D2.5

InteropEHRate Architecture - V2

ABSTRACT

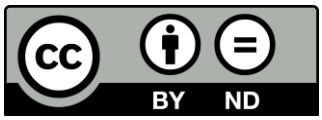
This report describes a novel architecture for citizen centred EHR interoperability and provides an overview of its reference implementation.

The "InteropEHRate standard architecture" specifies how different actors using applications offered by different vendors may interoperate for exchanging health data (coming from an EHR or from the person), thanks to open (vendor independent) communication protocols. This document also provides an introduction to the "InteropEHRate framework", a reference implementation of the standard architecture. The InteropEHRate framework provides a concrete example of implementation of the elements of the standard architecture and also includes additional components to support their usage. A more detailed description of each protocol and software component is described in referred deliverables that complement the present one.

Delivery Date	17th December 2020
Work Package	WP2
Task	T2.2
Dissemination Level	Public
Type of Deliverable	Report
Lead partner	ENG

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

This document has been produced in the context of the InteropEHRate Project which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 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	Julien Henrard, Lucie Keunen	A7
	Debora Desideri, Alessio Graziani, Francesco Torelli	ENG
	Thanos Kiourtis, Argyro Mavrogiorgou	UPRC
	Sofianna Menesidou	UBIT
	Gabor Bella, Simone Bocca	UNITN
	Chrysostomos Symvoulidis	Singular Logic
Reviewers	Paolo Marcheschi	FTGM
Reviewers	Gabor Bella	UNITN

LOGTABLE

Version	Date	Change	Author	Partner
0.1	24-02-20	Creation of new TOC and proposal on sections to update	Francesco Torelli	ENG
0.2	26-02-20	Updates to section 1.4, 1.5	Francesco Torelli	ENG
0.3	06-04-20	General revision and updating of content from previous version	Francesco Torelli	ENG
0.4	22-06-20	Updates to text and images of chapter 3 “InteropEHRate Framework” and of chapter 2 “Standard InteropEHRate Architecture”. General reformatting	Francesco Torelli	ENG

0.5	26-05-20	Updates to section 1.5	Francesco Torelli	ENG
0.6	06-07-20	Updates to section 2.4.2, 2.4.3	Francesco Torelli	ENG
0.7	13-07-20	Added new section “RDS protocol”	Francesco Torelli	ENG
0.8	02-08-20	Updates to sections 2.4.1, 2.4.2. Added new section 2.4.7	Francesco Torelli	ENG
0.9	23-09-20	Added new chapter 3 “Usage of protocols within scenarios” and related subsections	Francesco Torelli	ENG
0.10	29-09-20	Added new section “HR Index” updated sections “D2D protocol”, “Conclusions”	Thanos Kiourtis	UPRC
0.11	29-09-20	General correction to the document, Updated section “4.8 Example of HCP App”, “5 Conclusions”	Nicu Jalba	SIMAVI
0.12	29-09-20	Updated section “4.7 S-EHR Cloud RI”, “5 Conclusions”	Chrysostomos Symvoulidis	BYTE
0.13	30-09-20	Updated new sections “2.4.7 Research Network Central Node”, “4.9 InteropEHRate Health Services (IHS)”, “4.9.1 S- EHR Conversion and Translation Services”	Simone Bocca	UNITN
0.14	30-09-20	Updated section “4.6 S-EHR Mobile App RI”, “5 Conclusions”	Martin Marot	A7
0.15	05-10-20	Updated section “R2D Access protocol”	Alessio Graziani	ENG
0.16	08-10-20	Update of section 2.4.4. Added new section 2.4.5, Updated sections “2.5.6 RDS protocol”,	Gabor Bella	UNITN

		"4.10 InteropEHRate Research Services (IRS)", "5 Conclusions"		
0.17	09-10-20	Updates to section 2.4, Added new section "R2D Backup protocol", Updated section 4 "InteropEHRate Framework" and related subsection	Francesco Torelli	ENG
0.18	09-10-20	Merging of section 2.5.1 and 2.5.2 and extension, Update of conclusions	Sofianna Menesidou	UBIT
0.19	09-10-20	Updated section 4.7 S-EHR Cloud RI, 5 Conclusions	Chrysostomos Symvoulidis	BYTE
0.20	15-10-20	Updated sections 1.3 Structure of the document, 1.4 Updates with respect to the previous version, 1.5 Relation to other project results, 2.1 Actors, 5 Conclusions. Revision of recent contributions	Francesco Torelli	ENG
0.21	28-10-20	Update of sections 2.5.1 and 5	Thanassis Giannetsos	UBIT
0.22	09-11-20	Update of sections 2.5.1 and 1.4	Thanassis Giannetsos	UBIT
1.0	09-11-20	General revision.	Francesco Torelli	ENG
1.1	24-11-20	Application of corrections and changes suggested by the internal reviewers to the overall document	Francesco Torelli	ENG
1.2	26-11-20	Update of section 2.4.5	Thanos Kiourtis	UPRC
1.2	27-11-20	Update of section 2.5.1	Sofianna Menesidou,	UBIT

			Thanassis Giannetsos	
1.2	30-11-20	Update of the glossary and alignment of terms within the text.	Francesco Torelli	ENG
1.3	07-12-20	Update of all activity diagrams of section 3 to include more details related to security	Sofianna Menesidou, Thanassis Giannetsos	UBIT
1.4	09-12-20	Further updates to activity diagrams of section 3 and correction of references	Francesco Torelli	ENG
1.5	15-12-20	Quality Check	Argyro Mavrogiorgou	UPRC
1.6	16-12-20	Quality corrections	Francesco Torelli	ENG
Vfinal	17-12-20	Final version and submission	Laura Pucci	ENG

ACRONYMS

Acronym	Description
API	Application Programming Interface.
CN	(Research Network) Central Node
CTMS	Clinical Trial Management System
D2D	Device to Device Protocol
EHR	Electronic Health Record (System)
HCP	Healthcare Professional
HCP App	Healthcare Professional Application
HD	Health data
HTTP	Hypertext Transfer Protocol
IHS	InteropEHRate Health Services
IHT	InteropEHRate Health Tools
IRS	InteropEHRate Research Services
KDF	Key Derivation Function
MD2DI	Mobile Device to Device Interface
PHR	Personal Health Record (System)
R2D	Remote to Device protocol
R2DI	Remote to Device Interface
RD	Research Data
RDS	Research Data Sharing (protocol)
RSI	Research Interface
SAAS	Software As A Service

S-EHR	Smart EHR (shorthand of Smart EHR mobile Application)
S-EHR App	Smart EHR Application (shorthand of Smart EHR mobile Application)
S-EHR Mobile App	Smart EHR mobile Application
S-EHR-C	S-EHR Cloud
TD2DI	Terminal Device to Device Interface

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 Scope of the document

The present document describes the InteropEHRate standard architecture. It provides an overview of several kinds of software services and applications for the direct management of health data by the citizens and of an integrated set of interoperability protocols that such applications and services are required to support. The specification of protocols (provided in the referred documents) is open, in the sense that any vendor of software for healthcare and health research is free to implement and support the specified protocols.

First of all, the document identifies individual actors and organisations that (especially in the EU context) need to exchange health data in a secure and interoperable way. Afterward it describes how new applications and protocols defined by the InteropEHRate project support such an exchange by means of the citizens' mediation.

A complementary goal of this document is to describe the architecture of the InteropEHRate Framework, which offers a reference implementation of the elements of the standard architecture and includes additional components to support the interoperability. These two architectures summarize the technical results expected from the project.

1.2 Intended audience

The document is intended to policymakers, architects and developers interested (1) to have an overview of how the InteropEHRate protocols and applications support the exchange of health data among EU parties in a secure and trustable way, (2) to understand which other reports provide additional details, and (3) to identify software results they can reuse.

1.3 Structure of the document

Section 1 (this section) explains the goal and structure of the document and its relation to other reports. Section "2. InteropEHRate Standard Architecture" goes into the details of the standard architecture. Section "3. Usage of protocols within scenarios" describes how the elements of the InteropEHRate architecture interact to realise the InteropEHRate scenarios (defined in deliverable D2.2-User Requirements for cross-border HR integration - V2 **[D2.2]**). Section "4. Architecture of the InteropEHRate Framework" presents the extended architecture of the reference implementation. Section "5. Conclusions and next steps" describes the expected improvement to be applied in the third and final version of the InteropEHRate architecture.

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

This document updates and supersedes the previous version "D2.4 - InteropEHRate Architecture V1". Main novelties with respect to the previous version are the inclusion in the architecture of new components and related organisations that are needed to support the additional (with respect to D2D and R2D Access) communication protocols that now have a first design: R2D Backup, R2D Emergency, RDS. New sections have been added to describe new components and conceptual steps of each protocol. Other sections have also been updated to take into account the connections with new elements and better clarify the relationship with legacy systems.

In particular, a completely new chapter - “3 Usage of protocols within scenarios” - has been added to describe, by means of UML Activity Diagrams, which functionalities offered by the InteropEHRate APIs are specifically exploited to realise the scenarios defined in deliverable **[D2.2]**.

Also, the following sections are new:

- “2.4.4 Central Knowledge provider”
- “2.4.6 HR Index”
- “2.4.6 Research Network Central Node”
- “2.5.1 Data Interoperability”
- “2.5.4 R2D Backup protocol”
- “2.5.5 R2D Emergency protocol”
- “4.2 Additional organisations”

Moreover, relevant changes have been applied to the following sections:

- “2.1 Actors”: new actors (PI of the Study, PI of the Research Centre) have been added.
- “2.2 organisations”: new organisations have been added (Certification authority, Central Node Provider, Central Knowledge Provider, Pseudonym Provider, HR Index Provider).
- “2.3 Overview”: figure and text have been updated to make clearer that R2D Access is not tied to a specific kind of health data source but may be supported by any kind of healthcare organisations.
- “2.4 Standard applications and interfaces”: the standard architecture now distinguishes the APIs (R2D CloudWriter, R2DCloudReader) required by different R2D protocols, additional legacy systems, and new optional and mandatory systems involved in RDS and R2D Cloud protocols.
    - “2.4.2 S-EHR Cloud”: the description of functionalities and related protocols has been extended.
    - “2.4.6 Research Centre System”: the description of this legacy system has been updated to distinguish it from the Research Network Central Node.
- “2.5.2 Security Protocols”: (merging subsections previously called “2.5.1 R2D Security Protocol” and “2.5.2 D2D Security Protocol") has been extended to cover the security mechanism needed by the RDS protocol and new versions of the R2D protocols. The section provides a detailed description of the operation and underpinnings of the security schemes that have been adopted in InteropEHRate, towards the provision of enhanced user authentication, data integrity, user privacy and trust services during health data exchange. These specifications have also been coupled with the documentation of the new components and related authorization entities that are needed to support such advanced cryptographic primitives following the current standard recommendations.
- “2.5.3 R2D Access protocol”: (previously called “2.5.3 R2D protocol”) provides more details on the protocol R2D Access, while the R2D protocols related to S-EHR Cloud are now more extensively described in new sections 2.5.4 and 2.5.5.
- “2.5.6 D2D protocol”: now describes the functional steps of the D2D protocol.
- “2.5.7 RDS protocol”: (previously called “2.5.7 Research protocol”) includes additional details recently designed.
- “4.3 Component view”: (previously numbered 3.2) the component diagram now includes the reference implementation of new components.
- “4.4 Deployment view”: (previously numbered 3.3) presents an updated deployment diagram including the new components.

- "4.6 S-EHR Mobile App RI": (previously numbered 3.4) contains an updated list of functionalities provided by the reference implementation.
- "4.7 S-EHR Cloud RI": (previously numbered 3.5) presents the new version of the S-EHR Cloud design.
- "4.8 Example HCP App": (previously numbered 3.6) the component diagram showing the design of the app has been updated to include the usage of new sub-components and the description has been updated accordingly.
- "4.9 InteropEHRate Health Services (IHS)": (previously numbered 3.7) now describes Information extraction capabilities and gives details on two different kinds of approaches for Machine Translation that are supported.
- "4.12 Interactions between the HCP App, IHS, and Legacy Systems": this section was thoroughly revised to reflect the progress made on the design and implementation of IHS and the underlying conversion and translation services.

Other sections provide the same information of the previous version, but some minor change to the text has been applied to remove errors, improve clarity and reduce redundancy.

1.5 Relation to other project results

The InteropEHRate project has the goal of complementing the current European approaches for EHR interoperability, mainly based on the usage of central services for the access by HCPs to citizen's health data, with a more decentralized model, based on "citizen mediation" and on services offered directly from data producers and consumers.

The main result of InteropEHRate is an **open specification**, classifying new kinds of applications and defining new open interoperability protocols, allowing the citizens to:

- access (also) cross-border to their health data;
- interact (also) cross-border with healthcare organisations and research institutions;
- use also applications developed by private companies to exchange health data.

The open specification is composed of the following elements, each one described by a separate document:

- **FHIR profiles for EHR interoperability** (described in the report D2.8-FHIR profile for EHR interoperability - V2 **[D2.8]**): common data model, based on the FHIR standard, shared by all the InteropEHRate protocols.
- **S-EHR conformance levels** (described in the report D3.1- Specification of S-EHR mobile privacy and security conformance levels - V1 **[D3.1]**): constraints and guidelines that a S-EHR Mobile App or a cloud storage service for health data has to fulfil to be considered secure, reliable and compliant to InteropEHRate.
- **D2D protocol** - for EHR interoperability (described in the report D4.2- Specification of remote and D2D protocol and APIs for HR exchange - V2 **[D4.2]**): secure communication protocol (and remote APIs) for exchanging health data between two nearby devices (not using internet), one running a S-EHR App and the other running an HCP App.
- **R2D protocols** - for EHR interoperability (also described in the report **[D4.2]**):

- **R2D Access:** Secure IT communication protocol (and remote API) used by a S-EHR App for receiving, over the Internet, health data from and healthcare organisation.
- **R2D Backup:** Secure IT communication protocol (and remote API) for the backup of health data from a S-EHR App on a S-EHR Cloud.
- **R2D Emergency:** Secure IT communication protocol (and remote API) for the exchange of health data between an HCP App and a S-EHR Cloud during emergency care.

- **RDS protocol** - for research health data sharing (described in the report D4.8- Specification of protocol and APIs for research health data sharing - V1 **[D4.8]**): secure communication protocol (and remote API) for exchange of health data, over the Internet, between any S-EHR Mobile App and any Research Centre.

By remote API we mean an API exposed by a system to another system (that must be physically near systems in the case of D2D), while by remote protocol we mean a protocol for communication that may happen among physically far systems.

The main purpose of the present document is to describe the **InteropEHRate standard architecture**. The InteropEHRate standard architecture is a high-level view of the open specification, correlating and constraining the other specific reports.

The InteropEHRate project also provides a **reference implementation**, called **InteropEHRate framework** (also called, more informally, "InteropEHRate platform"[1]), composed of different software components, each one implementing a different part of the specification and reusable one independently from the others. The InteropEHRate framework will also contain a set of complementary tools, supporting the usage of the interoperability protocols. A software developer may realize its own implementation of the InteropEHRate open specification or can reuse components provided by the InteropEHRate framework.

Both the InteropEHRate standard architecture and the InteropEHRate framework are intended to realize the scenarios and to satisfy the requirements specified in the report **[D2.2]**. While the report [D2.2] adopts a point of view more oriented to the final users, this report is more intended for developers and therefore adopts a more technical language. Where possible anyway the two documents adopt a common terminology.

The following section will describe the current InteropEHRate standard architecture, while the successive one will describe the current architecture of the InteropEHRate framework.

[1] In the Software Engineering domain a "software framework" is usually intended as a software that facilitates the development of specific kinds of applications (e.g. the Apache Spark framework for cluster-computing), while a "software platform" is intended as a software or hardware environment in which applications are executed (e.g. Android platform). Following this distinction, this deliverable prefers to adopt the name "InteropEHRate framework" to refer to the integrated set of software results of the project. Anyway the project adopts also the denomination "InteropEHRate platform" because in the market the semantics of the terms "platform" and "framework" overlaps and because in the health domain the term "platform" is usually used to refer to a software, while the term "framework" is often used to refer to specific rules, methodologies or other abstract concepts (e.g. a legal framework or a quality evaluation framework).

2 INTEROPEHRATE STANDARD ARCHITECTURE

The InteropEHRate standard architecture is a high-level view of the InteropEHRate open specification. It enables citizen centred and decentralised health data sharing, through the secure storage of health data on Citizen's personal mobile devices and the direct exchange of health data between citizens and healthcare organisations or research centres trusted by the citizens, avoiding sharing health data with app vendors or other third parties.

The specification(s) defines a family of open source communication protocols and a set of constraints for mobile applications and optional cloud services that support the secure cross any border exchange of health data with or without Internet, with or without cloud storage, in a GDPR compliant way.

The InteropEHRate open specification is open in the sense that each one of the specified protocols and applications may have different implementations, possibly provided by different competing vendors. Conformance to the open specifications assure the interoperability among implementations of different vendors.

The InteropEHRate open specification is also modular: it is not required to implement the entire InteropEHRate standard architecture; each protocol may be used individually or in combination with the other ones, therefore in each context only the required portion of the InteropEHRate standard architecture may be implemented, depending from the usage scenario.

The purpose of this section is to describe the InteropEHRate standard architecture for EHR interoperability, in particular, it provides an overview of the involved actors and organisations, standard software services and applications, and standard interaction protocols.

2.1 Actors

The InteropEHRate standard architecture is intended to allow different kinds of users to exchange in a secure way a set of trusted health data. The following table describes the different kinds of (individual) final users (called "actors", following the UML terminology). The same actors are defined in **[D2.2]** (replied here for simplifying the reading of the document).

Actors	Description
Citizen	A person of a specific country whose health data are managed by an application included in the InteropEHRate architecture.
HCP	A Healthcare professional that produces and/or has access to the health data of a Citizen.
Researcher	A person that desires to exploit the citizens' health data for research purposes.
PI of the Study	Principal Investigator of the Study. The researcher (person) in charge of a specific research study at the Coordinating Research Centre (CRC).
PI of the Research Centre	Principal Investigator of a Research Centre. The researcher (person) in charge of the citizens enrolled for a specific research study at a Research Centre (RC).

Table 1 - Actors

2.2 Organisations

Hereafter a description of the standard types of organisations that may interact by using the InteropEHRate protocols. As some interaction may be performed by different types of organisations belonging to a more general type, the types of organisations are hereby reported in a hierarchy of concrete and more abstract types of organisations. The following set of terms includes and extends the one adopted in the deliverable **[D2.2]**.

Type of organisation	Description	More abstract type of organisation
Health Data Provider	An organisation maintaining health data and capable of providing them to authorised consumers.	
Healthcare organisation	An organisation that provides (directly or indirectly) healthcare services to citizens (e.g. a single Hospital or an entire national healthcare system).	Health Data Provider
Healthcare Provider	A private or public local organisation directly providing healthcare services (e.g. a Hospital, a General Practitioner).	Healthcare Organisation
National Healthcare System	An institution providing or managing at central level the public healthcare services of a country.	Healthcare organisation
Research Centre	An institution exploiting the personal health data of citizens for research purposes.	
S-EHR Cloud Provider	A public or private organisation that offers a cloud service to individual citizens for the storage of encrypted personal health data. The InteropEHRate architecture supports the existence of different S-EHR Cloud providers. The Citizen is allowed to access and exchange health data without the usage of any S-EHR Cloud provider.	Health Data Provider
S-EHR Provider	A provider (for free or for sale) of a S-EHR Mobile App.	
National Identity Provider	Public administrations or private sector organisations "issuing the electronic identification means and the party operating the authentication procedure". They provide their user base with a secure online identity which is used with a national eID scheme/s The identity provider is a national entity and provides electronic identifications that are accepted at national level[2].	
Certification authority	A trusted organisation that offers credential management services by issuing, certifying and revoking digital certificates and the corresponding public keys linked to the	

[2] https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=71776009

	long-term identity of their owners.	
Member state	A state of EU community providing an eIDAS node[3].	
Healthcare Solution Provider	A provider (for free or for sale) of software products used by Healthcare organisations.	
Central Node Provider	The provider of the central node of the research network, i.e. of the service that stores the Research Definition Documents (RDDs), describing research studies and published by the research centres that are part of the research network. The Central Node provides a central access point to S-EHR Apps for retrieving the RDDs.	
Central Knowledge Provider	A single European actor whose role is to maintain and provide easy-to-reuse computer-readable versions of health knowledge used for cross-border interoperability, such as FHIR data schemas or coding standards and their mappings. Such knowledge is downloaded by Health Data Providers and Healthcare Solution Providers who plug it into their systems, facilitating the implementation of interoperability-related — data integration, conversion, translation — tasks.	
Pseudonym Provider	A trusted organisation that is responsible for the pseudonym management of the short-term anonymous credentials (according to the 1609.2 specification **[1609.2-2016]**), to be provided to the S-EHR App as part of RDS protocol and used for the anonymous communication of the citizen's health data to a (Reference) Research Centre. Once the S-EHR App is authenticated (using its public certificate from the CA), it can then request pseudonyms from the Pseudonym Provider (PP). A certified pseudonym is a digital signature, produced by the PP, for this specific (citizen's) public certificate.	
HR Index Provider	A European trusted organisation that provides the HR Index service to all citizens and organisations that are willing to exploit the R2D Emergency protocol. The HR Index, and therefore the existence of its provider, are not mandated by the R2D Emergency protocol but may be useful to increase its flexibility.	

Table 2 - Organisations

[3] https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=82773030

2.3 Overview of applications and services

The following figure shows in an informal and simplified way a typical set of actors, software services, and applications exploiting the new applications and protocols specified by InteropEHRate. The picture is intended as an introduction to the main elements of the architecture and is informal both because it does not use a standard specification language and because the depicted components and interactions are not exhaustive, but merely represent common examples. A more formal description using UML notation is provided in the following sections.

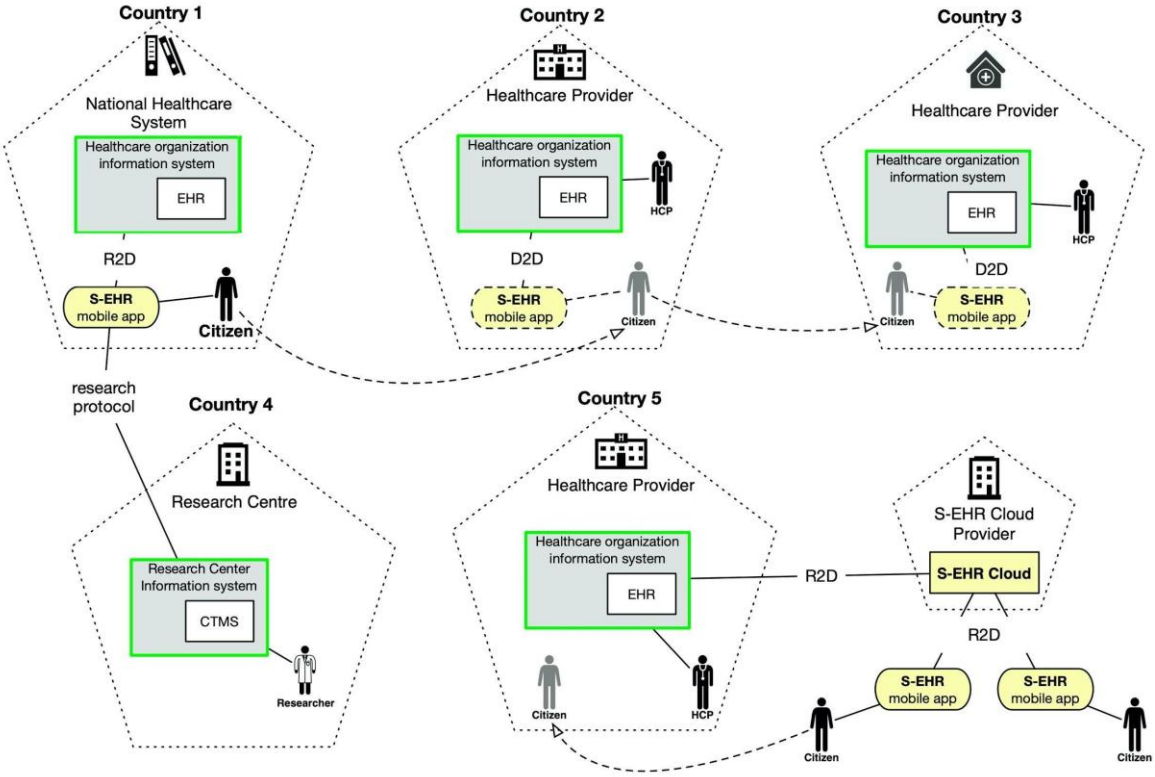


Figure 1 - Examples of health data exchange using a S-EHR Mobile App and a S-EHR Cloud

The main objective of InteropEHRate is to ease the exchange of health data between citizens, healthcare organisations and research centres. The InteropEHRate architecture assumes that in the near future the EU citizens will own standard kinds of mobile applications called Smart EHRs (S-EHRs). Note that a S-EHR is not a specific software, but a standard kind of software. Citizens will be able to choose among different standard S-EHRs offered by different vendors. To emphasize the fact that it is a user application, throughout all this specification, a S-EHR is also called S-EHR Mobile App or S-EHR App. It is able to store in a secure (encrypted) way on a mobile device any health data related to the history of the person that owns the device.

By mobile devices we mean mainly modern smartphones or tablets, but it could include in the future also other types of mobile devices with advanced computational capabilities, like smartwatches or smart bracelets and other kinds of smart devices that may move with the citizen. The stored health data may be produced by healthcare professionals, by sensors, or by any citizen in the role of a patient.

A S-EHR is able to receive health data from any healthcare organisation that adopts the standard protocols specified by the InteropEHRate project. These protocols guarantee the integrity of exchanged data, the traceability of their provenance and their trustability.

More specifically the S-EHR uses the so called Remote-to-Device (R2D) protocol to exchange health data at distance (on the Internet) with healthcare organisations while the Device-to-device (D2D) protocol allows exchanging health data with healthcare organisations during face to face encounters (without the usage of internet, but adopting short range communication technologies like Bluetooth). The portion of the information system of the healthcare organisation used by HCPs to interact with the S-EHR is called HCP App.

The above picture shows an example of a citizen using a S-EHR for importing health data from an EHR that is connected to the National Healthcare System of the country of residence (e.g. the EHR of a specific healthcare organisation or a national EHR) and for exchanging the same data and new health data with the EHR system of a hospital located in a different country.

In particular, the R2D protocol is intended not only for the exchange of health data directly with data producers, like Hospitals and Clinical laboratories but also for importing health data from existing repositories such as cloud based PHRs and national EHRs already provided to the citizens of EU countries.

In order to allow the exchange of health data with S-EHRs, the health data providers will need to extend their information systems (e.g. internal general-purpose EHRs or more specific health applications) to provide the remote interfaces, and the extended functionalities, required by the InteropEHRate protocols.

In the case of the R2D protocol, the person that is the subject of the data (the Citizen in the picture) exchanges health data using his or her S-EHR that interacts with a remote interface offered by the healthcare organisation, while in the case of the D2D protocol the health data are exchanged between a S-EHR and a local interface offered by a terminal near to the S-EHR (e.g. a desktop computer or a tablet) used by the Healthcare operator (HCP). The application (part of the health organisation information system) used by the HCP is informally called HCP App and may be a legacy application already used by the healthcare organisation and extended to support the D2D protocol or may be a completely new standalone application. The InteropEHRate open specification does not specify any constraint for the HCP App, but just requires that the information system of the healthcare organisation offers a D2D interface.

