D3.7

Specification of consent management and decentralized authorization mechanisms for HR Exchange - V1

ABSTRACT

This deliverable provides the first version of the specification of consent management and decentralized authorization mechanisms for health records in InteropEHRate. This document also provides a detailed technical background, which is a necessary step to move forward. The final and more detailed specification will be provided in the second forthcoming deliverable on March 2021.

Delivery Date	5th July 2019
Work Package	WP3
Task	3.3
Dissemination Level	Public
Type of Deliverable	Report
Lead partner	UBIT

InteropEHRate project is co-funded by the European Union (EU) Horizon 2020 program under Grant number 826106.

This document has been produced in the context of the InteropEHRate Project which is co-funded by the European Commission (grant agreement n° 826106). All information provided in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose.

CONTRIBUTORS

	Name	Partner
Contributors	Sofianna Menesidou	UBIT
	Marcel Klötgen, Salima Houta	FRAU
	Marie-Catherine Wagner, Katerina Polychronopoulos	UNIVIE
	Simona Bica	SIVECO
Reviewers	Thanos Kiourtis	UPRC
	Alessio Graziani	ENG

LOGTABLE

Version	Date	Change	Author	Partner
0.1	09-05-2019	First draft of ToC	Sofianna Menesidou	UBIT
0.2	27-05-2019	Input at Chapter 2	Sofianna Menesidou	UBIT
0.3	01-06-2019	Input at Chapter 1 and 2	Sofianna Menesidou	UBIT
0.4	03-06-2019	Input at Chapter 3	Sofianna Menesidou	UBIT
0.5	05-06-2019	Input at Chapter 2	Marcel Klötgen, Salima Houta	FRAU
0.6	05-06-2019	Input at Chapter 2	Marie-Catherine Wagner, Katerina Polychronopoulos	UNIVIE
0.7	05-06-2019	Input at Chapter 2	Simona Bica	SIVECO
0.8	24-06-2019	Input at Chapter 3	Sofianna Menesidou	UBIT
0.9	25-06-2019	Input at Chapter 3	Sofianna Menesidou	UBIT
1.0	26-06-2019	Input at Chapter 2 and 3	Sofianna Menesidou	UBIT
1.1	27-06-2019	Input at Chapter 3	Sofianna Menesidou	UBIT
1.2	28-06-2019	Internal review	Thanos Kiourtis	UPRC
1.3	29-06-2019	Changes based on reviewers'	Sofianna Menesidou	UBIT

		comments		
1.4	30-06-2019	Changes based on reviewers' comments	Sofianna Menesidou	UBIT
1.5	03-07-2019	Changes based on reviewers' comments	Simona Bica	SIVECO
1.6	04-07-2019	Internal review	Alessio Graziani	ENG
1.7	04-07-2019	Changes based on reviewers' comments	Sofianna Menesidou	UBIT
1.8	05-07-2019	Completed quality check	Argyro Mavrogiorgou	UPRC
vFinal	05-07-2019	Final check and version for submission	Laura Pucci	ENG

ACRONYMS

Acronym	Description
ABAC	Attribute Based Access Control
APPC	Advanced Patient Privacy Consents
BPPC	Basic Patient Privacy Consents
CM	Consent Management
D2D	Device-to-Device
DAC	Discretionary Access Control
EHR	Electronic Health Records
EPP	Event Processing Point
GDPR	General Data Protection Regulation
HCP	Health Care Professional
HR	Health Record
IDM	Identity Management
MAC	Mandatory Access Control
MD2DI	Mobile Device-to-Device Interface
NGAC	Next Generation Access Control
PAP	Policy Administration Point
PAP	Policy Access Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PHI	Protected Health Information
PHR	Patient Health Records
PIP	Policy Information Point
R2D	Remote-to-Device
R2DI	Remote-to-Device Interface

RAP	Resource Access Points
RBAC	Role-Based Access Control
RSI	Research Interface
S-HER	Smart Electronic Health Record
XACML	eXtensible Access Control Markup Language

TABLE OF CONTENT

LIST OF FIGURES

1. INTRODUCTION

1.1. Scope of the document

The main goal of the present document is to describe the InteropEHRate specification of consent management and decentralized authorization mechanisms for health record (HR) exchange focused on the objectives of the first year of the project regarding the D2D scenario.

1.2. Intended audience

The document is intended to security engineers, policy makers, architects, developers and all the project participants and partners interested to have an overview of how InteropEHRate will support the consent management and decentralized authorization mechanism to exchange health records.

1.3. Structure of the document

This deliverable is structured as follows. This Chapter explains the goal and structure of the document. In Chapter 2, we describe and review the research background regarding both consent management and decentralized authorization, starting by a general overview and then focusing on other european research initiatives. The overall consent management and decentralized authorization in terms of InteropEHRate is presented in Chapter 3, where the latter are analysed in detail. Finally, Chapter 4 concludes the deliverable, mentioning the future goals.

1.4. Updates with respect to previous version (if any)

This deliverable contains the first version of the InteropEHRate architecture.

1.5. Relation to other deliverables

Similarly to other reports of the InteropEHRate project, this document presents just a first draft of the specification of consent management and decentralized authorization mechanisms for HRs exchange. One additional version of this document is planned on March 2021. The final version will be more detailed based on the new knowledge acquired from the experience of development during the first year. This first version of the deliverable D3.7 considers the work of WP2 regarding the architecture, user requirements and the interoperability profile and serves as a basis for the WP4 interoperability protocols. Figure 1 below presents the main relation with the other deliverables.

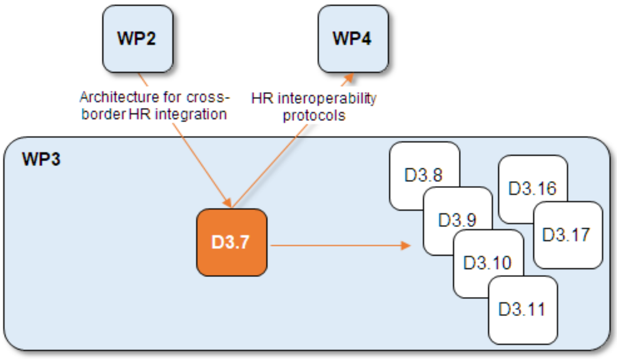

WP2
WP4
Architecture for cross-border HR integration
HR interoperability protocols
WP3
D3.7
D3.8
D3.16
D3.9
D3.17
D3.10
D3.11

Figure 1 - Relation with other deliverables

2. TECHNICAL BACKGROUND

The chapter commenced with a thorough review of the literature to gain a clear understanding of the current state of the art related to the decentralized authorization and consent management. Below it is listed what is authorization and consent management for the sake of completeness.

