Italian Electronic Health Record: a proposal of a Federated Authentication and Authorization Infrastructure

M. Claudia Buzzi¹, Francesco Donini¹, Abraham Gebrehiwot¹, Alessio Lunardelli¹, Cristian Lucchesi¹, Paolo Mori¹

¹ CNR-IIT, Pisa, Italy

Abstract. The Electronic Health Record (EHR) is a systematic collection of electronic health information about patients that can improve health care and personal safety through more accurate evidence-based decision support. EHRs comprise medical history, medication and allergies, immunization status, laboratory test results, radiology images, vital signs, personal stats such as age and weight, demographics and billing information. EHR is in digital format so can be shared across different healthcare settings/organizations. Healthcare organizations, primarily in different regions/local governments, can have different architectural solutions, procedures and access control policies, thus making it necessary to adopt a single Federated infrastructure model. Furthermore, data stored in the EHR Infrastructure concerns the health status of patients so are critical, and their confidentiality and integrity must be protected by proper security support. In this paper we present some ideas on how to manage federation and security issues for the management of the Electronic Health Record in Italy.

Keywords: eHealth, Electronic Health Record, SOA, infrastructure, federation, security.

1. INTRODUCTION

The Electronic Health Record (EHR) is a systematic collection of electronic health information about patients that can improve health care and personal safety through more accurate evidence-based decision support. EHRs can include medical history, medication and allergies, immunization status, laboratory test results, radiology images, vital signs, personal stats such as age and weight, demographics, billing information and other information that can be distributed to different Health Care Organizations (HCOs). EHR is in digital format so can be shared across different health care settings/organizations. Some healthcare agencies also provide a patient summary containing all relevant information such as blood group, allergies, vital medicines and others; the patient summary is very useful in emergencies or to describe the general health conditions of a patient. The development and use of
Electronic health record systems (EHR) will improve coordination of healthcare services. Different health care organizations follow different procedures, and thus may have various access control policies [1], so there is the need to define and implement common rules supported by infrastructure solutions for the effective administration and direction of EHRs.

In order to facilitate the creation of the Electronic Health Record by reassembling data maintained in different health care organizations, the Italian Ministry for the Public Administration and Innovation is supporting the process of building an interoperability framework for EHR management; this framework will allow all citizens and authorized health professionals to access the EHR wherever they are located. The health information will be available for primary uses such as emergency assistance or evidence-based decision support, but also for epidemiological studies, administrative purposes and government.

A basic requirement for the technological infrastructure of the interoperability framework is that it should be compliant with the architectural solutions previously developed by the different regions/local governments. This requirement can be satisfied using a single federated infrastructure model that allows each entity to follow the overall model implementing its own technology choices and business rules. An additional requirement concerns the technological infrastructure that needs to be consistent with Italian law regarding the Public Connectivity System (SPC), which specifically regulates the rules for the Public Administration communication. Furthermore, since data stored in the EHR Infrastructure concern the health status of patients (and are thus sensitive and highly confidential), their confidentiality and integrity must be protected by proper privacy and security support although it may be necessary to access them (for instance, in emergencies) [1]. Finally, Italian guidelines for privacy in managing electronic health records [2] are based on patient consent: each patient can choose his/her access control policies, specifying whether his/her EHR should be created, for how long, who if anyone may access a specific document of the electronic health records, and the time interval when he/she can have access.

In this chapter we will describe the analysis of federation and security aspects for management of the infrastructure for Electronic Health Records in Italy; this work is an early result of the Italian OpenInFSE project, that specifically support the process of building an interoperability framework for EHR management. After related work, we will illustrate the interoperability framework of the Italian Public Connectivity System (SPC) and the proposal for the interoperability framework for Electronic Health Record (EHR) systems developed in the OpenInFSE [1] project. After this presentation, the core of the topic will be described with a discussion on federated identity management and security aspects and issues, and the solutions for the management of the security policy. Conclusions will end the chapter.

---

2. RELATED WORK

Creation and management of the Electronic Health Record is a topic widely discussed in the literature, specifically regarding the benefits and opportunities that EHR offers, but to the best of our knowledge few papers specifically concern infrastructure aspects. Bergmann et al. presented a survey of architectural approaches for EHR architecture, proposing a model for a virtual shared EHR that combines a patient-centered integration policy with provider-oriented document management and developing a system prototype [4]. A dated paper (2002) discusses priorities and trends in development of the EHR infrastructure, describing the implementation of the infrastructure for the regional health information network of Crete, Greece [5]. In 2006, Eyers et al. proposed a prototype for secure, scalable access control infrastructure for management of the EHR in the United Kingdom. The system was based on an OASIS open architecture for secure interworking services, using the CASSANDRA language to express role-based access control policies with the distributed model PERMIS. Our proposal is similar but we use XACML (eXtensible Access Control Markup Language, [3]) for access control policies [1].