In the InteropEHRate vision, different vendors may offer different S-EHRs to the final users and each user may choose the preferred one, according to his or her needs and to the added-value functionalities offered by the specific S-EHR. Regardless of the differences, all S-EHRs have to satisfy a set of standard rules and requirements aimed to guarantee strong levels of security and trustability (specified in report **[D3.1]**) to citizens and organisations that interact with them.

A S-EHR is different from many mobile applications and SaaS (Software as a Service) currently available on the market because it adopts open exchange protocols that are vendor-independent (so avoiding the lock of citizen's data in proprietary data silos) and also because the user moves among countries (see dotted arrows in the picture) bringing the health data with him or her, stored on the mobile device. The user does not need to access any cloud service to consult the health data and does not need to allow a service provider to store and control all the collected personal health data. The health data of the user are always

available on the mobile device and are fully controlled by the user. This approach allows access to the stored data also in situations where, for whatever reason, the Internet is not available. Also, data exchange may be supported without sending the data on the Internet, so reducing the risk of interception and corruption of the data. The distributed nature of the storage model (i.e. data of different citizens are stored on different devices) avoids the security risks of models where data of many citizens and coming from different data sources (e.g. different hospitals) are stored in the same central repository accessible from the Internet and where a single hacker's attack put at risk the data of all users.

With InteropEHRate, users may still choose to maintain a backup copy of their personal health data on a cloud service, but this is an optional choice and any user may choose a different cloud storage service called S-EHR Cloud (see section 2.4.2), possibly offered by a vendor distinct from the one that offers the S-EHR App. Moreover, the data are sent to the cloud service in an encrypted format not intelligible to the service provider, therefore the risk of unauthorized usage of the data from malicious service providers or hackers is sensibly reduced. As shown in the figure, the communication between a S-EHR App and a S-EHR Cloud is also specified by the R2D protocol (that is actually a set of different remote APIs and rules covering different scenarios for exchange of health data at distance).

A S-EHR may also support the Research Data Sharing (RDS) protocol, an electronic communication protocol that allows any person to send personal health data (over the Internet) in a secure way to a specific remote Research Centre, in order for the data to be exploited for research purposes. The RDS protocol allows scientists to engage voluntary citizens at cross-national levels in new research trials or retrospective studies and allows citizens to easily and securely share health data, including both certified (i.e. clinical) and wellness data, in pseudonymized or anonymized form. The protocol specifies both how the data must be sent and how the research centre may communicate to the citizen the aims of the research and how the research centre may ask the needed consent for specific usage of the data.

Each one of the InteropEHRate protocols includes specific security protocols, aimed to guarantee the cross-border identification of the citizens and the privacy, integrity and trustability of data exchange.

The security protocols (see section 2.5.2) involve several organisations and services not shown in the simplified figure above. The InteropEHRate protocols leverage existing standards like International Patient Summary (IPS)[4] and regulations like EIDAS and related EU services like CEF eID[5].

Traditional models for the exchange of health data among different Healthcare providers adopt central services for health data access. Typical examples are national EHRs, accessible by healthcare providers of the same country or region. Other examples are national contact points (like in the eHDSI infrastructure for EHR interoperability) that a country offers to national contact points of other countries to allow the authorized Healthcare providers of these other countries to access citizen's health data. Such models are "top-down" in the sense that the access to data provided by different healthcare providers is coordinated from central services that are "on the top" of these organisations and of the citizens that receive the services. InteropEHRate is intended to integrate this "top-down" model of interoperability with a "bottom-up" approach where single vendors and healthcare providers may choose to implement and adopt the InteropEHRate protocols from the bottom, i.e. without the need of a central service above them. In this

[4] http://hl7.org/fhir/uv/ips/
[5] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID

more decentralised model, the exchange of health data is not mediated by institutions providing central services but is mediated by the citizens that permit access to their health data stored on their personal S-EHRs.

The traditional model and the InteropEHRate one are intended to coexist and complement each other in order to cover more usage scenarios.

InteropEHRate is aimed to promote the growth of a new market based on the offer of S-EHR Apps and related services. It is also aimed to empower the citizens, giving them more immediate access to their data, more control over their usage and more possibilities of exploiting health data both for improving personal health and for contributing to the increment of medical knowledge at the disposal of all EU citizens.

2.4 Standard applications and interfaces

This section and its sub-sections describe in a more formal way, using UML notation and textual descriptions, the standard type of systems and remote interfaces specified by InteropEHRate, for supporting the communication between Citizens, Healthcare organisations and Research Centres, in a same country or in a cross-border context (i.e. for exchange of health data from within different countries).

The software systems and interfaces constrained by the InteropEHRate standard architecture are shown on the following UML component diagram. Each software system is represented as a component offering and requiring different interfaces. For better clarity, different colours are adopted:

- grey, for legacy systems,
- blue, for standard legacy interfaces and systems,
- yellow, for (new) systems specified by InteropEHRate,
- green, for (new) interfaces specified by InteropEHRate.

The only mandatory element of this architecture is the S-EHR App. All other components are involved only in specific communication protocols, so their actual usage depends on specific use cases and from the preferences of the citizens and institutions. For instance, a citizen may decide to not exploit any S-EHR Cloud or institutions may decide to not provide an HR Index (see section 2.4.5). Some types of systems require a single instance, while other ones may or must have different instances. These distinctions are clarified below.

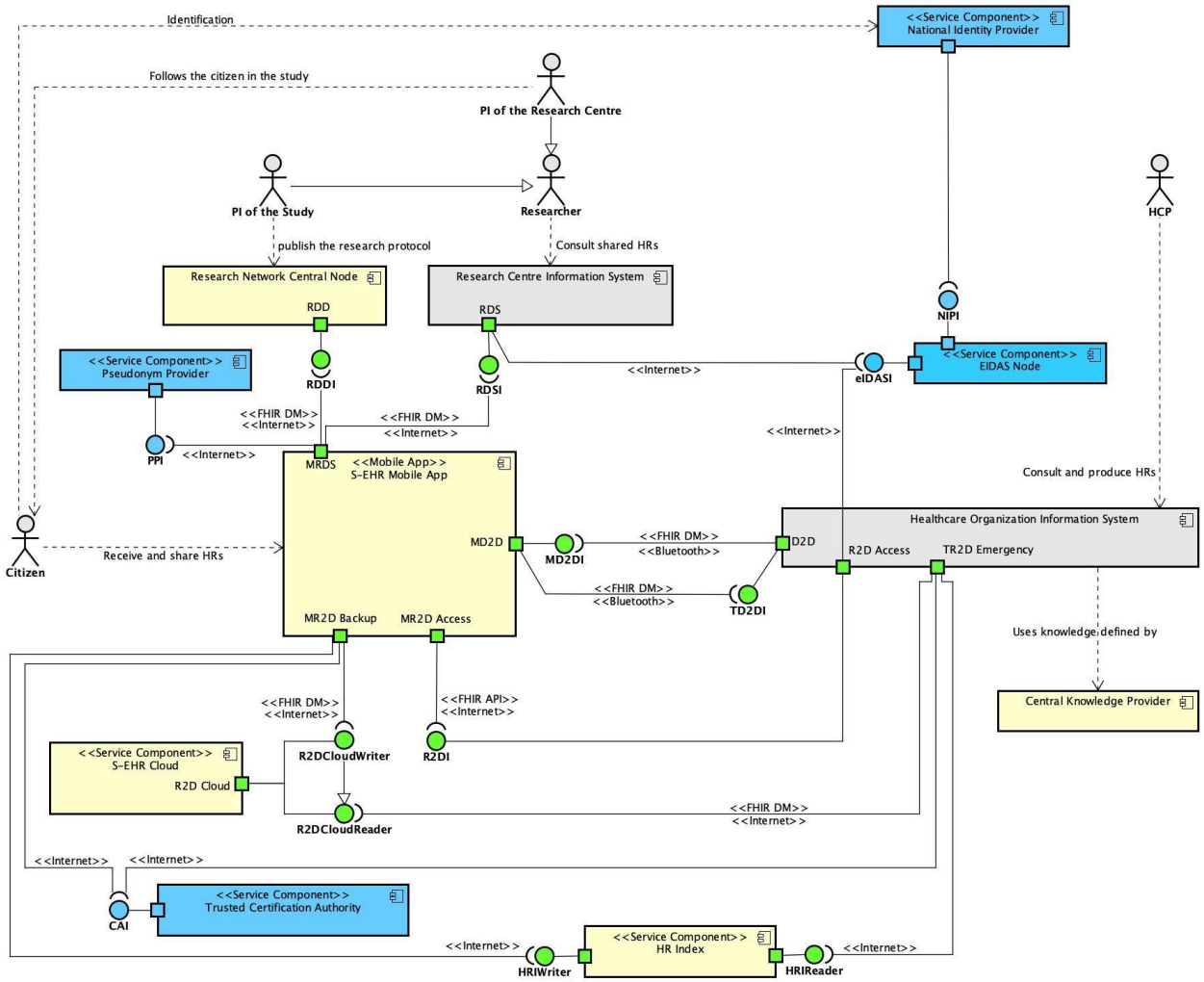


Figure 2 - InteropEHRate standard architecture

The InteropEHRate protocols constrain the interactions among three kinds of software systems:

1. S-EHR Mobile App, one for each Citizen: the mobile application, used by the Citizen, to store and exchange personal health data using the InteropEHRate protocols.

2. Healthcare organisation information system, one for each Healthcare organisation: a system composed of all software applications used by the Healthcare Operators (HCPs) within a Healthcare organisation, extended to support the InteropEHRate protocols for health data exchange with S-EHR. There is one per healthcare organisation.

3. Research Centre Information system, one for each Research centre: a system composed of all software used by any Researcher (i.e. scientist), to produce and access Citizens' health data.

4. Research Network Central node, a single system provided by the Central Node Provider: gives a central access point to S-EHR Apps for retrieving the descriptions of research studies.

Moreover, the InteropEHRate protocols involve the following standard systems:

5. eIDAS (electronic IDentification Authentication and Signature) Node, one per country, to support services capable of identifying citizens and businesses from other Member States. The eIDAS Regulation ensures that people and businesses can use their own national eIDs to access online public services in other EU countries, where eIDAS node are available. The eIDAS Network consists of a series of eIDAS-Nodes implemented at the Member State level. National Identity Providers Interface (NIPI) is used to connect the eIDAS-Node in the user's Member State to their National Identity Provider. The procedure of user authentication takes place between the user and the National Identity Provider, it is outside both the eIDAS Network and InteropEHRate system.

6. CA (Certification authority) System, one per Certification authority: issuing, certifying and revoking digital certificates and the corresponding public keys linked to the long-term identity of their owners. Certificates are used for the authenticated communication between the S-EHR App and HCP App, S-EHR App and (Reference) Research Centres and HCP App and S-EHR Cloud.

Finally, the protocols may also involve the following optional[6] system:

7. S-EHR Cloud, offered by a specific vendor, to support the remote storage/backup of personal health data.

8. HR Index (Health Record Index), a mediator for informing the healthcare practitioners about the location of the S-EHR Cloud of the citizens, in order to address emergency cases also in case that the Emergency QR-code has not been updated.

The new (open standard) interfaces introduced by InteropEHRate for the interactions among the different subsystems are listed in the following tables. Such remote interfaces are part of the interoperability protocols, the current version of which is described in the reports D3.3-Specification of remote and D2D IDM mechanisms for HRs Interoperability - V1 **[D3.3]** and D4.5-Design of libraries for remote and D2D HR exchange - V2 **[D4.5]**. The current version of the protocols covers just a portion of the functionalities of the architecture, while full coverage will be provided with the final version. The data model adopted by the protocols and interfaces will be defined as a set of constraints and extensions on top of the standard **[HL7 FHIR]** and will be specified in **[D2.8]**.

[6] These systems are optional in the sense that the Citizen may choose to not adopt them.

Protocol	Defined Remote API	Description
D2D	MD2DI	Mobile Device to Device Interface: offered by the S-EHR to support the D2D protocol, i.e. to exchange health data with citizen's S-EHRs at a short distance, without using the Internet.
	TD2DI	Terminal Device to Device Interface: offered any application used by HCPs to support the D2D protocol, i.e. to exchange health data with citizen's S-EHRs at a short distance, without using the Internet.
R2D Access	R2DI	Remote to Device interface: offered by the Healthcare organisation to support the R2D Access protocol. It allows the S-EHR App to access at distance (by means of the Internet) the health data of the Citizen produced by the organisation.
R2D Backup	R2DCloud Writer	Remote to Device Cloud Writer interface: offered by a S-EHR Cloud to any citizen to support the R2D Backup and Emergency protocols. It allows a S-EHR App to store health data on a S-EHR Cloud for backup reasons and/or for allowing HCPs to access the data in emergency situations also in case the S-EHR App is not available.
R2D Emergency	R2DCloud Reader	Remote to Device Cloud Reader interface: offered by a S-EHR Cloud to any HealthCare organisation to support the R2D Emergency protocol. It allows a trusted HCP App to access by means of the Internet, in emergency situations, the health data of the Citizen stored on the S-EHR Cloud. It is useful when for some reason the HCP cannot access, using the D2D protocol, directly the health data stored on the S-EHR App of the citizen.
	HRIReader	HR Index Reader Interface: offered by the HR Index to any trusted HCP App. It allows the HCP App to find the location of the S-EHR Cloud of a Citizen also if a Citizen has changed it but has not updated the emergency token shared with HCPs.
	HRIWriter	HR Index Writer Interface: offered by the HR Index to any S-EHR App. It allows a S-EHR App to share, only with trusted HCPs, the location of the S-EHR Cloud of the Citizen, to be used during emergency situations. A Citizen may choose to not use the HR Index and share the location of the S-EHR Cloud by means of the emergency token.
RDS	RDDI	Research Definition Document Interface: offered by the Research Network Central Node to the S-EHR App to retrieve the RDDs describing the research studies that citizens may participate in.

	RDSI	Research Data Sharing Interface: offered by the Research Centre Information System to the S-EHR App. Allow the citizens to upload the health data required by the research studies they are participating in.

Table 3 - Remote APIs defined and used by the InteropEHRate protocols

Other than the new remote APIs defined by InteropEHRate, the specified protocols also exploit the following legacy APIs:

Legacy Remote API	Using Protocols	Description
CAI	R2D, D2D, RDS,	The interface offered by the Certification Authorities to retrieve digital certificates.
PPI	RDS	The interface offered by the Pseudonym Provider for creating Pseudonyms.
eIDASI	R2D, RDS	The interface offered by the eIDAS Nodes for cross-border identification and authentication of Citizens.

Table 4 – Legacy remote APIs used by the InteropEHRate protocols

The usage relations with each API, depicted on the UML component diagrams, show the different communication channels (Internet or Bluetooth) used to interact with the remote API and which ones exploit the FHIR Data Model (DM) or also the FHIR API.
The following sections provide a description of the main functionalities provided and required from each subsystem.

2.4.1 S-EHR Mobile App

A S-EHR is any application installed on a personal mobile device that is able to store the personal health data of a user in a secure (encrypted) way according to the constraints specified by the deliverable "Specification of S-EHR mobile privacy and security conformance levels" **[D3.1]** and that supports the InteropEHRate protocols, deliverables **[D4.2][D4.8]**. Different vendors may develop different S-EHRs.

A S-EHR contains the health records of the user, possibly signed (for better traceability and trustability) by the healthcare organisation that produced them but can also contain other health data produced by the citizens themselves or by their sensors. The provenance and author of each health data item is unambiguously persisted on a S-EHR and the principles of integrity and non-repudiation are guaranteed.

The S-EHR supports the storage and exchange of three kinds of health data:

- Unstructured health data (txt, pdf, images, videos, signals).
- Structured health data compliant to the standard [**[HL7 FHIR]**].
- Structured health data compliant to the "InteropEHRate profiles" **[D2.8]**.

A S-EHR supports the natural language of the user and all structured health data that are compliant to the InteropEHRate profiles are presented in the user's natural language.

Text content of the health data is always stored and presented in the form (and natural language) produced by its author but may be enriched with translated versions (obtained by manual or automatic translation) that are also presented to the user.

Structured data containing semantic codes conformant to the "InteropEHRate profiles" and obtained by converting (in a manual or automatic way) local semantic codes (i.e. codes specific to a particular organisation), always contains also the original local semantic codes.

A S-EHR allows the user to access his or her health data independently from the availability of the Internet and does not mandate the support of any cloud service for the storage of health data. In other terms, the user is not obliged to access any cloud service to consult the health data and does not need to allow a service provider to store and control the personal health data.

Which data are stored on the mobile application and which actor may access them by using the InteropEHRate protocol is fully under the control of the user.

The main functionalities offered from a standard S-EHR Mobile App are:

- To show to the authorized user all stored health data.
- To import/share health data from/with a Healthcare Organisation.
- To exchange data with the organisation Information System by means of the D2D (device to device) communication protocol (short-range and wireless). These functionalities are supportive of use cases in which patients and HCPs want to exchange health data during a face-to-face encounter and the use of "servers on the Internet" is not possible (e.g. because the Internet is not available) or desirable (for security reasons). To this end a S-EHR implements the interface MD2D and uses the interface TD2DI offered by the computer terminal (part of the Healthcare organisation Information System) of the HCP.
- To import health data from an EHR using the remote R2D Access protocol. These functionalities are used when citizens and health data are in different places, for example, to allow the citizen to receive from a healthcare organisation a report produced after an encounter. To this end, the S-EHR uses the interface R2DI offered by the Healthcare organisation Information System.
- To receive and show Research Definition Documents (RDDs). An RDD describes a research study that the citizen is invited to participate in, by sending his or her health data. In particular the RDD contains the Health Research Protocol (HRP)[7], i.e. the description approved by an Ethical Committee of the purposes and methodology to collect and process the specific set of health

[7] Note that "Health Research Protocol" is different from "Research Health Data Sharing protocol", also called "Research Data Sharing" (RDS) protocol. The first one is a description of the rationale, objectives, and methodology of a clinical research trial. The second one is the set of rules specified by the InteropEHRate project that a S-EHR has to follow to exchange health data with the information system of a Research Centre.

and/or social data needed by the research study, to learn more about human health and treatments.

- To automatically determine if a Citizen is eligible to be enrolled in a research study.
- To send (in particular, donate) consent and health data in aggregated or anonymized or pseudonymized form to a research centre for a specific research study. To this end a S-EHR uses the interface RSI offered by the Research Centre Information System.
- To import/store data on an S-EHR Cloud service. This is useful to securely backup or move their data on another device. This operation is performed by using the interface R2DI offered by the S-EHR Cloud selected by the user.
- To authorise or de-authorise a specific Healthcare organisation to access, using the R2D or D2D protocol, to specific health data stored on S-EHR. This operation does not use external interfaces, but is completely performed on a S-EHR Mobile App.
- To authorise or de-authorise any Healthcare organisation to access during an emergency, using the R2D protocol, to a specific set of health data stored on the S-EHR Cloud. This operation uses the interface R2DI offered by a S-EHR Cloud to communicate the consent to a S-EHR Cloud.
- To trace any access to the user's health data. This operation does not use external interfaces, but is completely performed on a S-EHR Mobile App.

2.4.2 S-EHR Cloud

A S-EHR Cloud is any service for secure storage on the cloud of user's health data, that supports the InteropEHRate protocols called R2D Backup and R2D Emergency **[D4.2]** and that fulfils the "S-EHR conformance levels" **[D3.1]**.

A S-EHR Cloud may be offered by a vendor different from the one providing the S-EHR Mobile App. The main characteristics that distinguish a S-EHR Cloud from other cloud services available on the market is that health data are exchanged with a S-EHR Cloud in an encrypted format that cannot be decrypted by the S-EHR Cloud provider, because only the citizen that is the subject of the data owns the key to decrypt the data. As the data exchange protocols supported by the S-EHR Cloud do not involve the real identity of the citizen, the service may be potentially offered also to anonymous citizens.

A citizen interacts with a S-EHR Cloud using a S-EHR Mobile App, but a citizen may choose to use a S-EHR Mobile App without using any S-EHR Cloud.

A citizen may use a S-EHR Cloud only for the backup of health data (and for moving of data to other devices) exploiting just the R2D Backup protocol, or may also authorize any healthcare organisations belonging to a specific trusted list to access and decrypt the health data stored on a S-EHR Cloud in emergency situations, exploiting also the R2D emergency protocol. While the S-EHR Cloud is not required to know the real identity of the citizen, it is required to:

- know the real identity of the healthcare organisations in a trusted list and assure they are publicly recognised healthcare organisations;
- make the citizens aware of the organisations in the trusted list;

- allow only to organisations in the trusted list to download the encrypted health data;
- allow the healthcare organisations to download only the encrypted health data of the citizens that authorised the access in emergency;
- permanently maintain a non rejectable history of all accesses to the encrypted data, including all data needed to identify the person that requested to access the data;
- allow the citizen to download at any moment the access history to the encrypted data of that citizen.

A S-EHR Cloud is not able to provide to the healthcare organisations the key to decrypt the downloaded data, but the key can be obtained only by the healthcare organisation, during the emergency situation, directly from the citizen.

A S-EHR Cloud implements the remote interface R2DCloudWriter:

1. To allow the user of any authorized S-EHR app to upload and store encrypted health data.
2. To allow the user of any authorized S-EHR app to download encrypted health data previously stored by the same user.

A S-EHR Cloud implements the remote interface R2DCloudReader:

3. To provide access to an HCP of a healthcare organisation to the encrypted health data of a citizen in "emergency mode".

2.4.3 Healthcare organisation Information System

A *Healthcare organisation Information System* is the software system of any healthcare organisation that manages citizen's health records and exchanges them with authorised citizens using the InteropEHRate R2D or the D2D protocol.

Possible examples of a Healthcare organisation Information System are a Laboratory Information System, a Hospital EHR, or a National EHR that have been extended to allow the Citizens of a nation to import at distance in their S-EHR app, using the R2D Access protocol, any personal health data stored within those systems.

More in general, a *Healthcare organisation Information System* provides one or more of the following functionalities:

1. Allows authorized citizens to download their health data into their S-EHR App using the R2D Access protocol. To this end the Healthcare organisation Information System offers the interface R2DI used by a S-EHR app of the citizen.
2. Is able to upload health data shared by a citizen to the information system of a Healthcare organisation during a face-to-face encounter. To this end, the Healthcare organisation Information System uses the interface MD2DI offered by a S-EHR app of the citizen.
3. Allows the citizens to import on their S-EHR app their health records shared by the Healthcare Organisation during a face-to-face encounter. To this end, the Healthcare organisation Information System offers the interface TD2DI to the S-EHR app of the citizen.

4. Is able to access in emergency cases to the health data of a citizen stored on a S-EHR Cloud. To this end, the Healthcare organisation Information System uses the interface R2DCloudReader offered by the S-EHR Cloud of the citizen.

In order to exchange health data using the InteropEHRate protocols, the Healthcare organisation Information System must adopt a syntactic and semantic representation of the health records that is compliant to the InteropEHRate FHIR profiles or it must be able to convert the health records from the representation required from the InteropEHRate FHIR profiles to the local format and vice versa. An advanced Healthcare organisation Information System should also be able to translate the health data received by the citizen to the language spoken by the HCPs and vice versa. The conversion and translation operations are out of the scope of the InteropEHRate open specification, but specific tools for these operations are provided by the InteropEHRate framework.

A *Healthcare organisation Information System* that supports the protocol R2D Access also uses the interface eIDASI, offered by the eIDAS node, for cross-border identification of the citizens. Through this interface, the Healthcare organisation Information System sends authentication requests to the eIDAS-Node and receives the authentication responses. The procedure of user authentication takes place between the user and the Identity Provider; thus, it is independent of both the eIDAS Network and the InteropEHRate systems.

2.4.4 Central Knowledge Provider

In the InteropEHRate approach, healthcare information systems use a mechanism based on formal, computer-readable health knowledge in order to ensure the conversion of health data into robustly cross-border-interoperable representations. The role of the Central Knowledge Provider, which is envisaged as a Europe-wide institution, is to manage a single, centralised, up-to-date version of the portion of shared formal knowledge, i.e. knowledge that is shared across countries and healthcare institutions. Management means:

- the implementation of standards as formal knowledge;
- providing these implementations for download using standard representations that can be directly imported into health systems that conform to the InteropEHRate specifications;
- maintaining the formal knowledge up to date, following the evolution of international standards (such as moving from ICD-10 to ICD-11, the definition of a new LOINC code, or the evolution of FHIR) upon which it is based.

While in theory the adoption of international data exchange standards should in itself guarantee interoperability, in practice the various system-level implementations of the same standard tend not to be identical, due to the complexity of the standard, divergences in interpretation, or other motives. The availability of standards implemented as formal knowledge and downloadable by system providers leads to a lower risk of diverging implementations and, thus, better real-world interoperability across systems.

2.4.5 HR Index

The HR Index (Heath Record Index) is a mediator for informing the healthcare practitioners about the cloud location of the stored EHR data of the citizens, without directly providing the data to them, in order to address emergency cases where the citizens are not able to provide their consent for third-party accessing

of this EHR data (supposing that in the past such consent has been already approved by the citizen for granting access to the stored data to healthcare practitioners with pre-specified data access tokens).

In order for the HR index to be correctly used by the HCP, some preconditions apply, as described below:

- the citizen has an anonymous unique ID stored within a QR code generated by the S-EHR App;
- the citizen has agreed to store the personal health data on the S-EHR cloud;
- after the storage of the health data to the S-EHR cloud, the S-EHR App sent to the HR index the unique ID of the citizen and the address of the S-EHR Cloud where the data are stored.

The role of the HR index starts when an emergency occurs, and the HCP scans (using the HCP app) the QR-code of the citizen that contains the citizen's unique ID and the address of the HR Index. This scanning redirects the HCP app to the HR index. On the base of the ID of the specific citizen sent by the HCP app, the HR index returns the cloud address.
The usage of the HR Index is not mandatory, as the S-EHR App is allowed to store directly the address of the S-EHR Cloud within the QR-code of the citizen. In case the citizen decides to change the S-EHR cLoud provider and no HR Index is used the citizen will have to generate a new QR-code. Instead, when a HR Index is used, in the case that the Citizen decides to use another S-EHR cloud service, there is no need to generate a new QR-code: the HCP will be able to access the S-EHR data using the previous QR-code, since the HR index is able to dynamically provide the new address of the Citizen's S-EHR Cloud.

2.4.6 Research Centre System

The *Research Centre Information System* is the software system of any research centre that is able to manage the participation of consenting citizens in research studies. This involves, using the InteropEHRate *RDS Protocol*, the management of citizens' formal consent to data sharing, as well as the actual reception of health data retrieved from citizens' mobile devices. As a research study may involve citizens from multiple European countries, each citizen is attached to his or her local *Reference Research Centre* that takes charge of all communication with the citizen. To this end, the *RDSI interface* of the RDS Protocol, implemented between the citizen's S-EHR App and the Reference Research Centre, provides secure and, when applicable, anonymous mechanisms for consent transmission, health data transfer, and the management of withdrawal from the study.

2.4.7 Research Network Central Node

The *Research Network Central Node* (CN) is the software information system used by the RDS protocol to receive, maintain and share the RDDs of research studies.

The CN implements the interface RDDI offering the publishing operation invoked by the Coordinating Research Centre to share, with all Citizens participating in the InteropEHRate Research Network, the RDD (Research Definition Document) describing a new research study (see 2.4.6). The RDDs maintained in the CN, are automatically checked before the publication, in order to allow the publication of documents which are compliant to the InteropEHRate document profile defined for the RDD.

The interface RDDI also offers a query operation invoked by the S-EHR apps of the Citizens participating in the InteropEHRate Research Network to retrieve the published RDDs. When that call is performed by the S-EHR apps, the Central Node provides the RDDs of all the Research Studies which are currently open,

checking automatically the enrolment period specified within the RDDs. When applicable, the S-EHR app may automatically compare the enrolment criteria to the content of the S-EHR app, for example, to avoid presenting to the citizens studies that they cannot be enrolled in.