- **Consent Management (CM)**: is a system, process or set of policies for allowing consumers and patients to determine what health information they are willing to permit their various care providers to access. It enables patients and consumers to affirm their participation in e-health initiatives and to establish consent directives to determine who will have access to their protected health information (PHI), for what purpose and under what circumstances. Consent management supports the dynamic creation, management and enforcement of consumer, organizational and jurisdictional privacy policies [CM].
- **Authorization**: is the function of specifying access rights/privileges to resources, which is related to information security and computer security in general and to access control in particular [FRASER1997].

2.1. Consent Management

The informed consent of the citizen is essential for data exchange. The EU general data protection regulation 2016/679 (GDPR) forms the legal basis for data processing. Articles 4 (11), 6 (1)(a), 7, 8, and 9(2)(a) and Recitals 32, 33, 38, 42, and 43 of the GPPR deals with the conditions for consent.

The relevant paragraphs and recitals are listed in the following:

***Article 4** Definitions (11)*

11. 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

***Article 6** Lawfulness of processing (1)(a)*

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
   a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

***Article 7** Conditions for consent*

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject’s consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly

distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. *The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.*
4. *When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*

***Article 8** Conditions applicable to child's consent in relation to information society services*

1. *Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.*
2. *The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.*
3. *Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.*

***Article 9** Processing of special categories of personal data (1), (2)(a)*

1. *Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*
2. *Paragraph 1 shall not apply if one of the following applies:*
    a. *the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject*

***Recital 32** Conditions for consent*

Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to *him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.*

***Recital 33** Consent to certain areas of scientific research*

It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

***Recital 38** Special protection of children's personal data*

Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

***Recital 42** Burden of proof and requirements for consent*

Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC[1] a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

***Recital 43** Freely given consent*

In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

In addition to the GDPR which applies to all European Union countries, there may also be country-specific regulations.

Legally, the consent acquired from citizens must contain the following building blocks according to Art. 7 of the GDPR:

- It must be clearly written in simple and plain language, understandable to the citizen and must be provided on a separate form or if not, the consent must be clearly distinguishable from other matters on the form which the citizen will sign
- Demographic data of the citizen
- The identity of the controller (Recital 42)
- A statement about the citizen's right to withdraw consent and that consenting to the processing is not a condition for the performance of any contract, information about the citizen's privacy protection rights and/or data exchange processing (Recital 42)
- Separate consent must be possible to be given to different personal data processing operations (Recital 43). Consent should cover all processing activities carried out for the same purpose or purposes (Recital 32). When the processing has multiple purposes, consent should be given for all of them (Recital 32).
- General information about the data exchange and/or processing
  - type and purpose of electronic data exchange and/or processing (if the data exchange or processing has multiple purposes, consent should be given for all of them)
  - scope of data exchange (information objects which will be exchanged)
  - list of access permissions (for example, hospitals, medical care centres)
- Citizen's declaration
  - of voluntary and informed consent to the specified data processing activities for the specified consent and time period
  - that he or she received information about withdrawal of consent, privacy protection rights and/or data exchange processing

Please also note that Articles 13 and 14 require that specific information be given to the data subject whose personal data is being processed.

2.1.1. Existing Standards for structural representation of consents

The IHE Advanced Patient Privacy Consents (APPC) Profile [APPC] defines a structural and semantic representation of a privacy consent policy to enable consent(s) to be captured, managed and exchanged between systems. The aim of the APPC Profile is to enforce interoperability between access control systems and to support system-wide authorization mechanisms.

The profile defines two actors:

- Content Creator: system which creates a structured machine-readable consent document.
- Content Consumer: system which consumes a structured consent document. This system shall be able to process and interpret the structured policies contained in the APPC consent document.

The following sequence diagram illustrates this process (Figure 2). The presentation is generic and does not specify how the consent document is transmitted. The Content Creator (as part of healthcare related application) captures all the information needed for consent creation. In cross-facility supply scenarios, the unique identification of service providers, such as through the provider information directory service, is essential. The unique ID can be used to check whether there is a right of access for the organization/person with this ID. The resulting consent document is transferred to systems that implement access management. The content consumer can be an extension of these systems.