Data protection is a main concern in the adoption of EHR in a real scenario. Several studies have been performed to determine the security of the solutions adopted to implement EHR in several countries. As an example, in 1995 the British Medical Association (BMA), asked R.J. Anderson to analyze the main threats to the system developed by the UK National Health Service (NHS) to manage personal health information. In [6, 7], he reported some issues in the NHS threat model, security policy and architecture, and he defined a new security policy model by “translating the traditional ethics of the profession into a concise set of rules that would provide a clear and unambiguous basis of communication between patients, clinicians and policy makers on one hand, and computer system builders on the other”. In 2005, K.T. Win [8] investigates whether current information security technologies are adequate for protecting medical data. In particular, he compares the security requirements defined by the legislations of the United States of America and Canada with the available technologies for information security, concluding that there is still room for improvement. D. Acharya, in [9], also presents an overview of the security threats in pervasive healthcare applications, and analyzes some open issues. Instead, B. Hewitt, in [10], investigates how the security features affect the use of EHR and proposed a model that incorporates into a hybrid Technology Acceptance Model a set of security measures including biometric authentication, Multiple Access Systems, and Single Sign On systems, to explore whether these measures influence the healthcare organization decision to use the Electronic Patient Record. Finally, guaranteeing secure access to clinical information is the main issue of [11], where the authors formally specify access control policies in clinical information systems by means of temporal linear first-order logic.
3. THE ITALIAN INTEROPERABILITY FRAMEWORK

The legal framework for the Italian e-Government strategy is the Code of Digital Administration (CAD, in Italian), which establishes a framework for the digitization of public administrations, thus enabling the efficiency and effectiveness of the eHealth domain. The CAD regulates the creation, management, preservation and transmission of electronic documents used by the Public Administration and promotes the reutilization of public information systems. The Code also introduces the Public Connectivity System (SPC), i.e., the connectivity infrastructure for Italian PAs, and the Public Connection and Cooperation System (SPCoop), the infrastructure for the interoperability and cooperation between Public Administrations. The Public Connection and Cooperation System is a complex system including technical communications infrastructures, services, registries, rules and guidelines (about 30 documents) for the entity connection. SPC is fully mandated by the Law on Digital Administration (CAD).

The aims of the SPC can be summarized as follows:

- Provide a set of common, shared connectivity services for administrations
- Ensure interaction of central and local administrations with anyone connected to the Internet, promoting the provision of quality services for citizens and business
- Provide a central communications infrastructure
- Provide services to administrations who wish to connect to the infrastructure
- Drive a multi-vendor delivery model for the infrastructure implementation
- Ensure data security, confidentiality and privacy on SPC systems
- Respect the autonomy of information assets of the administrations.

The governance of SPC employs a multi-layer model. The Italian National Agency for the Digitalization of Italian Public Administration (DigitPA) governs the implementation of SPC guidelines and standards in multiple ways:

- by overseeing the implementation of the national SPC communications infrastructure (including public tendering) and associated services (such as identity management)
- by evaluating IT projects in governments beforehand and afterwards, including a certification program to validate eServices that connect to SPC.

The SPC and the Applied Cooperation Services are governed according to a federal model in which a Coordination Commission (presided over by DigitPA), is responsible for strategic governance while all the entities (Regions and DigitPA) are responsible for the management of the shared resources, for their quality and security, and for the planning, implementation and development of SPC.

From a technical point of view the SPC is characterized by a three-layer architecture:

- communication infrastructure
- interoperability services
- applied cooperation services.

SPC is a fundamental instrument for achieving eGovernment objectives by defining and sharing laws, technical regulations, guidelines and standards and by sharing specific infrastructural services. The SPC model includes a Public Administration
Index (IPA) and a Registry of the SPC Coop agreements. In the Registry, service agreements which govern and specify the technical aspects of the services provided by the administrations and the cooperation agreement describing the services provided by several cooperating administrations are listed. Public administrations should adopt technical solutions which are compatible with the SPC standard (as envisaged in the CAD).

The model proposed for SPCoop is based on the following principles:

- the PAs cooperate through the supply and the use of application services; these services are offered by the single administration through a unique (logic) element belonging to its own information system called Domain Gateway. In this way the complete autonomy of the administration is guaranteed, as far as the implementation and management of the provided application services, since they can be based on any application platform supplied through the Domain Gateway (which handles the routing of the application requests of a node -- administration or structure -- towards the SPCoop infrastructure). The fruition of the application services is carried out through the exchange of messages, whose format is formally specified in the Italian standard referred to as e-Gov Envelope. Such a standard is basically an extension of SOAP and represents the data structure used for the interactions between the domains, also ensuring all security principles.

- service works on the basis of an agreement between at least two subjects (supplier and client); such agreements have a technical basis and an institutional/jurisdictional basis. These agreements should be formalized in order to support the development and the life-cycle of services in a (semi-)automatic way. The agreement specification is called Service Agreement and is based on the XML language.

In order to support these principles, SPCoop includes the following components:

- **Agreements Repository** is the software component used to register and maintain the Service Agreements. It can be considered the “database” that allows cooperation. This component offers functionalities for the registration, access, update and search of the agreements.