2.5 Interoperability protocols

The following section introduces the general approach to data interoperability and the different kinds of interaction protocols.

2.5.1 Data interoperability

The InteropEHRate protocols are based on the HL7 FHIR standard. More precisely all the defined protocols are based on the HL7 FHIR data model with JSON serialisation, while the R2D Access protocol also adopts a portion of the standard HL7 FHIR API. The InteropEHRate open specification defines a set of FHIR profiles that constrain the FHIR core model, in order to forbid unsupported information and to add specific extensions needed to exchange additional data not supported by the FHIR core model.

The InteropEHRate FHIR profiles (report **[D2.8]**) allow the exchange of unstructured data and structured data. In the case of structured health data, the profiles indicate specific coding systems to adopt for representing specific kinds of health information. While alternative coding systems may be adopted, the use of the international standards indicated by the InteropEHRate FHIR profiles is the preferred approach. First of all, these standards are widely accepted throughout the EU and are more likely to be understood abroad and to be mapped to local representations. Secondly, internationally accepted codes and terms often already have official translations into EU languages, allowing the S-EHR Apps and HCP Apps to present the collected health data in the specific natural language of the Citizen or of the HCP, independently from the country where the data have been produced. The translation in the language of the citizen may be performed by the S-EHR App or directly by the data producer. To this end, the InteropEHRate FHIR profiles can include into the health data both the semantic codes and their translations in different languages, including in particular the language of the citizen. When the health data contain some translated information, they have also to indicate who performed the translation.

In the InteropEHRate vision, all FHIR profiles and coding systems adopted by the InteropEHRate protocols, together with their standard translation in different languages, should be governed and published by a single authoritative European organisation (see section 2.4.4).

A healthcare organisation may create and store the health data directly using the InteropEHRate FHIR profiles, so that the correct international terms are selected directly from the author of the data and, at the moment of data exchange, no conversion from local data structures and terminologies to FHIR data structure and international terminologies is needed, with minor risk of mismatch. Often this approach is not applicable; in this case the healthcare organisation has to convert the health data to and from the format mandated by the InteropEHRate FHIR profiles in order to be able to exchange them with the Citizen's S-EHR. The InteropEHRate framework (see section 4) provides specific tools for the conversion and translation operations, but any healthcare organisation is allowed to use different approaches and tools.

The InteropEHRate FHIR profiles also support the possibility to include additional semantic information (automatically) extracted by the unstructured data. Exploiting this additional information, the S-EHR Apps and the HCP Apps have the possibility to show to their users both the original unstructured content, produced by the author of the health data, and the information automatically extracted. The information

(automatically) extracted is represented by adopting the same standard coding systems adopted for the structured information, therefore it can be translated in different languages. In this case, the reliability of the translation depends on the reliability of the process adopted for information extraction. The data produced by information extraction are clearly separated from the original data, so the S-EHR App and the HCP App may highlight to the user which information was produced already in a structured format and which other information has been obtained by means of an information extraction process.

2.5.2 Security Protocols

The security protocols specify security schemes exploited by all the envisioned InteropEHRate protocols described in next sections. They are intended to satisfy the security goals, and the necessary technical measures needed for enhanced "security and privacy-by-design", following the current standards as defined in the ENISA's Minimum Security Measures for Operators of Essentials Services [**[ENISA 2020]**] and the requirements of the healthcare domain **[D2.2]**. These can be summarized as user and data privacy, confidentiality and access control, integrity and authenticity, availability, traceability and non-repudiation which, as explained below, are achieved through several state-of-the-art technical measures (see Table 4 in **[D3.1]**).

Security Infrastructure and Trusted Entities. Data security and user privacy protocols, leveraged in InteropEHRate, are based on the use of Public Key Infrastructures (PKIs) for credential management and privacy-friendly authentication services. The common denominator in such architectures is the existence of trusted (centralized) infrastructure entities for the support of services such as authenticated registration, pseudonym provision, revocation, etc., for either the system users or the S-EHR App. In this context, InteropEHRate security protocols are coupled with the use of (standardized) infrastructures that are a Certificate Authority (CA) as well as the electronic Identification, Authentication and Trust Services (eIDAS) regulation and EU services like CEF eID. All these infrastructure entities provide enhanced user authentication and identity management through the provision and verification of public-private key pairs and transient assertions and identifiers for identifying and managing the secure communication sessions during further execution of the protocols. In addition, data confidentiality and integrity - for both data storage and health data exchange - is provided through advanced encryption mechanisms based on the use of well-established and state-of-the-art solutions and Key Derivation Functions (KDFs), providing a 256-bit security level, while demonstrating high entropy on the generated secrets; according to NIST [**NIST 2020**, **NIST ENTR**,] as explained in the report **[D3.1]**. In the same line of operation, integrity aspects are achieved through the use of strong and efficient digital signatures upon the exchanged messages leveraging the certificates that have been provided by the CA.

D2D Security Interaction Mechanisms. The D2D Security protocol defines the set of operations towards the establishment of secure communication sessions between the devices managed by the users (i.e., citizens) and the physicians for health data exchange. In this context, the main novelty of InteropEHRate is the instantiation of appropriate models leveraging two supported variants for secure and authenticated Identity Management. The first variant is linked to the ID-Card of the citizen and a QR code, generated by the hospital, which provides stronger (physical) security properties and demonstrates high feasibility and applicability features, as a possible enabler to be put immediately in practice after the end of the project. This variant, however, assumes the user authentication through physical presence and the use of identifiable documents (ID card) which might hinder its scalability. Compounding this issue, the second

variant proposes to leverage citizen's Qualified Digital Signatures. A qualified electronic signature is an advanced electronic signature with a qualified digital certificate that has been created by a (qualified) signature creation device (QSCD). This variant overcomes the (aforementioned) scalability issues, however, it is based on the use of trusted computing technologies where a decentralized "root-of-trust" (e.g., Hardware Security Storage Module (HSM), Trusted Platform Module (TPM), etc.) needs to be attached to the user's end device. While the integration of such advanced trusted computing technologies provides confidence in a system, especially if the system's behaviour isn't fully secure or might become insecure, thus, requiring verifiable evidence on the correct execution of the security protocols by the system (provided by the "root-of-trust" crypto signing operations), it adds additional deployment costs. Therefore, the goal is the adoption of such solutions when the smart-phone technology will be mature enough for supporting qualified digital signatures through appropriate hardware- or software-based roots-of-trust. Apart from the usage of digital signatures for identification, such primitives were also leveraged for signing the citizen's consent (when participating in the system and starting to share data with the backend S-EHR Cloud infrastructure). In addition, as it pertains to confidentiality, state-of-the-art key agreement protocols were leveraged based on the use of the Diffie Hellman scheme and strong Pseudo-Random Number Generators (RNG), exhibiting high entropy, thus, enabling the provision of strong security levels, tailored to Bluetooth as the underlying network mechanism. This is also in alignment with the currently proposed BLE standard.

R2D Security Interaction Mechanisms. Identity Management and Authentication services, in R2D Access protocol, use an eIDAS-based solution so as to support cross-border identification and user authentication to healthcare organisations supporting the trust services and electronic identification, as defined by the current eIDAS standard. In addition, all established communication sessions are protected with the most suitable and robust encryption technologies needed to secure different types of information, while still allowing for (future) advanced knowledge discovery through the provision of enhanced data search services (i.e., Attribute-based Encryption) and advanced security and privacy-preserving primitives (i.e., data anonymization and pseudonymisation techniques) for authentication, authorization and data integrity verification. More specifically, all exchanged information (leveraging the R2D family of security protocols) is symmetrically encrypted with AES-256, using encryption keys generated from a strong KDF that demonstrates high entropy and randomness **NIST ENTR**. The main advantage of such a mechanism is the efficiency and effectiveness provided, through the use of appropriate lightweight cryptographic primitives. However, the main challenge is the need for the user's symmetric key to be released to the physicians in the context of emergency situations (currently done through the QR codes). As will be described in Section 5, the goal is to alleviate this prerequisite through the introduction of advanced security mechanisms such as ABE and the use of Blockchains as the underlying distributed ledger technology for offering secure and auditable data sharing amongst all involved actors.

RDS Security Interaction Mechanisms. Identity Management and Authentication services, in the RDS protocol, also leverage an eIDAS-based architecture for cross-border identification/authentication of the citizen to a trusted Pseudonym Provider (PP). A PP is a trusted organisation responsible for the pseudonym (pseudo-identity) management of the short term anonymous credentials (according to the IEEE 1609.2 specification), to be provided to the S-EHR App, and use for the anonymous communication of the citizen's health data to a (Research) Reference Centre. Each country should maintain an eIDAS node and a Pseudonym Provider Service for successful completion of these security protocols, based on the use of

standard PKIs and certification authorities. The need for a PP per country stems from the specific privacy requirements and healthcare data protection legislation that differs significantly between countries. In this context, for instance, standards development organisations, such as ETSI, ISO and IEEE, specify a functional split between an enrolment authority and an authorization authority. This corresponds to the integration of pseudonym schemes (as the one adopted in InteropEHRate), with multiple CAs and PPs (one per country), where each enrolment authority (CA) manages user identities and issues long-term certificates while each authorization authority (PP) is responsible for verifying the long-term enrolment of users, in one administrative domain (country), and issuing short-term pseudonymous certificates that users can then use for privacy-preserving health data exchange. Such a scheme provides higher user privacy levels even in the complex scenario where users move around different domains (i.e., countries or member states) and they need to acquire pseudonyms without revealing personal information regarding their country of origin. Furthermore, this specification also copes with important aspects of the pseudonym lifecycle like pseudonym resolution (when there is a need for linking - anonymized - data back to users in case of a health emergency), protection from misuse by authorities, and even pseudonym change while demonstrating high levels of scalability and efficiency. The exchanged information is symmetrically encrypted following the current AES-256 crypto standard.

2.5.3 R2D Access protocol

The R2D Access protocol defines a set of operations enabling the in-border and cross-border transmission of health data from any provider of health data to the citizen's S-EHR Mobile Apps, with the usage of the Internet (complementary to the D2D, that is the protocol to exchange health data without the usage of the Internet).

The operations of the R2D Access protocol are provided by the interface R2DI offered by the Healthcare Organisation Information System to the S-EHR Mobile App. Other than the remote interface R2DI, this protocol also exploits the interfaces eIDASI offered by the eIDAS nodes to the Healthcare Organisation Information System and the identification service offered by the national identity provider of the Citizen.

A peculiar characteristic of R2D Access, with respect to health data access mechanisms provided by proprietary applications, is that it is based on an open specification, therefore it can be adopted by any producer of health data. Moreover, it adopts the eIDAS infrastructure for identification and authentication of users, so a citizen is not forced to use different systems and credentials to access the services of different providers, but uses one single identification mechanism to log into any data provider in its same country or across different countries that adopt eIDAS.

The interface R2DI is defined on top of HL7 FHIR, by profiling its standard API, so it can be potentially used to exchange any kind of health data supported by FHIR and that refers to the citizen (FHIR data that makes sense only to the healthcare organisation are excluded by the protocol).

In this sense, R2D Access objectives may be considered complementary to eHDSI objectives: while eHDSI is a system available to HCOs and HCPs, the primary actors of R2D Access are the citizens. Each citizen downloads his or her data from the Health Data Providers to his or her smartphone and may then exchange them with other parties using the other InteropEHRate protocols.

More details of the R2D Access protocol are provided in the next chapter and in the report [**[D4.2]**, where information regarding the used technologies, the sequence of exchanged messages and the involved actors, and involved components are fully described.

2.5.4 R2D Backup protocol

The role of the R2D Backup protocol is to support the communication between any authorized S-EHR Mobile App and any compliant S-EHR Cloud, for the exchange of encrypted health data among these entities over the Internet.

The R2D Backup protocol defines the standard remote API for the interaction between the S-EHR Mobile App and the S-EHR compatible storage clouds. This API offers a set of functionalities that can be exploited by the Citizens by means of a S-EHR Mobile App, including the ability to:

- create an account on the S-EHR Cloud in order to back up their health data;
- upload their encrypted health data;
- download their encrypted health data;
- give or withdraw consent to the usage of the emergency protocol by HCPs;
- remove all uploaded data.

More details regarding the R2D Backup protocol, including its design and specifications will be available in the report D6.7-Design of a service for cloud storage of S-EHR content (S-EHR cloud) **[D6.7]** where detailed information with respect to the used technologies, the sequence of communication steps, involved actors, and involved components will be mentioned and discussed.

2.5.5 R2D Emergency protocol

The role of the R2D Emergency protocol is to support the communication between any authorized HCP through their HCP App and a compatible S-EHR Cloud during an emergency, for the exchange of encrypted health data among these entities over the Internet.

The R2D Emergency protocol defines the standard remote API for the interaction between the HCP app and the S-EHR compatible storage clouds. This API implements a set of functionalities that can be exploited by an HCP when an emergency occurs, by means of the HCP app, including:

- the download of the encrypted health data (e.g. IPS, Prescription, Laboratory results, Medical Images, Hospital discharge reports) of the patient by means of a QR code provided by the patient;
- the upload of new health data regarding the patient during the emergency;
- the upload of the report at patient discharge once the emergency is over.

More details regarding the R2D Emergency protocol, including its design and specifications will be available in the report **[D6.7]** where detailed information with respect to the used technologies, the sequence of communication steps, involved actors, and involved components will be mentioned and discussed.

2.5.6 D2D protocol

The D2D protocol defines a set of patterns for exchanging messages and healthcare-related data between the Healthcare organisation Information System used by HCPs and the S-EHR Apps used by citizens, to be adopted at EU level, without the usage of internet connection. This protocol is based on short-range wireless technologies and in particular Bluetooth.

Bluetooth technology is most commonly associated with exchanging data between two Bluetooth enabled devices in a short distance (±10 meters), through which a Bluetooth enabled device as soon as it listens to the initialization advertisement message of a different Bluetooth enabled device, connects to it, being thus

able to exchange and display information between them, without needing any other technologies or types of connection (e.g. internet connection). Adopting Bluetooth, the proposed D2D protocol will facilitate the information exchange between patients (i.e. through smartphones) and healthcare practitioners (i.e. through a desktop computer including a Bluetooth adapter), without the usage of any cloud services or any other parties. The overall pairing and connection process is based on the Bluetooth Serial Port Profile (SPP) (for Android OS devices) and Bluetooth Personal Area Network (PAN) (for iOS (i.e. Apple) devices).

The D2D protocol defines Bluetooth services (represented by the interface TD2DI) to be offered by healthcare organisations to share health data contained in their EHR with the S-EHR Mobile App, as well as Bluetooth services (represented by the interface MD2DI) to be offered by the S-EHR Mobile App for receiving requests from the Healthcare organisation Information System. The D2D protocol will also exploit D2D Security protocol (which interfaces are extended by R2DI and MD2DI) to perform Identity Management, Consent Management, and Authorization Management. The interactions between the interfaces MD2DI and the TD2DI are classified into five (5) main categories: (i) Bluetooth Connection, (ii) Demographic Data Exchange, (iii) Consent Exchange, (iv) Healthcare Data Exchange, and (v) Bluetooth Connection Closure.

(i) Bluetooth Connection

- The S-EHR app gets a connection's unique session identifier, in the form of a String. This String will be used by both sides (S-EHR app and HCP app), for the current connection identification purpose.

(ii) Demographic Data Exchange

- The S-EHR app gets the Healthcare organisation identity, for allowing the citizen to check if the identity is valid or not.
- The HCP app gets the citizen's decision from the side of the S-EHR app, regarding whether the provided Health organisation identity is approved or not and in a positive case receives the demographic data of the citizen.
- In the case that the Healthcare organisation identity has been approved, the S-EHR app gets the decision from the side of the HCP app, regarding whether the provided demographic data are approved or not by the healthcare organisation.

(iii) Consent Exchange

- The HCP app gets the decision from the side of the S-EHR app, regarding whether the consent for getting the S-EHR app owner's data has been approved or not.

(iv) Healthcare Data Exchange

- After that, in the case that the consent is approved, the requested healthcare data are provided to the HCP app. Similarly, the S-EHR app may get from the side of the HCP App new health data produced by the healthcare organisation, in order to be stored into the citizen's smart device.

(v) Bluetooth Connection Closure

- The last step includes the HCP app that gets the final message of the connection closure after the overall interaction has successfully ended with the provision of the evaluation data.

More details of the D2D protocol design and specification are available in the report D4.2, where information regarding the used technologies, the sequence of exchanged messages and the involved actors, and involved components are mentioned and thoroughly discussed.

2.5.7 RDS protocol

The RDS Protocol, also called Research Data Sharing protocol, supports health data exchange among the S-EHRs of citizens and Research Centres. Using the service components released by the project or any other implementation compliant with the specification of the InteropEHRate protocols, scientists are able to provide detailed information to the citizens about a research initiative, obtain their consent, and actually query the subset of patient data required for research.

The RDS protocol defines the IT interactions between the following systems each controlled by a specific actor:

- Research Network Central System (controlled by the CN)
- Research Centre Information Systems (each one controlled by a Research Centre)
- S-EHR Mobile Apps (each one controlled by a Citizen)

The RDS protocol assumes that a so-called InteropEHRate Research Network (IRN) has been established at EU level. An IRN is a network composed of Research Centres, Citizens and an additional organisation called Research Network Central Node (CN). The CN offers to both the Research Centres and the Citizens a central service for sharing the description of research studies looking for participating citizens satisfying specific enrolment criteria. Each Research Centre may participate in several research studies. Each research study involves a subset of all the Research Centres of the IRN. Within a specific research study, any participating Research Centre plays the role of Reference Research Centre or the role of Coordinating Research Centre.

Each research study has a single Coordinating Research Centre that is responsible for obtaining the approval of the specific research study and publishing its description in the form of a Research Definition Document (RDD). A Research Centre may play the role of a Coordinating Research Centre for one or more studies and simultaneously participate in other studies where it does not play that role.

Each citizen may freely propose themselves for participation in one or more research studies if they satisfy the corresponding enrolment criteria. Each citizen that is willing to participate in a specific research study is assigned to a specific Research Centre called the Reference Research Centre of that Citizen. For some studies, the citizen may choose among different Reference Research Centre. A Research Centre may play different roles in different studies. For the same research study, a specific Research Centre may play both the role of Coordinating Research Centre and Reference Research Centre. The protocol covers the following interactions in the order specified:

1. A Research Centre Information System, controlled by a Research Centre playing the role of the Coordinating Research Centre of a specific research study, publishes, using the RDDI interface exposed by the CN, an already approved RDD. The RDD contains, among other information, a machine-interpretable description of the enrolment criteria, as well as a machine-interpretable description of the health data to be downloaded from S-EHR Apps of citizens that satisfies the enrolment criteria. The machine-interpretable description of enrolment criteria and requested health data correspond to a formal set of FHIR attributes and resources, and related constraints equivalent to an FHIR query. Therefore, checking the enrolment criteria or extracting the required health data is equivalent to executing a FHIR query against the content of a S-EHR app.
2. The mobile apps of Citizens query the CN to retrieve all published RDDs which are open in the current period.
3. The mobile app sends the citizen's consent to participate in a specific research study.

   a. The protocol assumes that before this, the mobile app evaluates if the Citizen satisfies the enrolment criteria. If the evaluation is positive, then the Citizen is requested by the S-EHR App for the consent to data collection, providing him or her details on the data collection and the motivations.

4. The mobile app shares the Citizen's requested data with the Reference Research Centre.
   a. Upon positive consent, the S-EHR App executes an initial set of privacy-preserving operations on the requested data, such as de-identification.
   b. A S-EHR App transmits the requested data in a privacy-aware and secure manner.
5. Upon reception, the Research Centre Information System may perform further privacy-preserving operations on the data collected, such as further de-identification and aggregation across the entire cohort.
6. The mobile app, through the RDSI interface (exposed by the Research Centre Information System), sends to the Research Centre Information System the notification that the Citizen will not participate in a specific research study anymore. This notification can be sent for two different reasons:
   a. the Citizen is exiting a research study because He/She doesn't respect the enrolment criteria anymore;
   b. the Citizen decides to withdraw from an ongoing research study.

Communication between the Researchers and the Research Centre Information System i.e., for the initial research description, its approval and for the final transmission of de-identified and aggregated research data to the researchers, is not covered by the RDS protocol.
Additional details may be found in section 3.3, while the full specification of the first draft of RDS protocol is reported in deliverable **[D4.8]**.

3 USAGE OF PROTOCOLS WITHIN SCENARIOS

The following sections describe, by means of UML activity diagrams, how the systems and protocols of the InteropEHRate standard architecture are exploited to perform the actions described in the scenarios defined by deliverable **[D2.2]**and to perform related complementary actions.

Due to the big dimension of UML diagrams, each figure shows only a portion of the entire diagram and only a portion of the flow of data. The diagram adopts nested partitions. The outermost partition (with blue title) represents a country; the first nested partition (with light blue title) represents an organisation located in the country; the partition at the further level of nesting (with yellow or grey title) represents an information system; finally, the innermost partitions represent software systems (still with the yellow title or grey title) and their users (with green title).

The external partitions contain the names of specific countries, but as in scenarios defined by deliverable **[D2.2]**, they are just examples that can be replaced with the name of any European country. Different partitions can also be associated with the same country, i.e. the InteropEHRate protocols can be exploited not only for cross-border data exchange but also for exchanging health data within the same country.

Different colours are also used to help distinguish the purpose of each graphical element. Gray is used for activities performed by means of remote APIs non specified by InteropEHRate, green elements represent human activities, yellow elements represent activities that are specified by the InteropEHRate protocols and white elements represent additional software activities (e.g. conversion or translation) that are not part of the communication protocol (and therefore are not covered by the standard architecture) but are specific to the scenario or are a prerequisite to perform the communication activities. The InteropEHRate framework (see section 4) includes both libraries for the communication activities and for other activities of the scenarios. The description of operations performed by means of the InteropEHRate protocols (rounded yellow rectangles in the diagrams) is provided here at the business/conceptual level, while the technical specification of exchanged messages is provided in dedicated deliverables **[D4.2]** and **[D4.8]**.

Following is a complete list of UML notations and additional conventions adopted in the diagrams:

- *purple*: countries
- *light blue*: parties (i.e. citizens or organisations) in the communication
- *green*: human users and activities
- *yellow*: InteropEHRate remote APIs, systems and activities
- *grey*: APIs, systems and activities used by the InteropEHRate protocols but not specified by the InteropEHRate standard architecture
- *white*: systems and activities that are not part of the InteropEHRate protocols
- *black circle*: start of the process
- *black circle within white circle*: end of the process
- *circles with numbers*: points of attachment of split arrows (used to avoid drawing long arrow lines crossing the entire diagram; an arrow line entering in a circle goes where there is another circle with the same number and with an arrow line coming out from it)
- *rounded rectangles*: activities
- *orange rectangles*: data
- *black arrows*: the flow of action and direct flow of data (i.e. showing production and the first destination of data)
- *orange arrows*: an indirect flow of data (i.e. showing other main destinations of data)

- *dashed orange arrows*: reference to data updated by an activity
- *pointed banner*: invocation of a remote API of another party
- *double pointed banner*: an activity that waits for a specific event (e.g. waiting for an API invocation)
- *hourglass*: an activity that waits for a time event
- *diamond*: alternative flows of decision (or merge of alternative flows of action)
- *text in square brackets on arrows*: a necessary condition for the transition to happen
- *black bar*: parallel flows of action (or merge of parallel flows of action)
- *rectangle with folded corner*: comment
- *partitions* (swim lanes): different agents (the title on top represent the name of the agent followed by the name of the offered interface); the title has a different colour depending on the kind of agent: organisation, human, machine; each activity is depicted in the partition of the agent that executes it; in particular storing and processing activities are in the partition of the agent that processes the data.

3.1 Scenario S1: Medical Visit abroad

The UML activity diagram depicted in the following figures shows how the D2D and R2D protocols are exploited in "Scenario S1 - Medical visit abroad" **[D2.2]** and in phases that precede or follow it.

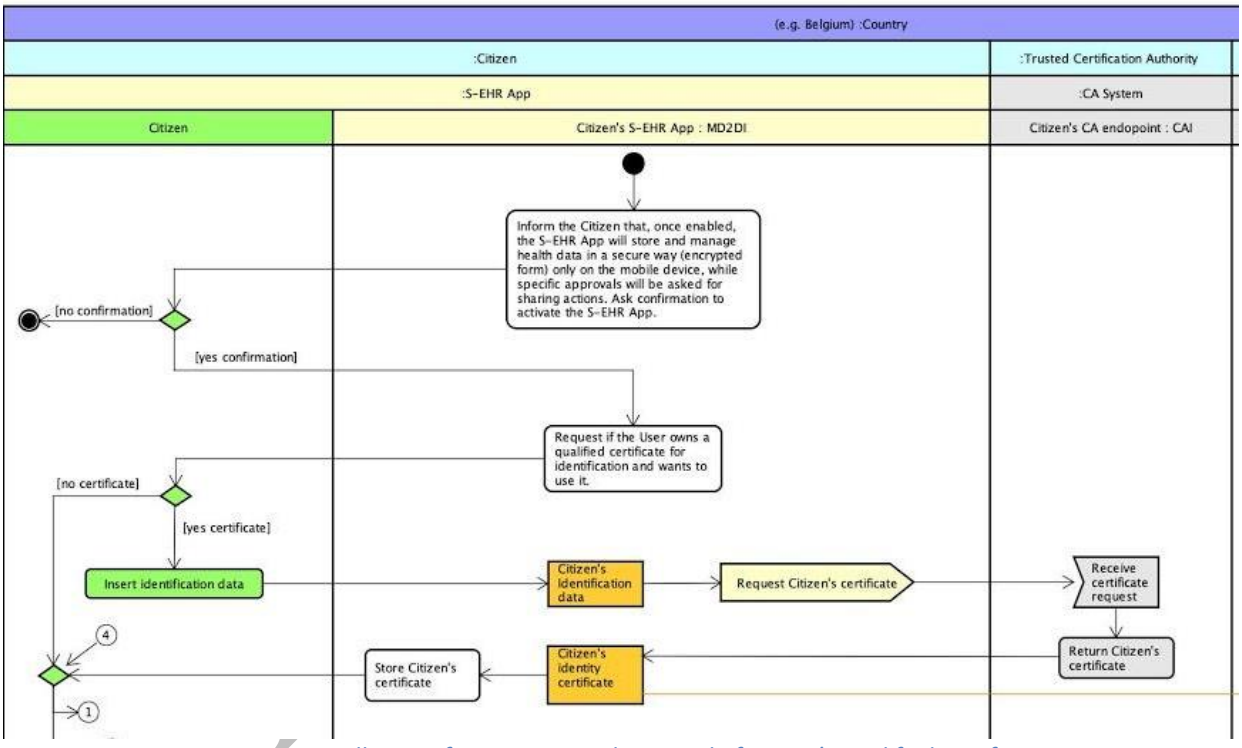


Figure 3 - Installation of S-EHR App and retrieval of citizen's qualified certificate

The portion of the diagrams in the figure above shows typical activities that are performed at the first installation of the S-EHR App. First of all, the Citizen confirms the willingness to use the app to store in a secure way his or her own health data directly on the mobile device. Then the Citizen is asked if he or she owns a qualified certificate and if wants to use it. In this case the certificate is retrieved form the CA. The usage of a qualified certificate is optional and used by the second variant of the D2D protocol **[D4.2]**.