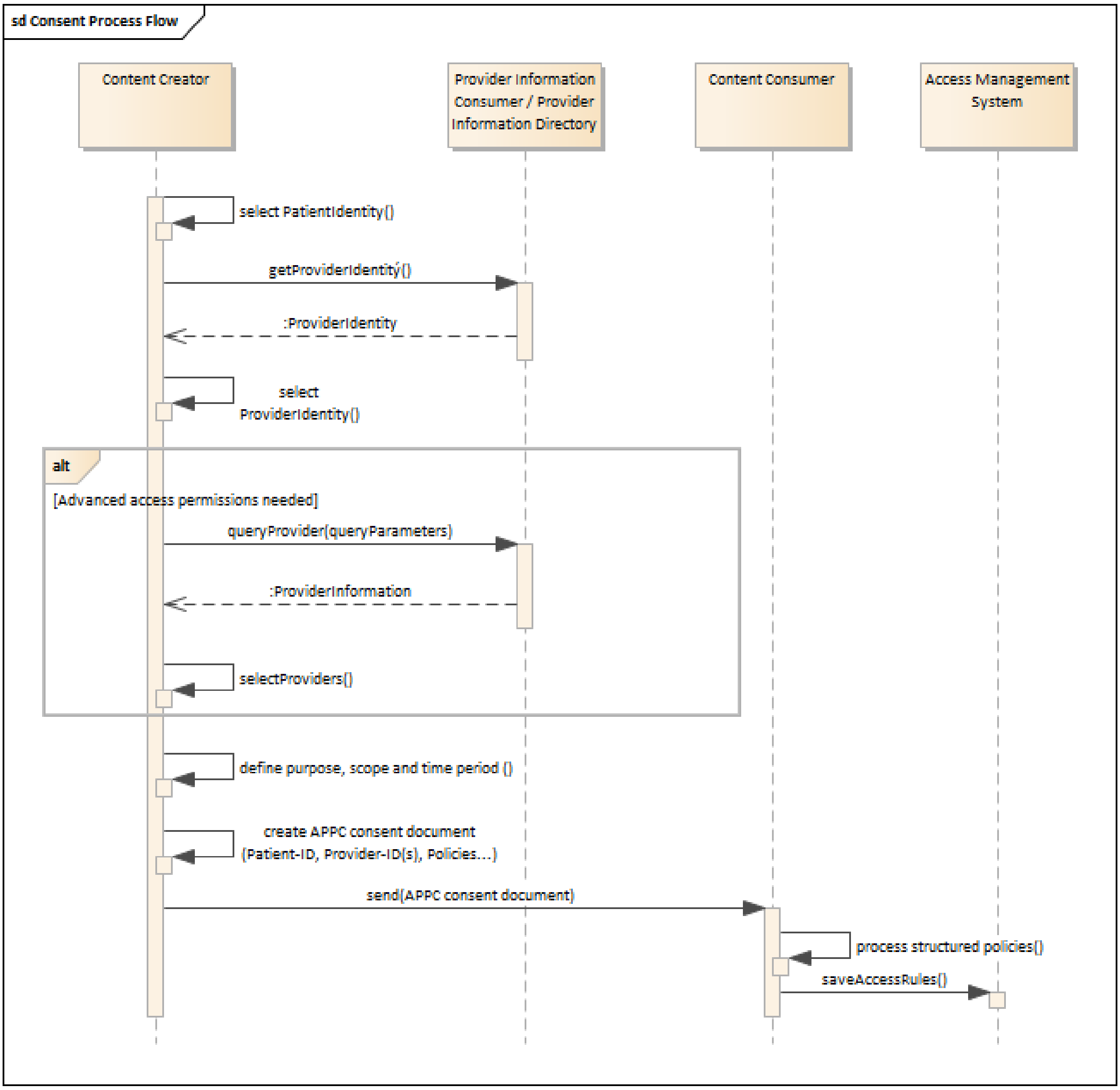

sd Consent Process Flow
Content Creator
Provider Information Consumer / Provider Information Directory
Content Consumer
Access Management System
select PatientIdentity()
getProviderIdentity()
:ProviderIdentity
select ProviderIdentity()
alt
[Advanced access permissions needed]
queryProvider(queryParameters)
:ProviderInformation
selectProviders()
define purpose, scope and time period ()
create APPC consent document (Patient-ID, Provider-ID(s), Policies...)
send(APPC consent document)
process structured policies()
saveAccessRules()

Figure 2 - Consent Process Flow

The structure of the APPC consent document is based on XACML [XACML]. Details to the structure of the policies will be described in the following sections.

Another profile is the IHE Basic Patient Privacy Consents (BPPC) [BPPC]. However, it is not described in more detail due to the lack of expressiveness of access rules.

2.2. Decentralized Authorization

In decentralized authorization, the decision to grant or deny access is based on two distinct processes, authentication and authorization. Authentication involves the verification of credentials. Whereas, authorization is the process of granting or denying access to system resources based on credentials. In deliverable D3.3 [D3.3] it is summarized a detailed state-of-the-art regarding identification and authentication. Access control is one of the main methodologies used to perform the verification of the authorization of an end user requesting access to specific restricted resources.

In the literature, many commonly used authorization/access control models are defined. The most known are the Mandatory Access Control (MAC), the Discretionary Access Control (DAC) and the Role-Based Access Control (RBAC). All these models are known as identity-based access control models where users (subjects) and resources (objects) are identified by unique names. Static access control models, usually, provide a list of permissions that each subject has on certain objects. The literature on combining context and security mainly concentrates on context-based RBAC. Moreover, in the literature, a fourth type has been identified, the Attribute Based Access Control (ABAC). Such a scheme is by nature dynamic. The main difference of ABAC with the previews schemes is the fact that the concept of provided policies can express a complex Boolean rule set that can evaluate many different attributes. In ABAC, there are not static lists of permissions that associate subjects with objects, but instead there are “snapshots” of such associations that can be generated and dynamically change based on the current context. Any ABAC system should implement the conceptual flow that is depicted on Figure 3 below.

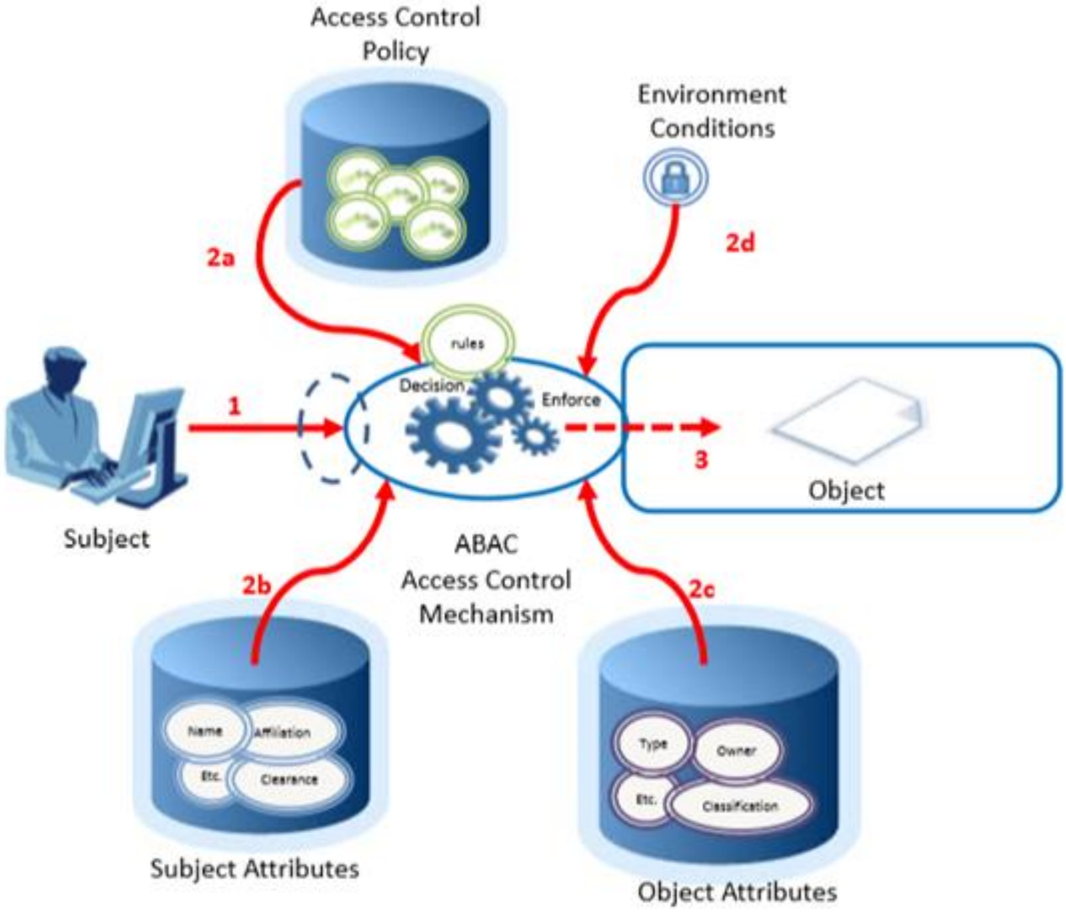


Figure 3 - ABAC Indicative Information Flow

The access request is handled by the ABAC Access Control Mechanism which consults a policy repository (step 2a) in order to obtain the set of attributes that have to be examined in order to reach a decision of "allow" or "deny". The attribute examination phase checks subject attributes (step 2b), object attributes (step 2c) and environmental attributes (step 2d) in order to perform the actual assessment (step 3).

In general, ABAC avoids the need for capabilities to be directly assigned to subject requesters or to their roles or groups before the request is made. Instead, when a subject requests access, the ABAC-compliant engine can make an access control decision based on the assigned attributes of the requester, the assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions.