- **Schemas/Ontologies Repository** is the software component that offers functionalities to deal with the service and information semantics, in order to discover services that are most suitable for providing the required functionalities. This component acts as a structure to store ontologies and conceptual schemas, offering functionalities of registration, access, update and reasoning on them.

- **Federated Identity Management** is used to authorize and control access to application services over SPCoop; the federation is needed to reuse the already in-place identity management systems of regional/national authorities. Integration is done through specific interfaces supporting SAML v2.0.

- **Monitoring Service** for the monitoring of the Service Level Agreements (SLAs).
A service agreement is a well-specified XML document that regulates the relationships of an application service between a supplier and a client regarding the following aspects:

(i) service interface
(ii) conversations admitted by the service
(iii) access points
(iv) Service Level Agreements (SLAs)
(v) security characteristics
(vi) descriptions of the semantics of the service.

The public nature of the service agreement makes it easier to establish domain ontologies that allow aggregating services with similar semantics. In the context of a set of public administrations (i.e., a Cooperation Domain), services can be composed and orchestrated, thus generating other services described in turn by service agreements.

A Service Agreement describes a 2-party collaboration/cooperation, with a subject offering a SPCoop application service and another subject using such a service. Many administrative processes do not concern only a single administration, but involve different subjects. The Cooperation Domain is the formalization of the desire of different subjects to join together to cooperate for the automation of administrative processes.

---

![Fig. 1. SPC high-level architecture (© CNIPA) 2](http://archivio.cnipa.gov.it/HTML/docs/SPCoop-Introduzione%20ai%20Servizi%20SICA%20V_1.0.pdf)

The ICAR 3 (“Infrastructure for Application services Cooperation among Italian Regional authorities”) project is an Italian eGovernment initiative that addresses the

---

2 http://archivio.cnipa.gov.it/HTML/docs/SPCoop-Introduzione%20ai%20Servizi%20SICA%20V_1.0.pdf

3 www.progettoicar.it/
establishment of SPCoop infrastructure for central and local governments authorities, deliver interoperability (IO) and applications cooperation (AC) services to them. The ICAR initiative was started approximately in June 2006 and basically is an implementation of the SPCoop specification. Since the management of electronic identities and security policies in Italy is left/delegated to the Regions, the ICAR initiative is attempting to implement an interregional Federated Authentication System. The ICAR project covers 16 Italian regional authorities and the autonomous province of Trento, i.e., almost all Italian authorities are covered by the project.

4. OPENINFSE INTEROPERABILITY FRAMEWORK

All the medical documents relating to the same patient could be stored in different Italian health care organizations and each organization could have different architectural and organizational systems. In order to avoid loss of data (health information scattered throughout the territory) and to allow localization and propagation of the health information, the OpenInFSE project has designed an infrastructure for EHR. The OpenInFSE project in fact specifically aims to implement an operational infrastructure to support interoperability for the management and recomposition of health records (HER); the infrastructure is able to operate at a national level by integrating all healthcare organizations involved in the production or consultation of events related to a patient.

OpenInFSE meets the basic requirements for the eHealth:

- Multiple actors create and own (remaining responsible) health information according to different roles
- Multiple actors use health information according to different authorizations
- Multiple uses of health information (primary and secondary).

To allow logic interaction between HCOs, the OpenInFSE project uses infrastructure components developed ad hoc and localized in the Regions and the HCOs (all or just one for administrative district), depending on the Region’s interoperability policies. The architectural model of the EHR, based on decentralized and distributed architecture, is then composed of first-level nodes and second-level nodes (local nodes, the HCOs: hospital, laboratory test agency, pharmacies, etc.). The nature of the node is determined by the numbers of the components present (some or all) within the node:

- first-level nodes (Regional nodes): independent nodes that contain all the infrastructure components. An independent node is able to ensure all the features related to retrieval and management of the information

---

4 [http://ehealth.icar.cnr.it](http://ehealth.icar.cnr.it)

5 Primary uses are clinical uses; secondary uses are administrative uses, government uses, research uses, etc.
• second-level nodes (local nodes): a local node can contain some or all infrastructure components. In the first case is called Assisted local node, in the latter Complete local node, similar to the Regional node.

At least each first-level node should be connected to the EHR infrastructure through a Domain Gateway, in order to allow SPC-compliant inter-regional communications, whereas a local node could be connected through its own Domain Gateway or indirectly through a Regional Node.

The EHR model is SOA (Service Oriented Architecture) based on three levels:
1. Connectivity Layer: the Public Connectivity System (SPC) used for cooperation between administrations through the exchange of "eGov Envelope"
2. Component Layer: specific infrastructure components developed ad hoc for EHR infrastructure
3. Business Layer: services to support medical processes, such as “ePrescription”.

Services can be identified as part of the actors participating in the information process.

The Components layer extends partly the SPC architecture; the components proposed by the OpenInFSE for this infrastructure are:

Access Interface (AI): present in each node (regional or local). The AI represents the access point of the infrastructure and receives all the requests made by regional actors (e.g., healthcare professionals or paraprofessionals, administrative staff, but also patients, who can access their EHRs) or by an AI of other regions. The AI interacts with other infrastructure components to fulfill the request by notifying the broker nodes and the registers of the event. The AI has two functions, one is to offer access services to interact with the active actors at the local node, another function is to intercept, propagate and notify (in the infrastructure) events produced by the legacy system at local node.