The following picture shows the usage of R2D Access for importing health data from a healthcare

organisation that the citizen visited. To this end, the citizen selects the healthcare organisations previously visited (step "Configure import of HD form EHRs") and then the S-EHR App uses the R2D Access protocol (interface MD2DI) to query the selected data sources for obtaining data not yet imported. While in this example the data are imported from a health organisation belonging to the same country of the citizen, the R2D Access protocol may be used also cross-border, thanks to the usage of eIDAS authentication. The first step performed by the S-EHR App is the authentication on the national eIDAS (Interface eIDASI) to obtain an identity token that will be passed to the R2D endpoint, to allow it to check the citizen identity (the step of identity checking on the side of the R2D endpoint is not shown for simplicity). After checking the compliance of the received HD to the InteropEHRate profiles **[D2.8]**the S-EHR App will store them in encrypted format on the mobile device (the encryption step is also not depicted for simplicity).

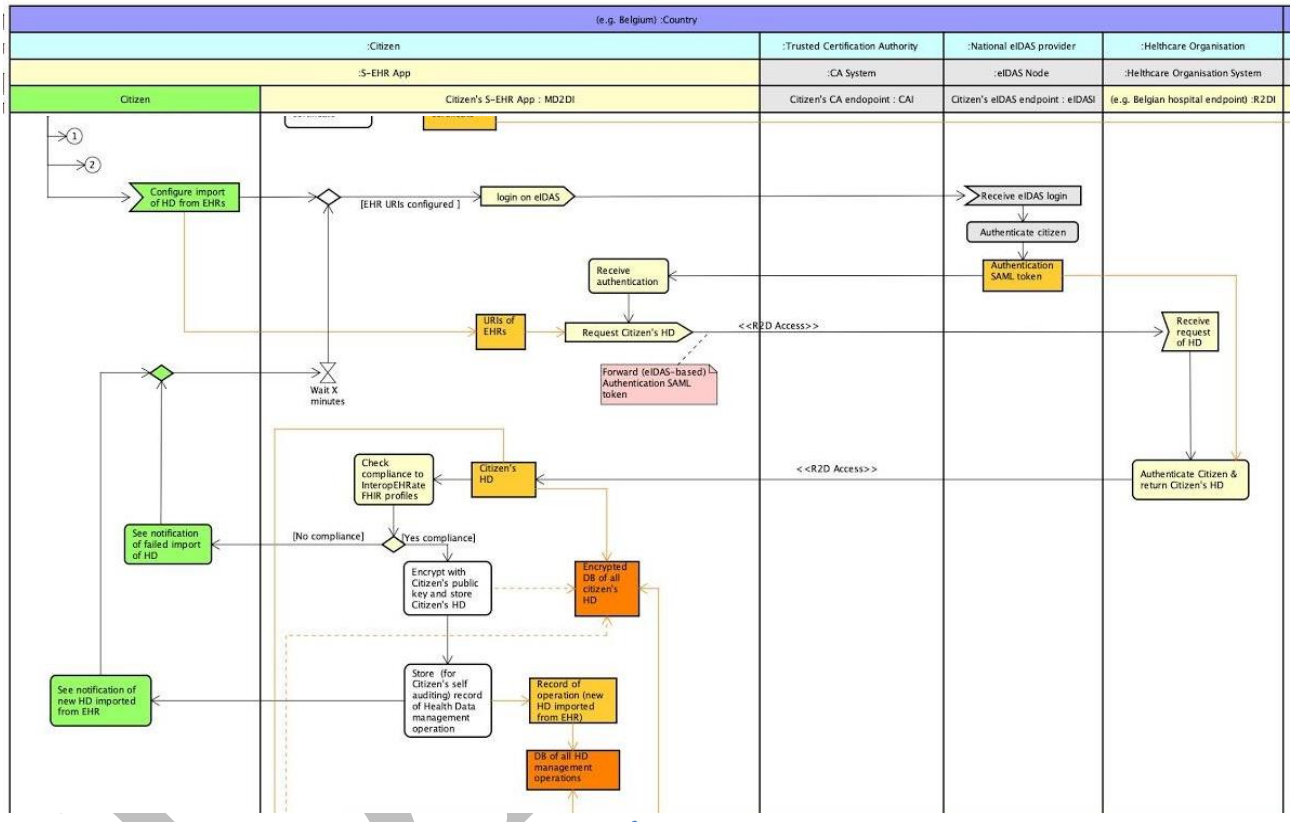


Figure 4 - Import of HD using R2D Access

The user is typically notified of the storage of new records or of the failure of the import operations due to non-conformance reasons. Depending on the user configuration, the R2D import operation can be periodically repeated in the future, in an automatic way, to check for new health data available from the same source (useful, for example, if the citizen periodically visits the same hospital or if the R2D Access endpoint is offered by the national EHR of the citizen).

The next picture shows what happens in the steps of scenario S1 when the citizen visits a hospital for a medical visit. In these steps, the D2D protocol is exploited for the exchange of health data on Bluetooth, without the Internet. Firstly, the HCP (on the right) activates the D2D protocol on its device. The HCP app turns on the Bluetooth, in order to communicate with the citizen's device and generates a QR code (a one-time password) to be shown only to the S-EHR app of the Citizen in front of the HCP, to allow an exclusive and secure pairing with it. On the other side, the Citizen also turns on the D2D protocol and reads the QR-Code so to complete the temporary pairing of the S-EHR App with the HCP App. The Citizen receives from

the S-EHR App (interface TD2DI) the description of the healthcare organisation that the HCP belongs to and approves the pairing. The Citizen can turn off the pairing at any moment. If the pairing is approved, the identification data of the citizen are sent to the HCP App. In case the Citizen owns a qualified certificate, the corresponding public key is sent to the HCP App to allow the HCP to verify electronically the identity of the Citizen. If the Citizen does not own a qualified certificate, it will also present to the HCP her ID card. The HCP will check the identity of the citizen on the basis of the qualified certificate or of the ID card and will conform it so as to complete the pairing between the S-EHR App and the HCP App.

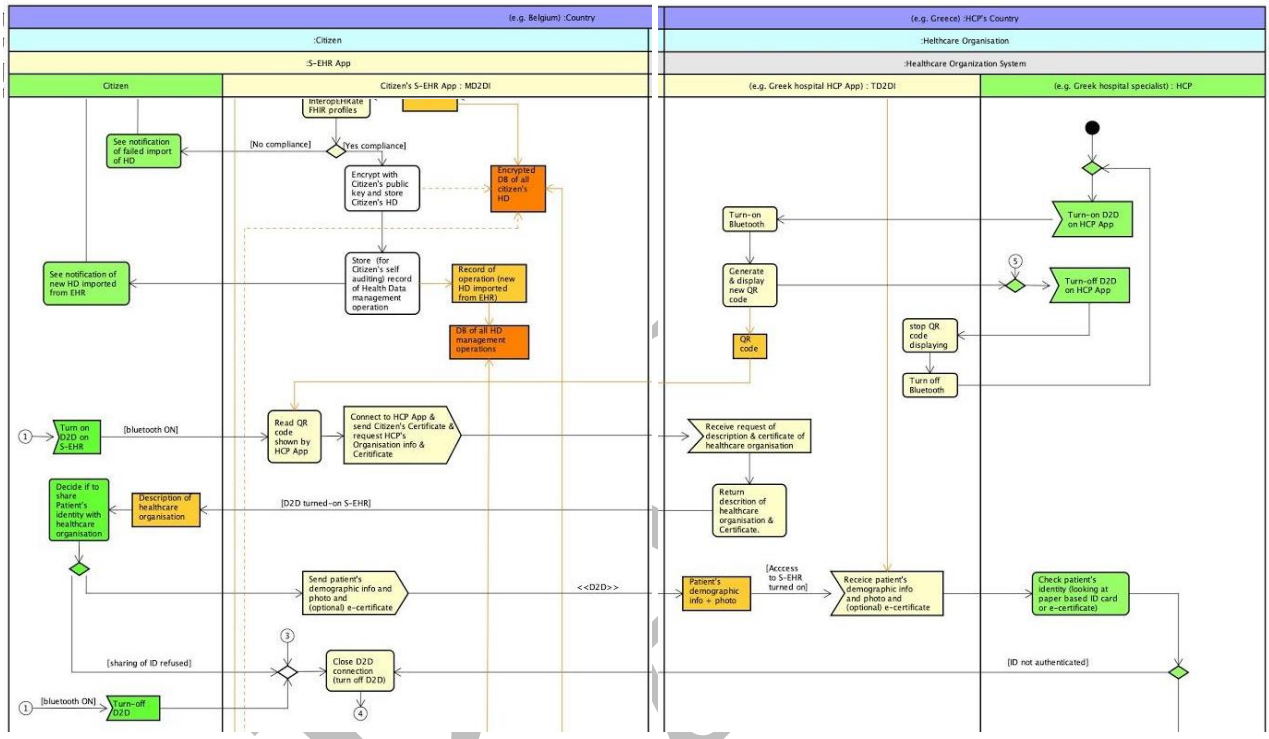


Figure 5 - D2D pairing of S-EHR App and HCP App

The next figure below shows the actual exchange of health data by means of the D2D protocol. The HCP app (on the right) sent to the S-EHR App (interface MD2DI) the request of consent to data exchange. The Citizen looks at the consent and signs it. The D2D protocol supports both a digital signature and a paper-based signature. After the reception of the signed consent is confirmed by the HCP, the HCP App asks the S-EHR App for the health data of the patient. Then the HCP App receives the health data that are compliant with the InteropEHRate FHIR profiles. The HCP App may be an extended version of a legacy EHR or can be an app integrated with it. In these cases, a conversion of the health data to the legacy format may be needed in order to store them within the legacy EHR. As the local HCP may speak a different language than the one of the authors of the health data, translation may also be needed. These operations are not part of the InteropEHRate protocols (that is the reason why they are displayed in white colour), but the InteropEHRate Framework (see section 4) provides tools and components that may support these operations. Afterward the HCP app will display the received and translated health data to the HCP.

After the examination, the HCP may decide to produce new health data. Also, in this case, conversion and translation may be needed to convert the new health data into the InteropEHRate format and to translate text into the language of the Citizen. After these operations, the new health data are sent to the S-EHR App, again using the D2D protocol. Similarly, to the R2D case, the S-EHR App will check the compliance of the health data to the InteropEHRate profiles and then will store them in an encrypted format on the mobile

device of the Citizen. Typical S-EHR Apps will show a notification to the user to inform of the reception and storing of new health data.

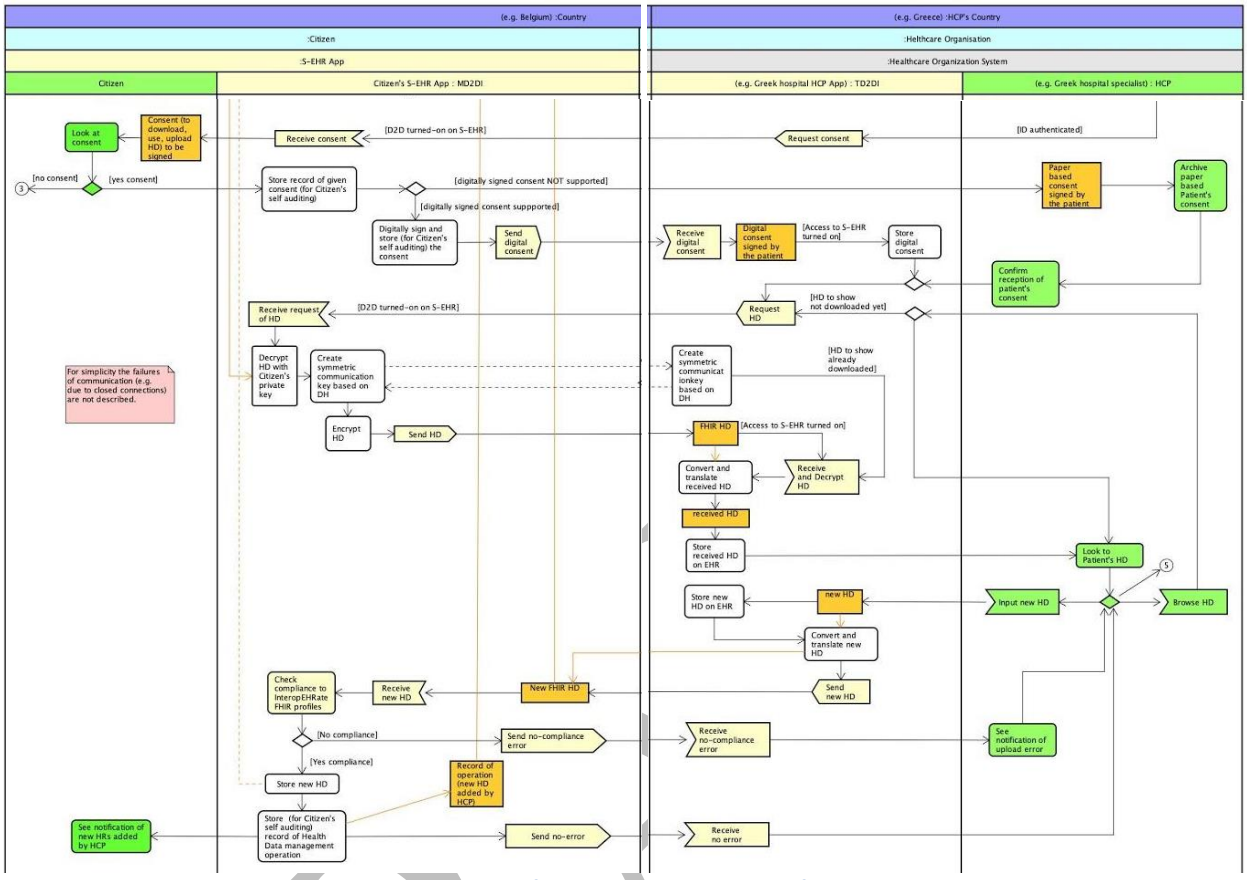


Figure 6 - Exchange of health data by means of D2D protocol

3.2 Scenario S2: Emergency access

The UML activity diagram depicted in the following figures shows how the R2D Backup and R2D Emergency protocols are exploited in "Scenario S2 - Emergency access" **[D2.2]** and also for moving the health data from a device to another.

The portion of the diagram shown in the figure below describes the operations performed the first time that a citizen decides to use a S-EHR Cloud. The S-EHR Cloud is an optional service, so its activation must be explicitly requested. In order to use the S-EHR Cloud, the citizen has to give explicit consent and has to own a digital certificate needed both to sign the consent and to encrypt the health data before sending them to the S-EHR Cloud. Therefore, if it has not been done previously, the Citizen certificate must be loaded on the smart device of the Citizen, using the CAI interface offered by the Certification Authority (CA) that issues the certificate. There can be several S-EHR Cloud providers, so the citizen has to choose the specific one to be used. After selecting the provider, the citizen creates an account on the S-EHR Cloud and sends to it the consent signed with the digital certificate.

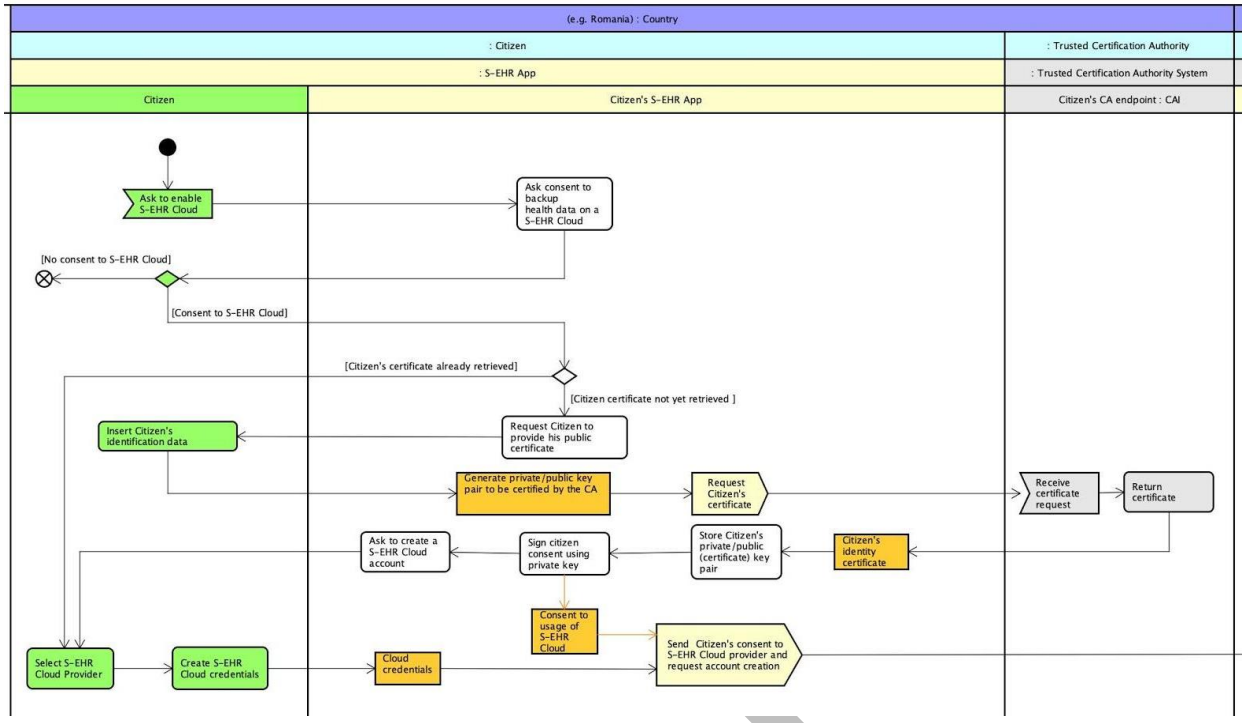


Figure 7 - Activation of the S-EHR Cloud by the citizen

The following figure describes how the content of the S-EHR App is backed up on the S-EHR Cloud by invoking operations offered by the interface R2DCloudWriter. First of all, the consent is received by the S-EHR Cloud and an account for the citizen is created. The account is anonymous, in the sense that the S-EHR provider does not receive the identity of the citizen. The signed consent contains an encrypted version of the Citizen identity that only an authorized trusted authority, distinct from the S-EHR provider, can decrypt, in case it is needed for legal reasons. After the creation of the account the S-EHR App stores the credentials of the account for automatic access to it. From that moment on, the S-EHR App will periodically check if new health data have been stored on the S-EHR App and will copy an encrypted version of them on the S-EHR Cloud. The structured health data are stored as encrypted FHIR bundles.

The encryption is performed with a private key owned only by the specific S-EHR App of the Citizen (so that no other app may encrypt new health data), while the decryption may be performed using a corresponding asymmetric key that is stored, on turn in an encrypted form, within the QR code and can be decrypted only by trusted HCPs (see next figure). The S-EHR App also periodically checks if an HCP, during emergency, stored new health data on the S-EHR Cloud.

The health data produced by the HCP are stored on the S-EHR Cloud in a similar way, but they are encrypted with the HCP key. The S-EHR Cloud does know nor the S-EHR App key, nor the HCP key, so the health data of the patient are hidden to the S-EHR Cloud provider. The S-EHR App stores in separated bundles the Patient Summary of the Citizen, single images and single documents referred by the PS.

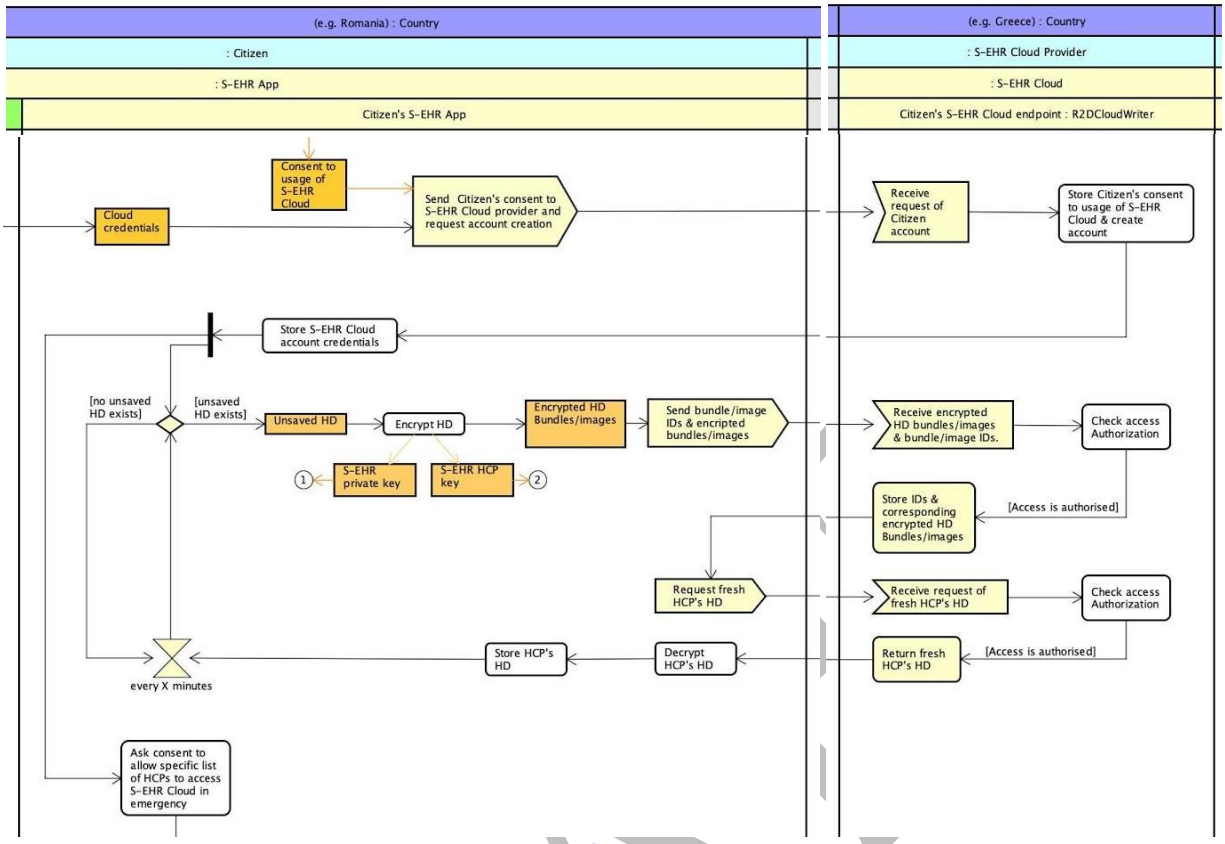


Figure 8 - Automatic backup of S-EHR content on the S-EHR Cloud

As shown in the next figure, the Citizen can decide to use the S-EHR Cloud not only for personal backup of health data but also to give access to them in emergency to trusted Healthcare organisations. In this case the Citizen has to provide an explicit consent that is sent to the S-EHR Cloud to authorize the HCP of the healthcare organisation to download the health data in case of emergency.

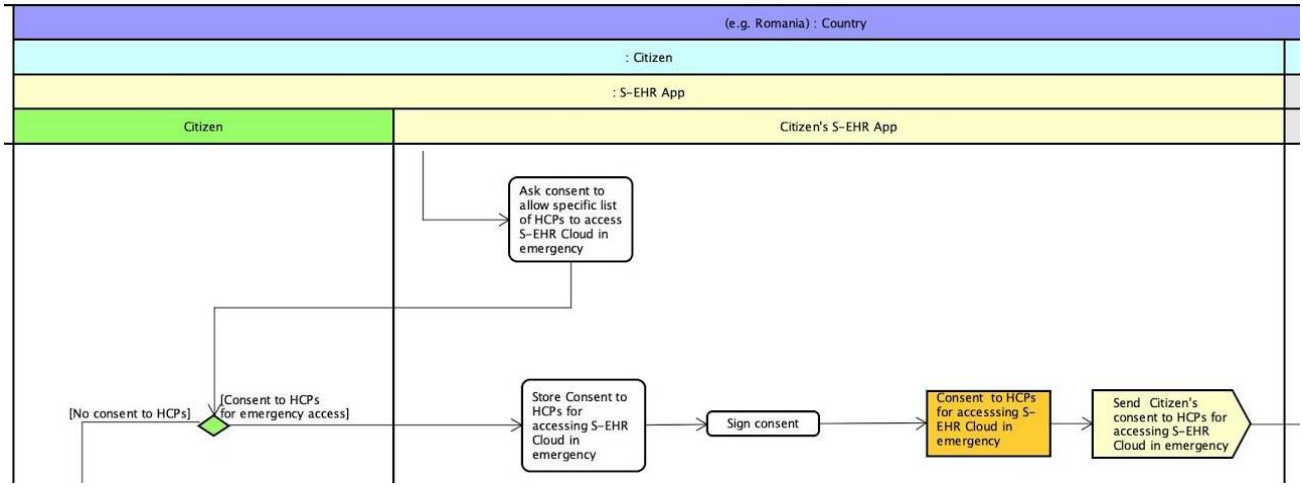


Figure 9 - Consent to the HCP's access to the S-EHR Cloud in case of emergency

The following figure shows that the consent to the HCPs access involves the interface R2DCloudWriter offered by the S-EHR Cloud (used to communicate the consent) and the interface HRI offered by the HR Index. As the HR Index is an optional component of the InteropEHRate architecture, this interface is invoked only if the HR Index actually exists and the S-EHR App is aware of it. In this case, the HR Index is used to publish, in an encrypted format that can be decrypted only by trusted Healthcare organisations, the location of the S-EHR Cloud of the citizen, in order to allow to find it also in case that the location has been changed after the production of the QR code.

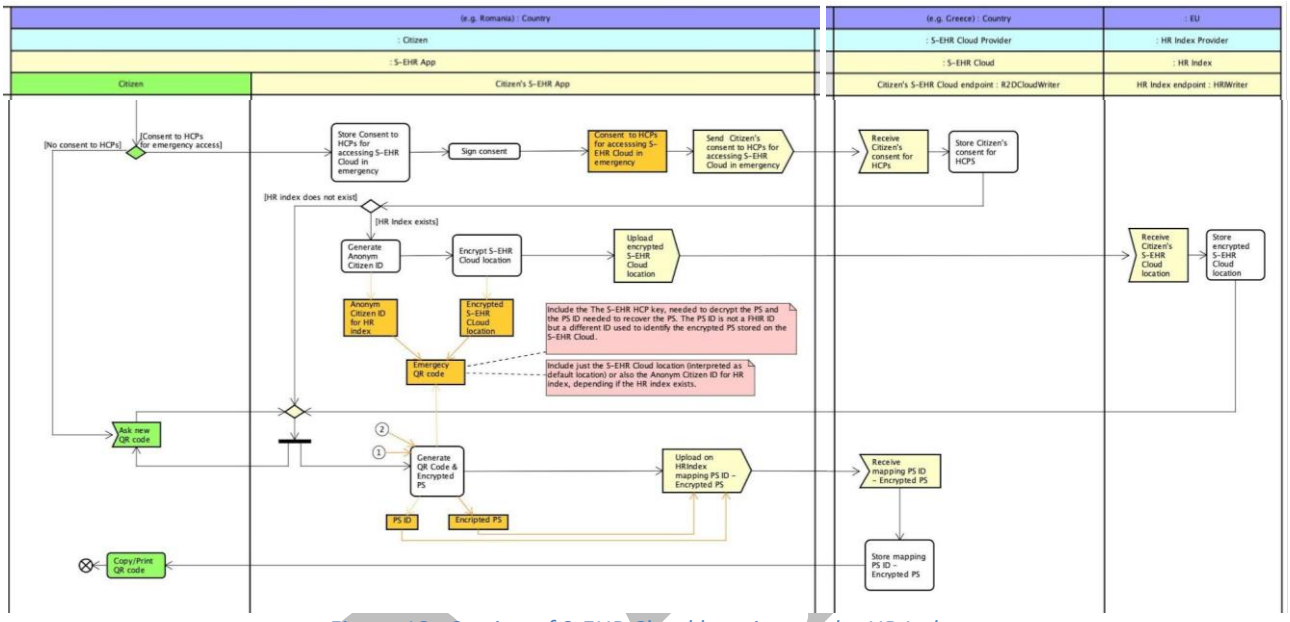


Figure 10 - Storing of S-EHR Cloud location on the HR Index

The HR Index does not store the real identity of the citizen but associates the location of the S-EHR Cloud just to an anonymous citizen ID that is stored within the QR code that will be shared with the HCPs. Independently from the existence of the HR Index, the access to health data by HCPs during the emergency requires that the HCP owns the emergency QR code generated by the S-EHR App of the citizen. The citizen has to print this code and wear it so that the HCP can find it in case of emergency. The emergency QR code includes the following information: the anonymous ID of the patient, the S-EHR Cloud location, an ID to retrieve the initial bundle of health data of the patient (called PS ID), the HCP key needed to decrypt health data retrieved from the S-EHR Cloud. The initial bundle includes the Patient Summary of the patient and references to other health data of the citizens.

