the federal government's central service. Only healthcare professionals, groups of healthcare

professionals and institutions are synchronised via the central service. Data entered by ancillary staff and EPR administrators are stored exclusively in the local directories of the (core) communities.

The (core) communities make the data available to connected systems via standard interfaces, in particular for the purpose of searching for healthcare professionals and groups of healthcare professionals so that patients can administer access rights.

For this purpose the service supports the DSML (LDAP) and XML SOAP-based interfaces of the IHE profile Healthcare Provider Directory (HPD) with national modifications of the EPRO-FDHA and user interfaces for administration by administrators of the (core) communities.

There are plans to introduce FHIR-based interfaces. The intention is to support the Mobile Care Services Discovery (mCSD) profile for this purpose.

Access to the data is authenticated in the network layer (mTLS). Establishment of connections is only granted to systems which are registered in the (core) communities and have valid X.509 certificates.

The data held in the directory are designed to fulfil the minimum requirements for document exchange in the EPR. The comprehensive revision of the EPRA should make the service usable for other purposes as well.

The integrity of the data is the responsibility of the (core) communities in which the data are recorded.

3.3.3 XDS Document Registry

The EPR uses document management in line with the international Cross-Enterprise Document Sharing (XDS) standard from IHE International. The Document Registry Service implements interfaces to store XDS metadata for the registration of and search for medical documents in a distributed infrastructure.

The data in the document registry are designated for this purpose only and contain only the data legally stipulated for the EPR, in particular:

- Coded values for document type and class.
- Information about the author of the document.
- Coded values for the specialist field of the author and the institution.
- Coded information on the confidentiality level.

The data are captured by the connected systems of the (core) communities when documents are saved and are registered via interfaces.

The data can be queried by all the systems connected to the EPR via interfaces, both within a (core) community and across communities.

For this purpose the service supports the ebXML and SOAP-based interfaces of the IHE profile Cross-Enterprise Document Sharing (XDS.b) with national modifications of the EPRO-FDHA and user interfaces for administration by administrators of the (core) communities.

There are plans to introduce FHIR-based interfaces. The intention is to support the profile Mobile Access to Health Documents (MHD) for this purpose.

Access to the data is authenticated in the network layer (mTLS). Establishment of connections is only granted to systems which are registered in the (core) communities and have valid X.509 certificates.

Access to data and documents is controlled by the authorisation system of the EPR. Access control is based on access rights determined by patients. For this purpose the service uses the data from the security tokens and the access control services in the EPR.

All calls to the service are logged in a standard format in accordance with the requirements of the IHE profiles and the national extensions, and they are stored in the ATNA Audit Record Repositories of the (core) communities.

The integrity of the data is the responsibility of the users of the (core) communities and the connected systems in which the data are recorded.

3.3.4 XDS Document Repositories

The EPR uses document management in line with the international Cross-Enterprise Document Sharing (XDS) standard from IHE International. The Document Repository Service implements interfaces to store and query the binary objects[2] of the XDS documents.

The data are captured by the connected systems of the (core) communities when documents are saved and are registered via interfaces.

The data can be queried by all the systems connected to the EPR via interfaces, both within a (core) community and across communities.

For this purpose the service supports the ebXML and SOAP-based interfaces of the IHE profile Cross-Enterprise Document Sharing (XDS.b) with national modifications of the EPRO-FDHA.

There are plans to introduce FHIR-based interfaces. The intention is to support the profile Mobile Access to Health Documents (MHD) for this purpose.

Access to the EPR is authenticated in the network layer (mTLS). Establishment of connections is only granted to systems which are registered in the (core) communities and have valid X.509 certificates.

Access to data and documents is controlled by the authorisation system of the EPR. Access control is based on access rights determined by patients. For this purpose the service uses the data from the security tokens and the access control services in the EPR.

All calls to the service are logged in a standard format in accordance with the requirements of the IHE profiles and the national extensions, and they are stored in the ATNA Audit Record Repositories of the (core) communities.

The integrity of the data is the responsibility of the users of the (core) communities and the connected systems in which the data are recorded.

3.3.5 Assertion Provider (STS)

Access to data and documents in the EPR is protected by security tokens based on the WS-Trust protocol. The Assertion Provider service implements the WS-Trust secure token service required for this with the associated interfaces.

The data of the service are recorded by the (core) communities. The service uses data from other services to issue security tokens, in particular the data of healthcare professionals, groups of healthcare professionals and institutions in the Healthcare Provider Directory (HPD).

The service supports the SOAP-based interfaces in the WS-Trust standard with national modifications of the EPRO-FDHA.