Document Manager (DM): through the AI the DM is the component qualified to store documents associated with health events in a persistent, reliable and secure way; appropriate repository are located at local and regional nodes. Each node of the infrastructure, local and regional, can interact with one or more repositories through one or more components of the Document Manager.

The main operations the DM provides are:
• Retrieving of one or more health documents from one or more repository from by a initial reference
• Storing a health document into one or more repository

The Document Manager is able to process medical documents structured according to the standard HL7 CDA Rel-2.0, but could also be compatible with other formats of documents.

Federated Index Registry (FIR): through the AI the FIR serves as an index of documents and index of services. It is an index of documents because it stores information (metadata) related to medical records present in the repositories in order to facilitate search and localization. Moreover, it is an index of services because it stores service addresses represented by metadata (e.g., URIs) enabling the location of the services that expose local nodes. The FIR is made up of federated registries and
the users can access the infrastructure by means of every federated registry; generally each one of these should store information related to its own domain. Registered members of the federation are aligned with each other through a notification mechanism based on publish/subscribe paradigm events in order to manage the redundancy of metadata.

**Hierarchical Event Manager (HEM):** is the component that through the AI manages routing and notification of health events to all stakeholders. The event management in the OpenInFSE infrastructure is geographically wide so implies a distributed and decentralized solution based on a local broker federation. To make management and event notification more efficient, a hierarchical model for classification of events using a publish/subscribe model based on a broker is used.

**Security Manager (SM):** implements the security support of the EHR framework. Since data stored by the EHR infrastructure are critical, proper security support is required to protect them. The Security Manager is based on the security as a service model (commonly in object-oriented architectures), and it controls the Federated Authentication and the Authorization processes. The SM is indicated and is a unique component but it includes some other components that will be described in the following.

![EHR architectural model](image_url)
To allow SPC communication, the OpenInFSE project must be integrated in an implementation of the SPCoop specification, for instance ICAR. Each infrastructure component is treated as Cooperation Service and configured on the SPCoop solution chosen. Through a careful definition of service agreements, actors and infrastructure components from different domains can communicate easily.

5. FEDERATED IDENTITY MANAGEMENT IN OPENINFSE

Identity management is a broad administrative area that deals with identifying individuals in a network and controlling access to resources in that system by placing restrictions on the established identities of the individuals. Federated identity management is the means of linking a person's electronic identity and attributes, stored across trusted multiple distinct identity management systems.

The OpenInFSE identity management architecture is compliant with the reference implementation for Identity management released by the ICAR initiative (in the following referred as ICAR INF-3); reuse of the reference implementations is one of the requirements of the OpenInFSE project to better guarantee integration with the Regions infrastructures. At the moment, ICAR INF-3 implementation supports only the Web Single Sign On (Web SSO) profile, so compliance is possible only on this profile. Instead, the federated identity management in OpenInFSE should use two SAML profiles: Web SSO and also Web Services. In the following, we will describe OpenInFSE requirements for the implementation of a federated identity management model, based on the distinct existing identity management systems of the Italian Regions. Furthermore, the interaction of the ICAR INF-3 components for the WEB SSO profile and a solution to extend the Web Services profile for the ICAR INF-3 reference implementation will be presented.
5.1. The OpenInFSE identity management constraints

Each Italian Region is responsible for the healthcare of citizens residing within their region. In some cases, they have already implemented heterogeneous identity management infrastructures. A requirement of the OpenInFSE project is to maintain the already deployed infrastructures and to implement an interoperable federated identity management system between the various regions using the SAML2 standard protocol. The constraints are the following:

1. The identity of an individual is managed by the Italian Region where a citizen/patient resides
2. Individuals are identified by an Identity Provider (IDP) using an authentication mechanism that is decided by the Region
3. An authenticated user is identified by various attributes such as: first name, surname, date of birth, citizenship, sex, municipality of residence, stature, eye color, etc.
4. A Role Based Authorization system is adopted (see Section 6) and the role of the authenticated user is identified by various Attribute Authorities (AA) using attributes such as: general practitioner, emergency room doctor, patient, nurse, professional organization membership, administrative employee of a hospital, pharmacist, etc.;
5. The electronic identity of an individual is composed of the aggregate values of the identity and the role of the subject. The aggregation is managed by an additional authority called the Profile Authority (PA).

The services offered by the Federation are distributed among the various Italian Regional health care organizations using components called Service Providers (SP). Access to services is managed through federated authentication and authorization mechanisms. For federated identity access, the internal SPs within a particular region appoint the Local Proxy (LP) to authenticate and retrieve the appropriate profile of a user belonging to the Federation. The local proxy implements a Discovery Service (DS) to locate the origin of the user Profile Authority. The interaction between the common infrastructure components SP, IDP, AA, PA, LP and DS uses the SAML2 standard protocol.

