D2.6

InteropEHRate Architecture - V3

ABSTRACT

This report describes a novel architecture for citizen centred EHR interoperability and provides an overview of its reference implementation. This is the third and final version of the specification.
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	11th, August 2021
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, Martin Marot	A7
	Debora Desideri, Alessio Graziani, Francesco Torelli	ENG
	Thanos Kiourtis, Argyro Mavrogiorgou	UPRC
	Sofianna Menesidou, Thanassis Giannetsos	UBIT
	Gabor Bella, Simone Bocca	UNITN
	Chrysostomos Symvoulidis	BYTE
	Nicu Jalba, Mihai-Dragos Seceleanu	SIMAVI
Reviewers	Paolo Marcheschi	FTGM
Reviewers	Gabor Bella	UNITN

LOGTABLE

Version	Date	Change	Author	Partner
0.1	28-03-21	Creation of new TOC and proposal on sections to update	Francesco Torelli	ENG
0.2	27-05-21	Addition of new sections, update of introduction sections and update of contribution plan	Francesco Torelli	ENG
0.3	04-06-21	Update of section “Example HCP App”	Mihai-Dragos Seceleanu	SIMAVI

0.4	07-06-21	Updated references of all sections and content of section “S-EHR Mobile App”, “R2D Access protocol”, “RDS protocols”	Francesco Torelli	ENG
0.5	01-07-21	Update of sections “S-EHR Mobile App” and “S-EHR Mobile App RI”	Martin Marot	A7
0.6	14-06-21	Updated sections “S-EHR Cloud”, “S-EHR Cloud RI”, “R2D Access protocol”, “R2D Emergency protocol”, “Reusable libraries”, “Conclusions”	Chrysostomos Symvoulidis, Francesco Torelli	BYTE, ENG
0.7	17-06-21	Updated section “Security protocols”, “Reusable libraries”, “Conclusions”	Sofianna Menesidou	UBIT
0.8	18-06-21	Updated sections “D2D protocol”, “HR Index”, “Reusable libraries”, “Conclusions”	Thanos Kiourtis	UPRC
0.9	18-06-21	Updated section “Example HCP App”	Nicu Jalba	SIMAVI
0.10	24-06-21	Reviewed contributions, alignment of glossary and nomenclature in the full deliverable.	Francesco Torelli	ENG
0.11	01-07-21	Updated previous contributions	All	All
0.12	07-07-21	Corrections and adding of section “Scenario S0”	Alessio Graziani, Francesco Torelli	ENG
0.13	12-07-21	Update of sections “Scenario S1” and “Scenario S2”	Francesco Torelli	ENG

0.14	21-07-21	Update of sections “Scenario S3” and “Scenario S4”.	Francesco Torelli	ENG
0.15	23-07-21	Added section “R2D Access Server” and update of “Conclusions and Next steps”	Alessio Graziani, Francesco Torelli	ENG
0.16	24-07-21	Update of all figures and section “Updates with respect to the previous version”.	Francesco Torelli	ENG
0.17	28-07-21	Review of results of first internal review	Francesco Torelli	ENG
0.18	01-08-21	Update of sections “InteropEHRate Health Services”, “InteropEHRate Research Services”, “InteropEHRate Health Tools” and addition of section “InteropEHRate Research Services (IRS)”	Gabor Bella, Simone Bocca	UNITN
0.19	02-08-21	Review of results of second internal review and update of captions, lists and table of content, references.	Francesco Torelli	ENG
Vfinal	11-08-21	Quality check and version for submission	Laura Pucci	ENG

ACRONYMS

Acronym	Description
API	Application Programming Interface.
BLE	Bluetooth Low Energy technology
CN	(Research Network) Central Node
CTMS	Clinical Trial Management System
DICOM	Digital Imaging and Communications in Medicine Standard
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
MD2D	Mobile Device to Device
PHR	Personal Health Record (System)
R2D	Remote to Device
RD	Research Data
RDS	Research Data Sharing (protocol)
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
D2D	Device to Device

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 and integrate them in their applications.

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 **[D2.3]**). 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 "D2.5 — InteropEHRate Architecture V2". Main novelties with respect to the previous version are the extension of capabilities and interfaces offered by the protocols R2D Access, D2D and RDS and a restructuring of the protocols R2D Backup and R2D Emergency. Following is the list of the main updated/new sections:

- "2.4 Standard applications and interfaces": the standard architecture and its description has been updated with the inclusion of new remote interfaces (R2RAccess, R2RAccessDICOM, D2DClientSecurity, R2DAccessIdentificatiom, R2DAccessDICOM), the update of names of previous interfaces and the deletion of interfaces (CAI and eIDAS) that are not more considered part of the

InteropEHRate protocols (the protocols depend on only from the output of these APIs). The tables and descriptions have been updated accordingly.

- "2.4.1 S-EHR Mobile App": the description has been extended and updated to add the usage of new interfaces R2DAccessIdentification and R2DAccessDICOM
- "2.4.2 S-EHR Cloud": interfaces offered by the S-EHR Cloud have been renamed (now called R2DEmergency and R2DBackup) and restructured to better separate what is used by the protocols R2D Emergency and what is used by the protocol R2D Backup. The descriptions have been updated accordingly.
- "2.4.3 Healthcare organisation Information System": added description of new offered and used interfaces.
- "2.5.2 Security Protocols": details related to the security aspects of new interfaces have been added.
- "2.5.3 R2D Access protocol: the description has been extended to describe the new support for DICOM studies and additional identification attributes of Citizens.
- "2.5.4 R2D Backup protocol" : the description has been updated to reflect the new interfaces.
- "2.5.5 R2D Emergency protocol": the description has been updated to reflect the new interfaces.
- "2.5.6 D2D protocol" : the description has been updated to reflect the new version of the D2D protocol, where the S-EHR app and the HCP are no more peers, but the S-EHR app has a server role and the HCP app has a client role.
- [new] "3.1 Scenario S0: Initial S-EHR feed": this section is completely new and presents the activity diagram (AD) for new scenario S0 introduced by deliverable **[D2.3]**. It explains how the different APIs of the protocol R2D Access are involved in the realisation of the scenario. The new AD shows how health data is download from foreign healthcare organisations and several novelties of R2D Access: how asynchronous interactions are supported, how to collect identification data of citizens not provided by eIDAS, how to support the download of DICOM studies by means of WADO-RS standard.
- "3.2 Scenario S1: Medical Visit abroad": the activity diagram has been updated to reflect the new version of scenario 1 presented in deliverable **[D2.3]** and new remote interfaces. The new diagram does not include anymore the usage of R2D Access (now part of scenario 0) and adds two novelties: support for DICOM studies and establishing of D2D connections with HCP terminal without repeating the reading of QRCode.
- "3.2 Scenario S2: Emergency access": the activity diagram has been updated to reflect the new version of scenario 2 presented in deliverable **[D2.3]** and new remote interfaces. In particular, it shows how DICOM studies may be downloaded in an emergency using the interface R2DAccessDICOM.
- "3.4 Scenario S3: Health research study": the activity diagram has been updated to reflect the new version of scenario S3 presented in deliverable **[D2.3]**. In particular, it now shows the usage of either pseudonym or pseudo-identity, new support for questionnaires and the possibility to download anonymised health data directly from the producer organisation instead of from the S-EHR App (using the remote interfaces R2DAccess and R2RAccessDICOM).
- "4.3 component view": also the architecture of the InteropEHRate Framework has been aligned to the new remote interfaces.
- "4.5 reusable libraries": new libraries for R2D Cloud has been described

- "4.7 S-EHR Cloud RI": the new architecture of the reference implementation of the S-EHR Cloud has been described
- [new] "4.9 R2D Access Server": this section is new and describes the reference implementation of R2D Access service. In the previous version the reference implementation of the R2D service had no specific description and was considered just a subcomponent of IHS.
- "4.10 InteropEHRate Health Services (IHS)" has been updated to align the content to simplify the content and to reflect the decision to separate the R2D Access Service from the IHS, to ease the reuse of only one of the two.
- [new] "4.11 Research Network Central Node RI": this section is new and describes the reference implementation of the Research Network Central Node.
- "5 Conclusions and next steps" has been updated to reflect the novelties of the deliverable.

Section 4.14 has been removed, as the interactions among components of the InteropEHRate Framework are described in the specific deliverables of each component. Other sections provide the same information of the previous version, but some minor changes to the text have been applied to remove errors and improve clarity.

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**[D2.9]**): common data model, based on the FHIR standard, shared by all the InteropEHRate protocols.
- **S-EHR conformance levels** (described in the report **[D3.2]**): guidelines and constraints 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** (described in the report **[D4.3]**): secure communication protocol (and remote APIs) for exchanging health data between two nearby devices (not using the Internet), one running a S-EHR App and the other running an HCP App.
- **R2D protocols** (described in the report **[D4.3]**):
    - **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** (described in the report **[D4.9]**): 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 named, more informally, "InteropEHRate platform"[1]), composed of different software components, each one implementing a different part of the specification and reusable one independently of the others. The InteropEHRate framework also contains 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 **[D2.3]**. While the report [D2.3] 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 on the usage scenario.

The purpose of this section is to describe the InteropEHRate standard architecture for EHR interoperability. 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 securely 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 **[D2.3]** (copied here to simplify the reading of the document).

Actors	Description
Citizen	A person of a specific country and speaking a specific language whose health data is 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, we provide 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 **[D2.3]**.

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 or individual 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 actor 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 long-term identity of their owners.	
Member state	A state of the EU community.	

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

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 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 tasks such as data integration, conversion, or translation.	
Pseudonym Provider	A trusted organisation that is responsible for the management of the short-term anonymous credentials (called certified pseudo-identities or pseudonyms), according to the IEEE standard specification **[1609.2-2016]**. Certified pseudonyms are used by the RDS protocol 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

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.