2.2.1. Existing ABAC Standards

As already discussed, there are many reference implementations of the ABAC model. One example of an access control framework that is consistent with ABAC is the eXtensible Access Control Markup Language (XACML) [XACML]. Another example is the Next Generation Access Control (NGAC) standard [NGAC]. These two are considered to be the most notable ones [FERRAIOLO2016].

2.2.1.1. XACML in a Nutshell

XACML is an OASIS [XACML] standard that describes both a policy language and an access control decision request/response language. Both languages use XSD notations; hence policy definition and request/response elements are serialized as XML elements. The policy language details general access control requirements, and has standard extension points for defining new functions, data types, combining logic, etc. The request/response language lets you form a query to ask whether or not a given action should be allowed, and interpret the result. The response always includes an answer about whether the request should be allowed using one of four values: Permit, Deny, Indeterminate (an error occurred or some required value was missing, so a decision cannot be made) or Not Applicable (no policy available to this service addresses this request).

The specification defines five main components (Figure 4) that handle access decisions; namely Policy Enforcement Point (PEP), Policy Administration Point (PAP), Policy Decision Point (PDP), Policy Information Point (PIP), and a Context Handler.

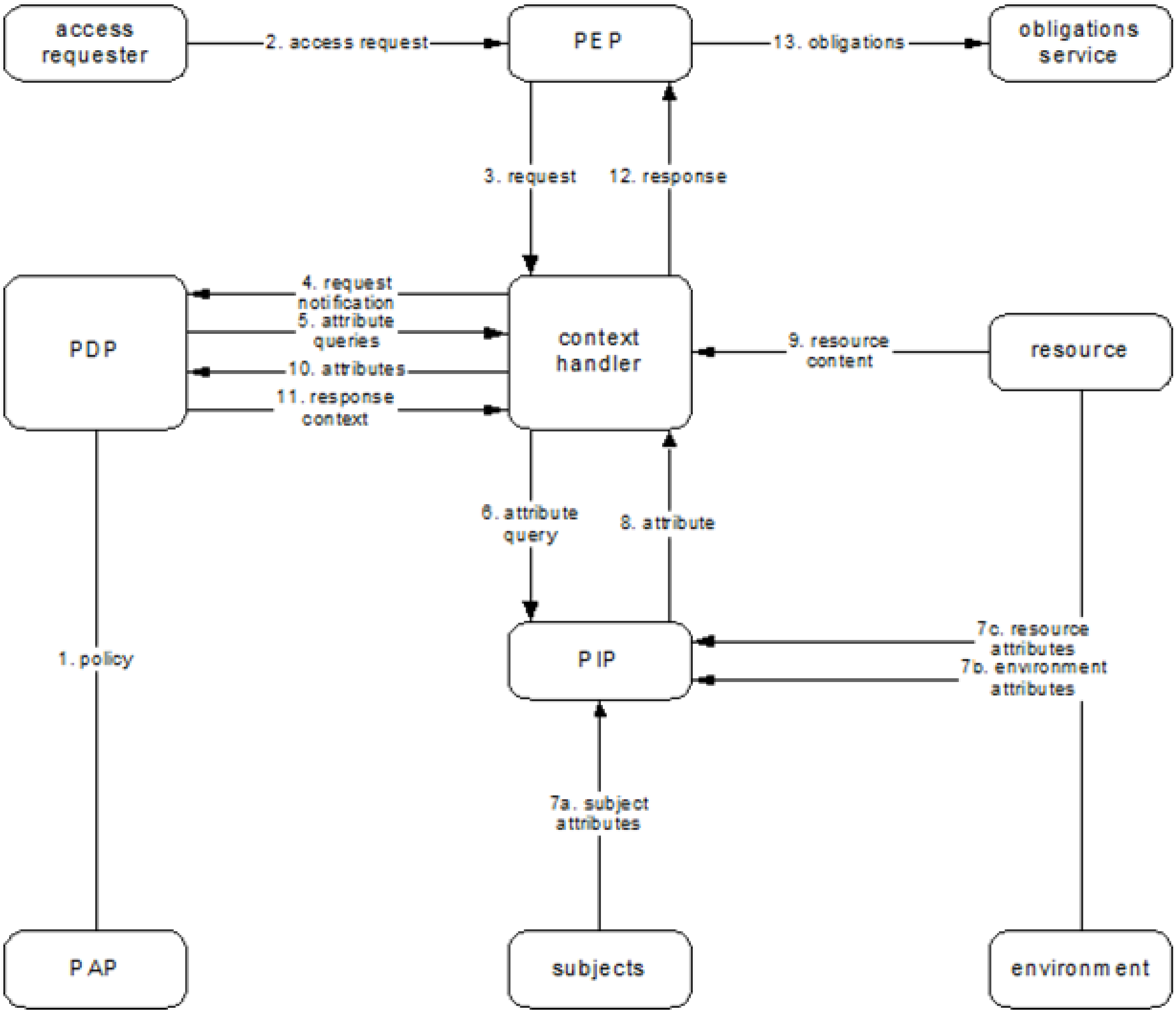


Figure 4 - XACML data-flow diagram

The functional purpose of the main components is:

- The Policy Administration Point (PAP) provides an interface or API to manage the policies that are stored in the repository and provides the policies to the Policy Decision Point (PDP).
- The Policy Enforcement Point (PEP) is the interface to the external world. It receives the application specific access requests and translates them to XACML access control requests, then it denies or allows access based on the result provided by the PDP.
- Policy Decision Point (PDP) is the main decision point for the access requests. It collects all the necessary information from other actors and yields a decision.
- Policy Information Point (PIP) is the point where the necessary attributes for the policy evaluation are retrieved from several external or internal actors. The attributes can be retrieved from the resource to be accessed, environment (e.g. time), subjects, and so forth.
- Context Handler entity converts decision requests in the native request format to the XACML canonical form, coordinates with Policy Information Points to add attribute values to the request context, and converts authorization decisions in the XACML canonical form to the native response format.

2.2.1.2. NGAC in a Nutshell

NGAC [NGAC] is a fundamental reworking of traditional access control into a form that suits the needs of the modern distributed interconnected enterprise. NGAC diverges from traditional approaches to access control in defining a generic architecture that is separate from any particular policy or type of policy. NGAC is not an extension of, or adaption of, any existing access control mechanism, but instead is a redefinition of access control in terms of a fundamental and reusable set of data abstractions and functions. NGAC provides a unifying framework capable without extension of supporting not only current access control approaches, but also novel types of policies that have been conceived but never implemented due to the lack of a suitable enforcement mechanism.