5.2 Interaction of OpenInFSE components for the Web SSO profile

This part presents an example of interaction for the Web SSO profile. A Web browser of a user coming from Region B attempts to access a protected resource (an item of the HCR) by a Service Provider (SP) in Region A using his federated identity (see Fig. 4). In this example we will describe OpenInFSE Web SSO component interaction assuming that the user browser does not have a valid SSO session. In case of a Web browser with a valid Web SSO session, the interactions are much more simple than the one described here and many steps are carried out without needing to involve the end user.
Fig. 4. Interaction of OpenInFSE components for Web SSO profile

The SP in region A does not have the knowledge of the complexity of the Italian federated identity management system. It simply forwards every authentication and attribute request to the LP within its region. The LP is a SAML proxy. It forwards each authentication received and attributes requests, using the infrastructure of a trusted federation, to the various authorities (PA, IDP and AA) of the Italian Federation. The LP acts as PA, IDP and AA to the local SP. However, it acts as an SP when the LP interacts with the rest of the Italian Federated infrastructure. The browser redirected to the LP contains the SAML authentication/attribute request generated by the SP. If it is a valid request, the LP interacts with the user via browser to identify the proper PA of the user. At this stage the LP acts as a Discovery Service. The LP also has a trust relationship with all the rest of the Italian federation infrastructure. After the choice of the PA, the LP will redirect the user's browser to the selected PA regenerating a new SAML authentication/attribute request. At this stage the LP acts as a SAML SP with respect to the PA while the PA acts as a SAML IDP or AA to the LP. The PA in turn is another SAML proxy, so it may act as an IDP, AA, SP or a Discovery Service depending on the role it takes. The PA verifies the received SAML authentication request; if it is valid, the PA interacts with the user via the browser to identify the proper IDP of the user. At this stage the PA acts as a Discovery Service. After the user selects the proper IDP, the PA act as an SP and redirect the user's browser, regenerating a new authentication request to the selected IDP. The IDP verifies the validity of the authentication request and if it is valid, only at this stage does the user authenticate himself directly to his home region. After a valid authentication, the user's browser, containing the SAML authentication response, will be redirected back to the PA. The PA checks the validity of the SAML response and if it is valid it will offer the user the choice of the profile selection and if the user has only one profile this stage will be done automatically. In OpenInFSE it is used to select the role of the user; as one example, this stage may be necessary for medical doctors who may act as patient or as doctor. After the selection of the profile,
the PA redirect the user’s browser to the appropriate AA to retrieve the attributes for
the selected role of the user. Then the PA aggregate SAML responses obtained from
the IDP and AA and redirect/POST the user's browser back to the LP. The LP then
redirect the user's browser regenerating a new SAML response back to the SP that
originated the initial request. At this point the user will access the requested service if
the user profile passes the authorization process. Otherwise, access will be denied.
Details of the overall interaction are described in Fig. 4.

5.3 Interaction of OpenInFSE components for the Web Services

The OpenInFSE Web Services infrastructure is implemented using the OASIS Web
Services Security (WS-Security) profile with the objective of providing
authentication, data integrity, and confidentiality of SOAP messages. WS-Security
defines a <Security> element that may be included in a SOAP message header. This
element specifies how the message is protected. WS-Security makes use of
mechanisms defined in the W3C XML Signature and XML Encryption specifications
to sign and encrypt message data in both the SOAP header and body. The information
in the <Security> element specifies what operations were performed and in what
order, what keys were used for these operations, and what attributes and identity
information are associated with that information. WS-Security also contains other
features, such as the ability to timestamp the security information and to address it to
a specified Role. In WS-Security, security data is specified using security tokens.
Tokens can either be binary or structured XML. Binary tokens, such as X.509
certificates and Kerberos tickets, are carried in an XML wrapper. XML tokens, such
as SAML assertions, are inserted directly as sub-elements of the <Security> element.
The use of SAML assertions with WS-Security is described in the SAML Token
Profile. The characteristics of the use of SAML assertions as defined by WS-Security
are as follows:

- The SAML assertions are carried in a <Security> element within the header
  of the SOAP envelope as shown in Fig. 5

- The SAML assertions usually play a role in the protection of the messages
  they are carried in; typically they contain a key used for digitally signing
  data within the body of the SOAP message

- The SAML assertions will have been obtained previously and typically
  pertain to the identity of the sender of the SOAP message.
SAML assertions can be conveyed by means other than the SAML Request/Response protocols or profiles defined by the SAML specification set. The WS-Security: SAML Token Profile does not use SAML Request/Response protocols, instead it describes the usage of three subject confirmation methods: bearer, holder-of-key, and sender-vouches.