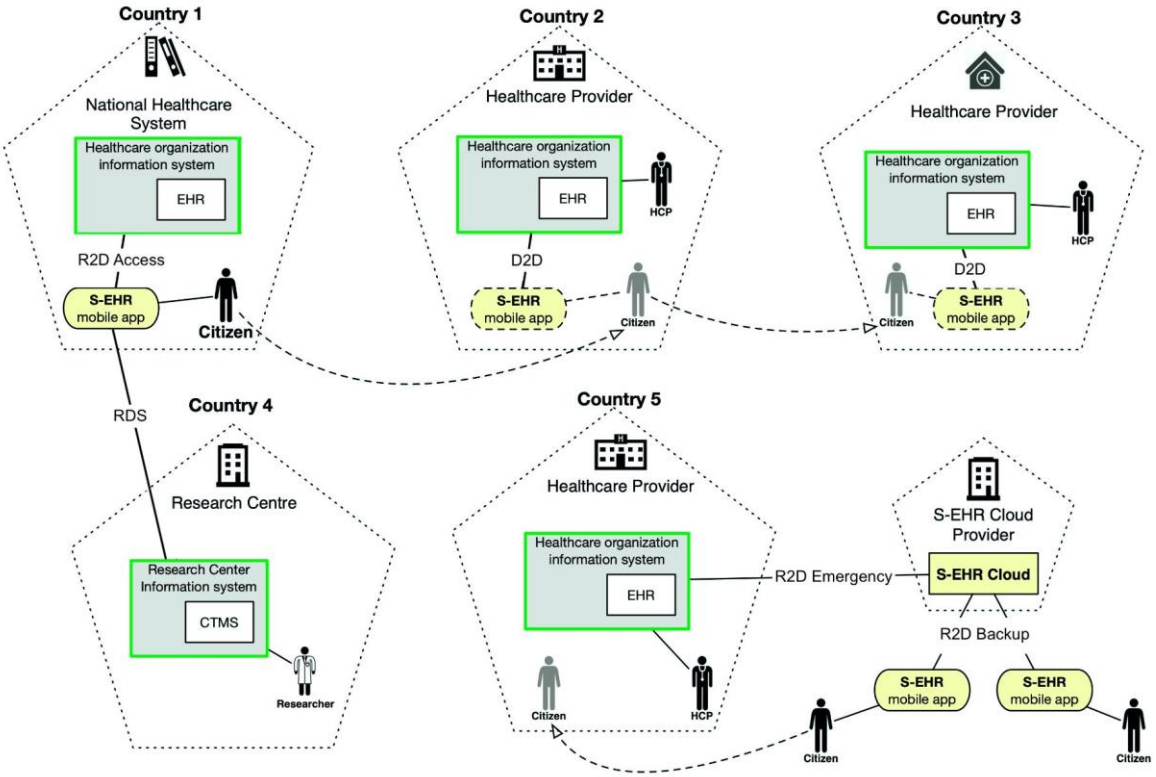

Figure 1- Examples of health data exchange using a S-EHR Mobile App and a S-EHR Cloud

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 S-EHRs, conformant with InteropEHRate, 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 the citizen that is the data subject.

A S-EHR can 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) protocols 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 the 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 the 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 protocols are 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 Access 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 information system, while in the case of the D2D protocol the health data is 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 professional (HCP). The application (part of the health organisation information system) used by the HCP is 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 must satisfy a set of rules and requirements aimed to guarantee strong levels of security and trustability (specified in report **[D3.2]**) 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 across 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 process 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 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 could 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). This cloud service can be offered by a vendor distinct from the one that offers the S-EHR App. Moreover, the data is 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 Backup protocol, while the communication between the Healthcare organisation information system and the S-EHR Cloud is specified by the R2D Emergency protocol.

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) securely to a specific remote Research Centre, 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 only with the specific studies they want to be enrolled in. 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 for 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)[3] and regulations like EIDAS and related EU infrastructure (CEF eID[4]).

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 up, i.e. without the need of a central service above them. In this

[3] http://hl7.org/fhir/uv/ips/
[4] 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 share 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 aims to promote the development 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, to support 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:

- blue, for standard legacy interfaces and systems,
- grey, for other legacy 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. Moreover, a S-EHR App is not required to support all the InteropEHRate protocols. For example, it could support only the D2D protocol. These distinctions are clarified below.

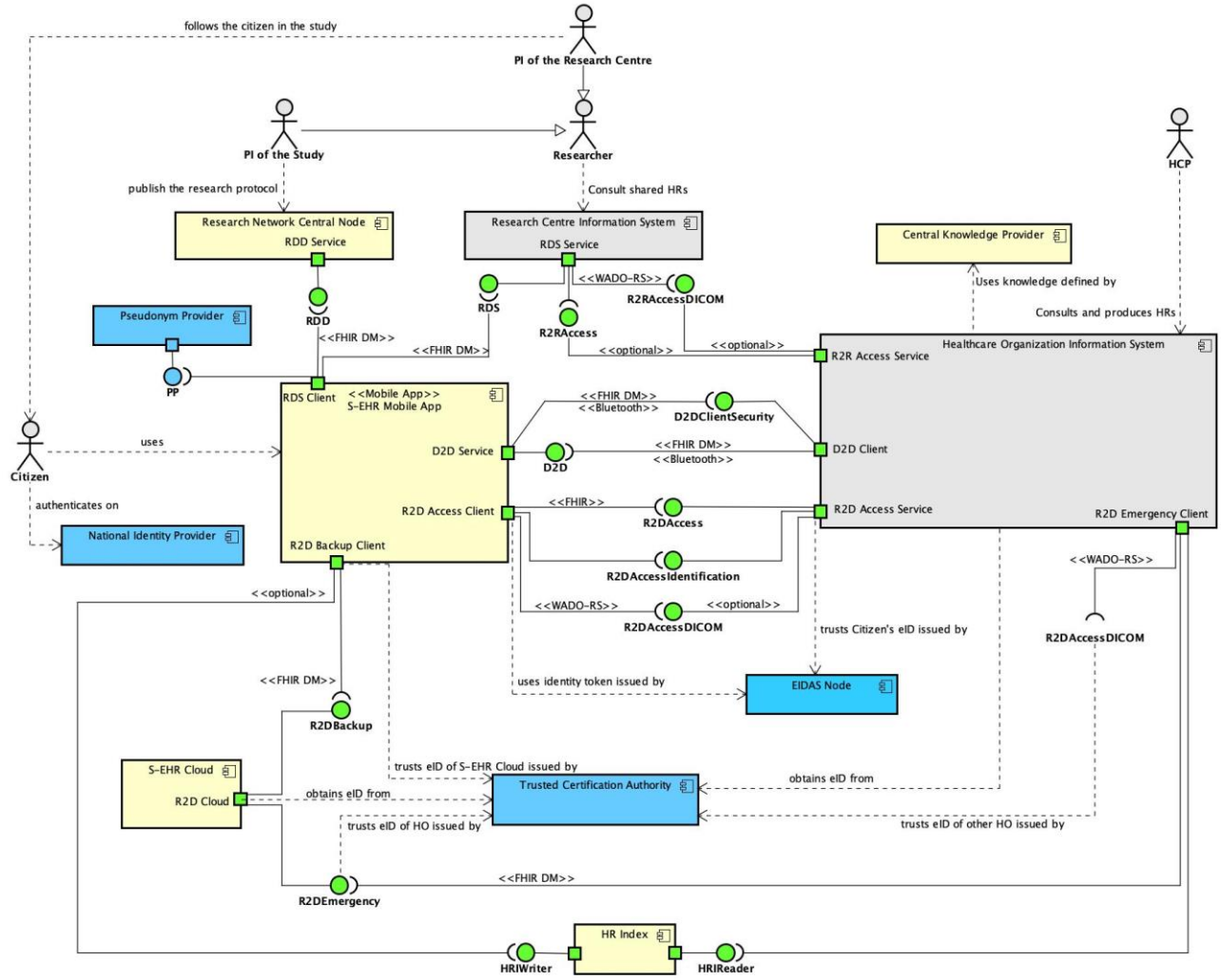

Figure 2 - InteropEHRate standard architecture

The InteropEHRate protocols constrain the interactions among three main 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. The S-EHR App may support one or more of the five protocols called: D2D, R2D Access, R2D Backup, R2D Emergency, RDS.

2. Healthcare Organisation Information System, one for each Healthcare organisation: the IT system of a Healthcare organisation, including all software applications used by the Healthcare Professionals (HCPs), extended to support the InteropEHRate protocols for health data exchange with S-EHR. This system may support one or more of four protocols: D2D, R2D Access, R2D Emergency, R2R Access (optional extension of the RDS protocol).

3. Research Centre Information System, one for each Research centre: an IT system composed of all software used by any Researcher (i.e. scientist), to produce and access Citizens' health data. This system is involved only in the RDS protocol.

The InteropEHRate protocols also involve, in a direct or indirect way, the following standard systems:

4. 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 nodes are available. The eIDAS Network consists of a series of eIDAS-Nodes implemented at the Member State level. The eIDAS nodes are involved in the protocol R2D Access.

5. National Identity Providers, one per country, used by the citizen to authenticate their identity. They are connected to the eIDAS-Node of their country and are involved in the protocol R2D Access.

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. The certificates are involved in the protocols R2D Backup, R2D Emergency, RDS and in the optional variant of the protocol D2D.

7. Pseudonym Provider (System): The system offering the electronic service for the management of short-term anonymous credentials, called pseudonyms, according to IEEE standard **[1609.2-2016]**. This system is involved in the optional variant of the protocol RDS.

Moreover, specific protocols involve the following complementary systems defined by InteropEHRate:

8. Research Network Central Node, a single IT service provided by the Central Node Provider: gives a central access point to S-EHR Apps for retrieving the descriptions of research studies. Used only by the RDS protocol.

9. S-EHR Cloud, an optional kind of system offered by specific vendors, to support the remote storage/backup of personal health data. Offers the protocols called R2D Backup and R2D Emergency. It is not required by the other InteropEHRate protocols.

10. HR Index (Health Record Index), a mediator for informing healthcare practitioners about the location of the S-EHR Cloud of the citizens, to address emergency cases also in case that the Emergency QR-code has not been updated. This is an optional IT system that extends the capabilities of the protocol R2D Emergency.

The new (open standard) interfaces introduced by InteropEHRate for the interactions among the different systems are listed in the following tables. Such remote interfaces are part of the interoperability protocols specified in the reports **[D4.3]** and **[D4.9]**. The data model adopted by the protocols and interfaces is defined as a set of constraints and extensions on top of the standard **[HL7 FHIR]** and will be specified in [**[D2.9]**.