This standard contains an abstract functional description of an architecture. The description is abstract because it excludes all irrelevant details, and is functional because it partitions the entities comprising the architecture purely on the basis of their function and excludes all other constraints. NGAC does not express policies through rules, but instead through configurations of relations of four types: assignments (define membership in containers), associations (to derive privileges), prohibitions (to derive privilege exceptions), and obligations (to dynamically alter access state). The specification defines six main components (Figure 5) that handle access decisions; namely Policy Enforcement Point (PEP), Resource Access Points (RAP), Policy Decision Point (PDP), Policy Access Point (PAP), Policy Information Point (PIP), and optional Event Processing Point (EPP).

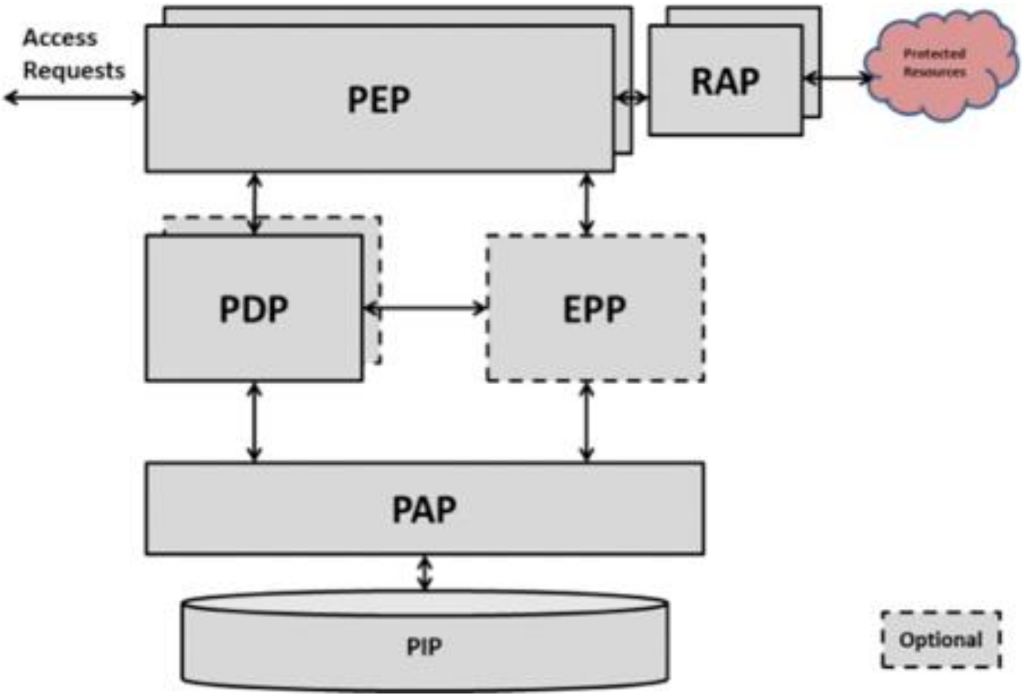


Figure 5 - NGAC data-flow diagram

2.3. Relation with other research projects

This category comprises EU-funded projects and EU large scale projects in the same field like InteropEHRate (eHealth / Digital Health).

In this section there are presented other complex representative eHealth projects which can be considered as having similarities with InteropEHRate, such as:

- cybersecurity in healthcare
- eHealth / mHealth
- HL7 compliance
- standardization specific to eHealth field.

The actual InteropEHRate project will benefit from the relevant experience, specific results and know-how acquired by these projects.

As regards the similarities between InteropEHRate and the related projects presented hereinafter, we can mention that all of these projects are intended to the healthcare sector and address the same categories of key stakeholders, such as:

- Industry (suppliers of digital wearables, suppliers of communication devices, suppliers of IT / eHealth solutions and services, suppliers of cyber security services)
- Healthcare organizations
- Research organizations
- Policymakers
- Governmental organizations and agencies
- Patients organizations / associations
- International networks (eHealth, cybersecurity, interoperability, standardization).

Moreover, all projects share the use of innovative technologies, technological platforms and software tools in the healthcare field, both in implementing the integrated IT solutions as well as ensuring interoperability with external systems developed on the same principles (compliant with HL7 / HL7 FHIR).

As concerns the benefits generated by the synergy among InteropEHRate and the projects mentioned below, InteropEHRate might catch up from these projects those results and the know-how necessary for the development of the platform as well as the specific business information regarding the business models and the marketing approach when exploiting the results of the project.

InteropEHRate will benefit from the following specific results of the other projects, namely: state-of-the-art aspects, collaboration for the development of an effective interoperability framework in the healthcare sector, user needs and specifications identified by each project, methodological approaches specific to eHealth, how to develop a synergy between various projects funded by the H2020 programme and the AAL programme.

We assume that the above mentioned aspects will enhance also the sustainability impact of the InteropEHRate project and will bring added value to Exploitation, Dissemination and Communication specific activities.

2.3.1. Electronic Health Record System (EHR) of Romania (Large Scale Project at national level)

The Romanian EHR is interconnected with the platforms of the IT systems within the Romanian Health Insurance House (CNAS), implemented within the same financing line: (i) SIPE – Electronic prescription that refers directly to the method of settlement and management of prescriptions; (ii) CEAS – National Health Card providing a unique identification of the insured persons (iii) SIUI – Single Integrated Information System provides uniform reporting system and data processing of health at national and county level. The Romanian EHR is the first national health system of EHR (Electronic Health Records) and PHR (Patient Health Records) type developed on the basis of the HL7 standard.

The Romanian EHR is the first national health system of EHR and PHR (Patient Health Records) developed on the HL7 standard (an interoperability standard in the IT medical field). The aim of the project has been to create a centralized IT system that collects a patient’s medical data from all medical providers, as well as its integration with the other IT platforms that the National Health Insurance House has. Data security is guaranteed by the implemented IT security mechanisms, such as authentication based on digital certificate and security matrices, encryption of communication between the user and the central IT platform of EHR, permanent access control and auditing, safe data storage.

2.3.2. LETITFLOW - Active Distributed Workflow System For Elderly (AAL Programme)

LetItFlow provides an innovative solution to support elderly hospital staff to accomplish their daily tasks optimally and to adopt and adapt to new procedures and methods via real-time context aware tools. LetItFlow combines two challenges: change management and workflow technologies dedicated to elderly employees. The solution enables assistance by means of tracking employees’ activity, portable communication tools, alarming, alerting and notifications services, adapted interaction interfaces or workflow management. It is based on fixed and mobile platforms that interact with the employees to guide them in their work activities. To address the specific requirements from the nurses in the ward, a dedicated interface for the mobile platform was designed based on LetItFlow solution together with new features such as a bed/room map, patient information, complementary tests, shift change reports and patient periodic reports.

LetItFlow proposes methods and tools, to facilitate the adaptation of elderly nurses to changeable work environment by supporting them with real-time context aware tool for guiding them in daily tasks. The final objective is to retain the older adult nurses, to avoid their demotivation and ease their daily works, to facilitate knowledge transfer, to increase their efficiency and safety issues. The LetItFlow tool alleviates the task of nurses by a better distribution of the workload. The tool also support knowledge transfer in real life scenarios, by putting together young and elderly employees in several works.