Since there is no public key or digital certificate associated with a bearer token, protection of the SOAP message, if required, must be performed using a transport level mechanism or another security token, such as an X.509 or Kerberos token, for message level protection. OpenInFSE Web Services infrastructure does not make use of the bearer subject confirmation method. The other two methods, holder-of-key and sender-vouches, used by OpenInFSE Web Services infrastructure, make use of public keys to secure the SOAP messages. When using the holder-of-key subject confirmation method, proof of the relationship between the subject and claims is established by signing part of the SOAP message with the key specified in the SAML assertion. Since there is key material associated with a holder-of-key token, this token can be used to provide message level protection (signing and encryption) of the SOAP message. The process is as follows:

- **A** = end user
- **B** = web service client
- **C** = Security Token Services (STS)
- **D** = web service

A = B (This is the Holder-Of-Key case)
B contacts C to get a SAML assertion for himself to access D. So B supplies its own certificate to C and C authenticates the certificate of B, creates an SAML assertion with B’s identity and puts the Certificate of B into the assertion, and C also signs the assertion. B sends the assertion to D and uses the key associated with the assertion to secure the message.

The sender-vouches confirmation method is used when a server needs to propagate the client identity with SOAP messages on behalf of the client. This method is similar to identity assertion, but it has the added flexibility of using SAML assertions to propagate not only the client’s identity, but also propagate client attributes. The attesting entity must protect the vouched SAML assertions and SOAP message content so that the receiver can verify that another party has not altered it. This is the preferred method for the OpenInFSE project. It allows scalability and interoperability between Italian regions in OpenInFSE and allows hiding the locally used authentication methods within each participating region. A receiver verifies that a sender digitally signs the SAML assertions with the containing SOAP message using a security token reference transformation algorithm. There should be a trust relationship between the sender and the receiver. A sender can use either SSL or SOAP message encryption to protect confidentiality. In either case, the SAML assertions are either issued by an external Security Token Services (STS) or self-issued by the application server.

A = end user, B = web service client, C = STS, D = web service
A ! = B: (This is the sender-vouches case)

B contacts C to get a SAML assertion on behalf of A to access D. The method used to retrieve the SAML assertion can be similar to the one described in the Web SSO section which involves the end user. C creates a SAML assertion with A’s identity in the assertion, and C also signs the assertion. B sends the assertion to D and uses B’s certificate to secure the message.

The federated identity management architecture for Web Services is shown in Fig. 6.
Recovery of the SAML assertions containing the user profile is previously obtained through Web SSO, as indicated in Fig. 5. The public key of the “sender” is included as a SAML attribute in the assertion. Subsequently, the interaction between the Front End and the Back End to protect the SOAP message is described in the following steps:

1. The “sender” constructs the SOAP message, including a SOAP header with a WS-Security header. A SAML assertion is placed within a WS-Security token and included in the security header. The key referred to by the SAML assertion is used to construct a digital signature over data in the SOAP message body. Signature information is also included in the security header.
2. The message receiver verifies the digital signature.
3. The information in the SAML assertion is used for purposes such as Access Control and Audit logging.

6. AUTHORIZATION

Data protection is fundamental in EHR management infrastructure, since stored data includes sensitive information that is highly confidential. Obviously, health data are critical and must be properly protected. Metadata (i.e., pointers to health data/records) could also be considered critical, since they could reveal that certain treatments or tests have been carried out on a patient, providing indirect but clear information about his/her health status. Moreover, the need for an advanced and flexible security support that provides an effective protection of the patients’ data is also stated in the Italian guidelines for the EHR management [2] issued by the Italian data protection authority.
Authorization is the decision process that determines the right of a given subject to access one of the components of the EHR infrastructure to register new data or to read or even modify the stored ones. The authorization process is performed after authentication, in which the identity of the subject requesting access has been verified, and the SAML assertions representing the attributes the subject wishes to exploit in the authorization process have been collected. The attributes collection is a very important step, because the security policy will exploit those attributes to determine the access rights. Hence, the attribute assertions must be added by the Access Interface to the access request messages sent to the Component Layer services to enable the authorization process.

The features of the reference scenario complicate the authorization phase. First of all, the clinical document related to an event (examination, surgery, treatment, and so on) are stored in the Document Manager paired with the HCO (Hospital, Laboratory) where the data were produced, even if the patient belongs to another Italian Region. This is a restriction imposed by the Italian data protection authority, that also forbids the replication of such data on other servers. As an example, let us consider a person residing in Pisa, Toscana, who has an accident while visiting Rome, Lazio. Some examinations are performed and this person receives several treatments. In this case, the clinical documents related to this event are stored in the Document Manager paired with the hospital in Rome where the examinations and the treatments have been performed. Hence, the Document Managers of the Toscana Region domain are not updated with data related to this event, while the Federated Index Registries are updated with the pointer to these documents.

Moreover, access requests to medical data stored in the Document Managers of a given Italian Region can come from subjects that belong to other Italian Regions. As a matter of fact, in the previous example, the general practitioner of the patient, who belongs to the Toscana Region domain, could request access to the medical data of his patient related to the accident, which are stored in a Document Manager of the Lazio Region domain.

6.1 Security Policy

The security policy is at the base of the authorization system because it defines the rules that are evaluated during the decision process to determine the right of a subject to execute actions on resources. The first step toward defining a security policy is to determine how rights are assigned to subjects, and consequently choose a language for expressing these assignments.