Protocol	Defined Remote API	Description
D2D	D2D	*Device to Device*: Bluetooth 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.
	D2DClient Security	*Device to Device Client Security*: a security related Bluetooth interface, offered to the S-EHR by any application used by HCPs to exchange health data with citizen's S-EHRs at a short distance, without using the Internet.
R2D Access	R2DAccess	*Remote to Device* Access: remote interface compliant with the HL7 FHIR API 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.
	R2DAccess Identification	*Remote to Device* Access *Identification*: remote interface offered by the Healthcare organisation to support the R2D Access protocol. It allows the S-EHR App to trigger the eIDAS authentication of the Citizen identity required by R2DAccess.
	R2DAccessDICOM	*Remote to Device Access to DICOM*: remote interface compliant to **[WADO-RS]**[5] specification that requires the eIDAS token of the Citizen for the client authentication. It allows the S-EHR App to access at distance (by means of the Internet) any DICOM study of the subject citizen referred by FHIR resources imported by means of R2DAccess or D2D. The interface R2DAccessDICOM is optional, i.e. a HCO System may offer the R2DAccess without offering R2DAccessDICOM.
R2D Backup	R2DBackup	Remote to Device for Backup: remote interface offered by a S-EHR Cloud to any S-EHR App to store encrypted health data 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. A citizen may choose to not use a S-EHR Cloud.
R2D Emergency	R2DEmergency	Remote to Device for Emergency: remote interface offered by a S-EHR Cloud to any Healthcare Organisation System 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. A citizen may choose to not use a S-EHR Cloud or to not enable the emergency protocol.

[5] "Retrieve (WADO-RS) - DICOM Standard." https://www.dicomstandard.org/dicomweb/retrieve-wado-rs-and-wado-uri.

	HRIReader	HR Index Reader: remote 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: remote 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	RDD	Research Definition Document: remote 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.
	RDS	Research Data Sharing: remote 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.
	R2RAccess	Remote to Research: remote interface analogous to a subset of R2DAccess, but offered by an HCO System to the Research Centre Information Systems to download anonymised FHIR resources (e.g. anonymised PDFs). Differently from R2DAccess, this interface allows only to download resources by ID and the authentication requires that a citizen consent is transmitted to the HCO System to authorise the specific Research Centre to access the specific FHIR resource. This interface is part of an optional extension of the RDS protocol, called R2R Access.
	R2RAccessDICOM	Remote to Research Access for DICOM: remote interface similar to R2DAccessDICOM, but offered by an HCO System to the Research Centre Information Systems to download anonymised DICOM Studies. It is still a WADO-RS API, but the authentication requires that a citizen consent is transmitted to the HCO System to authorise the specific Research Centre to access a specific DICOM Study. This interface is optional: an HCO System may offer remote access to DICOM Studies (anonymised or not) just to the citizens (using R2DAccessDICOM), without providing an analogous service for researchers. This interface is part of an optional extension of the RDS protocol, called R2R Access.

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

Other than the remote APIs defined by InteropEHRate, the RDS protocol also exploits the remote API offered by the Pseudonym Provider for creating Pseudonyms as defined by IEEE standard **[1609.2-2016]**
All the remote interfaces that are accessed by means of the Internet, with the exception of the ones with usage relations depicted on the UML component diagrams, show the <<Bluetooth>> stereotype. The stereotypes on the usage relationship also show which APIs are compliant to the HL7 FHIR API and which ones use a different API but are still based on the FHIR Data Model (DM).

The following sections provide a description of the main functionalities provided by and required from each system.

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 "Specification of S-EHR mobile privacy and security conformance levels" **[D3.2]** and that supports the InteropEHRate protocols **[D4.3] [D4.9]**. 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" **[D2.9]**.

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 of 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 is stored on the mobile application and which actor may access them by using the InteropEHRate protocols 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's 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 identify a citizen using the European identification system eIDAS (before accessing their medical data for security reason)

- 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 remote interfaces R2DAccess, R2DAccessIdentification and R2DAccessDICOM 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 their health data. In particular, the RDD contains the Health Research Protocol (HRP)[6], i.e. the description approved by an Ethical Committee of the purposes and methodology to collect and process the specific set of health and/or social data needed by the research study, to learn more about human health and treatments. The RDD is downloaded by invoking the eponymous remote interface offered by the Research Network Central Node.

- 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 invokes the interface RDS offered by the Research Centre Information System. It also exploits the remote interface PP exposed by the Pseudonym Provider, in case that the specific research study requires identifying the citizen by means of a pseudonym that is not generated by the research centre but from a third party (the Pseudonym Provider).

- To import/store data on an S-EHR Cloud service. This is useful to securely back up or move their data to another device. This operation is performed by using the interface R2DBackup offered by the S-EHR Cloud selected by the user and exploited by the R2D Backup protocol.

- To authorise or deauthorize any trusted Healthcare organisation to access during an emergency, using the R2D Emergency protocol, to a specific set of health data stored on the S-EHR Cloud. This operation also uses the interface R2DBackup offered by a S-EHR Cloud to communicate the consent to a S-EHR Cloud. To this end, the S-EHR app trusts identity certificates of the Healthcare Organisation issued by a Trusted Certification Authority. In the optional case that an HR Index is available, this also involves the registration of the citizen on the HRIndex, by means of the interface HRIWriter.

[6] 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.

- To access (by means of R2DBackup) audit data provided by the S-EHR Cloud to check who accessed the stored data.
- To retrieve (by means of R2DBackup) new health data created in an emergency and stored on the S-EHR Cloud by a healthcare organisation.
- 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 **[D4.3]** and that fulfils the "S-EHR conformance levels" **[D3.2]**.

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 is 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 that are 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 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 an emergency;
- permanently maintain a non repudiable history of all accesses to the encrypted data, including all data needed to identify the person that requested access to the data;
- allow the citizen to download at any moment the access history to the encrypted data of that citizen.

The S-EHR Cloud is identified by means of electronic certificates issued by a Trusted Certification authority and interacts only with Healthcare organisations that also have electronic certificates that authenticate their identity.

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

A S-EHR Cloud provides the functionalities that are implemented by the R2D Backup and R2D Emergency protocols through the homonymous remote interfaces R2DBackup and R2DEmergency. More specifically, those functionalities include the following:

1. Allows the user of any authorized S-EHR app to upload and store encrypted health data.
2. Allows the user of any authorized S-EHR app to download encrypted health data previously stored by the same user or an authorized HCP.
3. Provides access to authorized HCPs of trusted (by the S-EHR Cloud) healthcare organizations to the encrypted data of a citizen in “emergency mode”.
4. Allows the above-mentioned authorized HCPs to upload to the S-EHR Cloud health data related to the emergency as well as the Discharge Report once the emergency is over.

2.4.3 Healthcare organisation Information System

A *Healthcare organisation Information System* is the software system of any healthcare organisation that manages citizens’ health records and exchanges them with authorised citizens using the protocol R2D Access or the protocol D2D. A Healthcare organisation may also offer to researchers, with the consent of citizens, an anonymised version of DICOM research studies by means of the protocol R2R Access.

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, 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 remote interfaces R2DAccess, R2DAccessIdentification and the optional interface R2DAccessDICOM, invoked by the S-EHR app of the citizen.
2. Can retrieve health data shared by a citizen during a face-to-face encounter. To this end, the Healthcare Organisation Information System uses the Bluetooth interface D2D offered by the S-EHR app of the citizen and offers the Bluetooth interface D2DClientSecurity needed to the S-EHR app to establish a secure connection and identify the Healthcare organisation.
3. Allows the citizens to receive 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 also uses the Bluetooth interface D2D (of the D2D protocol) offered by the S-EHR app of the citizen and offers (usually by means of an HCP App) the Bluetooth interface D2DClientSecurity.

4. Can access, in emergency cases, the health data of a citizen stored on a S-EHR Cloud. To this end, the Healthcare organisation Information System uses the remote interface R2DEmergency offered by the S-EHR Cloud of the citizen (in the case that the citizen enabled it). During the emergency, they may also use the interface R2DAccessDICOM, offered by other Healthcare Organisations, to access any DICOM Study that is referred to by health data stored on the S-EHR Cloud but not stored in the S-EHR Cloud.

5. Allows researchers that have an explicit consent of the subject patient, to access an anonymised version of specific DICOM Studies, to be used in specific research studies. To this end, they implement the remote interface R2DAccessDICOM.

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 interacts with the eIDAS Node of their country, for obtaining the cross-border identification of the citizens. The Healthcare organisation Information System sends authentication requests to the eIDAS-Node and receives the authentication responses through an interface that is country specific. 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 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 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 an optional mediator for informing the HCP App about the cloud location of the stored EHR data of the citizens (without directly providing the information to the Healthcare practitioners), in order to address emergency cases where the citizens are not able to provide access to their S-EHR (supposing that they have previously given consent for granting access to the stored data in emergency).

In order for the HR index to be correctly used by the HCP App, 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 has sent to the HR index the address of the S-EHR Cloud where the data is stored;
- the HR Index creates the anonymous unique ID and stores it with the S-EHR cloud address.

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 directly store 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 an 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 Information System

The *Research Centre Information System* is the software system of any research centre that can 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 tied, for that study, to the Research Centre Information System of his or her local *Reference Research Centre,* that takes charge of all communication with the citizen in the specific research study. To this end, the Research Centre implements the remote interface *RDS* to provide the citizen's S-EHR App 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 and offers to the Coordinating Research Centre the publishing operation to share the RDD (Research Definition Document) describing a new research study with all Citizens participating in the InteropEHRate Research Network. The RDDs maintained in the CN are both automatically and manually

checked before the publication, to allow the publication of documents which are compliant to the InteropEHRate document profile defined for the RDD.

The interface RDD 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, automatically checking 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, 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**[D2.9]**) 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, these standards are widely accepted throughout the EU and are more likely to be understood abroad and to be mappable 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 of the country where the data has 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 also have 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 such cases, 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.

InteropEHRate FHIR profiles also support the possibility to include additional semantic information (automatically) extracted from 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 the 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 [**[D2.3]**. 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 **[D3.2]**). Before digging into details of the protocols, there is a need to flesh out the exact security properties.