The following two figures show how the information stored on the S-EHR Cloud is exploited.
The first figure shows how the content of the S-EHR Cloud, saved from a S-EHR App of the Citizen, can be imported by the citizen on a new S-EHR app (on the same mobile device or on a new mobile device). To this purpose the citizen exploits the same QR code shared in emergency with the HCPs (indeed the QR code is generated by the S-EHR App also if the Citizen does not give the consent to HCPs access). After the installation of the S-EHR App the citizen has to scan the emergency QR code (to allow the S-EHR App to locate the S-EHR Cloud of the citizen and decrypt the health data) and then has to insert the credentials of

the citizen to actually download the previously encrypted and saved health data. Using the interface R2DCloudReader offered by the S-EHR Cloud the health data are downloaded and then decrypted with the HCP key stored within the QR code. As the previous S-EHR App key is lost, after the import operation, the S-EHR App will have to disable the S-EHR Cloud (see successive figures) and then enable it again in order to generate a new S-EHR App key, a new HCP key and a new QR code.

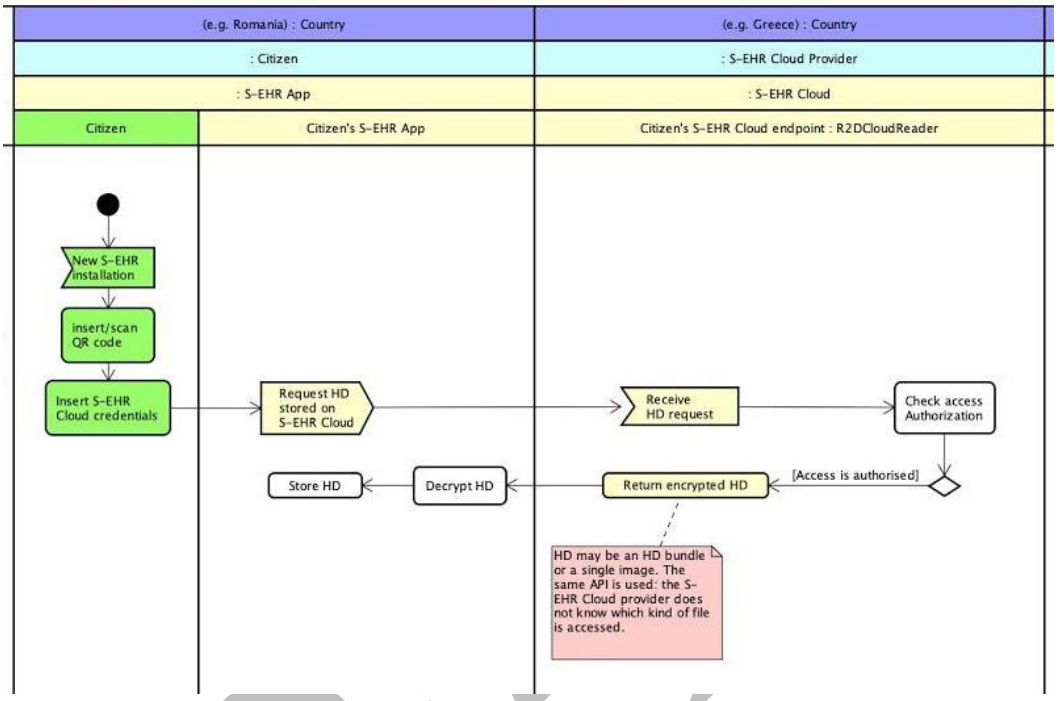


Figure 11 - Import of the S-EHR backup on a new S-EHR App

The second figure (below) shows instead how the HCPs can access the health data stored on the S-EHR Cloud in emergency situations, when for some reason (e.g. because the citizen is unconscious or because the mobile device of the citizen is not available) the D2D protocol.

Similarly to a Citizen, also the HCP (or its organisation) must own a digital certificate for authenticating their identity, qualification and access to the S-EHR Cloud. Moreover, in order to access the health data of a citizen the HCP needs to demonstrate that he or she owns the emergency QR code of the citizen. Therefore, as shown in the diagram the HCP has to scan the emergency QR code of the citizen. If an HR index exists, the HCP App will ask the HR index the location of the S-EHR Cloud of the citizen. The HR index will return an encrypted location that the HCP App will decrypt using the HCP key stored within the QR code. If an HR index does not exist, the HCP app will use just the S-EHR Cloud location stored within the QR code.

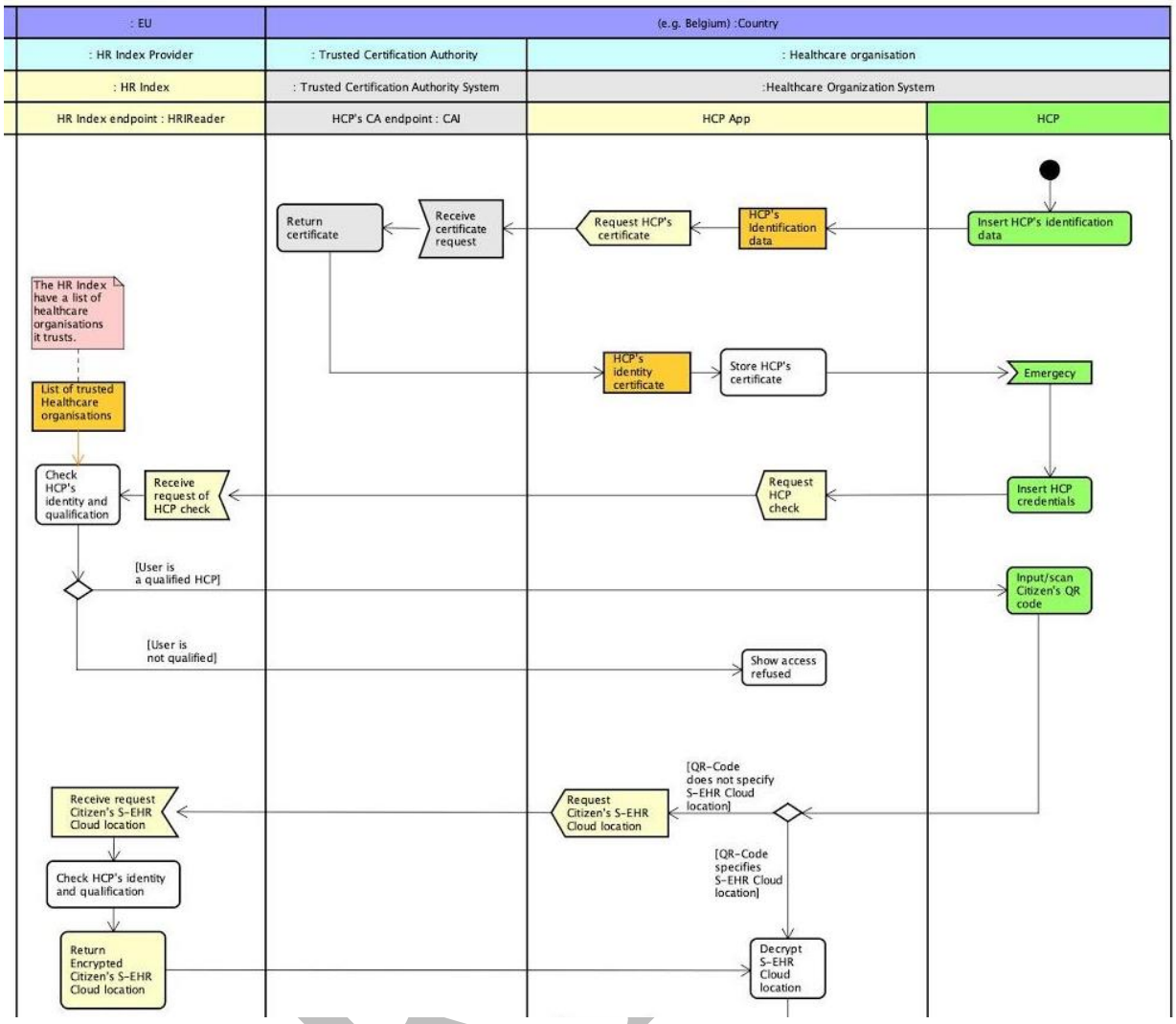


Figure 12 - Access to S-EHR Cloud by an HCP for emergency reasons

After determining the location of the S-EHR Cloud, the HCP App tries to invoke the interface R2DCloudReader offered by the S-EHR Cloud in order to retrieve the initial bundle of the citizen (containing the patient summary and the reference to other health data of the citizen). The S-EHR App sends to the S-EHR Cloud the ID of the initial bundle contained in the emergency QR code. The S-EHR Cloud maintains a list of trusted healthcare organisations; therefore, it will allow the retrieval of the encrypted bundle only to an organisation able to prove its identity with a digital certificate and belonging to the trusted list of the S-EHR Cloud. The S-EHR Cloud will log the data request for allowing the citizen to audit all accesses to her health data. The bundle is then decrypted from the S-EHR App by using the HCP key provided by the QR code. The HCP will look at the PS contained in the bundle and will decide if to retrieve the bundles of related health data following steps similar to the previous ones.

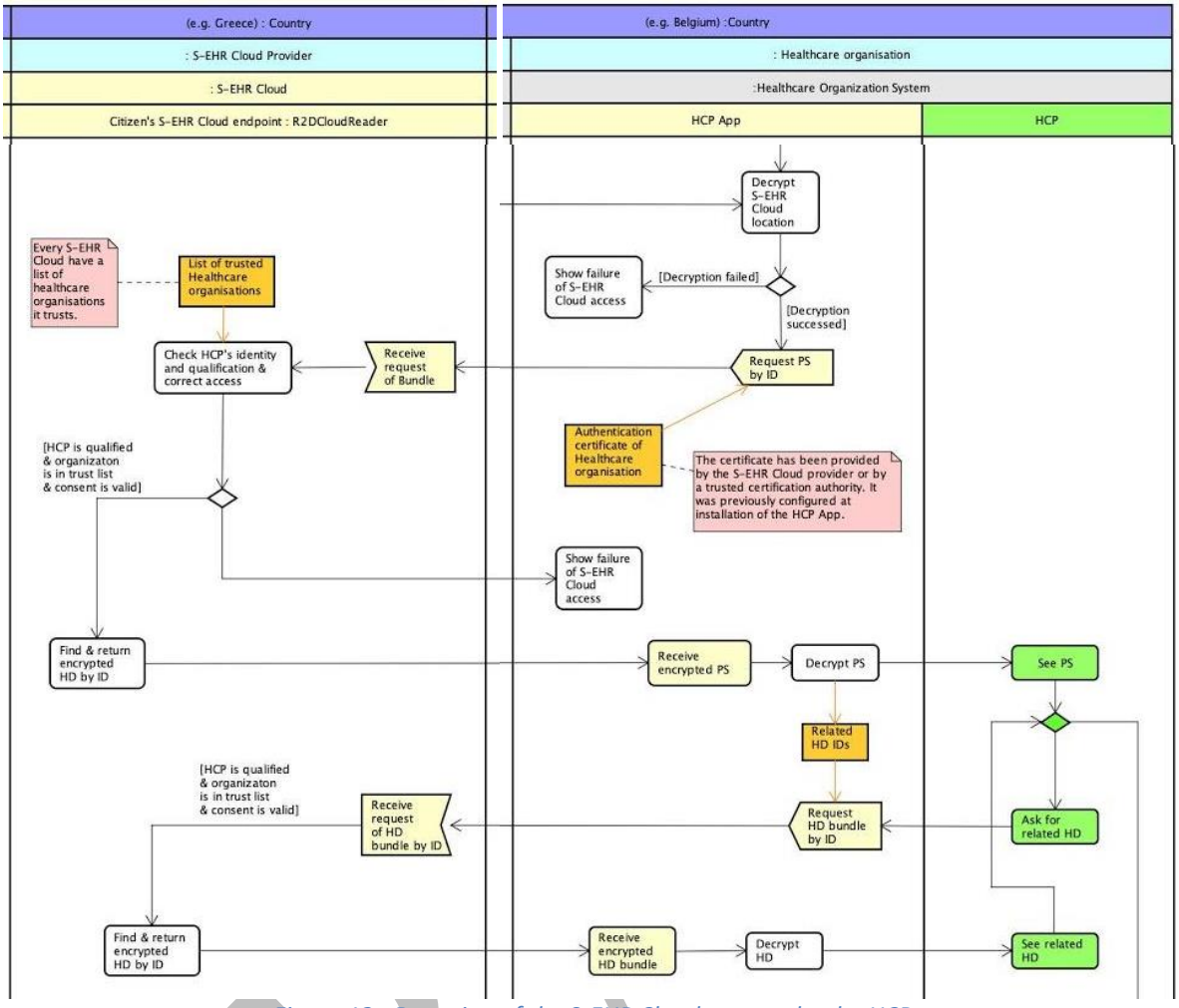


Figure 13 - Browsing of the S-EHR Cloud content by the HCP

During the healthcare process in an emergency the HCPs can produce new health data. For this reason, the interface R2DCloudReader offered by the S-EHR Cloud to the Healthcare organisation allows also to store new health data. This operation is different from the writing operation offered by the interface R2DCloudWriter to the S-EHR App, because the HCP App does not encrypt the records with the S-EHR App key, but with the HCP key, so they must be stored in a separate space. They will be integrated with the other health data only when the s-EHR App will download them and will encrypt them again with the HCP App (as shown in the previous figures).

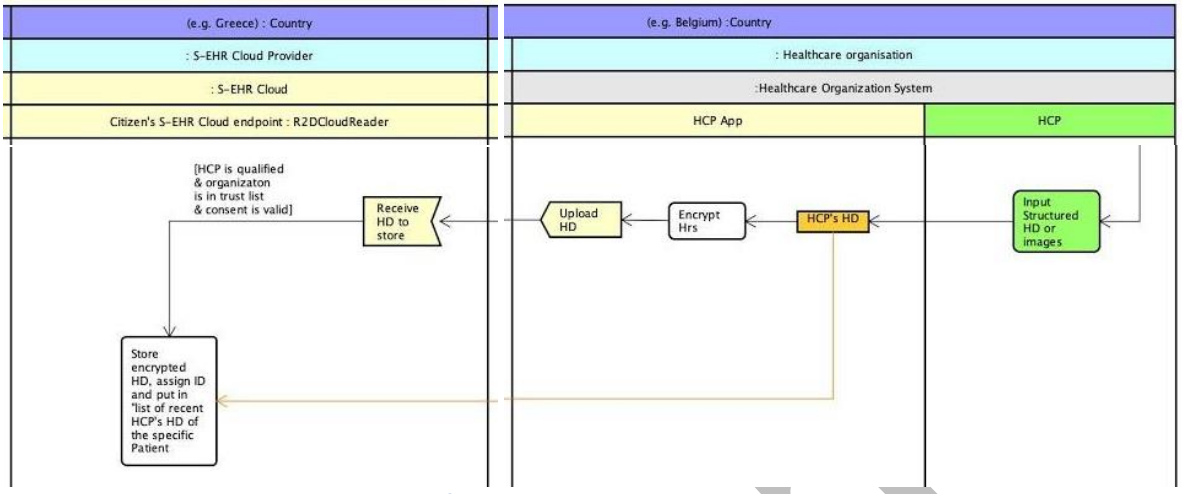


Figure 14 - Writing of new health data on the S-EHR Cloud by the HCP

The last figure below shows that the interface R2DCloudWriter offers to the Citizen the possibility to withdraw in any moment the consent to the HCP access or the consent to the usage of a specific S-EHR Cloud. When the citizen retrieves the consent, any information previously stored by the S-EHR APP of the citizen must be removed by the S-EHR Cloud and by the HR index (in case it exists).

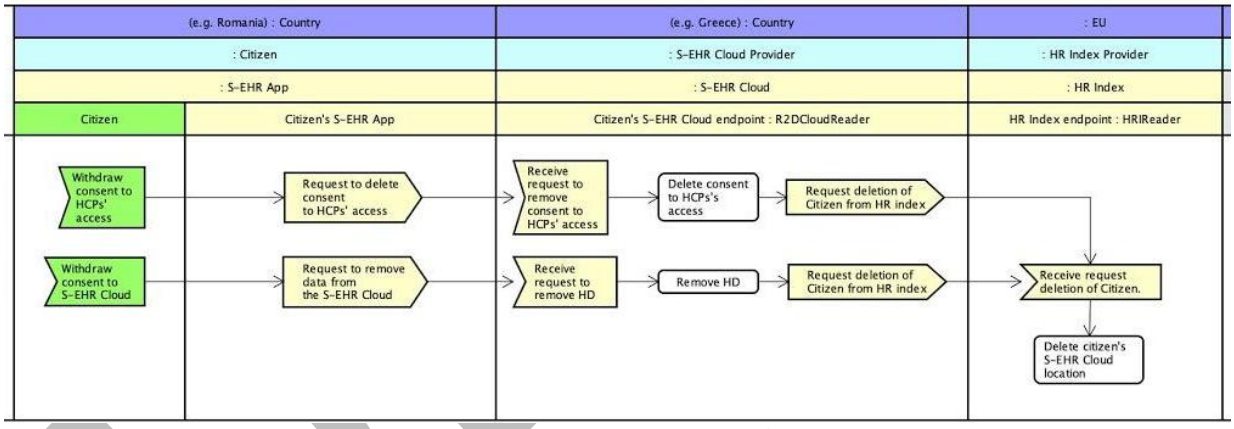


Figure 15 - Withdraw of consent to HCP access and/or to S-EHR Cloud usage

3.3 Scenario S3: Health research study

The UML activity diagram depicted in the following figures shows how the RDS protocol and its APIs are exploited in "Scenario S3 - Health research study". The first image below shows the portion of the diagram that describes how the Principal Investigator (PI) of a research Study publishes the description of a new research study. The research study is described by a Research Definition Document (RDD) that specifies in particular the data that are required by the citizen, the enrolment and exit criteria. All the RDDs are stored by the specific node called Research Network Central Node (CN).

The RDS protocol defines the standard format of the RDD and requires that the RDDs are published on the CN, but does not specify any remote API or any specific business process for publishing the RDD on the CN.

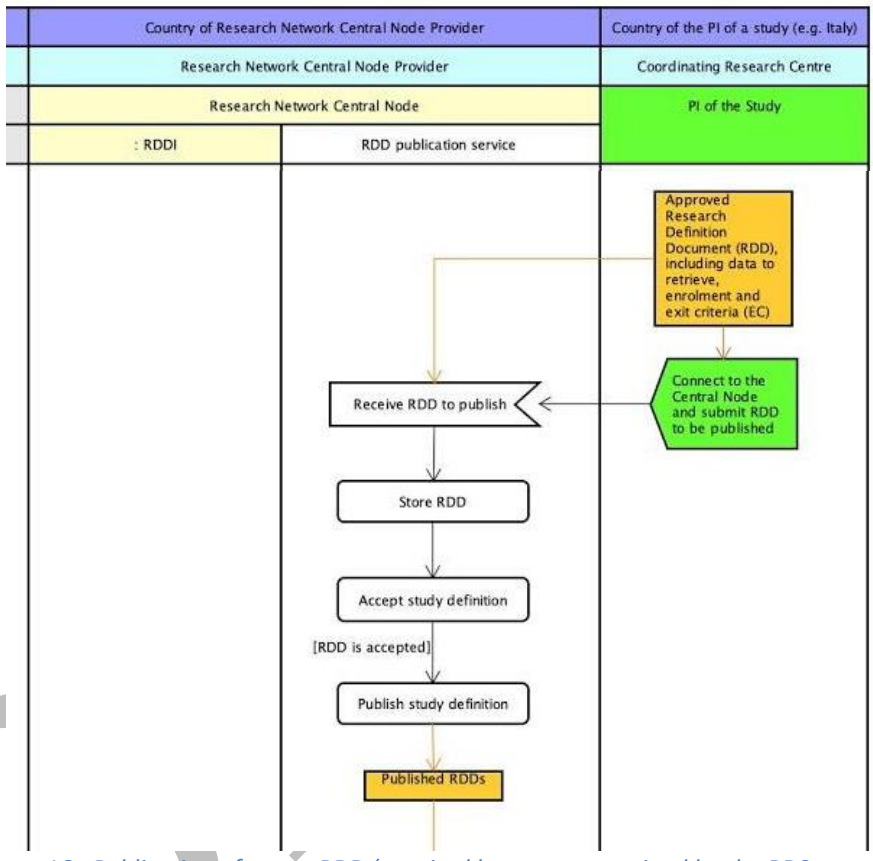


Figure 16 - Publication of a new RDD (required but not constrained by the RDS protocol)

The activity diagram shows just an example of a possible publication process and the publishing activities are depicted in white colour because they are out of the scope of the RDS specification. In the example shown by the diagram, the publishing is performed by the PI by means of a GUI (e.g. a remote interface offered by a web application) that is specific to the implementation of the implementation of the CN. The RDD may be subject to a revision before accepting the publication. If the publication succeeds, the RDD becomes visible to any citizen that participates in the Research Network. The following image shows how a citizen becomes a participant to the Research Network.

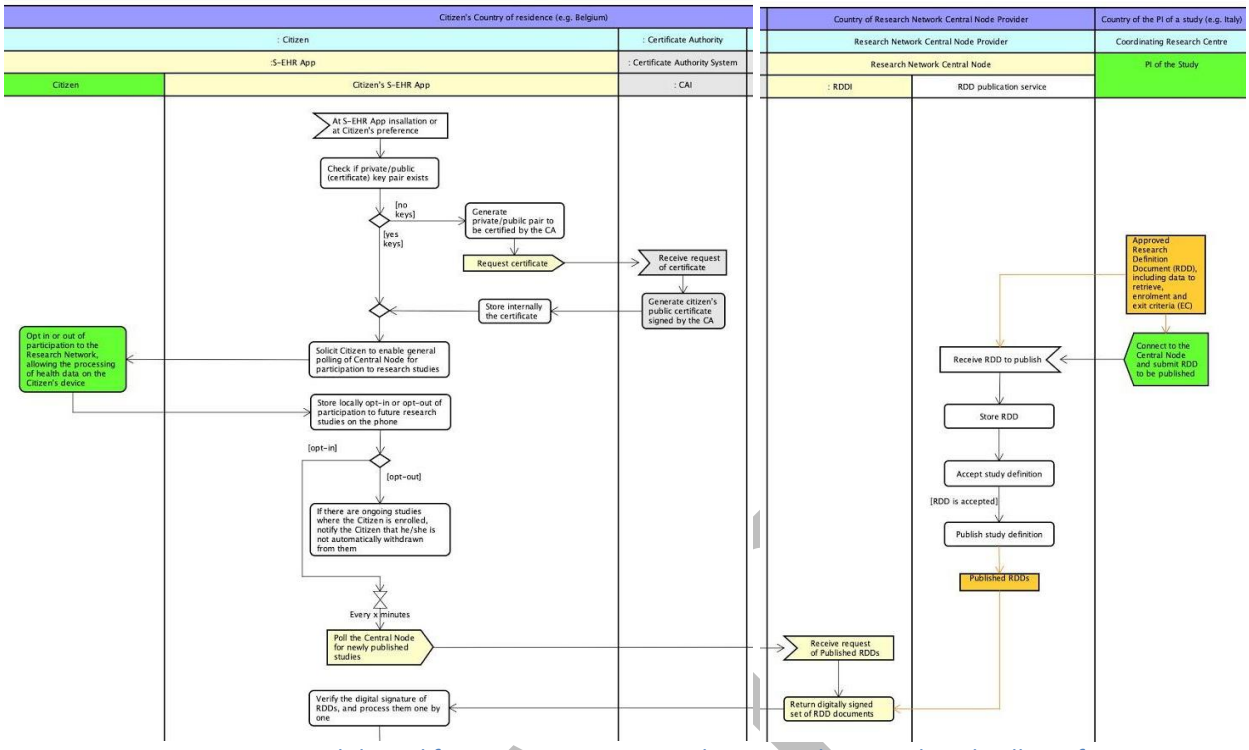


Figure 17 - Citizen withdrawal from or participation to the Research Network and polling of RDDs

At the installation of the S-EHR App, or also in a successive moment if the citizen asked to be reminded, the app proposes to the Citizen to become part of the Research Network.

If the citizen answers positively, the S-EHR App starts to periodically invoke the remote API RDDI offered by the CN to retrieve the updated list of RDDs. This operation does not share any information about the Citizen with any third party. The real enrolment of the citizen happens in successive steps. When citizens choose to not participate in the Research Network anymore, they are notified that they will continue to contribute to the studies they were already enrolled in.

The enrolment of the citizen in a specific research study is shown in the next figure below. After downloading the RDDs, the S-EHR App checks that they are digitally signed, to be sure of the provenance. All RDDs that are considered trustable are then processed one by one. The enrolment criteria of the RDD are compared to the health data stored on the S-EHR App. If there is no match, the RDD is skipped and no information is shown to the citizen or shared with third parties. If there is a positive or potentially positive match (in the sense that other data must be asked to the citizen to verify the match), the RDD is presented to the citizen. At this point, the citizen may decide if to participate or not in the research study described by the RDD. If the citizen consents to participate, the citizen is asked to select a reference research centre from its preferred region. If the research study requires the pseudonymisation of data, a specific pseudonym is created by invoking the remote API PPI offered by the Pseudonym Provider.

The consent of the citizen is then digitally signed and sent to the Reference Research Centre selected by the citizen for the specific research study, together with the created pseudonym.