In the Italian healthcare system, each actor has a specific qualification and a set of responsibilities that determine the set of task that he must carry on. Consequently, each actor is paired with a set of rights on patients' data that allows him to perform his tasks. As an example, a doctor working in the emergency room has the right to read and write medical data of any patient; the general practitioner has the right to read and write medical data only concerning his patients; the administrative employees of the healthcare system can read and write only personal data, i.e., they cannot access medical data.
In general, this organization can be easily represented adopting the Role Based Access Control model (RBAC) [13], which is based on defining a set of roles, assigning rights to these roles and then roles to subjects. In the EHR Infrastructure, the set of roles can be defined adopting a top-down approach by taking into account the functions of subjects in the healthcare system. As mentioned in Sec. 5.1, examples of roles are: general practitioner, emergency room doctor, patient, administrative employee of a hospital, pharmacist, etc. Adoption of the RBAC model in the EHR management scenario is convenient because it allows defining access control policies where rights are paired to roles instead of being assigned directly to subjects, thus simplifying system administrators’ work. Hence, once the role is assigned to a subject, his rights are automatically derived from it. An example of policy might be: subjects who have the role “Emergency Doctor” can read and write health and personal data of any patient; subjects with the role “Administrative Employee” can read patient’s personal data only; health data of a patient can be modified by the subject who wrote them.

However, the pure RBAC model may not be sufficient to describe the real access control requirements of the healthcare scenario. For instance, let us consider the case where, in an hospital, the ward doctor has the right to read the medical data of patients hospitalized in his ward, and has the right to write their therapies. Moreover, the Italian data protection authority states that patient must be able to impose some customized constraints on his medical data. As an example, he might want to show the data about a mental disease to his psychiatrist alone.

To address these issues, the security policy is expressed exploiting the XACML language [3], which is a well-known and widely used standard that naturally allows the use of roles in the authorization process [17]. The XACML language is adequate to express the security policies required for protecting EHRs because it allows representing roles for subjects and assigning rights to roles, exploiting attributes to perform the decision process, and it is flexible enough to also express specific access restrictions required by the patients.

Finally, another problem in defining a role-based authorization system for the EHR Infrastructure is that some Italian Regions that have already deployed their own infrastructure for managing EHR in their domain, have already defined their sets of roles and the related rights. In this case, the proposed solution is to define a mapping service that maps each global role onto a local one and vice versa. Some problems could arise when one-to-one mapping is not possible.

A reference set of roles has been proposed both by the OpenInFSE⁶ and by the IPSE projects.

---

6.2 Architecture

From an architectural point of view, the access control process requires integration of the authorization system components in the EHR Infrastructure defined by the OpenInFSE project. To design the authorization system architecture, we followed the reference architecture defined in [3], where the most relevant components are the Policy Enforcement Points (PEP) and the Policy Decision Point (PDP). The PEPs are in charge of allowing or denying the execution of requested accesses enforcing the access decisions taken by the PDP. In particular, a PEP has the task of intercepting the access requests that are relevant from a security point of view, to suspend their execution, and to invoke the PDP asking for an authorization decision. PEPs must be non-bypassable and tamper-proof, i.e., they must be able to intercept all the security-relevant actions before their execution and they cannot be circumvented to avoid the execution of the authorization phase. PEPs communicates with the PDP exploiting a well-known protocol, defined by the SAML profile of XACML [15]. In particular, a SAML message containing an <XACMLAuthzDecisionQuery> element is sent by the PEP to the PDP. This message includes all the data describing the access request, such as the name of the subject requesting the access, the name of the resource, the name of the action that the subject wants to perform on the resource, and other environmental data that could be useful for performing the decision process, such as the date and time. Moreover, the PEP also extracts from the access requests the assertions submitted by the user at authorization time, which represent his attributes, and embeds them in the SAML request as well. As a matter of fact, these assertions are expressed exploiting the SAML standard too, and hence can be easily embedded in the SAML message that is sent to the PDP. With reference to the previous example, the subject is the doctor of the emergency room of the hospital in Rome that asks to perform a read operation on the clinical data related to the tourist to decide the most proper treatment. The PEP waits for the result of the decision process before performing the real access. The PDP sends back a SAML message containing an <XACMLAuthzDecisionStatement> element that represents the result of the policy evaluation. If the right is granted, the PEP enforces this decision by resuming the execution of the access request, otherwise the access request is deleted, the access is not executed, and an error message is sent back to the Access Interface that requested the access.

A PEP must be embedded in each critical component of the OpenInFSE Infrastructure. Hence PEPs will be embedded in the services of the Component Layer: Federated Index Registry, Hierarchical Event Manager, and Document Manager, as shown in Fig. 6. The software components that will be released by the OpenInFSE project will already embed the proper PEPs, which will only require configuration with the address of the corresponding PDP. However, some regions could already have deployed their own components for managing clinical documents, and the PEP should be embedded in these components. The technique that could used for the integration depends on the component’s implementation, which could be different in distinct Italian regions. Some components could be already prepared for the integration of PEPs. As an example, the standard OASIS ebXML Registry 3.0 [14], which could be adopted for the implementation of the Federated Index Registry can
be configured to invoke the PDP. If the component is implemented as a web service, the PEP could be implemented exploiting the Inflow Handler Chain. Roughly speaking, the Inflow Handler Chain is a sequence of filters that are applied to any incoming message. Each filter takes as input the output message of the previous one in the chain, and can modify or even delete the message. In this case, a new handler that invokes the PDP is added to the original chain. This handler is invoked every time that a request message is received, and if the PDP response does not allow the execution of the request, the handler simply deletes the request message and returns an error to the requester. Another solution for integration of the PEP in components of the EHR infrastructure is to develop a wrapper component that is invoked instead of the original one. The wrapper component invokes the PDP, and then invokes the original service only if the PDP response is positive.