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 **[D3.2]**. In the same line of operation, integrity aspects are achieved using strong and efficient digital signatures upon the exchanged messages, leveraging the certificates that have been provided by the CA. The security properties for the D2D protocol are: a) confidentiality, b) integrity, c) authentication, d) freshness, e) immutability, and f) protocol correctness.

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 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. The security properties for the R2D protocols are: a) confidentiality, b) integrity, c) authentication, d) authorization and access control, e) freshness, f) immutability, and g) protocol correctness.

R2D Security Interaction Mechanisms. Identity Management and Authentication services in the scope of the R2D Access protocol use an eIDAS-based solution 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. Moreover, in R2D Backup, a username/password identification and authentication, while in R2D Emergency the utilisation of an Attribute Based Access Control (ABAC) engine can express a complex boolean rule set that can evaluate many different attributes for access control purposes of authorised HCPs to the cloud. 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 pseudonymization 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, using appropriate lightweight cryptographic

primitives. The security properties for the R2D protocols are: a) confidentiality, b) integrity, c) authentication, d) freshness, e) immutability, f) protocol correctness, g) privacy, and h) unlinkability.

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. The existence of the PP is optional for the RDS protocol, and necessary only for the 2nd variant. 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. In addition, the utilisation of an ABAC is used for access control purposes of authorised RRCs to Healthcare organisations to download DICOM images. The exchanged information is symmetrically encrypted following the current AES-256 crypto standard. Finally, the adoption of an optional private blockchain is used for secure on and off data management. More specifically, all the transactions are performed in a secure, auditable, and verifiable manner using blockchains (DLTs). Each research center has a private ledger that keeps all the data transactions. More details about the blockchain, the smart contract, and the ABAC are provided in D3.8.

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 primary actors of R2D Access are the citizens. Each citizen downloads his or her data from the Healthcare Organisation to his or her smartphone and may then exchange them with other parties using the other InteropEHRate protocols.

The operations of the R2D Access protocol are provided by the interfaces R2DAccess, R2DAccessIdentification and the optional interface R2DAccessDICOM offered by the Healthcare Organisation Information System to the S-EHR Mobile App. Other than on these remote interfaces, this

protocol relies on the authentication service offered by the eIDAS nodes to the Healthcare Organisation Information System and the identification service offered by the national identity provider of the Citizen.

Like the other InteropEHRate protocols, R2D Access is based on an open specification, therefore it can be adopted by any producer of health data and by any mobile application. 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. More specifically the interface R2DAccess offers the capability to download the health data in FHIR format, the interface R2DIdentification allows to log the citizen by means of eIDAS and the optional interface R2DAccessDICOM allows to download any DICOM study (e.g., images, signals) that are referred by the health data, but is not embedded in those data.

The interface R2DAccess is defined on top of HL7 FHIR, by profiling its standard API, so it is easy to be adopted by organisations that already use FHIR and very well documented for the ones that have never used it. The interface R2DAccessDICOM is a WADO-RS API (the REST version of the standard DICOM API), already supported by several PACS systems based on the DICOM standard, constrained to rely on the eIDAS authentication of the citizen. The S-EHR App has to provide to the interface the Citizen's electronic consent to download the health data on the S-EHR App.

More details of the R2D Access protocol are provided in the next chapter and in the report **[D4.3]** , where information regarding the used technologies, the sequence of exchanged messages and the involved actors 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.

The R2D Backup protocol defines the R2DBackup interface, which is used to implement the above-mentioned functionalities. In more detail, with the use of the R2Backup interface, a citizen may download his or her health data from the S-EHR Cloud he or she is using and decrypt locally on his or her S-EHR Mobile App. In addition, with the use of the same interface a citizen may upload, after having encrypted them, health data on the S-EHR Cloud provider he/she uses.

As far as the security interfaces the R2D Backup protocol exploits, the remote interfaces that are provided by the Security Protocol described in the previous section. With the exploitation of the Security Protocol, it is ensured that the communication between the server (i.e. the S-EHR Cloud) and the S-EHR mobile

application is secure, and all data that is exchanged is encrypted on the client-side (the citizen's side), so that the S-EHR Cloud does not have the ability to gain access to the actual content of the health data.
More details regarding the R2D Backup protocol, including its design and specifications, is available in the report D4.3 where detailed information with respect to the used technologies, the sequence of communication steps, involved actors, and involved components is provided.

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 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.

Like the R2D Backup protocol, the R2D Emergency utilises the R2DEmergency interface, which is used to implement the above-mentioned functionalities on the HCP's side. In more detail, with the use of the R2DEmergency interface an authorized HCP may request access to the health data of a citizen in emergency situations, download this health data from the S-EHR Cloud the citizen is using and decrypt it locally on the HCP app. In addition, an authorized HCP can upload to the S-EHR Cloud of that specific citizen in need, new health data regarding that emergency, and reports at patient discharge, once the emergency is over.

The R2D Emergency protocol exploits the interface R2DAcccessDICOM (which is part also of the R2D Access protocol). A healthcare organisation may invoke this interface to access the DICOM studies that are referred to by the health data accessed in an emergency. When the healthcare organisation invokes this interface, it has to provide the Citizen's electronic consent provided by the citizen at S-EHR Cloud activation that authorise all healthcare organisations that are in the S-EHR Cloud trust list to download the DICOM files in emergency situations.

The R2D Emergency protocol exploits the remote interfaces that are provided by the Security Protocol described in the previous section. With the exploitation of the Security Protocol, it is ensured that the communication between the server (i.e., the S-EHR Cloud) and the HCP Application is secure, and all data that is exchanged is encrypted on the client-side (the side of the HCP application), so that the S-EHR Cloud does not have the ability to gain access to the content of the health data.

More details regarding the R2D Emergency protocol, including its design, exposed interface, and specifications is available in the report **[D4.3]** where detailed information with respect to the used technologies, the sequence of communication steps, involved actors, and involved components is provided.

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) as defined and analysed in D4.3.

The D2D protocol defines Bluetooth services (represented by the interface D2D) to be offered by the S-EHR Mobile App for receiving from and providing Citizen's health data to the Healthcare organisation Information System. The D2D protocol also exploits the D2D Security protocol (involving the interface D2DClientSecurity offered by the Healthcare Organisation and D2DServerSecurity extended by D2D) to perform a trusted Bluetooth Connection, Identity Management, Consent Management, and Authorization Management. The interactions between the interfaces D2D and the D2DClientSecurity are classified into four fundamental categories: (i) Establishment of Bluetooth Connection, (ii) Security Handshake, (iii) Exchange of Requests for Healthcare Data, and (iv) Bluetooth Connection Closure.

(i) Establishment of 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. In more detail, the first step that needs to be followed is the HCP app to gather the connection details from the S-EHR app, based on the Bluetooth SPP profile, for the Bluetooth connection to take place, the HCP app has to provide the MAC address of the Bluetooth adapter to the S-EHR app. This happens after the scanning of a QR code from the S-EHR app, where this QR code contains the MAC address of the HCP app along with a signature that will be exchanged for assuring the integrity and non-corruptness of the MAC address. It should be noted that the scanning of the QR code can be bypassed, in the case that the S-EHR app owner is visiting a different HCP app owner in the same Health Organization. Then the first HCP app owner provides the necessary MAC address (of the other HCP app owner) to the citizen. The HCP App sends the digital signature of the MAC address, using the Bluetooth connection after the pairing and before any personal data is exchanged in order to allow the S-EHR app to immediately close the connection if the signature cannot be verified.

(ii) Security Handshake

- The S-EHR app gets the Healthcare Organisation's identity, 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 is

approved or not by the healthcare organisation, including a specific consent for accessing the citizen's data.

- The HCP app gets the decision from the side of the S-EHR app regarding whether the consent for requesting the S-EHR app owner's data has been approved or not.
- The S-EHR app owner and the HCP app exchange already specified certificates and public keys, to finally establish a trusted and secure Bluetooth Connection

(iii) Exchange of Requests for Healthcare Data

- After that, in the case that the consent is digitally signed and the secure connection has been established, the HCP app is able to send specific requests for healthcare data that are stored in the S-EHR app. These requests follow a specific pattern (specified in D4.3) and are provided over the Bluetooth channel in the form of JSON requests. The S-EHR app receives from the side of the HCP App these requests, it prepares the requested data based on what is stored inside the S-EHR app, and finally provides the response to the HCP app, in the form of a JSON Response. It should be noted that these requests refer to all the stored FHIR Resources, to specific FHIR Resources categories, to the most recent FHIR Resources, and to FHIR Resources with a specific ID.

(iv) 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.

More details of the D2D protocol design and specification are available in the next chapter and in the report **[D4.3]** , where information regarding the used technologies, the sequence of exchanged messages and the involved actors, and involved components are presented 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 can provide detailed information to the citizens about a research initiative, obtain their consent for sharing their health data, 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 Node 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 the 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 machine-readable 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 Centres. 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. The RDD of a specific study is uploaded onto the Central Node of a Research Network by the PI of the study and is subsequently approved and published for download by an administrator of the Central Node. These operations are done through a UI that is out of the scope of the RDS protocol. 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, by means of the remote interface RDD offered, the CN to retrieve all published RDDs which are open for enrolment in the current period.
3. The mobile app sends, invoking the remote interface RDS exposed by the Research Centre Information System, 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. As many times as required by the study, the mobile app shares, using the remote interface RDS, 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 RDS interface, 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 or she does not honour 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, for 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 the RDS protocol is reported in deliverable **[D4.9]**.

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 **[D2.3]** 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 **[D2.3]**, 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. Gary is used for activities performed by means of remote APIs or user interfaces 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 **[D4.3]** and **[D4.9]**.

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 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 S0: Initial S-EHR feed

The UML activity diagram depicted in the following figures shows how the protocol R2D Access is exploited in "Scenario S0 -Initial S-EHR feed" **[D2.3]**.