There are plans to introduce OAuth-based interfaces. The intention is to support the OAuth-based profile Internet User Authorisation (IUA) for this purpose.

Access to the data is authenticated in the network layer (mTLS). Establishment of connections is only granted to systems which are registered in the (core) communities and have valid X.509 certificates.

All calls to the service are logged in a standard format in accordance with the requirements of the IHE profiles and the national extensions, and they are stored in the ATNA Audit Record Repositories of the (core) communities.

The integrity of the data is the responsibility of the (core) communities.

[2] The OASIS document management standard defines a document as the combination of the binary object and the document metadata.

3.3.6 Policy Repository

The EPR uses an authorisation concept based on the XACML 2.0 standard. Here the service implements the actors “Policy Repository” and “Policy Administration Point” from the XACML reference architecture and the associated interfaces to manage access rights in the EPR.

The data are initially recorded by the (core) communities and can be expanded or modified by patients via the portals. If tasks are delegated, healthcare professionals can also modify the settings in their primary systems or in the healthcare professionals portal. For this purpose the settings for access rights are coded in XACML policies written by the connected systems.

Patients can query the data from their portal via interfaces; if tasks are delegated the data can also be queried from the primary systems or healthcare professionals portal.

Here the service supports the SAML 2.0 and SOAP-based interfaces of the national integration profile Privacy Policy Query (CH:PPQ) in accordance with the specification in the EPRO-FDHA.

There are plans to introduce FHIR-based interfaces. The intention is to support the national integration profile Privacy Policy Query for Mobile (CH:PPQm) for this purpose.

Access to the data is authenticated in the network layer (mTLS). Establishment of connections is only granted to systems which are registered in the (core) communities and have valid X.509 certificates.

Access to data and documents is controlled by the authorisation system of the EPR. Access control is based on access rights determined by patients. For this purpose the service uses the data from the security tokens and the access control services in the EPR.

All calls to the service are logged in a standard format in accordance with the requirements of the national integration profile, and they are stored in the ATNA Audit Record Repositories of the (core) communities.

The integrity of the data is the responsibility of the users of the (core) communities and the connected systems in which the data are recorded.

3.3.7 ATNA/ATC Audit Record Repository

The EPR uses a logging system based on the IHE standard, known as the Audit Trail and Node Authentication (ATNA) profile. Here transactions are logged by the querying system and the receiving system using the Syslog standard in XML format and the DICOM standard with the national modifications of the EPRO-FDHA. It must be possible to query logged data in all (core) communities through the patient portal in accordance with the Swiss integration profile Audit Trail Consumption (CH:ATC) in a format more comprehensible to patients so that they can obtain information about instances of access to their EPR.

Here the service supports the following integration profiles and the national modifications of the EPRO-FDHA:

- IHE Audit Trail and Node Authentication (ATNA),
- Audit Trail Consumption (CH:ATC).

Access to the data is authenticated in the network layer (mTLS). Establishment of connections is only granted to systems which are registered in the (core) communities and have valid X.509 certificates.

Access to data and documents is controlled by the authorisation system of the EPR. Access control is based on access rights determined by patients. For this purpose the service uses the data from the security tokens and the access control services in the EPR.

Calls to the service are logged in a standard format in accordance with the requirements of the national integration profile, and they are stored in the ATNA Audit Record Repositories of the (core) communities.

The integrity of the data is the responsibility of the (core) communities and the connected systems which log the transactions.

3.3.8 Patient portal

In order to fulfil the requirements of the EPRA, (core) communities must implement at least one patient portal which meets all the requirements of the EPRO-FDHA.

In this context, patient portals must provide the following functions for patients and their representatives in particular:

- Display of documents and document metadata,
- Storage of patients' own documents,
- Review and modification of access rights,
- Review of the CH:ATC protocols,
- Storage and processing of administrative settings,
- Storage of contact data (e-mail, telephone number, etc.).

(Core) communities must operate at least one patient portal which is accessible via the internet and implements all the functions stipulated in the EPRA and the EPRO-FDHA. (Core) communities may additionally offer additional portals – possibly with a restricted range of functions, e.g. for special, selected use cases.

In addition to functions for the EPR, patient portals may also integrate further, commercial services if users can clearly see at all times that they are separate from the functions of the EPR.

All instances of access via the patient portal must be authenticated by a certified identity provider (see 3.1).

The patient portal must use the above-mentioned services and interfaces to access data and documents. In particular, the patient portal must not bypass the access rights and must log all instances of access in the Audit Record Repository of the (core) community.

3.3.9 Healthcare professionals portal

In order to fulfil the requirements of the EPRA, (core) communities must implement at least one access portal for healthcare professionals which meets all the requirements of the EPRO-FDHA.