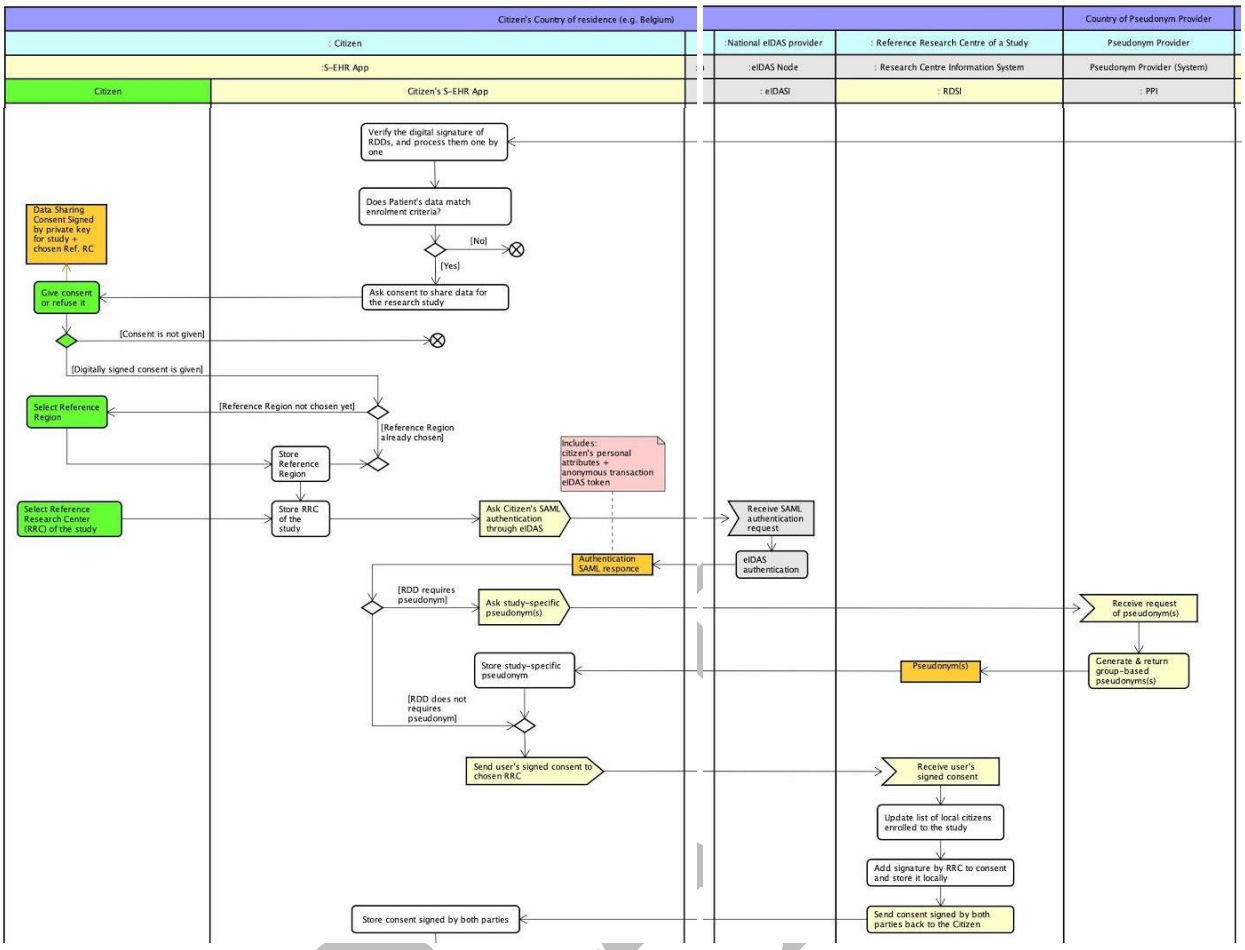


Figure 18 - Enrolment of a citizen in a research study

These are the first data that the S-EHR App shares. This step is performed by invoking the remote API RDSI offered by the Reference Research Centre, which will add the citizen to the list of participants to the study. From this moment the Reference Research Centre expects the S-EHR app to send the citizen's health data according to the time and data criteria specified by the RDD. This is shown in the Figure 19 below.

At the time specified or condition specified by the RDD, the S-EHR App checks the health data stored on the mobile device to determine if the exit criteria are verified. In a positive case, the S-EHR App stops sending data to share new data and notifies the Reference Research Centre that will remove the citizen's from the list of participants to the specific research study. If the exit criteria do not apply, the S-EHR app looks for new data to share. If required by the RDD the data are anonymised or pseudonymized, using the pseudonym previously assigned, and then the data are encrypted and sent to the Reference Research Centre, again by invoking an operation of the remote API RDSI. If the Citizen asked for it, a notification is shown, informing that new health data have been shared with the Reference Research Centre. The Reference Research Centre will forward the data to the PI following modalities that are specific to the research study and that are outside of the scope of the RDS protocol.

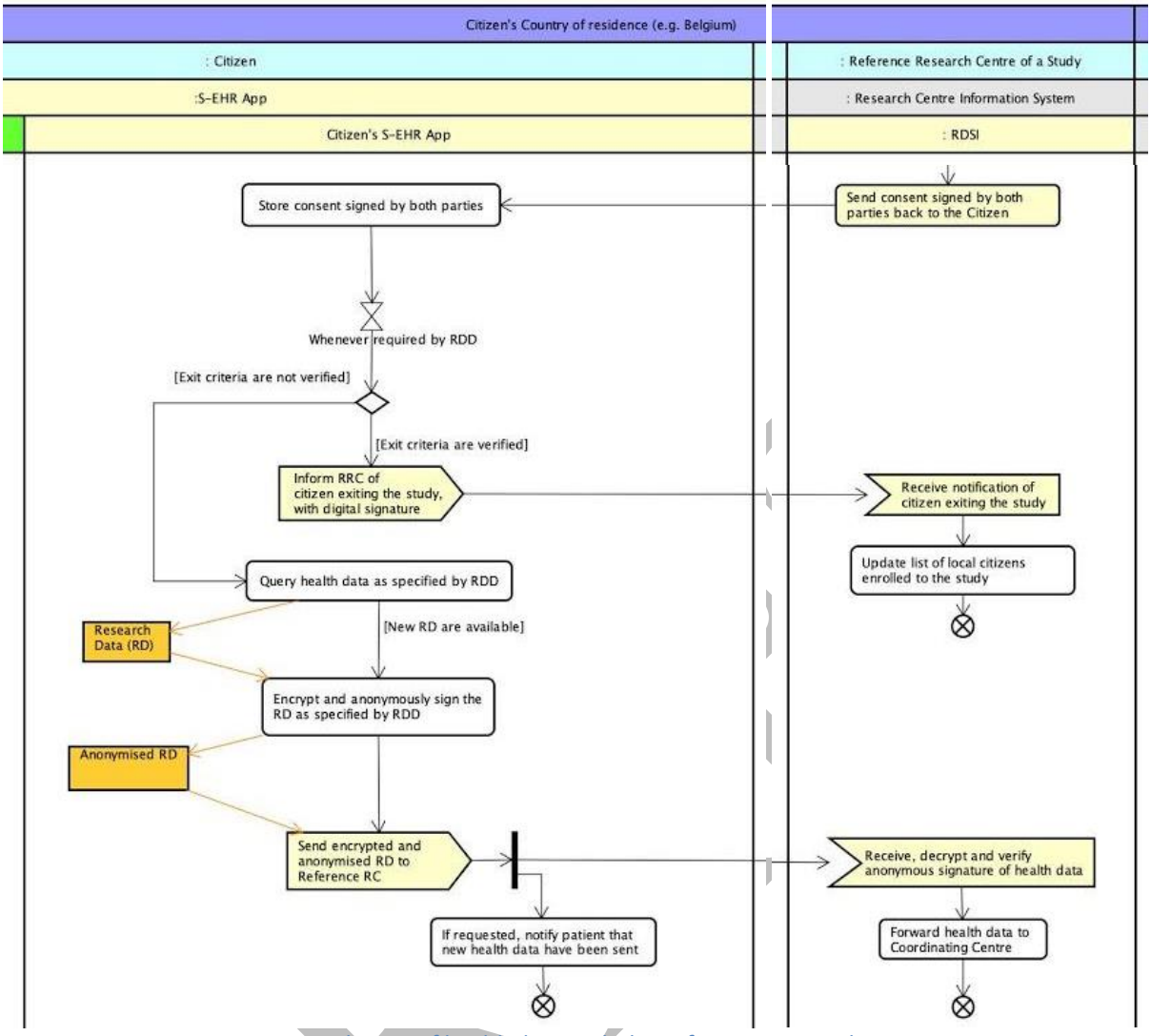


Figure 19 - Sharing of health data with the Reference Research Centre

The citizen may withdraw (Figure 20) at any moment from a research study. This is done by invoking another operation offered by the interface RDSI, as illustrated by the figure below. When a citizen withdraws from a research study, the Reference Research Centre has to delete any collected data and ask the PI to do the same.

The RDS protocols, like the other InteropEHRate protocols, specify the required APIs and the side effects expected by each one of these operations. The usage of the protocol does not guarantee that the involved parties respect the contract expressed by the RDD and the protocol itself. On the other hand, the protocol is designed to minimise the exchange of data and to guarantee the nonrepudiation of these contracts by means of encryption and digital signature.

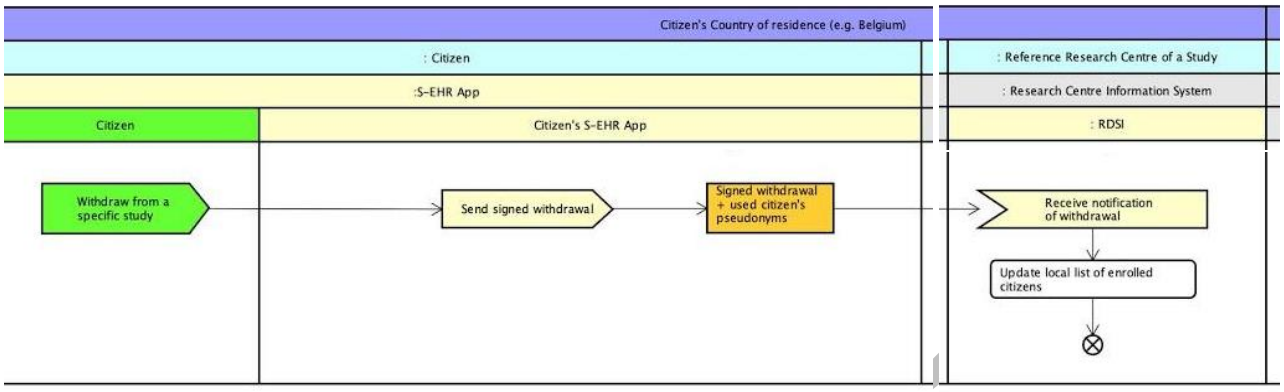


Figure 20 - Withdrawal from a research study

4 INTEROPEHRATE FRAMEWORK

As said in the previous sections, each element of the InteropEHRate standard architecture may have different implementations. Different implementations that are compliant to the InteropEHRate specification can interoperate. This section describes the particular set of implementations released by the InteropEHRate project, called *InteropEHRate framework*. The InteropEHRate framework offers a reference implementation of the remote APIs and systems that are part of the standard InteropEHRate architecture. It is intended to ease the concrete adoption of the InteropEHRate specification and to provide a base for testing the interoperability with other future implementations. Moreover, the InteropEHRate framework provides additional components that do not participate directly in data exchange interactions and for this reason, are not part of the standard InteropEHRate architecture, but supports the conversion and translation of exchanged health data.

The following picture shows in an informal way the components offered by the InteropEHRate Framework. Note that different colours are used, with respect to the informal picture shown in section 2, also for components that were already shown there (S-EHR Mobile App, S-EHR Cloud). This to stress that the InteropEHRate Framework offers specific implementations of the components specified by the standard architecture. For simplicity, the information systems of the healthcare organisation and the research centre are not shown, but just the components running within them are shown (IHT, IHS, HCP app and EHR are part of the healthcare organisation information system, IRS and CMTS are part of the research centre information system depicted in Figure 1).

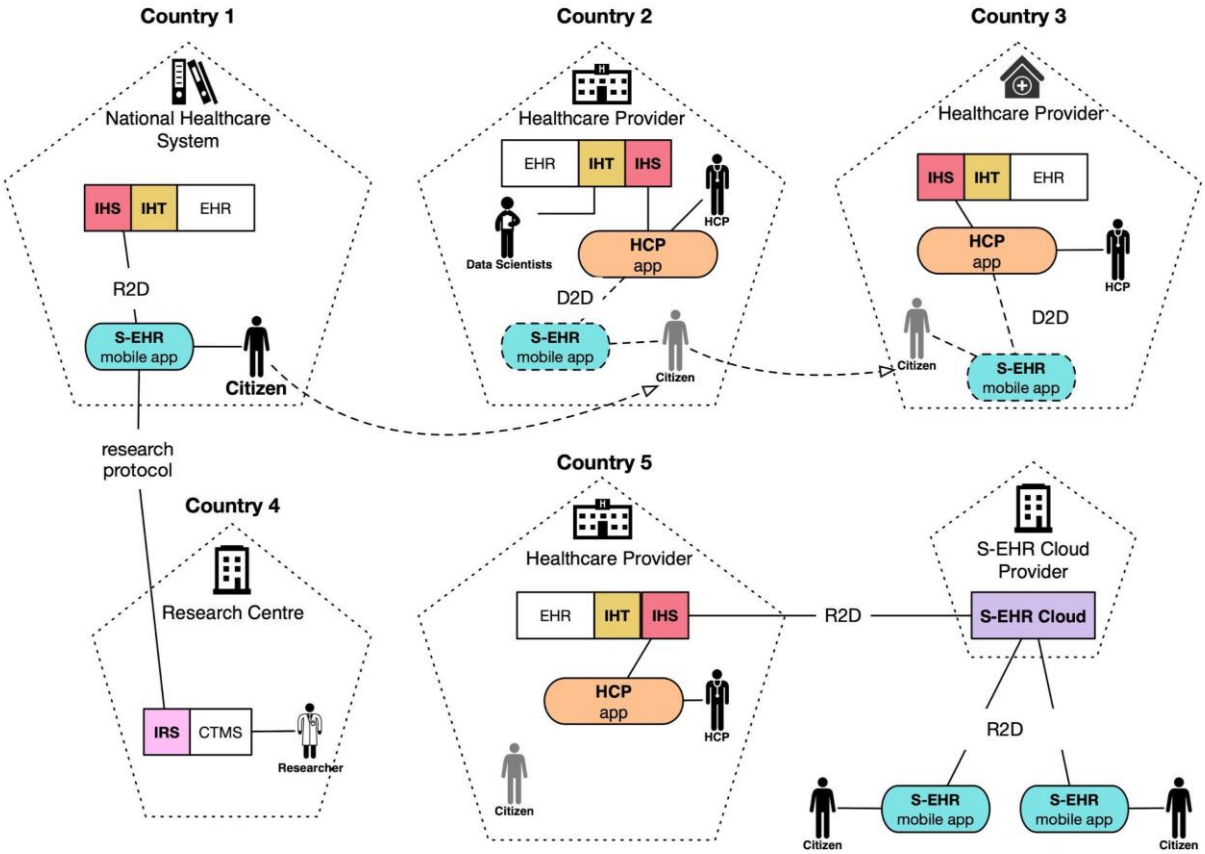


Figure 21 - Examples of health data exchange using the components offered by the InteropEHRate Framework

In the following, we describe the specific technologies chosen for the components of the framework, where they can be deployed, how they depend on each other, as well as the documents that further describe these components.

4.1 Additional actors

Other than the actors described in section 2.1, the InteropEHRate framework adds a "Data Scientist" actor, involved in the usage of the additional tools provided by the framework.

Actor	Description
Data Scientist	A person working for a healthcare organisation, with background knowledge in both the health and in the technical domain, who is able (1) to understand health data representations, standards, and local practices, and (2) to maintain the InteropEHRate knowledge and data mapping mechanisms using dedicated tools. In **[D2.2]** scenarios it is also called "domain expert".

Table 5 - Additional actors of the InteropEHRate framework

4.2 Additional organisations

Other than the organisations described in section 2.2, the InteropEHRate framework adds a further organisation, involved in the usage of the additional tools provided by the framework.

Type of organisation	Description
MT Provider	Third party provider of a machine translation service.

Table 6 - Additional organisations of the InteropEHRate framework

4.3 Component view

The following picture shows the high-level architecture of the InteropEHRate framework. For simplicity, the diagrams use the same names adopted by the Standard architecture, but those names actually refer to the reference implementations of the corresponding standard component. For instance, "S-EHR Mobile App" has to be read as "Reference Implementation (RI) of S-EHR Mobile App" or "S-EHR Mobile App RI".

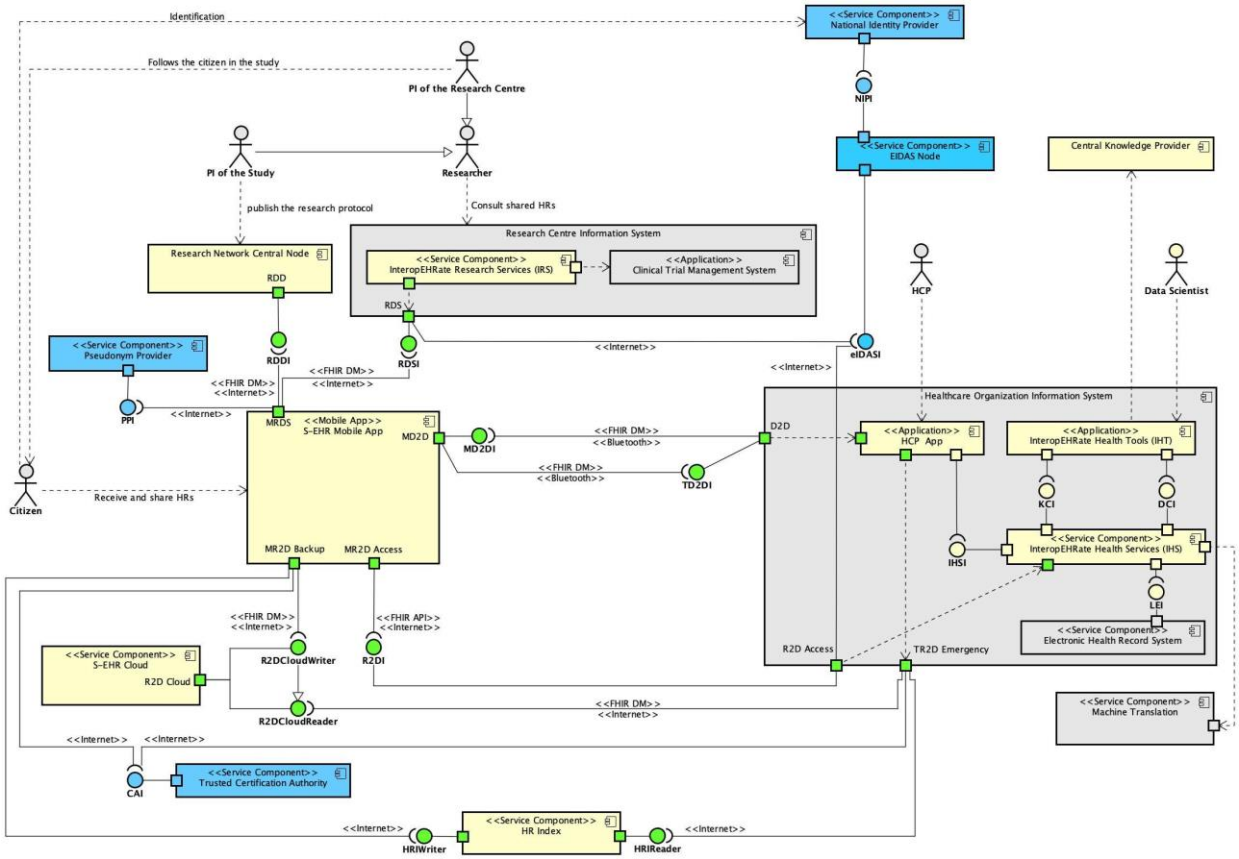


Figure 22 - Architecture of the InteropEHRate framework

The "InteropEHRate Framework", is composed of different systems, one usable independently from the others. These systems are in turn composed of reusable libraries, each one representing a reference implementation of a different remote APIs and their clients, specified by the InteropEHRate protocols.

Reference implementation of the standard InteropEHRate architecture

- ***Reference implementation libraries***: see section 4.5
- **S-EHR Mobile App RI**: reference implementation of S-EHR Mobile App, able to import/share data from/with healthcare organisations and with research centres, using short-range wireless D2D (device to device) communication or remote communication protocols. See section 4.6.
- **S-EHR Cloud RI**: reference implementation of S-EHR Cloud, able to store on the cloud the encrypted health data collected by S-EHRs, adopting the standard protocols defined by the project (section 4.7).
- **HR Index**: prototype of the HR Index, further described by the report D4.7-Design of Health Record Index **[D4.7]**.
- **Research Network Central Node (CN)**: prototype of the Research Network Central Node, able to publish RDDs accessible to any S-EHR.
- **InteropEHRate Research Services (IRS)**: a component offering a reference implementation of the interface RSI, that interoperates with any S-EHR, using the RDS protocol, allowing the scientists to

engage voluntary citizens at cross-national level in new research trials and retrospective studies and to receive health data from them. It produces data that may be exploited by the applications (e.g. in a Clinical Trial Management System) of a research centre.

Additional systems reusable by a Healthcare organisation

Other than the reference implementations, the InteropEHRate framework provides the following three components to help to integrate the InteropEHRate standard within the information systems of the healthcare organisation:

- **HCP App Prototype**: an example of a standalone HCP App, that can be integrated with a legacy EHR. As said, an HCP App may also be the extension of a legacy system EHR, therefore this prototype represents just one of the possible ways of realising the abstract concept of HCP App, that is of a software application for HCPs that supports the InteropEHRate protocols. The objective of this prototype is to demonstrate concretely how the HCP can use InteropEHRate protocols and how it can exploit the IHS (see below).
- **InteropEHRate Health Services (IHS)**: this component offers runtime functions for data conversions and translation. It interacts with existing legacy EHR systems through the LEI interface, which allows the import of health data from the legacy systems. The IHS can convert structured data from legacy to S-EHR and vice versa and uses an external service to translate free text to the local language and/or to the citizen language.
- **InteropEHRate Health Tools (IHT):** prototype of tools for
    - managing healthcare knowledge (lexical units, schemas, ontologies and encoding standards used by member countries). They interact with IHS through the KCI interface.
    - defining mapping rules for EHR data, usable both locally to serve the data integration needs of local services (such as a hospital) and Europe-wide for cross-jurisdictional data exchange. They interact with IHS through the DCI interface.

4.4 Deployment view

The following UML deployment diagram summarizes where the different components of the InteropEHRate framework are expected to be deployed. Deployment nodes offered by the same organisation are grouped in the same rectangle.

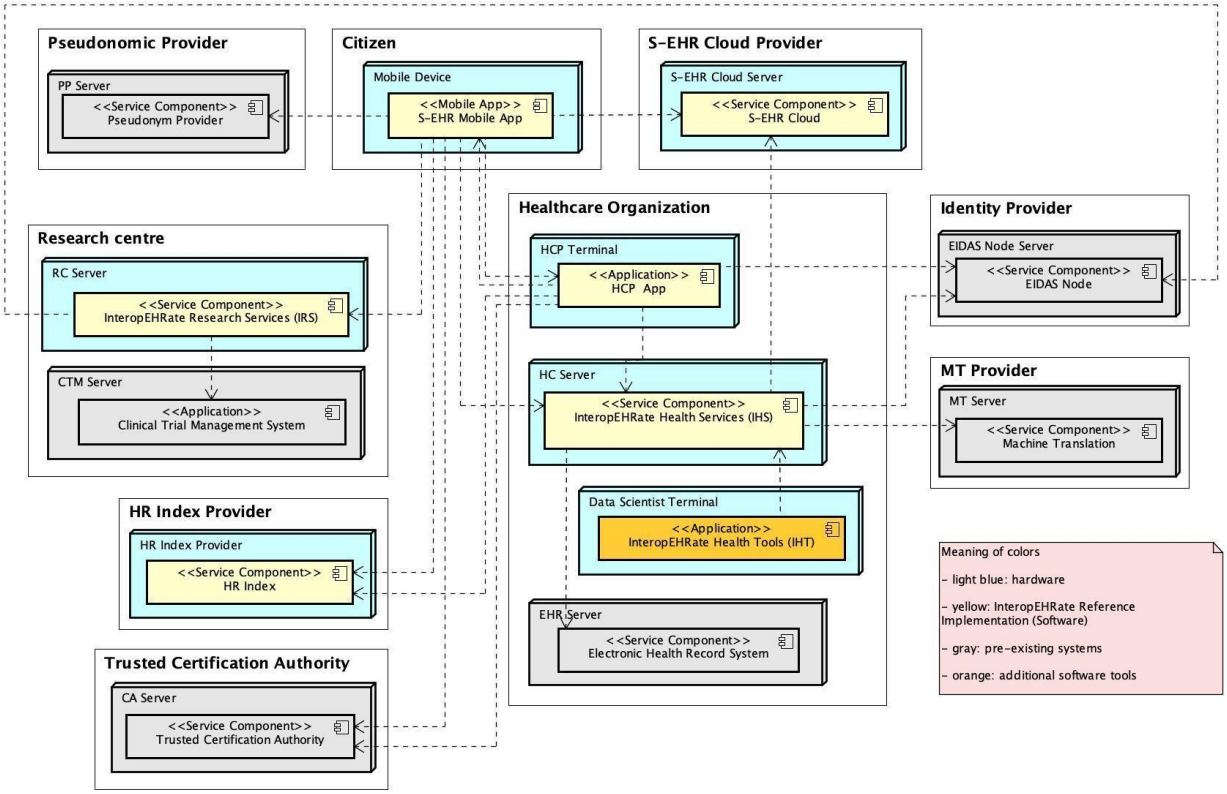


Figure 23 - Deployment view of the InteropEHRate framework

Each Citizen controls the personal mobile device where his or her S-EHR Mobile App is installed.

Each S-EHR Mobile App may interact with a S-EHR Cloud that is deployed on a different node (S-EHR Cloud Server) potentially offered by a different service provider (S-EHR Cloud Provider).

The S-EHR Mobile App may interact (using the D2D protocol) with the HCP App installed on the computer of any HCP (HCP Terminal) and with an R2D server. The health data exchanged with the S-EHR are converted in the correct format by exploiting the IHS installed typically on a different server (HC Server) of any healthcare organisation. If a healthcare organisation outsources its IT service to another provider, then the IHS could also be hosted on the servers of the same provider.

Within the healthcare organisation, the InteropEHRate Health Tools are usually also installed on the computer (Data Scientist Terminal) of one or more Data Scientists. The IHS may interact with the legacy EHRs of the same healthcare organisation, typically also running on a different server.

The S-EHR App may interact with the IRS installed on the machines (RC Server) of Research Centres. The IRS may interact with the legacy Clinical Trial Management System of the same Research Centre, installed on a different server (CTM Server). For completeness also the deployment nodes of the EIDAS node and the provider of external services for machine translation are depicted.

The following sections describe the single components of the InteropEHRate framework.

4.5 Reusable libraries

The framework will provide a reference implementation of the InteropEHRate protocols as a set of reusable libraries, each one implementing a portion of one of the protocols. Each library may be reusable independently from the others.

Security libraries:

- **Mobile R2D Security Management**, **Terminal R2D Security Management**, **Server R2D Security Management**: These three libraries implement the main security functionalities (Identity Management, Consent Management, Authorization Management) required by the R2D protocol. They are usable respectively for mobile applications (e.g. the S-EHR of the Citizen), for desktop applications (e.g. the HCP App) and for server-side services (e.g. for IHS and IRS).
- **Mobile D2D Security Management**, **Terminal D2D Security Management**: Similarly to the previous libraries, these two libraries implement the main security functionalities required by the D2D protocol.
- **Mobile Encrypted Storage**: this library implements the functionality to securely store encrypted health data on a mobile device in the respect of the "S-EHR mobile privacy and security conformance levels" **[D3.1]**.
- **Mobile Encrypted Communication**, **Terminal Encrypted Communication**, **Server Encrypted Communication**: this library offers useful functionalities for encrypted exchange of health data to be exploited respectively for the implementation of mobile applications, desktop applications and server-side services.

Details on the design of security libraries may be found in the upcoming report D3.10-*Design of libraries for HR security and privacy services - V2* **[D3.10]**.