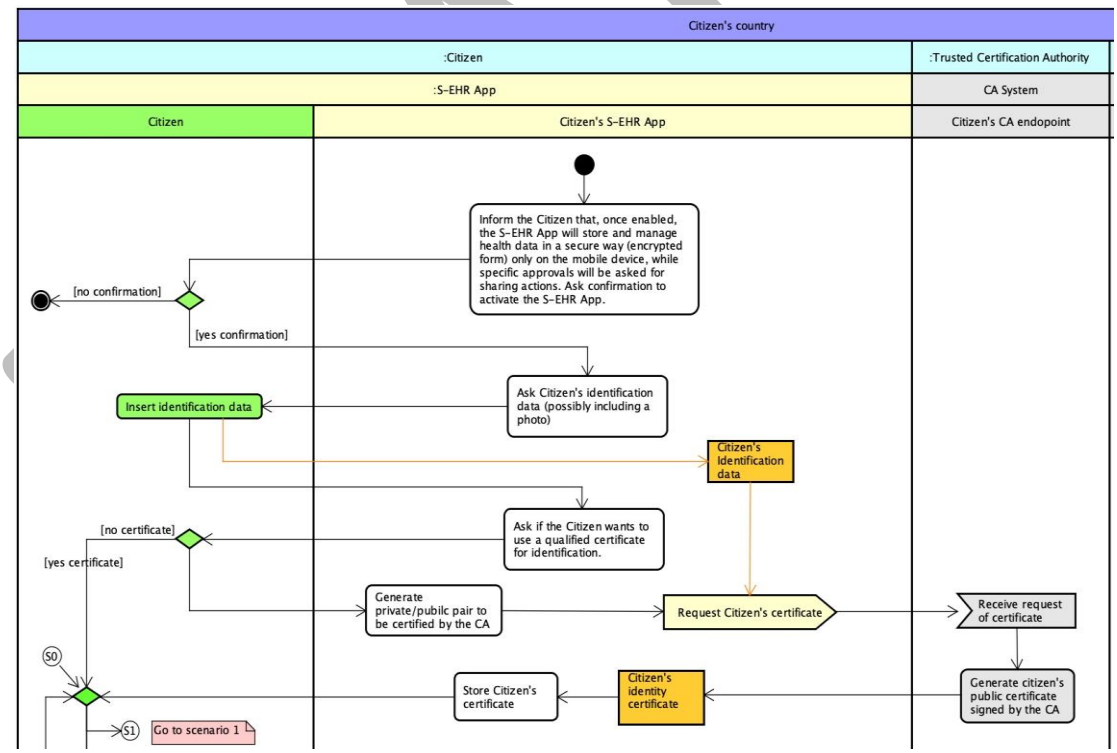

Figure 3 - Installation of S-EHR App and retrieval of citizen's qualified certificate

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 previously visited healthcare organisation (HCO) (step "Configure import of HD from EHRs") and then the S-EHR App uses the R2D Access protocol (interface R2DAccessIdentification) to authenticate on the selected HCO. The authentication is

done using eIDAS, therefore the HCO asks for the authentication to the eIDAS node of its country and then forwards the request to the eIDAS node of the Citizen's country that finally asks the Citizen to perform the authentication on the specific Identity Provider. The authentication process produces an identification token that is stored by the S-EHR App and that will be included in any next request done to the HCO.

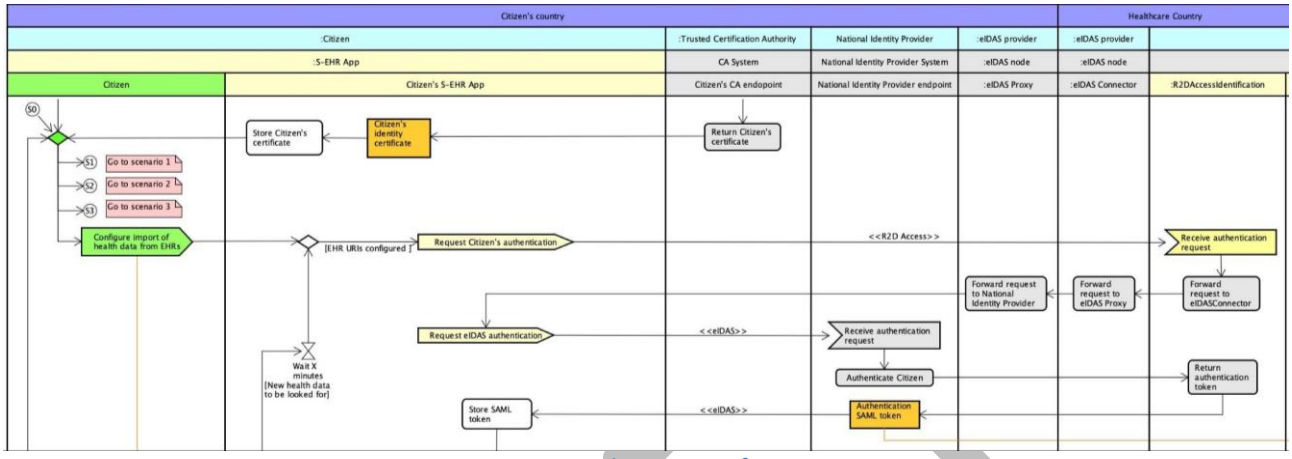

Figure 4 - eIDAS authentication for R2D Access

As shown in the next figure below, after the Citizen's authentication, the S-EHR App queries the HCO to obtain health data not yet imported. Depending on the HCO, the first time that the S-EHR App requests the health data (Interface R2DAccess), the HCO may ask the Citizen to provide additional identification information. This may be needed in the case that the HCO was not yet using the eIDAS identification when the health data were produced (so the HCO does not know the eIDAS identity of the Citizen) and the identification attributes provided by the eIDAS node are not sufficient to match the patient identity stored in the EHR of the HCO. In this case, the HCO replies with a list of items representing additional information to be provided by the citizen to complete the identification (i.e., "missing Citizen's identity attributes''). If the Citizen identity does not match the identity of any previous patient stored in the EHR, the HCO will notify that the patient is unknown. In the opposite case, after the successful identification of the patient, the HCO will reply with the required health data or with a URI that the S-EHR App must use to access the data. If the first or second kind of reply is returned depends on if the S-EHR App performed a synchronous or asynchronous request. The S-EHR App can perform a synchronous request to immediately obtain health data that are already available. If the health data is not actually available, the HCO will reply with a "data not ready" error message, otherwise the requested health data will be returned. If the S-EHR App does not know if the data is already available, it is better to perform a so-called asynchronous request[7]. In this case, the HCO will return a message of type "request accepted" that contains a URI to be used by the S-EHR App to check the status of provision of the requested health data.

[7] At HTTP level, the interaction pattern is actually synchronous, but it emulates an asynchronous interaction.

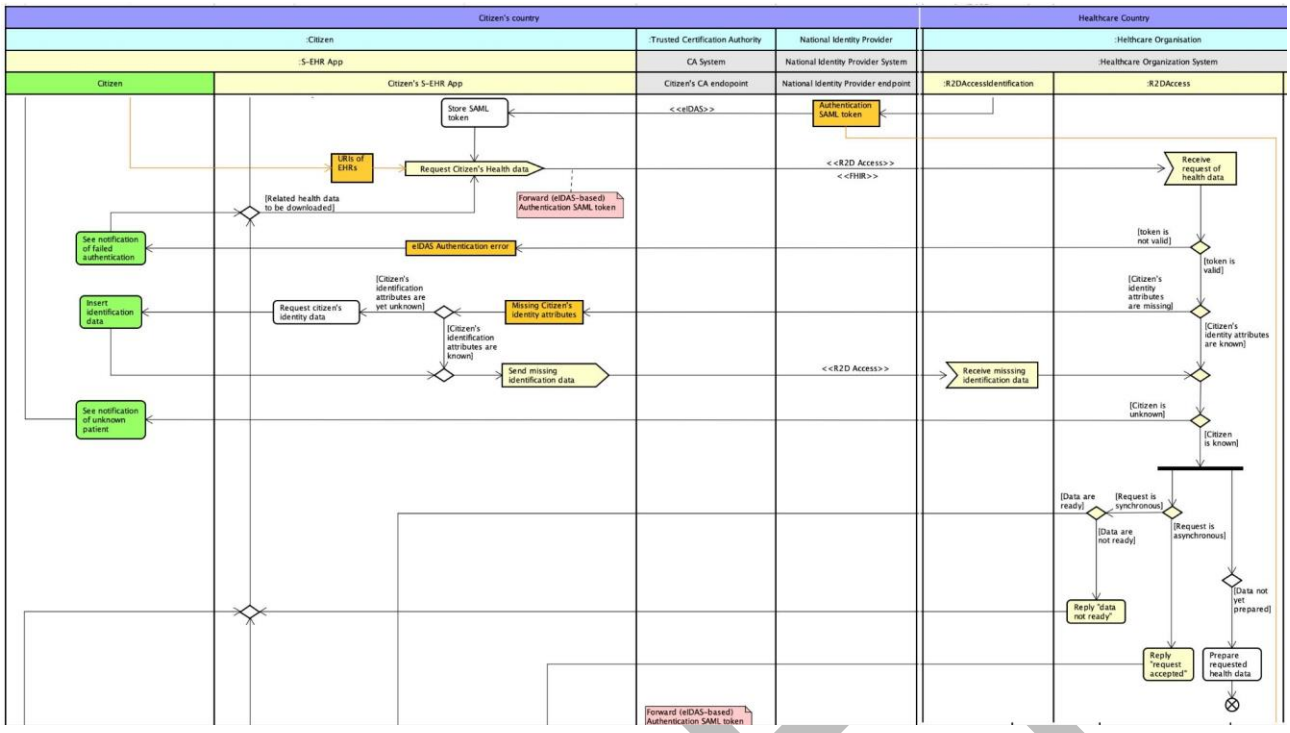

Figure 5 - Request of HD using R2D Access

As shown on the next figure, by invoking the interface R2DAccess the S-EHR App may check the status of health data and download them when they are ready.