2.3.3. SPHINX – A Universal Cyber Security Toolkit for Health-Care Industry (H2020)

The H2020 SPHINX project aims to introduce a health tailored Universal Cyber Security Toolkit, thus enhancing the cyber protection of the Health and care IT Ecosystem and ensuring patient data privacy and integrity. It will also provide an automated zero-touch device and service verification toolkit that will be easily adapted or embedded on existing, medical, clinical or health available infrastructures. Hospitals and care centres store and exchange large amounts of sensitive patients' data, so they are prime targets for cyber criminals. Since 2016 the published number of health records to have been stolen has been over 2.5 Million, this could be much higher. This varies from inside job attacks, poor security and hacking. At the same time medical devices and wearable devices collecting personal data, become more sophisticated and connected and the use of smartphones makes the whole health system more vulnerable. The health system has to face advanced persistent threats such as Ransomware, Human Threats, DdoS, Lost Info, active attacks and much more.

The SPHINX Toolkit will be validated through pan-European demonstrations in three different scenarios at different countries (Romania, Portugal and Greece). Hospitals, care centres and device manufacturers participating in the project's pilots will deploy and evaluate the solution at business as usual and emergency situations across various use case scenarios.

3. INTEROPEHRATE CONSENT MANAGEMENT AND DECENTRALIZED AUTHORIZATION

The purpose of this Section is to identify how InteropEHRate project will handle Consent Management and decentralized authorization, mainly focused on the D2D scenario, which is the scenario we focused for the first year of the project.

3.1. Decentralized Authorization based on Attribute-based Access Control (ABAC)

Access to devices and data will be regulated by a sophisticated authorization engine which will be distributed by design. Since InteropEHRate is a cross-border system that manages and analyses health data from several data sources, it is crucial to integrate support of attribute-based access control (ABAC). By exploiting both the end-users and the resource attributes, ABAC does not rely on explicit authorizations that are required prior to the access request to a resource. Also, ABAC is scalable, compared to other access control mechanisms, such as roles based access control and access lists, would be time inefficient.

Although there are a lot of frameworks that realize the concept of ABAC, the eXtensible Access Control Markup Language (XACML) framework has been selected by the community as a cornerstone standard for authorization. XACML can be referred to as a framework since it consists of both a conceptual architecture and a set of normative schemas that have to be used by any potential reference implementation.

More specifically, in terms of InteropEHRate an already existing ABAC authorization engine will be evolved, which is distributed by design. Using this engine, users (e.g. patient, doctors) will be able to author policies. These policies may use attributes that characterize the requestor, the resource and the contextual environment at the same time. Hence, the entity that verifies the value of the attributes is extremely crucial since tampering attributes may lead to policy circumvention. InteropEHRate will also support a hybrid mode of attribute-verifiability in order to satisfy diverse requirements. One mode, will be blockchain-based attributed verification and the second mode will be centralized federation of attributes. Irrelevant of the modality, attribute verification will be the cornerstone of consent management. Authorization in D2D communication [D2.1], is based on the successful identification of all parties and the citizens’ consent. ABAC authorization engine will be utilized in the second year of the project where the focus will be the remote communication (R2D scenario) as specified in D2.1.

3.2. Consent Management

The citizen must give her/his consent before any of her/his data is made available to the InteropEHRate network. As already described in D2.1 [D2.1] the citizen will be able to configure a set of default permissions.

The default set of permissions regarding consent should include the following:

- Consent to store data to S-EHR
- Consent to upload data to HCP
- Consent to download data from HCP
- Consent to backup data to S-EHR Cloud
- Consent to donate data to a research centre

During S-EHR app installation, a software key store (or certificate store) is needed in the mobile to store all the necessary certificates. This key store should be protected. Below we summarize the key stores on the Android and iOS devices, since the S-EHR app will have to be installed in one of these mobile operating systems.

- The Android Keystore system provides the ability to generate and store cryptographic keys in a container to make it more difficult to extract it from the device. In addition, it gives the ability to replace the certificate at a later time with a certificate signed by a different CA. When generating or importing a key into the Android Key Store the key will be used if the user has been authenticated first in the device. Once keys are in the keystore, they can be used for cryptographic operations with the key material remaining non-exportable. Moreover, it offers facilities to restrict when and how keys can be used, such as requiring user authentication for key use or restricting keys to be used only in certain cryptographic modes [ANDROID2019].
- The iOS keychain provides a mechanism to store small bits of user data in an encrypted database called a keychain. The keychain is not limited to passwords, other sensitive data such as cryptographic keys and certificates can also be stored to support secure communications and to establish trust with other users and devices. In addition, as in Android OS, iOS provides the ability to generate you own keys [APPLE2019].

Within InteropEHRate, the consent to store data should be signed by the citizen, while the consent to allow process upon the data to another party will be a double-signed. For instance, the consent to download/upload data to/from HCP will be double-signed from both the S-EHR user (e.g. citizen) and the HCP app user (e.g. HCP). In addition, consents should be aggregated in a central platform (in our case in the S-EHR cloud) when the S-EHR mobile application becomes online. This is helpful to resolve any disputes among the users in the future.

Consent will be based on APPC standard and will include information regarding the identification of both parties, the purpose, the scope and the time period. In addition, the declaration of consent should be signed twice, when involves a third party. In D3.3 [D3.3] it is described the process of how the S-EHR acquires the HCP's certificate in both variants, where no internet exists. This certificate is necessary for the digital signature validation of HCP. The following sequence diagram (Figure 6) provides a high-level overview of the consent management in the D2D scenario.