Libraries for D2D and R2D protocols:

- **Mobile R2D HR Exchange**, **Terminal R2D HR Exchange**, **Server R2D HR Exchange**: These three libraries extend the R2D security libraries to offer an implementation of the R2D protocol for the exchange of health data on the Internet **[D4.2]**. They are usable respectively for mobile applications, desktop applications and server-side services.
- **Mobile D2D HR Exchange**, **Terminal D2D HR Exchange**: These two libraries extend the D2D security libraries to offer an implementation of the D2D protocol for the exchange of health data on Bluetooth [D4.2]. They are usable respectively for mobile applications and desktop applications.

Details on the design of libraries for D2D and R2D protocol may be found in the upcoming report **[D4.5]**.

Libraries for RDS protocol:

- **Mobile Research Data Sharing**, **Server Research Data Sharing**: These two libraries offer an implementation of the RDS protocol for allowing the citizen to share health data for research purposes **[D4.8]**. They are usable respectively for the implementation of mobile applications and server-side services.

Details on the design of libraries for RDS protocol may be found in the upcoming report D4.10-Design of library for health data sharing for research - V1 **[D4.10]** .

4.6 S-EHR Mobile App RI

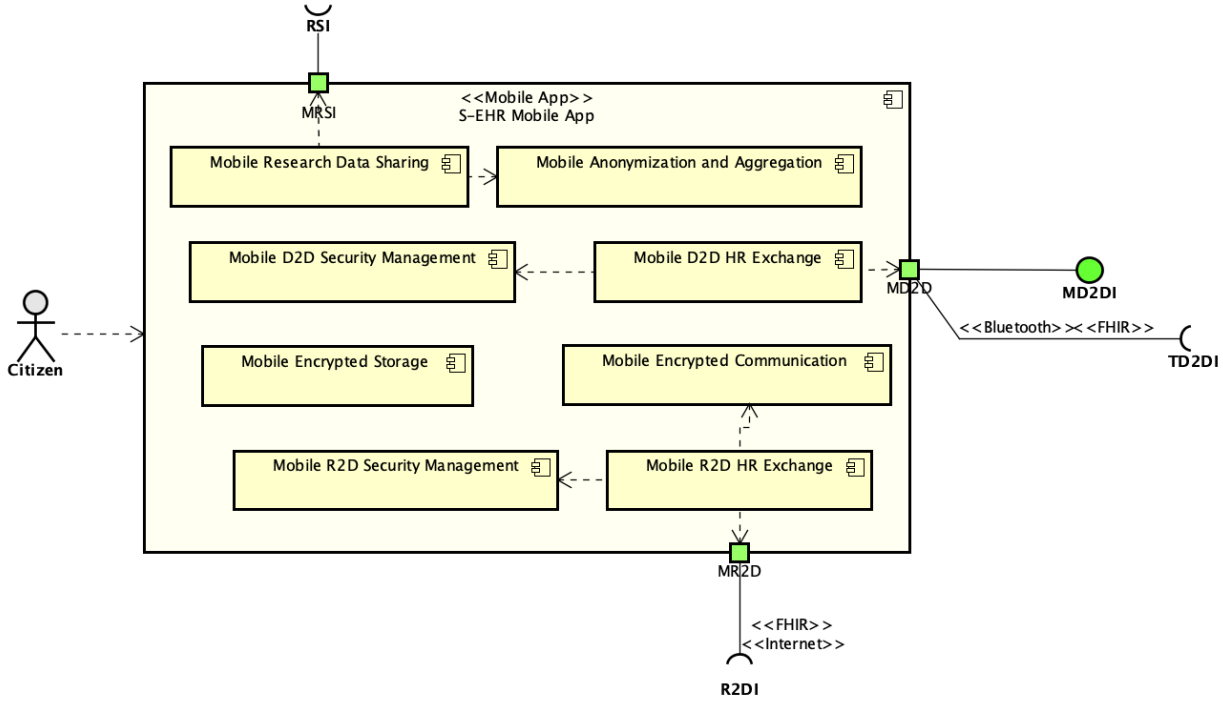


Figure 24 - S-EHR Mobile App internal view

The S-EHR Mobile App RI is the reference implementation of a S-EHR satisfying the privacy and security conformance levels defined by the standard architecture **[D3.1]**. It offers the possibility to collect and exchange health data with other actors or organisations, such as hospitals, research centres, etc.
The S-EHR Mobile App RI is an Android application that, as shown in the figure above, integrates some of the reusable libraries described in the previous section. It uses an encrypted data storage for all collected health data thanks to the library "Mobile Encrypted Storage". Moreover, it integrates other libraries offered by the InteropEHRate framework implementing the client side of the three protocols defined by InteropEHRate:

- "Mobile Research Data Sharing" to share health data with Research Centres. Before sharing health data with a research centre, they are anonymized and aggregated, using the library "Mobile Anonymization and Aggregation".
- "Mobile D2D HR Exchange" for the exchange of health data offline, through Bluetooth.
- "Mobile R2D HR Exchange" for the exchange of health data online, remotely.

All these libraries in turn use the libraries "Mobile Encrypted Communication" to assure that any remote communication is encrypted, and use the libraries for identification and authorization ("Mobile D2D Security Management" and "Mobile R2D Security Management").

The current version of the S-EHR Mobile App RI is able in particular to:

- trigger the Bluetooth connection through QRCode;

- collect and transmit patient's consent (connection Bluetooth, access and share of data, ...);
- collect and display to patient data produced by HCP;
- save personal health data on S-EHR cloud;
- give access to backed up data on S-EHR cloud to HCP;
- register citizen to research centre;

The S-EHR Mobile App RI will be available on the Android store for free.

4.7 S-EHR Cloud RI

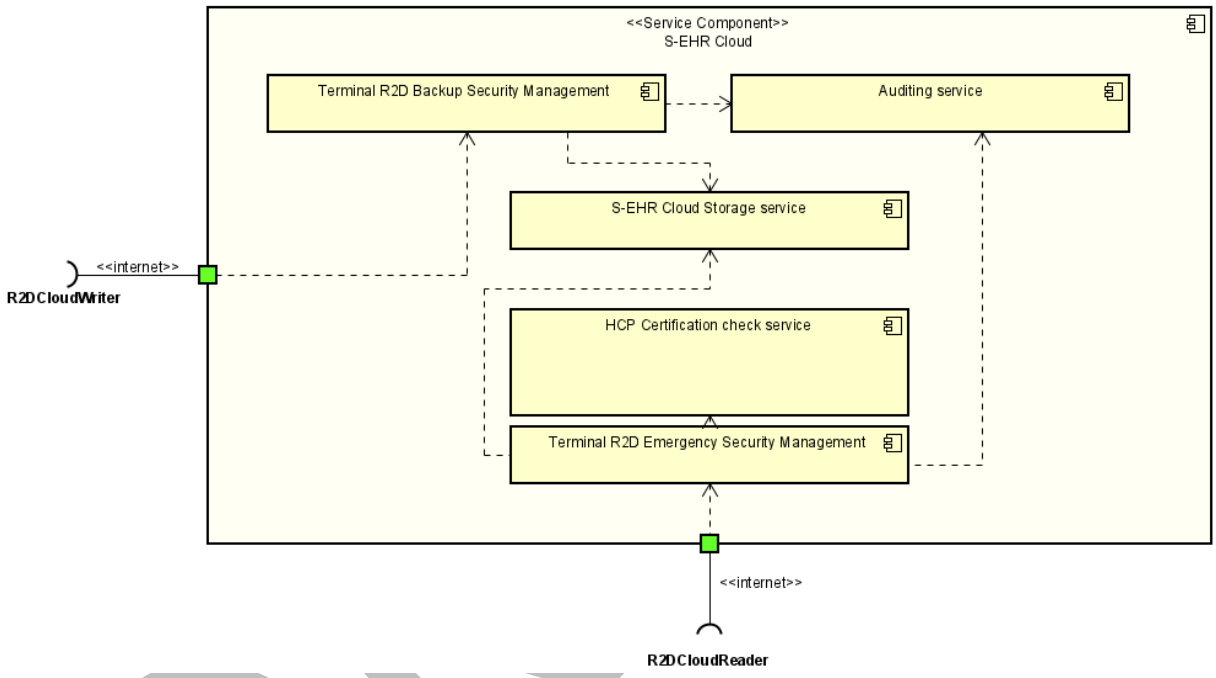


Figure 25 - S-EHR Cloud RI Internal view

The S-EHR Cloud RI regards the reference implementation of the optional service that can be enabled by a citizen through the S-EHR Mobile App, whose purpose is to give the citizen the ability to safely store their health data in the Cloud. In addition, using the S-EHR Cloud RI, a citizen may choose to grant access to the health data stored in the Cloud to authorized HCPs if an emergency occurs.

There are two possibilities with respect to the connection to the S-EHR Cloud RI. The first one regards the communication with the interface of the R2D Backup protocol, while the second one regards the communication between an HCP with the S-EHR Cloud during an emergency, which is established through the R2D Emergency protocol. The two protocols are described in sections 2.5.4 and 2.5.5 respectively.

The main components that comprehend the reference implementation of the S-EHR Cloud RI are the following:

- **Terminal R2D Backup Security Management:** This component ensures that the communication between the S-EHR Cloud RI and the S-EHR Mobile App RI is encrypted

- **Storage service:** This component is used to safely store the citizen's health data in the Cloud
- **Auditing service:** This component audits and keeps logs of every action that has been performed in the S-EHR Cloud on both the citizen and the HCP side. These actions may include the login from a S-EHR App device, the upload of encrypted health data content by the citizen, the requests to access the citizen's by HCPs, etc.
- **HCP Certification service:** This component needs to verify that the specific individual that requests access to the S-EHR Cloud is authorized by a trusted authentication authority as an HCP. If this authentication is successful, the HCP gains access to the citizen's content
- **Terminal R2D Backup Security Management:** This component ensures that the communication between the S-EHR Cloud RI and the HCP App RI is encrypted

4.8 Example HCP App

The InteropEHRate Framework includes a simple example HCP App. As explained in the previous sections, an HCP App is any software application able to provide medical staff with the ability to access and operate patients' data from S-EHR Mobile App, S-EHR Cloud and EHR of the Healthcare organisation. In other words, the HCP App is an application used by the HCPs to securely exchange health data of their EHRs with any S-EHR Mobile App and to read health data stored in S-EHR Cloud using the InteropEHRate protocols.

The HCPs of a Healthcare organisation are not required to use a new application to exploit the InteropEHRate protocols. Indeed, it is possible to extend the already used application to support the InteropEHRate protocols (one of the demonstrators developed by the project will indeed follow this approach). Such an extended application would have a lower impact on the health processes of an organisation and on the user experience of the HCPs. On the other hand, the example HCP App provided by the InteropEHRate framework is a generic and basic application built from scratch that can be potentially extended and integrated into different contexts. It has the purpose to show to application developers how the reusable libraries (see section 4.5) can be exploited to support the InteropEHRate protocols and how it is possible to exploit the IHS to interact with the content of an existing EHR.

While in the previous sections the term "HCP App" is used to refer to any application used by HCPs and able to support the InteropEHRate protocols, in this chapter the term refers only to the specific example HCP App provided by the InteropEHRate Framework. This example is also a demonstrator that can be easily distributed to show to the final users how HCPs can take advantage of the InteropEHRate protocols. In this respect this HCP App implementation have functionalities for:

- Importing health data from a S-EHR and export them back using the D2D protocol (TD2DI);
- Importing health data from the S-EHR cloud by the R2D Emergency protocol (R2DI);
- Importing health data from an EHR located within the healthcare organisation.

Considering the overall architecture, user requirements specified in **[D2.2]**] and technical solutions available at the moment, the HCP App is developed using web technologies. According to **[D4.2]** the D2D

protocol is implemented using Bluetooth, this requires installing the HCP app as a desktop application on a Healthcare professional's workstation (terminal)[8].

The HCP App is developed using Java technologies, thus ensuring Operating System independence and has direct communications with S-EHR Mobile App and IHS as is illustrated in the following figure. Healthcare organisations may use the HCP App or may choose to evolve the GUIs of their legacy systems to add the same functionality provided by HCP App. The figure also shows which reusable libraries of the InteropEHRate framework (italic) are exploited for exchanging information with S-EHR Mobile App and S-EHR Cloud. As said, looking at the code of the HCP App, the developers will more easily understand how to integrate the existing libraries also in their legacy systems, in order to offer functionalities similar to the ones of the HCP App. A description of the libraries integrated into the HCP App can be found in chapter 4.5 – Reusable libraries and in deliverable D5.4-Design of an integrated EHR web app for HCP - V1 **[D5.4]**.

terminal-d2d-hr-exchange is the component that ensures the communication with S-EHR Mobile App. On the one hand, it provides an implementation of the interface TD2DI to be consumed by the S-EHR Mobile App, on the other hand, implements a client that consumes the interface MD2DI implemented by the S-EHR Mobile App.

terminal-r2d-hr-exchange is the component responsible for consuming the R2DI in order to retrieve a patient's EHR for emergency cases.

[8] It would be advantageous to adopt a SaaS (Software as a Service) model of deployment, but this cannot be done yet in a reliable and secure way. The future standard to allow a (SaaS) Web Application to access the Bluetooth connection of the user terminal will be the so called "Web Bluetooth API" **[WBA]**. Because Web Bluetooth API specification is not finalized and well implemented by the main web browsers, it will not be used for establishing the communication between HCP App and S-EHR Mobile App, at least for the moment. Considering this limitation, the HCP App cannot be deployed as a centralized application even if it is developed as a web application.

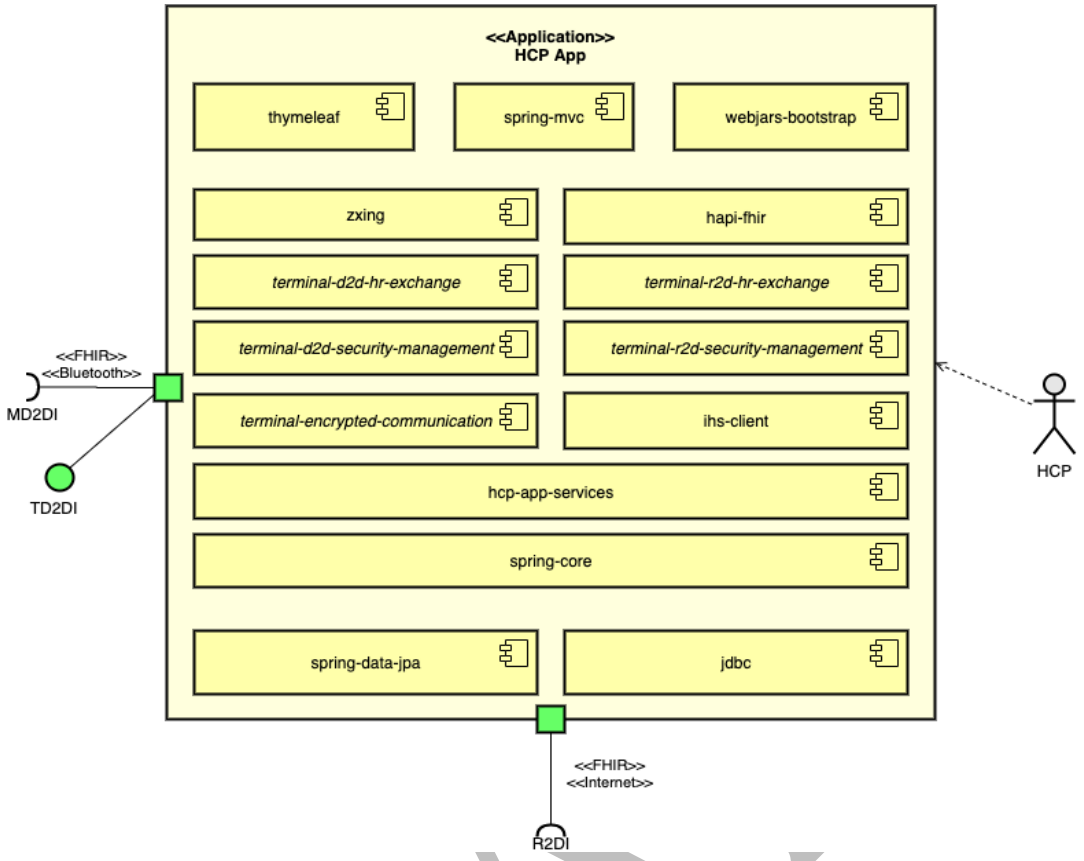


Figure 26 - HCP app internal view

The HCP App will be distributed as a micro-service with all components included and the installation on the Healthcare professional's terminal consisting of copying a single file.

4.9 InteropEHRate Health Services (IHS)

InteropEHRate Health Services is a high-level component in charge of the conversion of local EHR formats to the interoperable S-EHR representation and of their translation into multiple European languages. In order to do so, the IHS exposes a set of high-level and low-level *S-EHR conversion and translation services:*

- converting an entire legacy EHR into the common S-EHR representation, including the FHIR format and the use of interoperable medical coding systems;
- translating the contents of an entire S-EHR from one language to another;
- mapping individual coded values between local and international standards;
- providing the natural-language descriptions of such coded values in multiple European languages;
- providing translations of the natural-language text contained within EHRs;
- extraction of key healthcare terms and names from the natural-language text contained in health data and expressed in multiple European languages.

The IHS component supports three different levels of interoperability, each deployment site (e.g., hospital) being able to choose the level of support they are able to provide according to their technical and infrastructural capabilities:

1. secure: beyond assuring the security of the EHR content, no conversion or translation is applied;
2. syntactic: in addition to the previous level, the EHR is converted into S-EHR which uses standard FHIR profile(s) as defined in Deliverable 2.7; however, apart from structural changes, data values remain in their original representations, with the possibility of free-text translation being applied to them;
3. semantic: in addition to the previous level, data values in the S-EHR undergo meaning-level conversions, such as the mapping of health codes or the extraction of healthcare terms from natural-language text.

The following picture shows the main components of the IHS. It exploits the two reusable libraries "R2D Security Management" and "R2D HR Exchange" (see section 4.5), moreover it offers additional components further described in the next subsections.

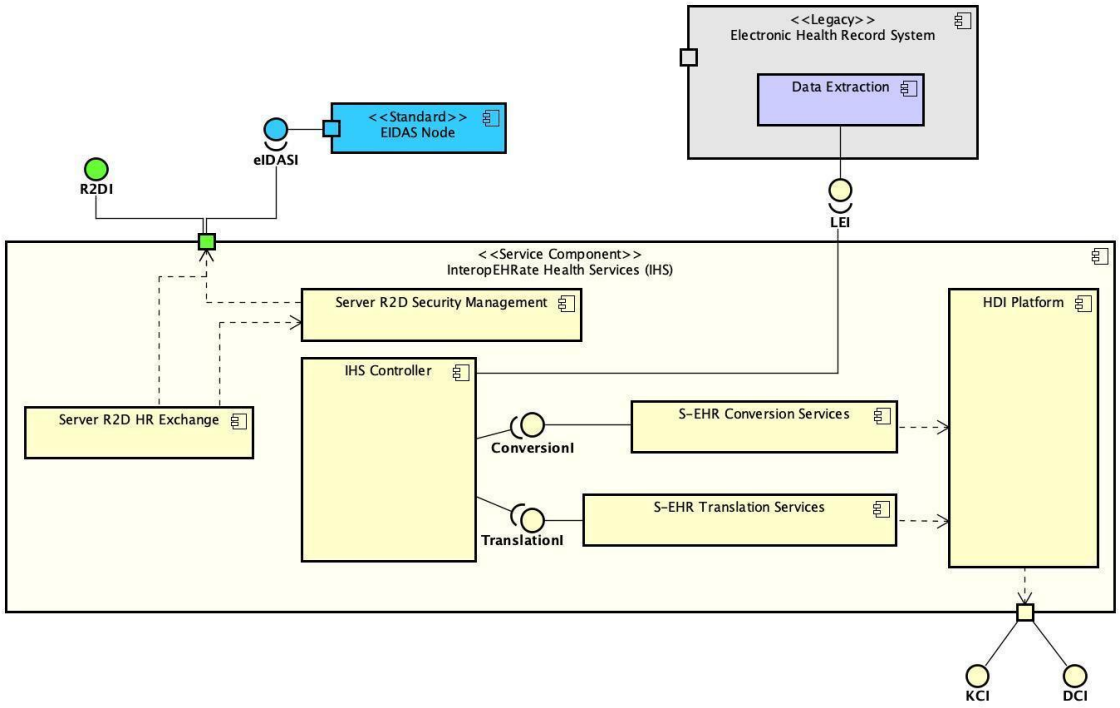


Figure 27 - IHS internal view

4.9.1 S- EHR Conversion and Translation Services

The EHR interoperability services offered by IHS are divided into two main categories, as realised by the components in the figure above:

- *conversion services:* these are implemented by the *S-EHR Conversion Services* component and are exposed through the Conversion Interface (*ConversionI*);
- *translation services:* these are implemented by the *S-EHR Translation Services* component and are exposed through the Translation Interface (*TranslationI*).

The table below provides the main functionalities provided by these two components for each interoperability level:

Level	Conversion Services	Translation Services
Secure	None	None
Syntactic	• Conversion of EHR data structures to FHIR.	• Free-text translation for an entire S-EHR; • free-text translation for individual labels.
Semantic	• Conversion of EHR data structures to FHIR; • mapping of coded values to interoperability standards; • extraction of medical terms from natural-language text and linking them to non-ambiguous meanings.	• Free-text translation for an entire S-EHR; • free-text translation for individual labels; • translation of attribute names; • providing human-readable definitions for coded values in multiple languages.

Table 7 - Conversion and Translation service functionalities

The S-EHR Translation Service adopts two different methods to translate the content of S-EHR, defined using two low-level translation services. The first one, used for providing free-text translation, called *MachineTranslation*, and a second one for the translation of "*concepts*" expressed through medical standard codes and terms, which is called *ConceptTranslation*. The two low-level translation services operate on different portions of the S-EHR content. While the *MachineTranslation* is based on an external, third-party machine translation (MT) component, the *ConceptTranslation* works thanks to the interaction with the knowledge-based *HDI Platform*.

The S-EHR Conversion Service converts coded values and single domain terms appearing in health data into formal and interoperable representations as defined by the Interoperability Profile. The service interacts with the *HDI Platform* in order to exploit the mapping knowledge for the conversion, on both the syntactic and semantic level, of the S-EHR content.

4.9.2 HDI Platform

The conversion and translation functionalities described in the previous section rely on an innovative knowledge-based data integration platform, shown as *Health Data Integration (HDI) Platform* in the figure above. The platform provides the following lower-level functionalities to the conversion and translation services:

- Multilingual natural language processing (NLP) for the health domain, for the extraction of health concept and relevant names from natural language text appearing in health data;
- cross-lingual knowledge management for the mapping and translation of medical terminology and coding standards;
- definition of legacy and FHIR data structures.

The HDI Platform is knowledge-based in the sense that data structures, terminology, labels in multiple languages, as well as locally specific NLP functions are all represented internally as adaptable and extensible knowledge. The initial bootstrapping and subsequent adaptation of knowledge is performed

partly programmatically by a local software developer and partly interactively by a local *data scientist*, using graphical knowledge management tools that connect to the HDI Platform through the interfaces *Knowledge Configuration Interface* and *Data Integration Configuration Interface*. The knowledge management tools are presented under the section *Interoperate Health Tools*.

4.9.3 IHS Controller

The role of the *IHS Controller* component is to provide high-level external interfaces for the IHS services and to adapt the (a priori generic) health services to the precise needs of the local environment. These involve:

- connecting to the legacy EHR system through a *Legacy EHR Interface (LEI)*, implemented by the local institution, for the reading and writing of legacy EHRs to/from local databases; in particular, legacy EHRs are provided by the local systems to IHS in an agreed meta-format to be defined in D5.7;
- connecting to the *HCP App* through the *IHS Interface (IHSI)* that provides high-level services such as "localize a S-EHR to the local environment", into lower-level conversion and translation operations;
- serving requests, via the internal *HR Exchange* component and the R2D protocol, to remote devices requesting patient data over the Internet;
- defining the level of interoperability supported and using conversion and translation services accordingly.

4.9.4 R2D Security Management

This library provides an implementation for the R2D Security protocol (see section 2.5.2), including identity management, authorization and consent management, as well as encrypted storage and communication, to be used over the R2D protocol when S-EHRs are transmitted through the Internet, as in the InteropEHRate emergency scenario.

4.9.5 R2D HR Exchange

The *R2D HR Exchange* library receives and serves S-EHR requests from the Internet through the R2D Access protocol (see section 2.5.3). It delegates requests to the IHS components in charge of EHR processing and uses the *Server R2D Security Management* component to assure the security of remote communication.

4.10 InteropEHRate Research Services (IRS)

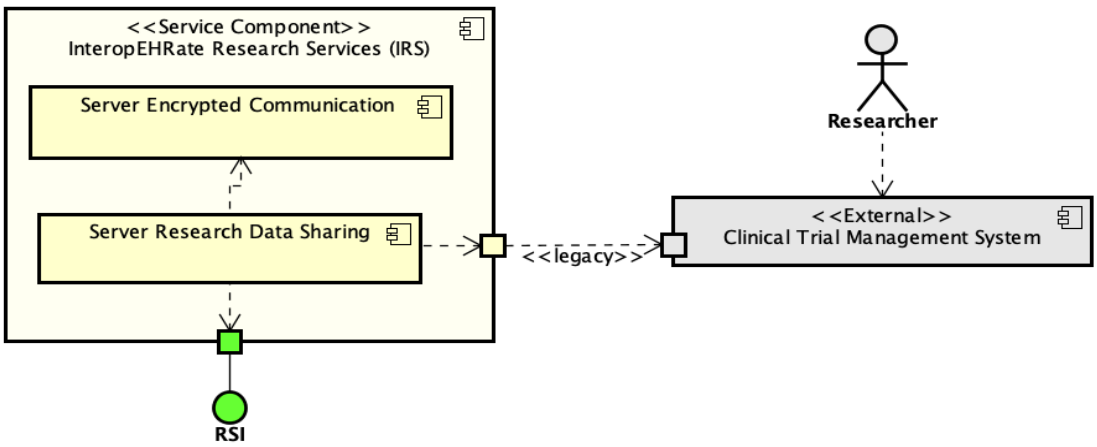


Figure 28 - IRS internal view

The *InteropEHRate Research Services (IRS)* implement functionalities that orchestrate data collection from the S-EHRs of patients in possession of the S-EHR Mobile App. As such, it is a software component that acts as a bridge between medical researchers (and their own IT infrastructure) and patients (and their S-EHR-enabled mobile devices). The role of IRS, running within a specific Research Centre, involves:

1. maintaining a (pseudonymized) list of citizens who have elected the Research Centre as their *Reference Research Centre*;
2. receiving and handling consent or refusal of citizens' participation in specific experiments;
3. receiving de-identified data collected from citizens;
4. forwarding citizen data to the requestor Research Centre.

4.11 InteropEHRate Health Tools (IHT)

As part of the InteropEHRate framework, the *InteropEHRate Health Tools* are interactive tools that serve the purpose of configuring and adapting the *HDI Platform*, and as such the entire IHS, to the specific needs of the local institution (e.g., hospital). Configuration and adaptation involve supporting:

- local language;
- international healthcare terminology and coding systems;
- FHIR data structure;
- locally used healthcare terminology and coding systems, and their mapping to international ones;
- local data structures and their mapping to FHIR.

Note that both local and international terminologies, codings, and data structures evolve over time: thus, their maintenance and adaptation is not a one-shot effort but rather a continuous process. Still, the bulk of the configuration effort is foreseen as part of the initial deployment phase of the IHS.

All of the configuration aspects above are represented in the HDI Platform as formal *knowledge*. This formalisation effort, that encodes local formats, standards, and semi-formal or informal practices as knowledge, is executed by a local *data scientist* using the interactive IHT tools. In case some of the efforts

need to be automated through scripting (e.g., uploading the definitions of thousands of terms), the data scientist can be assisted by a *software developer* in charge of programmatically automating some of the processes instead of using the IHT.