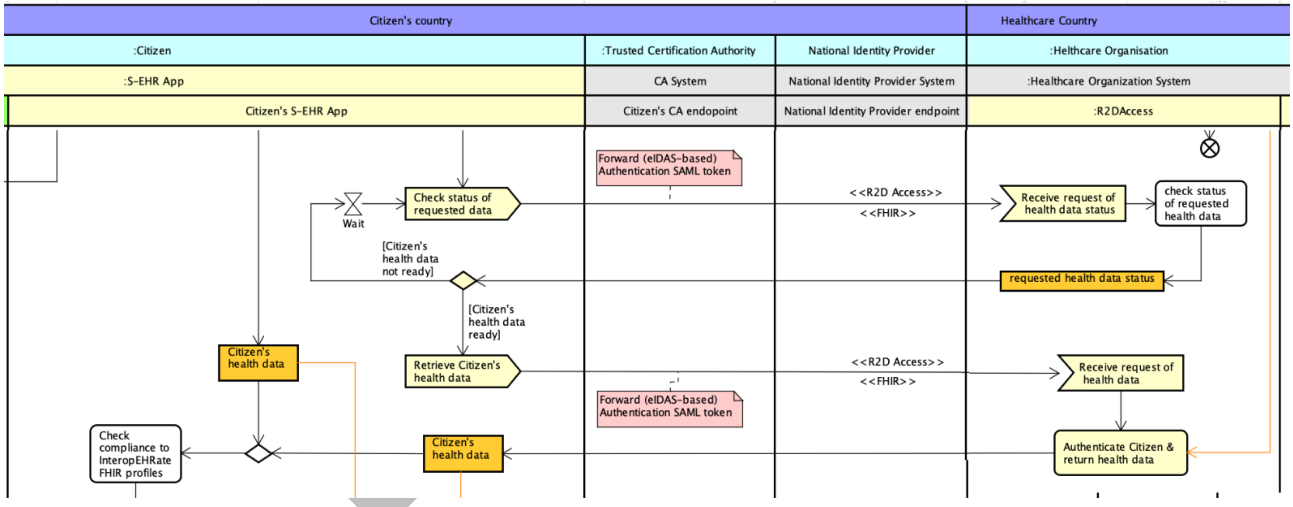

Figure 6 - Import of HD using R2D Access

After checking the compliance of the received HD to the InteropEHRate profiles **[D2.9]** the S-EHR App will store them in encrypted format on the mobile device.

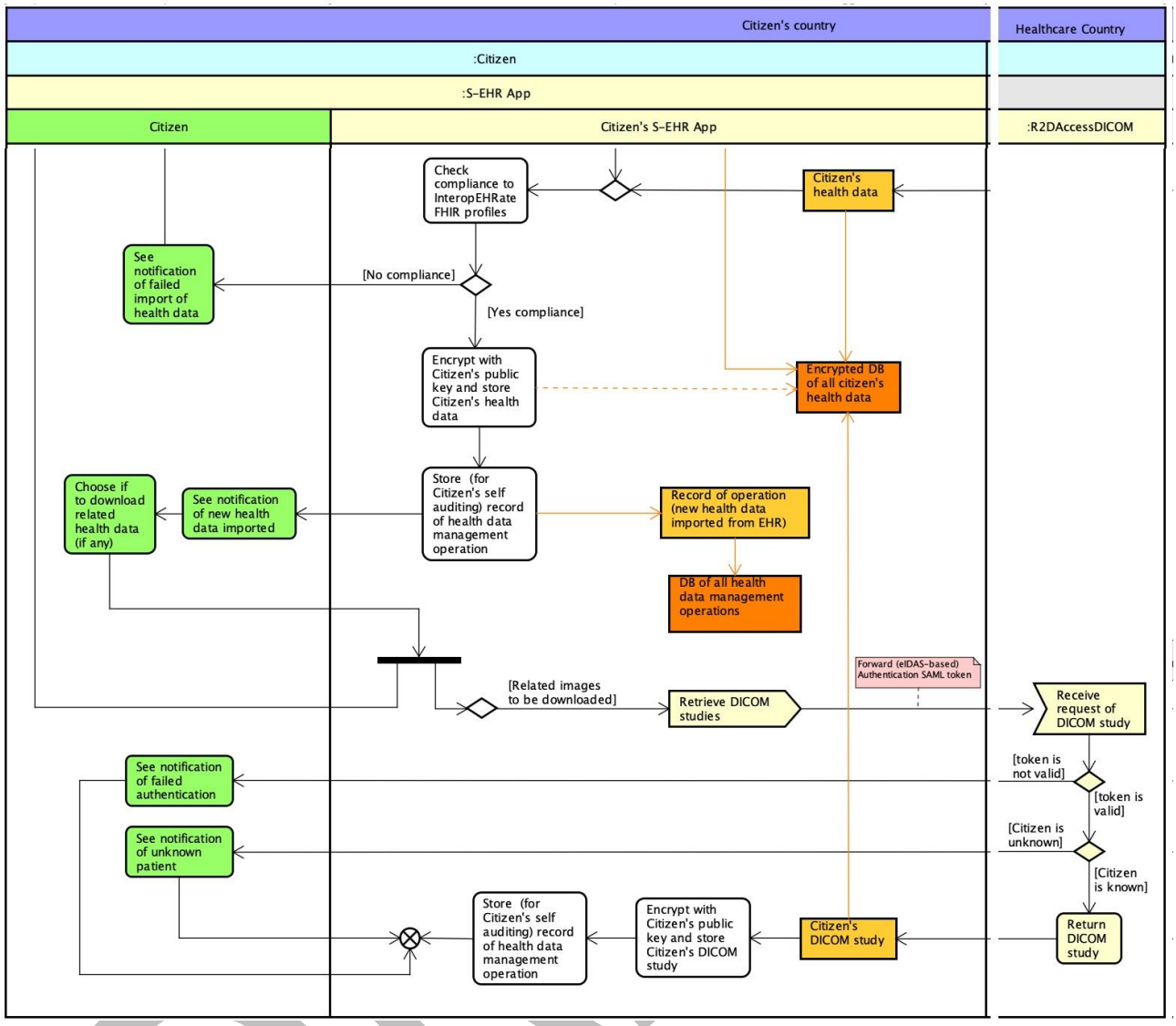

Figure 7 - Import of HD using R2D Access

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 (shown in fig. 4), 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 figure above also shows the usage of the interface R2DAccessDICOM. This interface is optionally offered by HCO that wants to share diagnostic images and signals with the patient using the DICOM standard. The HCO may embed an image directly in the shared HD (in this case there is no need to also implement the interface R2DAccessDICOM), but it can also decide to include in the HD just a reference to the actual image study. In this case, the S-EHR App is free to not download the actual image or to download it at a different time, depending on the availability of space on the user device and on the citizen preferences.

3.2 Scenario S1: Medical Visit abroad

The UML activity diagram depicted in the following figures shows how the D2D protocol is exploited in "Scenario S1 - Medical visit abroad" **[D2.3]** and in phases that precede or follow it.

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 to complete the temporary pairing of the S-EHR App with the HCP App. During a medical visit the S-EHR App may be paired with different HCP terminals, anyway the reading of the QR-Code is mandatorily needed only when the connection with the first terminal is established. During the first connection, the HCP App may share with the S-EHR App the IDs (MAC addresses) of all the terminals that will be used during the medical visit, so that the S-EHR App can trust them without any intervention of the Citizen (see guard [HCP terminal ID already shared with the S-EHR app] in the diagram). Similarly, the HCP App may share the MAC address of the S-EHR app with the other terminals that will trust it. When the S-EHR App and the HCP App already know one another and the medical visit is not yet finished, the connection is established automatically, and interaction continues as depicted in Figure 9 from the point labelled 4.

In the opposite case (see guard [HCP terminal ID not yet shared with the S-EHR app] in the diagram) the Citizen has to explicitly approve the connection. The Citizen receives from the S-EHR App (interface D2D) 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 is 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 his or her ID card. The HCP will check the identity of the citizen based on the qualified certificate or of the ID card and will confirm it to complete the pairing between the S-EHR App and the HCP App.

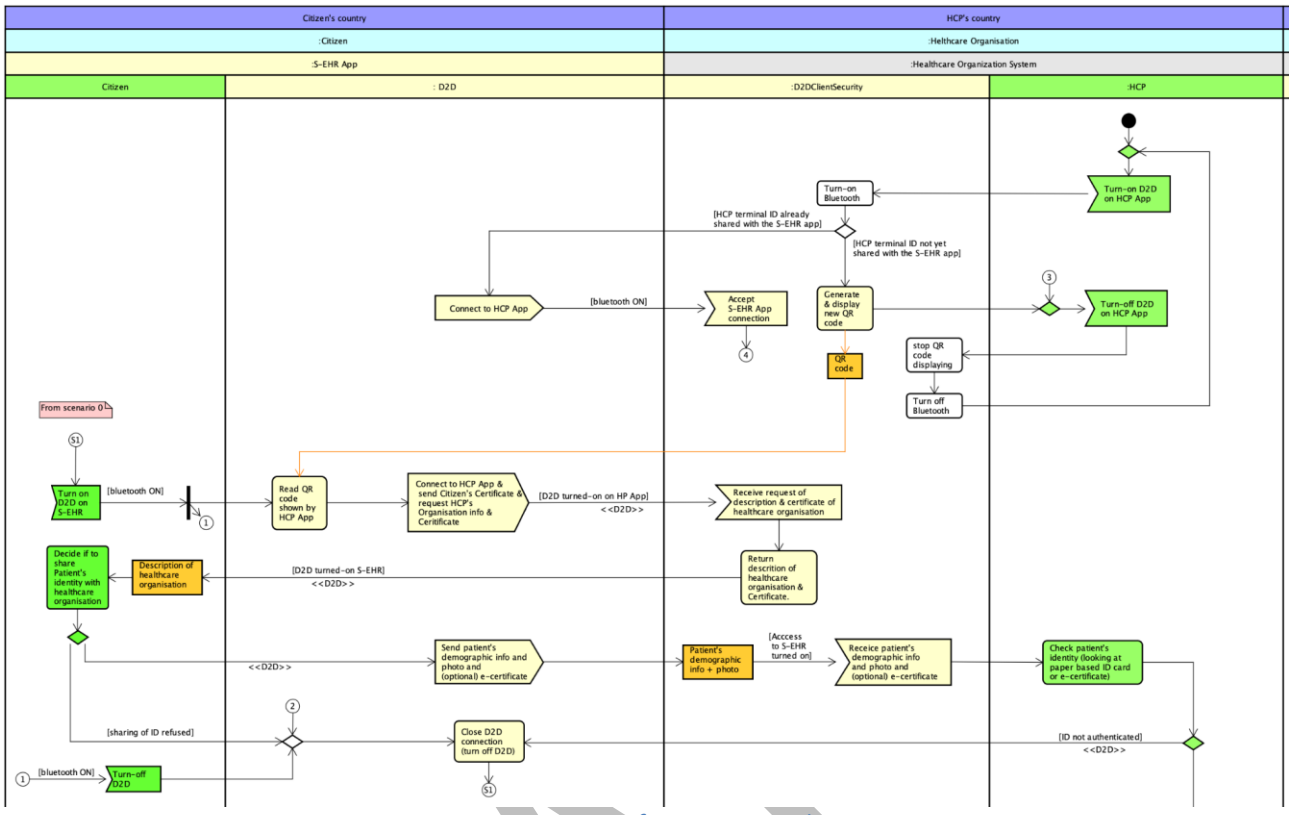

Figure 8 - D2D pairing of S-EHR App and HCP App

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 D2D) 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 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 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.