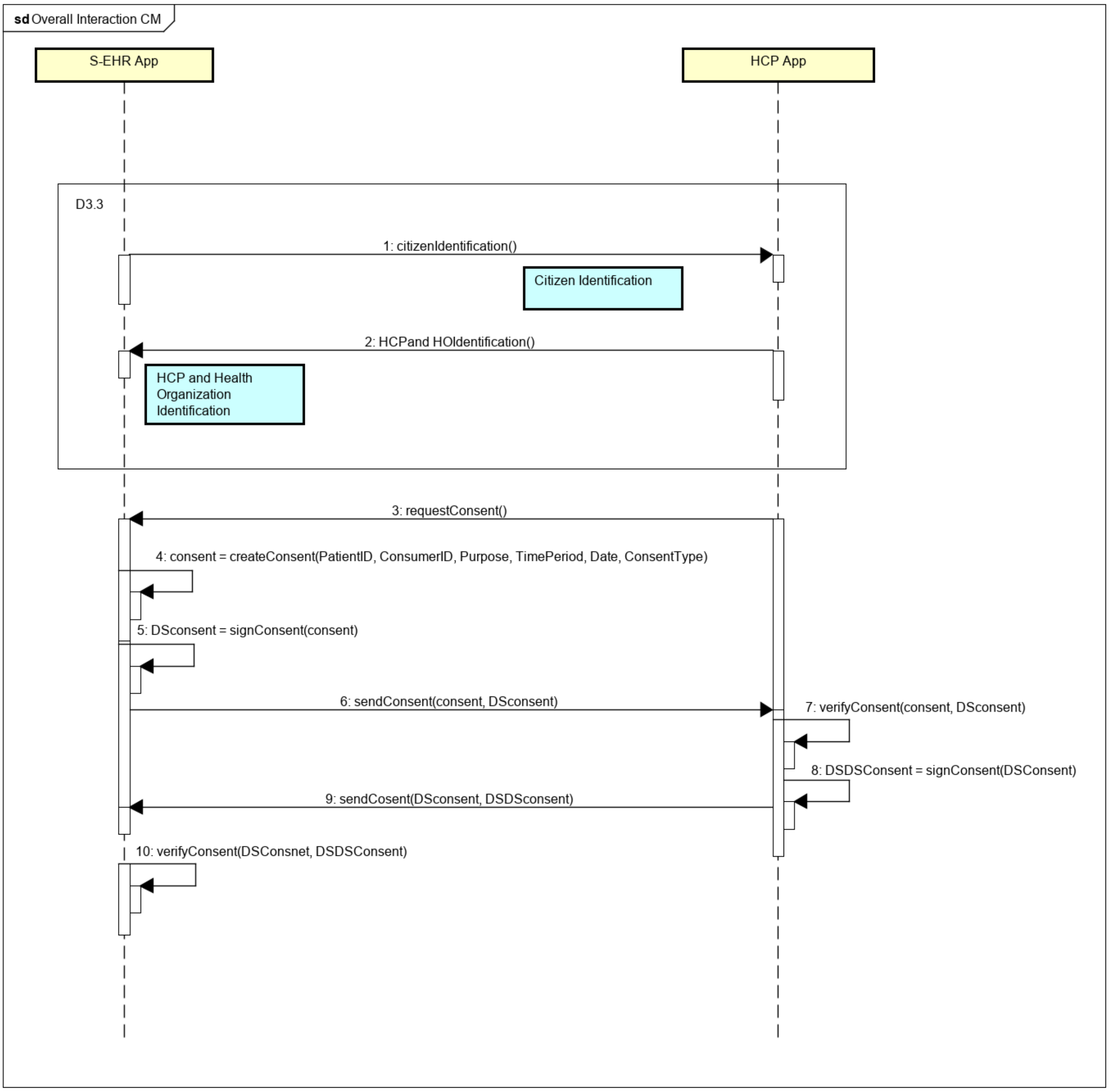

sd Overall Interaction CM
S-EHR App
HCP App
D3.3
1: citizenIdentification()
Citizen Identification
2: HCPand HOIdentification()
HCP and Health Organization Identification
3: requestConsent()
4: consent = createConsent(PatientID, ConsumerID, Purpose, TimePeriod, Date, ConsentType)
5: DSconsent = signConsent(consent)
6: sendConsent(consent, DSconsent)
7: verifyConsent(consent, DSconsent)
8: DSDSConsent = signConsent(DSConsent)
9: sendCosent(DSconsent, DSDSconsent)
10: verifyConsent(DSConsnet, DSDSConsent)

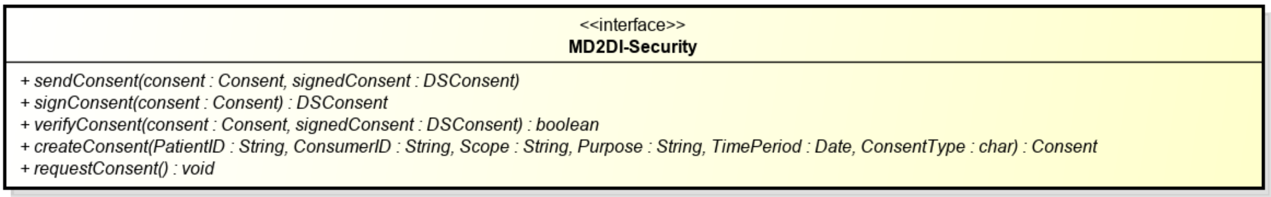
Figure 6 - Consent Management

Following a detailed description of the sequence diagram:

- **Step 1** - The citizen identification by the HCP App. More information regarding the two-variants of the identification is provided in [D3.3].
- **Step 2** - HCP and HO are identified by the S-EHR App. More information regarding the two-variants of the identification is provided in [D3.3].
- **Step 3** - The HCP request from the citizen to give his consent to upload data his personal data to HCP App.
- **Step 4** - The S-EHR App creates the consent ACCP document that contains information regarding the identification of both parties (PatientID and ConsumerID), the purpose (Purpose), the scope (ConsentType) and the time period (TimePeriod and Date).

- **Step 5** - The S-EHR App digitally signs the created consent (DSconsent).
- **Step 6** - The S-EHR App send to the HCP App the consent with the digitally signed consent (DSconsent) for verification.
- **Step 7** - The HCP App validates the digital signature of the citizen and the authenticity of the citizen.
- **Step 8** - The HCP App digitally double signs the already signed consent (DSDSconsent).
- **Step 9** - The HCP App send to the S-EHR App the digitally signed consent (DSconsent) with the double digitally signed consent for verification (DSDSconsent).
- **Step 10** - The S-ERH App validates the digital signature (DSDSconsent) of the HCP and the authenticity of the HCP.

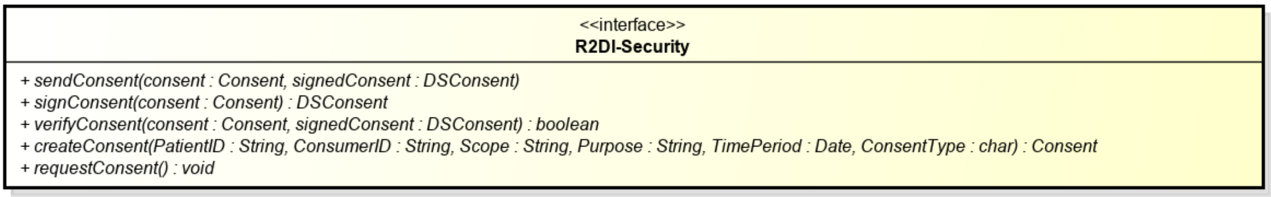
The following figures(Figure 7, Figure 8 and Figure 9) show the UML class diagrams representing the main interfaces.