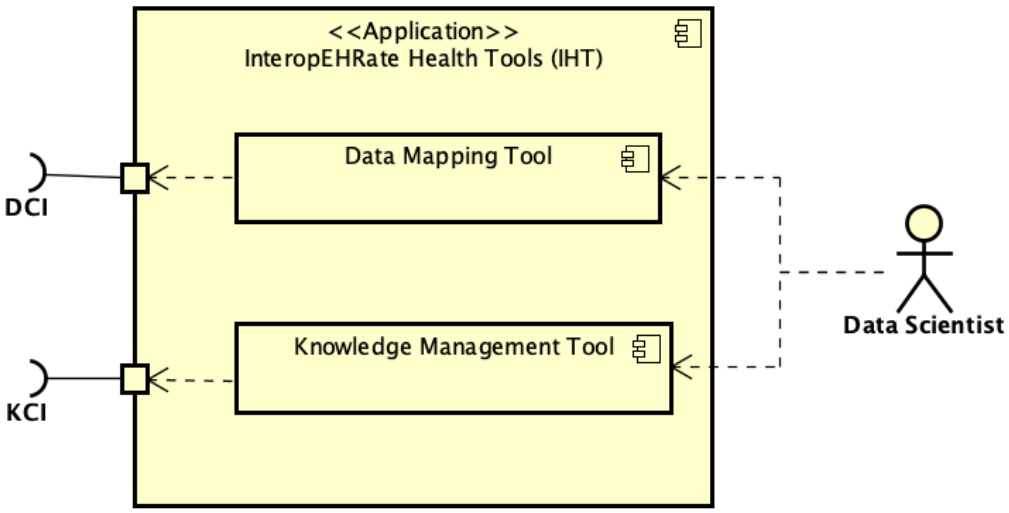


Figure 29 - IHT internal view

As depicted above, IHT is composed of two principal tools:

- a *Data Mapping Tool* with which the data scientist defines how to convert data from the legacy EHR structure to the FHIR-based structure;
- a *Knowledge Management Tool* which is used to define and describe the lexicon, medical terminology, medical encodings, and their mappings.

The tools are typically used in the following order and manner:

1. The knowledge that defines and describes interoperability standards (e.g., FHIR or international encodings) is *a priori* built into the HDI Platform, all the while remaining adaptable and extensible.
2. The Knowledge Management Tool is used:
    a. To define locally relevant concepts and their relatedness (underlying the meanings of terms, data attributes, coded values, etc., that are used by the local institution or on regional or national levels);
    b. to define natural-language labels associated with the concepts above (how the meanings above are expressed inside local datasets);
    c. to adapt and extend, if necessary, the FHIR reference schemas to which local EHRs or third-party S-EHRs are converted;
    d. to define mappings, wherever applicable, between locally relevant and international concepts.
3. The Data Mapper Tool is used interactively to define the mappings of local EHR data attributes to FHIR attributes, as well as corresponding data conversion methods. During the mapping procedure performed by the data scientist, the Data Mapper Tool allows for minor data modification on the EHR attributes, in order to format and align their values to the respective FHIR attributes structure.

Moreover, the Data Mapper Tool can interact with the HDI Platform to exploit the NLP and knowledge-based functionalities in order to extract concepts from the attribute values. The result is a data mapping "recipe", which includes all the operations performed by the data scientist. If similar mapping operations have to be performed, in the future, on different attribute values, the Data Mapping Tool allows reapplying, automatically, the *recipe* (also called *Mapping Model*) on the EHRs to be mapped.

4. The results of steps 2-3 are tested through the automated execution of the conversion and translation of a test set of EHRs. In case of problems encountered, steps 2-3-4 are repeated to fix the knowledge and/or the mappings and re-test the results.

As it appears from the IHT operational order described above, the Knowledge Management Tool as well as the Data Mapper Tool are used to preload the HDI Platform with the knowledge needed for the correct usage of the Conversion and Translation Services.

4.12 Interactions between HCP App, IHS and legacy systems

4.12.1 Extract S-EHR content from source hospital

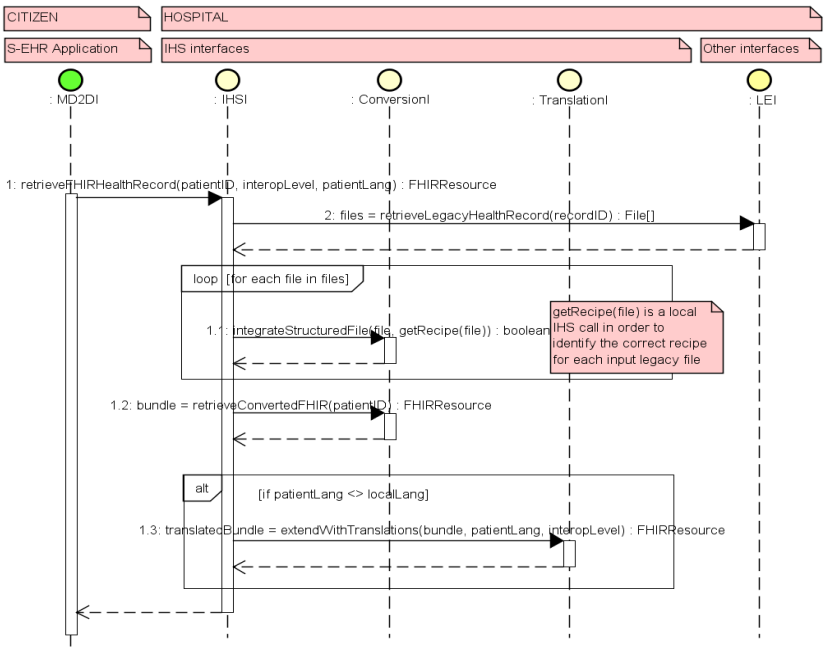


Figure 30 - Sequence diagram: extract S-EHR content from source hospital

The sequence diagram above describes a situation in which a patient wants to get his or her own health data from a hospital. The first actor in the diagram is the citizen, represented by a S-EHR App, and the second one is the hospital that is composed by:

- IHS Interfaces: the component that offers the usage of S-EHR conversion and translation components described in section 7.4.5;
- the legacy EHR system of the hospital, accessible through the Legacy EHR Interface (LEI).

The process begins by a request from a patient to obtain the health data on his or her mobile device. Upon this, the IHS component retrieves the legacy health data and converts it to the FHIR-based *Interoperability*

Profile. If the patient requests the translation of the health data to his or her own language (in case the health data is in a different language), translation is also applied, extending the original-language record. The conversion and translation details (e.g. the local language or the interoperability level (syntactic or semantic) to be applied by the conversion process) are pre-set as configuration parameters of the IHS. Finally, the converted and possibly translated health data are transferred to the S-EHR App.

4.12.2 Download and use S-EHR content at the target hospital

The sequence diagram below describes a situation in which a HCP downloads the citizen's health data from the mobile app in order to visualise and possibly update it through the HCP App. The actors and the components of this diagram are as in the previous section, with an added HCP App and an external machine translation component.

Before the HCP App can display the health data downloaded from the S-EHR App, it may need to be translated to the local language, in case the original language of the health data is different. It is then the responsibility of the HCP App to display the original data and the translations in a way that the result of these automated operations is clear and transparent to the HCP App. In case the HCP updates the Citizen's health record by new entries, these entries are generated by the HCP App as new FHIR resources. Such resources may, in turn, need to be converted and translated: terminology and codes entered by the HCP as simple strings can be converted to concepts, and text entered by the HCP translated to the patient's own language, if the patient requests it and the hospital is able to provide the translation capability.

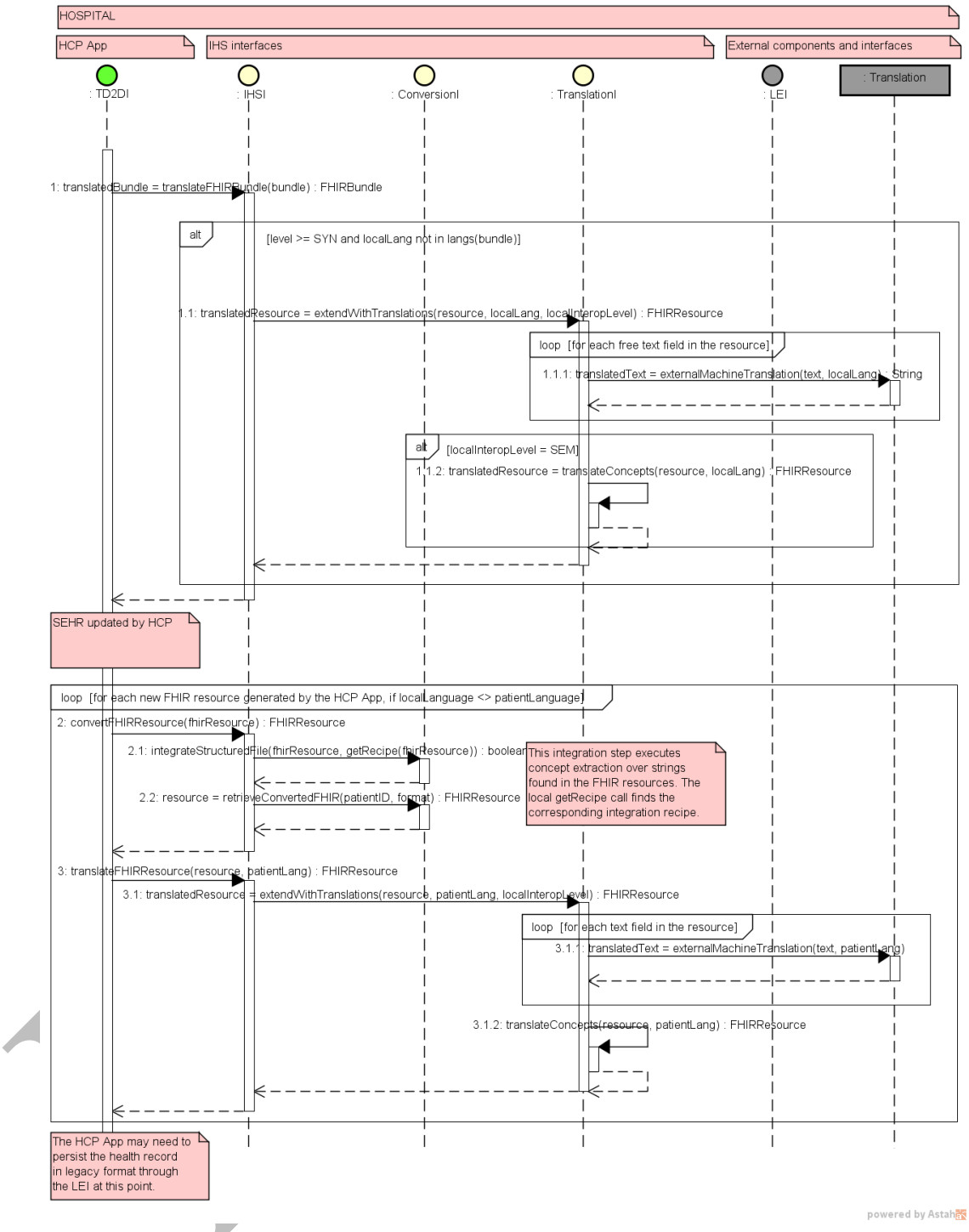


Figure 31 - Sequence diagram: download and use S-EHR content at target hospital

5 CONCLUSIONS AND NEXT STEPS

This report described the second version of the InteropEHRate standard architecture and of its reference implementation, the InteropEHRate framework. Similar to other reports of the InteropEHRate project, this document is a draft reflecting the current progress of the research project. A final version of this report is planned for 2021.

The following version is expected to update the architecture, based on the new knowledge acquired from the experience of development, from external feedback (e.g. from focus groups) and from the detailed design of components and interfaces that are planned for next year.

Major changes are expected in particular with respect to R2D Backup, R2D Emergency and RDS protocols which analysis is still not complete and will occur during the next months. Other changes could reflect updates to the scenarios that will be released as part of the deliverable **[D2.2]**.

As a consequence, the next version could include changes to functionalities required to any S-EHR Cloud as part of the standard architecture and the functionalities of the S-EHR Cloud RI. These include the ability of a Citizen to upload Medical Images, the auditing mechanisms of the S-EHR Cloud that keep reports of whoever gained access to the S-EHR Cloud and the actions that they made, along with the provision of the Discharge reports that are created after an emergency. In addition, an HCP will have the ability to upload new content to the S-EHR Cloud through the HCP app.

Another line of updates is also expected in the context of the various security protocols and interaction schemes. As mentioned before, there will be new functionalities added towards the support of auditing mechanisms from the S-EHR Cloud in order to keep records on access control actions (i.e., users, physicians that requested access to specific data sets) and data sharing transactions. To this end, we will consider the integration of Blockchains and Distributed Ledger Technologies (DLTs) for the provision of secure, trusted, and auditable (medical) data sharing across requesting actors by leveraging advanced crypto primitives including Attribute-based Encryption (ABE); encrypted data would be associated with a series of attributes and key management would be based on a set of policies that allow controlled decryption depending on the attributes exhibited by the data requestors. This would also alleviate the current need of users releasing the private symmetric keys (supported through the QR codes) which exhibits security and privacy concerns (related to users having to provide access to their private secrets) and performance challenges as it pertains to the scalability of such mechanisms. Towards this direction, the S-EHR Cloud should provide enhanced information protection, access control and secure (distributed) data management through the use of Blockchains, over the entire data lifecycle, ranging from data generation, collection and storage to data search and deletion.

Furthermore, some changes are expected in the context of the RDS protocol so as to identify the exact cryptographic primitives to be used for providing the required privacy properties when users are sharing their data with the (Reference) Research Centres. Based on the definition of the current models and workflow of actions for credential management and privacy-friendly authentication services through the use of short-term anonymous credentials (i.e., pseudonyms), a detailed investigation will be conducted for identifying the most appropriate lightweight crypto primitives (so as to be supported by the user's resource constrained mobile devices) in the context of group signatures and/or blind signatures. For the former, dynamic group signatures [**GS**]will be investigated that allow the dynamic addition of users (through the S-EHR App) as members of an anonymized group. Blind signatures [**BS**], on the other hand, will be leveraged

by users to anonymously sign their shared data while providing the necessary guarantees that they have been successfully authenticated and signed the necessary consent form; however, the RRC will not be able to link such messages back to the data contributors unless of a medical emergency.

Another important feature is expected to be investigated in the context of the medical visit scenario towards the enhancement of the D2D security protocol through the use of context-aware authentication schemes. The main motivation is to determine whether a user's device can leverage information from the surrounding environment for establishing a secret key with the other communicating party. The current protocol is based on the state-of-the-art key establishment and agreement schemes, such as the Diffie Hellman protocol, however, this exhibits a high computational complexity and energy consumption which might hinder its wide deployment in real-world scenarios **ZIA**. Therefore, the modelling of a lightweight zero-interaction pairing scheme will be investigated for devices using information about their environment to create an authentication key [**ZI14**]. "Zero-interaction" entails that the users are not involved in the authentication process, thus, increasing the applicability of such schemes.

Some change is also expected to better align the D2D protocol to the R2D Access protocol, to make more similar the operations offered by the two protocols. Moreover, it is within the future plans of the D2D protocol to be specified in a more platform independent way and avoid having mandatory one-to-one interactions (i.e. ping-pong communication), between the involved parties. Consequently, messages which are going to be sent from the one party, should not always receive a response message in the form of an acknowledgment, giving the ability to the protocol to be more flexible. To this end, it will be examined the possibility to divide the D2D protocol into sub-protocols (i.e. protocol chunks), which could be used in various conditions, depending on the current needs of the different scenarios (e.g. will be examined the possibility to have a D2D sub-protocol that will specify the messages that should be exchanged only for the identification purposes between the two involved parties, bypassing the steps of exchanging consent or healthcare data).

Other changes will be reported in the next version of this document, regarding new capabilities provided by the InteropEHRate framework for the data mapping operations. More in detail, a new service will be defined which will allow the Data Scientist to extract, in an automated way, medical concepts, terms and other information regarding the patient, starting from portions of natural language text inserted in the health data (such as medical reports). This service will also allow the Data Scientist to eventually anonymize sensible information relative to the patient, which has been identified and extracted from natural language texts within the health data.

Finally, the next version of this deliverable will reflect the progress of the example HCP App and the reference implementation of S-EHR Mobile App that, together with the other elements of the InteropEHRate Framework, will offer a more complete implementation of the functionalities required by the InteropEHRate scenarios and start an on the field experimentation with the final users.

For the next year, the HCP application will permit the healthcare professional to consult the medical images and hospital discharges as well as upload, into S-EHR, X-ray images and evaluation reports of the patient. The HCP will be able to author and store the clinical history and evaluation report of the citizen. The HCP application will permit also the storing in S-EHR Cloud of discharge reports.

In the case of an emergency, after gaining access to the Citizen's health data, the HCP may retrieve from the Citizen's S-EHR Cloud any medical images referred by the accessed health data.

The HCP application will implement the functionality that will let the healthcare team gain access to the patient's health data in an emergency case. When a qualified HCP gains access to the health data for emergency reasons, also the rest of the healthcare team that treats that patient for that specific emergency encounter automatically obtains access to the same health data. The HCP app will permanently store the emergency health data if and only if this is authorized by the patient or by the law.

GLOSSARY

Term	Definition
Application Programming Interface	Set of standardized request messages that a computer program can receive from another. An Application Programming Interface (API) is part of a communication protocol. Two common kinds of APIs are local APIs (API offered by a program, e.g. a software library, to another program running on the same computer) and remote APIs (API offered by server software, e.g. a web server, to client software, e.g. a mobile application, running on another computing device). All APIs specified by the InteropEHRate open specification are remote APIs. Remote APIs that use the HTTP methods for performing the requests are called Web APIs. The R2D and RDS protocols include Web APIs.
Clinical Trial Management System	A software system used by biotechnology and pharmaceutical industries to manage clinical trials in clinical research.
Communication protocol	A set of rules about how to format and transmit data between electronic devices. The rules specify the order, syntax, semantics and other constraints to be fulfilled by the messages (i.e. data) exchanged by the devices. The specification of syntax and semantics of the messages that a device in the communication must be able to receive is called remote API.
Device to Device (protocol)	Secure communication protocol (and remote APIs) for exchanging health data between two nearby devices (not using Internet), one running a S-EHR App and the other running an HCP App.
Electronic Health Record System	"A system for recording, retrieving and handling information in electronic health records" [[**ISO/TR 20514**]].
Health data	Data about a person's health, produced by a healthcare organisation, by the person or by a device, even unrelated to any healthcare episode.
Healthcare Professional	Member of a multidisciplinary team composed by several healthcare professions working together to execute healthcare processes (e.g. Medical Doctors, Nurses, Midwives, physiotherapists, …)
Healthcare Professional Application	Any software application used by HCPs to securely exchange health data with any S-EHR using the D2D and/or R2D Emergency protocols defined by InteropEHRate. An HCP App may be an advanced front end of an EHR, may be a distinct application integrated with an EHR, or it may be a completely independent application. It is part of the "Healthcare Organization Information System".

(Health) Research Protocol	Purposes and methodology specified to collect and process a dataset of health and social data, to learn more about human health and treatments (to be approved by an Ethical Committee).
(Health) Research Study	A human process performed by one or more researcher organizations intended to increase the knowledge on about human health and treatments. Each research study is executed according to a specific health research protocol
Hypertext Transfer Protocol	Hypertext Transfer Protocol (HTTP) is a communication protocol used by web browsers for accessing hypertext documents and other kinds of contents (called "resources") published on web servers that are part of the World Wide Web.
Interface	Synonymous with “Application Programming Interface”.
InteropEHRate FHIR profiles	Set of HL7 FHIR profiles and implementation guides that defines the formats of health data exchanged with the InteropEHRate protocols.
InteropEHRate Health Services	Components for converting structured health data extracted from local EHRs to the FHIR data format expected by the InteropEHRate protocols – and vice versa – and for translating them to the user language. They can be exploited to integrate HCP Apps and protocol services with legacy EHRs and to make the exchanged health records comprehensible to citizens and HCPs of different countries.
InteropEHRate Health Tools	Tools for managing healthcare knowledge (lexical units, schemas, ontologies and encoding standards used by member countries). They allow to define mapping rules for conversion of health records exploited by the IHS for data conversion.
InteropEHRate Research Services	Reusable components offered by the InteropEHRate Framework that interoperates with any S-EHR using the protocol for research health data sharing, allowing the scientists to engage voluntary citizens at the cross-national level in new research trials and retrospective studies and to receive health data from them.
Mobile Device to Device Interface	The interface offered by the S-EHR to support the D2D protocol, i.e. to exchange health data with citizen’s S-EHRs at a short distance, without using the Internet.
Remote to Device (protocols)	Set of three protocols for the exchange of health data using the Internet, called R2D Access, R2D Backup and R2D Emergency.
Research Data Sharing (protocol)	Secure IT communication protocol (and APIs) for publishing and retrieving machine processable descriptions of research studies and for sending citizen’s consents and health data from S-EHR Apps to research centres (that are RDS nodes), without any cloud storage of health records. The RDS protocol has not to be confused with a Research Protocol.

Remote to Device Interface	The interface offered by the HealthCare organisation to support the R2D protocol, i.e. to exchange health data with citizen's S-EHRs by means of the Internet.
Research Data	Any health data that a citizen shares with a specific research study.
Research Interface	The interface offered by the Research Centre to support the RDS protocol, i.e. to engage citizens and to receive their health data and consent to the usage.
RDS Node	Any node of a network of research centres and technical services that implement the RDS protocol.
R2D Access	Secure IT communication protocol (and remote API) used by a S-EHR App for receiving, over the Internet, health data from and healthcare organisation
R2D Backup	Secure IT communication protocol (and remote API) for the backup of health data from a S-EHR App on a S-EHR Cloud.
R2D Emergency	Secure IT communication protocol (and remote API) for the exchange of health data between an HCP App and a S-EHR Cloud during emergency care.
Smart EHR mobile App	Model of secure mobile applications for the storage, control, anonymization and exchange of health data on smart devices (e.g. smartphones or tablets), without the obligation to store data in the cloud. A S-EHR is able to import/share data from/with EHR/EMRs and with research centres, using short-range wireless D2D (device to device) communication or remote communication protocols. The S-EHR allows to store on a smart device the health data about a single citizen and produced by the citizen itself or by HCPs.
S-EHR Cloud	Any cloud storage service fulfilling the S-EHR conformance levels. In particular: supporting the R2D Backup & R2D Emergency protocols (to backup health data not decryptable by the cloud provider and to allow trusted organisations to access health data in emergency), under Citizen's control (deciding if to adopt it, from which provider, for which functions), compliant with specific security constraints. A citizen may choose to use a S-EHR Mobile App without using any S-EHR Cloud. In this case, the health data will be accessible to HCPs by using the short-range D2D protocol.
S-EHR conformance levels	Constraints that a mobile app or a cloud storage service for health data has to fulfil to be considered a S-EHR or a S-EHR Cloud
Terminal Device to Device Interface	The interface offered by any application used by HCPs to support the D2D protocol, i.e. to exchange health data with citizen's S-EHRs at a short distance, without using the Internet.

REFERENCES

- **[D2.2]** InteropEHRate Consortium, D2.2*: User Requirements for cross-border HR integration - V1*, 2020. www.interopehrate.eu/resources/#dels
- **[D2.8]** InteropEHRate Consortium, D2.8*: FHIR profile for EHR interoperability - V1*, , 2020. www.interopehrate.eu/resources/#dels
- **[D3.1]** InteropEHRate Consortium, *D3.1: Specification of S-EHR mobile privacy and security conformance levels - V1*, 2020. www.interopehrate.eu/resources/#dels
- **[D3.10]** InteropEHRate Consortium, D3.10*: Design of libraries for HR security and privacy services - V2*, 2021. www.interopehrate.eu/resources/#dels
- **[D4.2]** InteropEHRate Consortium, *D4.2: Specification of remote and D2D protocol and APIs for HR exchange - V1,* 2020. www.interopehrate.eu/resources/#dels
- **[D4.5]** InteropEHRate Consortium, D4.5*: Design of libraries for remote and D2D HR exchange - V2*, 2021. www.interopehrate.eu/resources/#dels
- **[D4.8]** InteropEHRate Consortium, *D4.8: Specification of protocol and APIs for research health data sharing - V1*, 2021. www.interopehrate.eu/resources/#dels
- **[D6.7]** InteropEHRate Consortium, *D6.7: Design of a service for cloud storage of S-EHR content (S-EHR Cloud) - V1,* 2021. www.interopehrate.eu/resources/#dels
- **[D3.3]** InteropEHRate Consortium, *D3.3-Specification of remote and D2D IDM mechanisms for HRs Interoperability - V1,* 2019. www.interopehrate.eu/resources/#dels
- **[D4.7]** InteropEHRate Consortium, *D4.7-Design of Health Record Index, 2021.* www.interopehrate.eu/resources/#dels
- **[D5.4]** InteropEHRate Consortium, *D5.4- Design of an integrated EHR web app for HCP - V1*, 2019. www.interopehrate.eu/resources/#dels
- **[D4.10]** InteropEHRate Consortium, *D4.10-Design of library for health data sharing for research - V1*, 2021. www.interopehrate.eu/resources/#dels
- **[HL7 FHIR]** HL7 Fast Healthcare Interoperability Resources Specification. http://hl7.org/fhir/
- **[EU CB ANNEX]** ANNEX to the Commission Recommendation of 6.2.2019 on a European Electronic Health Record exchange format
- **[WBA]** Web Bluetooth Draft Community Group Report, 1 July 2020. https://webBluetoothcg.github.io/web-Bluetooth/
- **[ISO/TR 20514]** ISO, TR. "20514: 2005 Health Informatics-Electronic Health Record Definition, Scope and Context Standard." International organization for Standardization (ISO), Geneva, Switzerland (2005).
- **[1609.2-2016]** *IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages," in IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013) , vol., no., pp.1-240, 1 March 2016, doi: 10.1109/IEEESTD.2016.7426684.* https://standards.ieee.org/standard/1609_2-2016.html
- **[ENISA 2020]** *ENISA. "Minimum Security Measures for Operators of Essentials Services". (2020).*
- **[NIST 2020]** *Draft NIST Special Publication 800-57 Part 1 Revision 5, Recommendation for Key Management: Part 1 – General, May 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf*

- **[NIST ENTR]** *National Institute of Standards and Technology. NIST SP 800-22, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf.*

- **[GS]** *J. Camenisch and J. Groth."Group signatures: Better efficiency and new theoretical aspects", in: Security in Communication Networks. Springer, 2005, pp. 120-133.*

- **[BS]** *Stadler M, Piveteau J-M, Camenisch JL (1995) Fair blind signatures. In: Guillou LC, Quisquater J-J (eds) Advances in cryptology: EUROCRYPT'95. Lecture notes in computer science, vol 921. Springer, Berlin, pp 209–219*

- **[ZI14]** *M. Miettinen, N. Asokan, T. D. Nguyen, A.-R. Sadeghi, and M. Sobhani, "Context-based zero-interaction pairing and key evolution for advanced personal devices", in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS '14. New York, NY, USA: ACM, 2014, pp. 880–891. [Online]. Available: http://doi.acm.org/10.1145/2660267.2660334*

- **[ZIA]** *H. T. T. Truong, X. Gao, B. Shrestha, N. Saxena, N. Asokan, and P. Nurmi, "Comparing and fusing different sensor modalities for relay attack resistance in Zero Interaction authentication", in 2014 IEEE International Conference on Pervasive Computing and Communications (PerCom), March 2014, pp. 163–171.*