The HCP App receives the first set of data (containing key data such as the Patient Summary and a list of other health data, such as the list of previous medical encounters of the Citizen, including ones performed in other healthcare organisations). The HCP may decide to browse the other health data. If the HCP App has not yet downloaded the other health data, it will perform a new request to the S-EHR App.

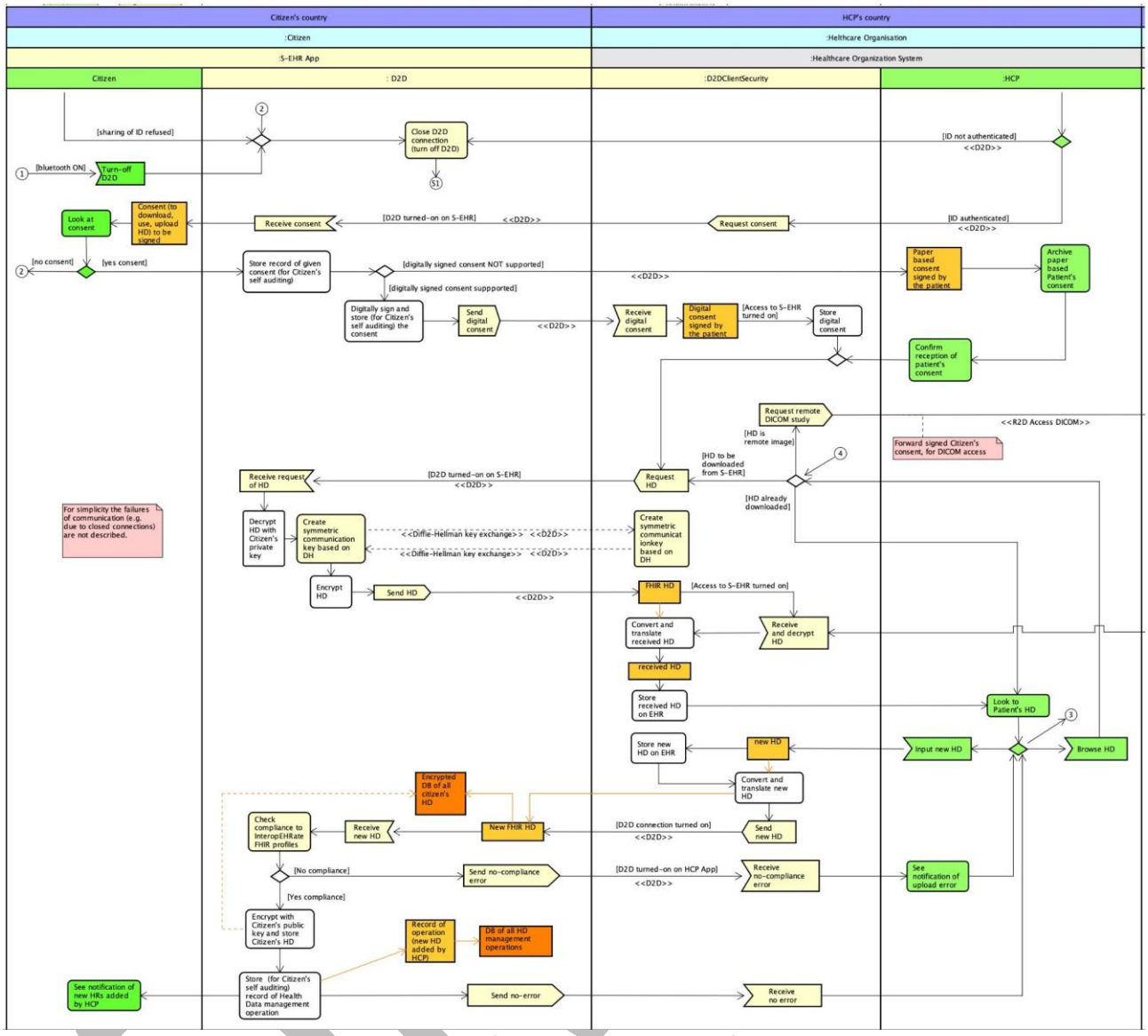

Figure 9 - Exchange of health data by means of D2D protocol

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 is 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.

The HCP may also ask for remote images, i.e., DICOM studies that are not stored on the S-EHR App but only referred to by the HD downloaded from the S-EHR app. In this case, the HCP App can download them directly from the (other) producer healthcare organisation, using the remote interface R2DAcessDICOM. This is an optional interface that healthcare organisations are required to offer when they decide not to embed a DICOM study within the HD shared with the patient, but to embed just a reference to it. In order to allow the download of remote images, the S-EHR Citizen's consent shared at the beginning of the D2D interaction must include an explicit digital and temporary consent for the download of referred images.

This consent must be forwarded to the interface R2DAcessDICOM and will be checked by the other healthcare organisation to authorise the access to the remote image. The next figure shows the steps of downloading the DICOM study.

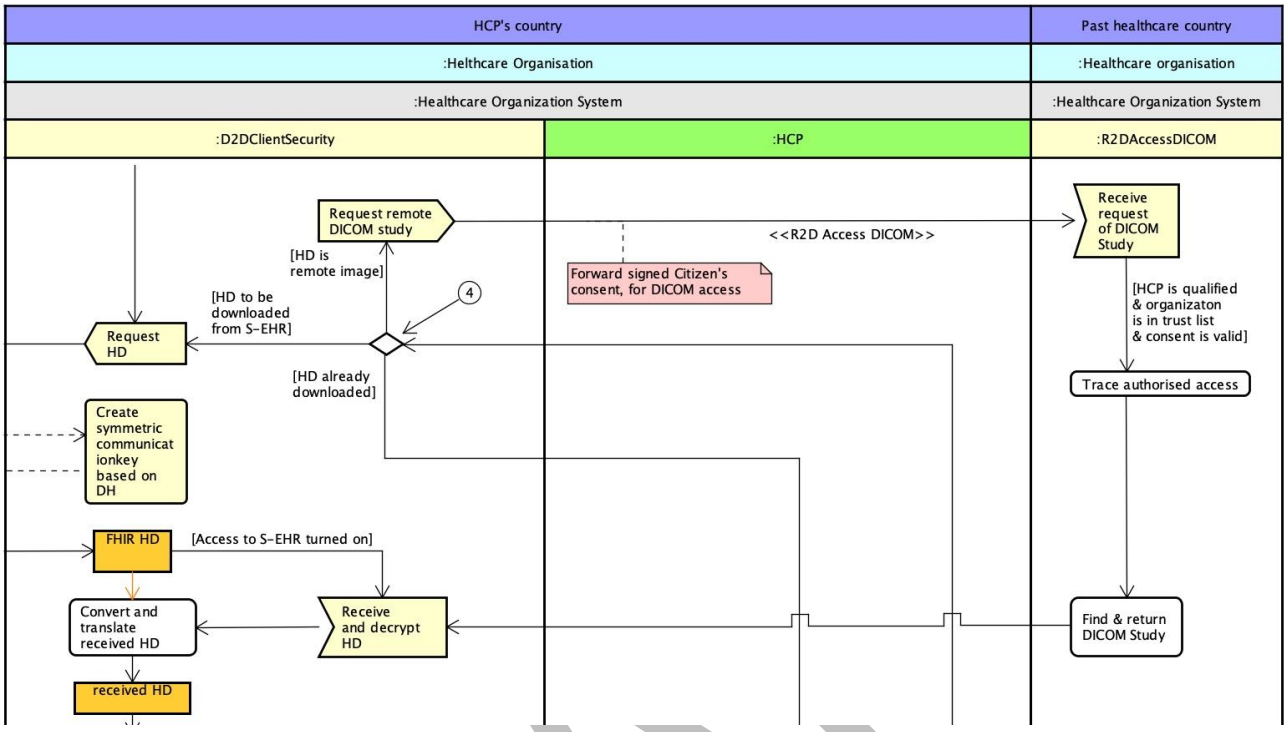

Figure 10 - Access to remote images referred by HD retrieved with D2D protocol

3.3 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" **[D2.3]** 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. 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 from 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.