<<interface>>
MD2DI-Security

+ sendConsent(consent : Consent, signedConsent : DSConsent)
+ signConsent(consent : Consent) : DSConsent
+ verifyConsent(consent : Consent, signedConsent : DSConsent) : boolean
+ createConsent(PatientID : String, ConsumerID : String, Scope : String, Purpose : String, TimePeriod : Date, ConsentType : char) : Consent
+ requestConsent() : void

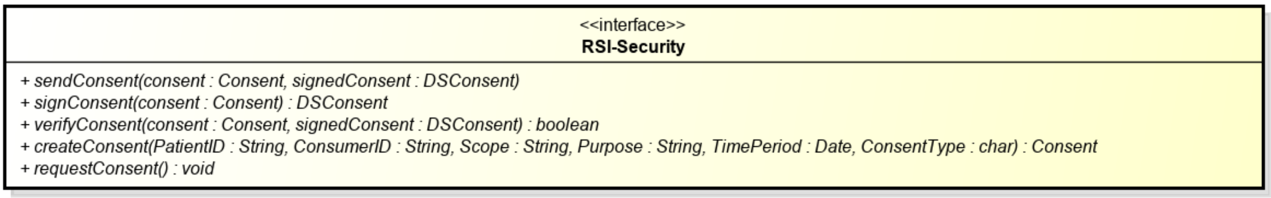
Figure 7 - Consent Conceptual API (MD2DI)



<<interface>>
R2DI-Security

+ sendConsent(consent : Consent, signedConsent : DSConsent)
+ signConsent(consent : Consent) : DSConsent
+ verifyConsent(consent : Consent, signedConsent : DSConsent) : boolean
+ createConsent(PatientID : String, ConsumerID : String, Scope : String, Purpose : String, TimePeriod : Date, ConsentType : char) : Consent
+ requestConsent() : void

Figure 8 - Consent Conceptual API (R2DI)



<<interface>>
RSI-Security

+ sendConsent(consent : Consent, signedConsent : DSConsent)
+ signConsent(consent : Consent) : DSConsent
+ verifyConsent(consent : Consent, signedConsent : DSConsent) : boolean
+ createConsent(PatientID : String, ConsumerID : String, Scope : String, Purpose : String, TimePeriod : Date, ConsentType : char) : Consent
+ requestConsent() : void

Figure 9 - Consent Conceptual API (RSI)

The following tables provide a complete description of all the methods, which is similar for all four interfaces.

Method sendConsent

Name	sendConsent
Description	This method sends the consent to the consumer.
Arguments	● **Consent consent**: the created consent. ● **DSConsent signedConsent**: the digital signature of the consent
Return Value	No return value is expected.
Exceptions	● Network exceptions related to failure during communication.
Preconditions	● Successful execution of the createConsent method before sending the consent ● Successful execution of the signConsent method before sending the consent ● An established connection regarding D2D or R2D.

Method signConsent

Name	signConsent
Description	This method digitally signs the created consent.
Arguments	● **Consent consent**: the created consent.
Return Value	● **DSConsent signedConsent**: the digital signature of the consent
Exceptions	● Cryptographic exceptions related to failure during signing.

Preconditions	● Successful execution of the createConsent method before signing the consent. ● An established connection D2D or R2D.

Method verifyConsent

Name	verifyConsent
Description	This method verifies the digital signature.
Arguments	● **Consent consent**: the created consent. ● **DSConsent signedConsent**: the digital signature of the consent
Return Value	● **Ture**: successful validation. ● **False**: unsuccessful validation.
Exceptions	● Cryptographic exceptions related to failure during signing (for verification purposes).
Preconditions	● Network exceptions related to failure during communication. ● Successful execution of the createConsent method before verifying the consent. ● Successful execution of the signConsent method before verifying the consent ● Successful execution of the sendConsent method before verifying the consent ● An established connection D2D or R2D.

Method createConsent

Name	createConsent
Description	This method creates the consent based on APPC standard, which is an XACML representation.

Arguments	● **String PatientID**: a unique string that identifies the citizen. Retrieved during the citizen identification. ● **String ConusmerID**: a unique string that identifies the consumer of the consent (e.g. the HCP). Retrieved during the HCPidentification. ● **String Purpose**: a string that clearly states the reason why the citizen should give his consent. ● **Date TimePeriod**: an expiration date of the consent. ● **Char ConsentType**: five different types of consent have been identified in terms of InteropEHRate. Store, Upload, Download, Backup and Research consents. The first character of each consent type is the possible value of this argument (e.g. s, u, d, b and r).
Return Value	● The actual consent in XACML representation.
Exceptions	● The citizen does not accept the informed consent.
Preconditions	● The citizen has read the informed consent and accepts it.

4. CONCLUSIONS AND NEXT STEPS

In this report, we defined the first version of the specification of consent management and decentralized authorization mechanisms for HR exchange focus on the objectives of the first year. A technical background with state-of-the-art mechanisms and standards was also provided. Similarly to other reports of the InteropEHRate project, this document presents a first draft of the consent management and authorization mechanisms, reflecting the current understanding by the project consortium. One second updated version (final version) of this report is planned on March 2021.

The following version will include a clearer view on the consent management and authorization mechanisms based on the new knowledge acquired from the first two years. Major changes are expected in particular with respect to consent management and authorization mechanisms needed in R2D and research protocols that are involved in usage scenarios [D2.1] that is still not analysed in detail.

REFERENCES

- **[XACML]** OASIS, XACML Oasis Specification. Website: https://www.oasisopen.org/committees/tc_home.php?wg_abbrev=xacml
- **[NGAC]** NGAC Functional Architecture. Website: http://www.incits.org/scopes/INCITS499.htm
- **[APPC]** Integrating the Healthcare Enterprise, Advanced Patient Privacy Consents (APPC), Rev. 1.2 – Trial Implementation, 2018. Website: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_APPC.pdf
- **[BPPC]** eHealth DSI Patient Summary and ePrescription, BPPC Profile, 2017.
- **[CM]** Wikipedia, Consent management, 2019. Website: https://en.wikipedia.org/wiki/Consent_management
- **[FRASER1997]** Fraser, B, *Site Security Handbook*, IETF, 1997.
- **[FERRAIOLO2016]** David Ferraiolo, Ramaswamy Chandramouli, Rick Kuhn, and Vincent Hu. 2016. Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC). In Proceedings of the *2016 ACM International Workshop on Attribute Based Access Control (ABAC '16)*. ACM, New York, NY, USA, 13-24,2016, DOI: https://doi.org/10.1145/2875491.2875496
- **[D2.1]** InteropEHRate consortium. *D2.7 : User Requirements for cross-border HR integration - V1*. InteropEHRate project, June 2019.
- **[D3.3]** InteropEHRate consortium. *D3.3 : Specification of remote and D2D IDM mechanisms for HRs Interoperability - V1*, InteropEHRate project, June 2019.
- **[ANDROID2019]** Google, Android keystore system, Website: https://developer.android.com/training/articles/keystore
- **[APPLE2019]** Apple, Keychain Services, Website: https://developer.apple.com/documentation/security/keychain_services