![Integration of PEPs in the EHR architecture components](image)

The Policy Decision Point (PDP) is located in the Security Manager, and it is the component of the architecture that performs the access decision process to determine whether a given subject has the right to perform the access he/she required. At initialization time, the PDP retrieves the security policy from a repository, managed by the Policy Administration Point (PAP), and it builds its internal data structures for policy representation. Next, the Context Handler (CH), also located in the Security Manager, receives the access requests from the PEPs embedded in the OpenInFSE Infrastructure components. Before invoking the PDP, the Context Handler checks the validity of the attribute assertions received in the access request (e.g., that the issuer is a trusted entity, the validity of the signature of the issuer, and the expiration date). The received requests are formatted as SAML messages including an \(<XACMLAuthzDecisionQuery>\) element and a set of attribute Assertions; the
Context Handler translates them in the format accepted by the PDP, XACML request context, and invokes the PDP. During the decision process, the PDP may need some attributes to perform the decision process that are not included in the request. In this case, the PDP invokes the CH, which in turn invokes the Policy Information Point (PIP). The PIP is the component that will contact the various attribute managers to retrieve the attribute values. These attributes refer to the resource, action or environment. Instead, concerning the subject's attributes, only the ones that have been explicitly selected by the subject at authentication time are used in the authorization process. This is meant to preserve the privacy of the subject. As a matter of fact, even if the subject has an attribute that grants him the access to some data, he may not want to disclose it for a given access. Hence, the PIP is in charge of retrieving the fresh values of the missing attributes by querying the correct component of the EHR Infrastructure. As an example, a subject could request to modify a clinical document, and the security policy could state that clinical documents can be modified only by the subjects who wrote them. In this case, the PDP will ask the PIP to retrieve the issuer of the requested document. A PDP can be paired with more than one PEP. Communication between the PEPs and the PDP and between the PAP and the PDP should be secure to protect both the integrity and the confidentiality of the requests and responses. Since the Security Manager is implemented as a web service, the SOAP Message Security standard, WS-Security, defined by the OASIS consortium [16] can be adopted to secure these interactions.

From an implementation point of view, some free implementation of the XACML framework that could be adopted to build the OpenInFSE authorization system is currently available. As an example, the reference implementation released by SUN currently provides a PDP only that supports the XACML version 2.0, while an extension of the SUN's PDP for managing XACML version 3.0 is provided by The Swedish Institute of Computer Science (SICS)8. Instead, Axiomatics9 provides a commercial version of the XACML framework that implements the full Policy Life Cycle Management for XACML policies, from editing to enforcement.

7 http://sunxacml.sourceforge.net/
8 http://www.sics.se/node/2465
9 http://www.axiomatics.com/products.html

7 8 9

7 8 9

7 8 9

7 8 9

CONCLUSION

This chapter describes the infrastructure defined by the OpenInFSE project to support the creation of an interoperability framework between the various organizations operating in the Italian healthcare scenario for the management and recomposition of Electronic Health Records. The scenario is complex and there are many crucial requirements, including compliance with previously developed local architectural solutions and with the Italian laws, distributed architecture, and sensitivity and confidentiality of managed data. Specifically, in this chapter we have focused on the adoption of a federated identity management system and proper security support for preserving the confidentiality and integrity of data stored in the Electronic Health
Records. Furthermore, the chapter proposed a possible solution for implementing federated authentication and authorization in the OpenInFSE infrastructure, based on the ICAR INF3 project and the OASIS XACML standard for the RBAC model.

Acknowledgments. This work was supported by the joint project CNR-Presidenza del Consiglio dei Ministri: Infrastruttura Operativa a Supporto dell'Interoperabilità delle Soluzioni Territoriali di FSE nel Contesto SPC.

REFERENCES

2. The Italian Data Protection Authority, Linee guida in tema di Fascicolo Sanitario Elettronico (FSE) e di dossier sanitario – 16 luglio 2009 (G.U. n. 178 del 3 agosto 2009)
3. OASIS, eXtensible Access Control Markup Language (XACML) v.3.0. 16 Apr 2009
14. OASIS, ebXML Registry Services and Protocols Version 3.0, OASIS, 2 May, 2005
15. OASIS, SAML 2.0 profile of XACML v2.0, OASIS Standard, 1 Feb 2005
17. OASIS, XACML Profile for Role Based Access Control (RBAC). 13 Feb 2004