In this context, healthcare professionals portals must, in particular, implement the following functions for healthcare professionals and their ancillary staff:

- Registration of patients,
- Display of documents and document metadata,
- Storage of documents in the EPR,
- Storage and processing of administrative settings,
- Storage of contact data (e-mail, telephone number, etc.).

(Core) communities must operate at least one healthcare professionals portal which is accessible via the internet and implements all the functions stipulated in the EPRA and the EPRO-FDHA. (Core) communities may additionally offer additional portals – possibly with a restricted range of functions, e.g. for special, selected use cases.

In addition to functions for the EPR, healthcare professionals portals may also integrate further, commercial services if users can clearly see at all times that they are separate from the functions of the EPR.

All instances of access via the healthcare professionals portal must be authenticated by a certified identity provider (see 3.1).

The healthcare professionals portal must use the above-mentioned services and interfaces to access data and documents. In particular, the healthcare professionals portal must not bypass the access rights and must log all instances of access in the Audit Record Repository of the (core) community.

3.3.10 Primary systems

In the EPRA, systems used by healthcare professionals and ancillary staff to support their everyday work in hospitals, homes and practices are referred to as primary systems.

Primary systems implement the above-mentioned services such as the healthcare professionals portals either directly or via intermediaries. They support the following functions in particular:

a. Reading and writing of documents in the EPR,
b. Registration of patient master data in the (core) community,
c. In some cases reading and writing of access rights for delegation (transfer of access rights, e.g. for temporary deputisation).

All instances of access to the EPR must be authenticated by a certified identity provider (see 3.1). In addition, primary systems authenticate themselves in the TLS network layer.

Primary systems must use the above-mentioned services and interfaces to access data and documents in the EPR, either deeply integrated or via intermediaries.

To ensure traceability, primary systems must log all instances of access in the Audit Record Repository of the (core) community.

3.3.11 Clinical archive systems

In the EPR, systems which save treatment-relevant documents in the EPR automatically and according to certain rules are referred to as clinical archive systems. Clinical archive systems are typically used in larger institutions (hospitals, residential homes, etc.) for archiving documents in the EPR, distribution within the institution and automatic storage in the EPR. They have a special user role (technical user) to access patients' EPR and write-only functionality.

(Core) communities must register all clinical archive systems. Archive systems authenticate themselves in the TLS network layer and use digital signatures to authenticate themselves for access control purposes.

Clinical archive systems must use the above-mentioned services and interfaces to access data and documents in the EPR, either deeply integrated or via intermediaries.

To ensure traceability, clinical archive systems must log all instances of access in the Audit Record Repository of the (core) community.

3.3.12 Image data archives

The EPR uses image data integration for X-ray images, CT studies, etc. based on the IHE XDS-I.b standard. Here it is not the image data that are stored in the repositories of the (core) communities but a reference to the image data in the image data archives. To view the image data, connected primary systems and portals download the reference data (key object selection, KOS) from the repositories and then, in a second step, the image data from the archive systems via the interfaces provided by the (core) communities.

The image data archives therefore play two roles in the EPR: as a provider of references to image data in the form of KOS objects, and as a provider of image data (e.g. DICOM studies) for the connected primary systems and portals.

Image data archives must use the above-mentioned services and interfaces to access the EPR when registering image data. They must authenticate themselves in the TLS network layer and use digital signatures to authenticate themselves for the purpose of access control (see 3.3.11).

Access by primary systems and portals to image data (e.g. DICOM studies) is controlled by the (core) communities, which also enforce the access rights.

To ensure traceability, the picture archives must also log all instances of access in the Audit Record Repository of the (core) community.

4 Appendix

4.1 Authorisation in the EPR

The authorisation system of the EPR reflects the requirements for data protection and data security stipulated in the EPRA and the EPRO-FDHA, in particular:

- Every read and write access to the EPR must be strongly authenticated.
- Natural persons must authenticate themselves to a certified identity provider, and technical systems must identify themselves using X.509 certificates which have previously been registered in the (core) communities.
- All (core) communities must enforce the access rights set by the patients in their (core) community.
- Extended access rights exist for emergency access by healthcare professionals, provided patients have not precluded emergency access.
- Healthcare professionals can inherit access rights from groups of healthcare professionals of which they are a member.

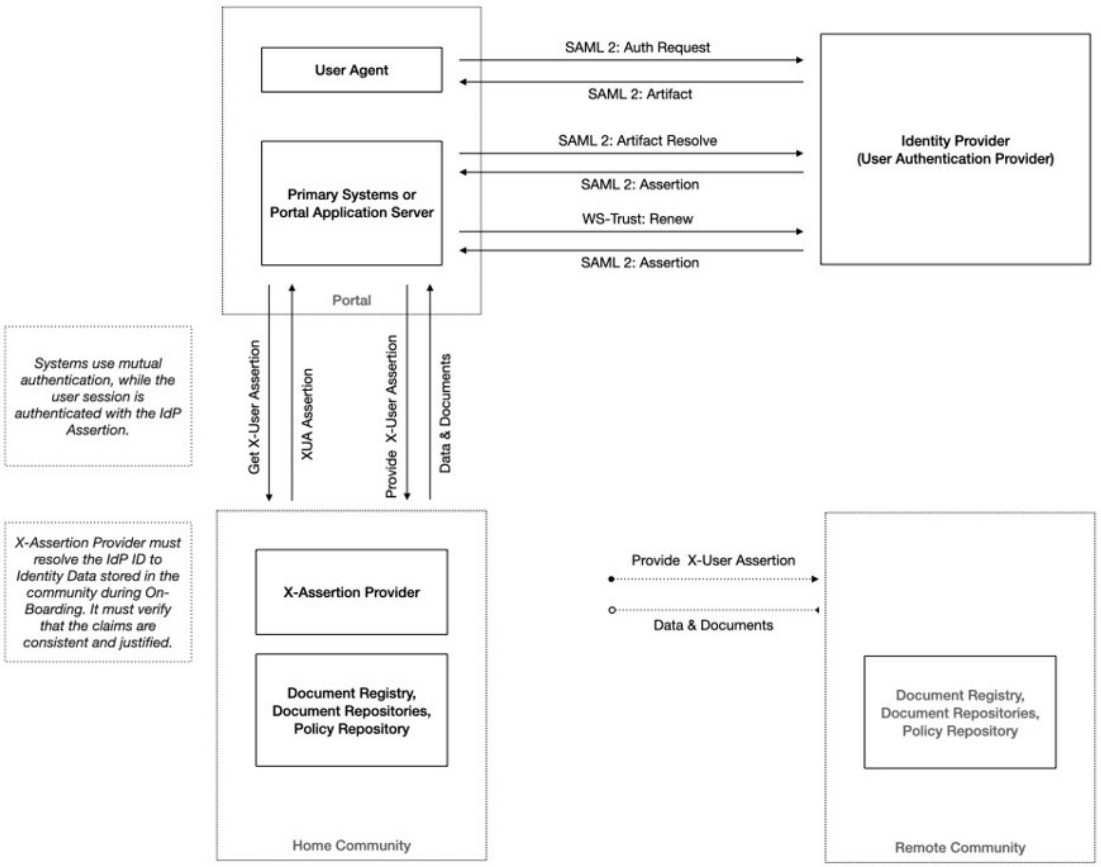

Fig. 3: Authentication and authorisation of access by natural persons in the EPR.

The authentication and authorisation of access to the EPR by natural persons is organised as follows (see Fig. 3):

- Natural persons who wish to access the ERP from portals or primary systems authenticate themselves to a certified identity provider (IdP or IHE XUA user authentication provider). Here the portal or primary system implements the steps of the SAML 2 Artifact Flow or WS-Trust renew protocol, each with the national modifications of the EPRO-FDHA.
- If authentication is successful, the identity provider responds with an IdP assertion in SAML 2 format which identifies the natural person in the EPR. The IdP assertion contains only minimal attributes that identify the person, and in particular no information about the context of the access (e.g. emergency access).
- Portals or primary systems exchange the IdP assertion for an authorisation token (X-user assertion) containing information about the context of the access and further attributes necessary for authorisation (e.g. the healthcare professional responsible for ancillary staff). Here access is authenticated by the certified identity of the identity provider.
- Portals and primary systems use the authorisation token in the security header of transactions to access services (e.g. to query documents) in the EPR.
- The services use the information in the authorisation token (X-user assertion) to implement access rights. Here they query access control to the Policy Repository Service of the patient's (core) community, in some instances in the form of a cross-community query.
- In all the above transactions the technical systems authorise each other reciprocally in the network layer (mTLS).

Note:

- The revision of the EPRO-FDHA now allows identity providers to use the Open ID Connect protocol with national modifications of the EPRO-FDHA to authenticate natural persons in the EPR. Here the above-mentioned process steps have been retained, the only difference being that Open ID Connect can also be supported instead of SAML 2.
- The intention of the comprehensive revision is to support the integration of native mobile apps by introducing OAuth to authorise access.

More information about the comprehensive revision of the EPRA, transitional funding and annual revision