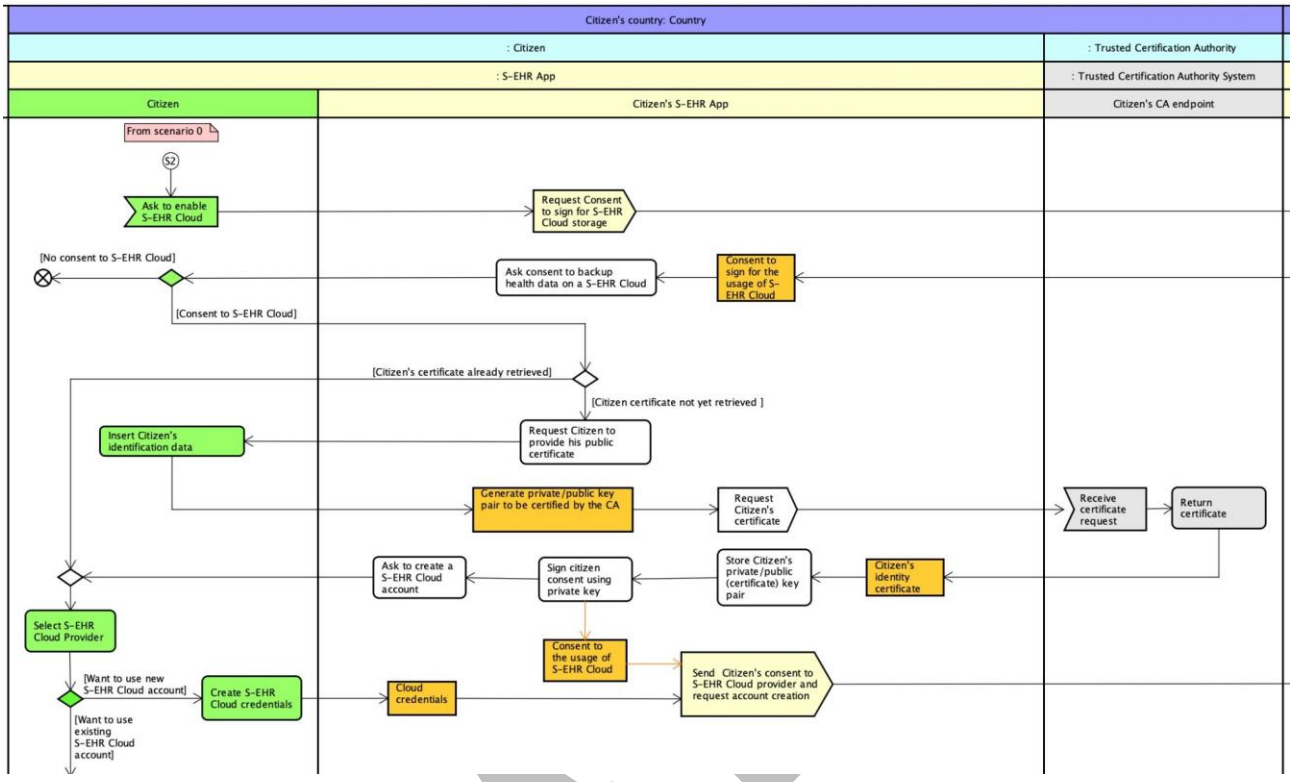

Figure 11 - Activation of the S-EHR Cloud by the citizen

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 R2DBackup. First, the signed 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 Cloud 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 has been stored on the S-EHR App and will copy an encrypted version of them on the S-EHR Cloud. The structured health data is 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, 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 a healthcare 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 not know the S-EHR App key, nor does it know 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, an initial bundle of health data, single images and single documents referred by the initial bundle.

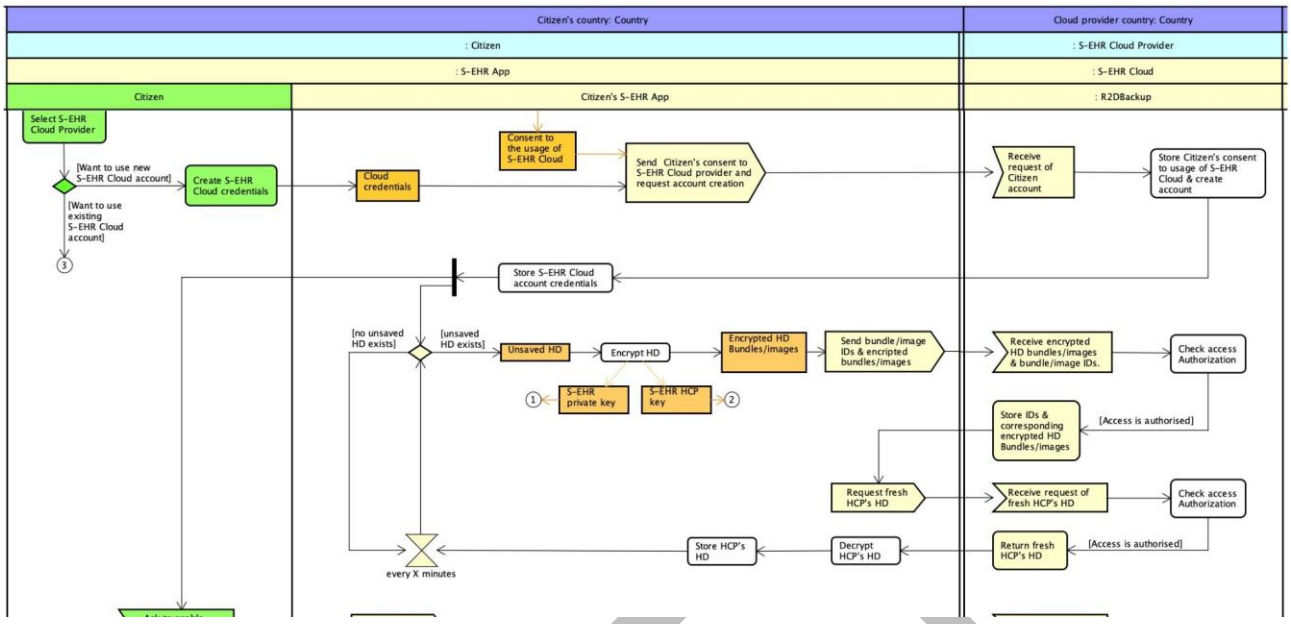

Figure 12 - Automatic backup of S-EHR content on the S-EHR Cloud

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 must provide an explicit consent that is sent to the S-EHR Cloud to authorize the HCPs of specific healthcare organisations to download the health data in case of emergency.

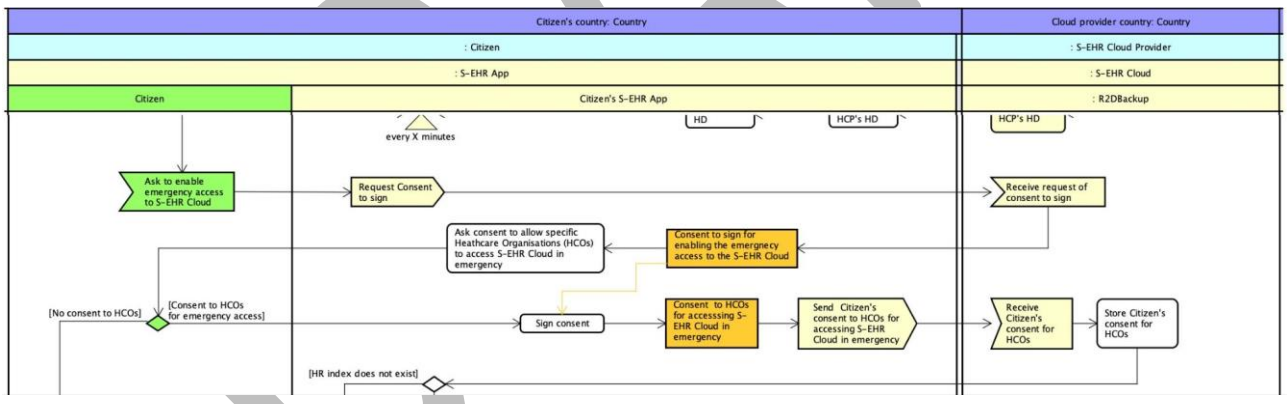

Figure 13 - Consent to the HCP's access to the S-EHR Cloud in case of emergency

The following figure shows that the consent to the HCOs for accessing the S-EHR Cloud in emergency involves the interface R2DBackup offered by the S-EHR Cloud (used to communicate the consent) and the interface HRIWriter 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, to allow to find it also in case that the location has been changed after the production of the QR code.

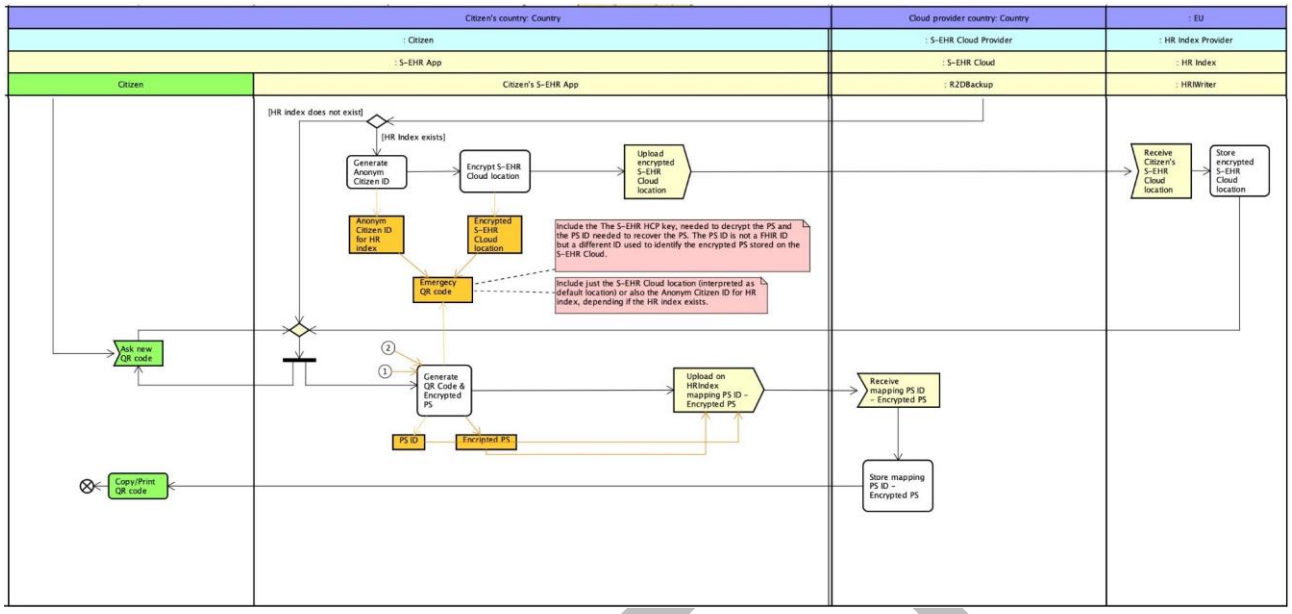

Figure 14 - Storing of S-EHR Cloud location on the HR Index

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 of the existence of the HR Index, the access to health data by HCPs during the emergency requires that the HCP own 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 to a new S-EHR app (on the same mobile device or on a new mobile device). For 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 R2DEmergency 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 to generate a new S-EHR App key, a new HCP key and a new QR code.

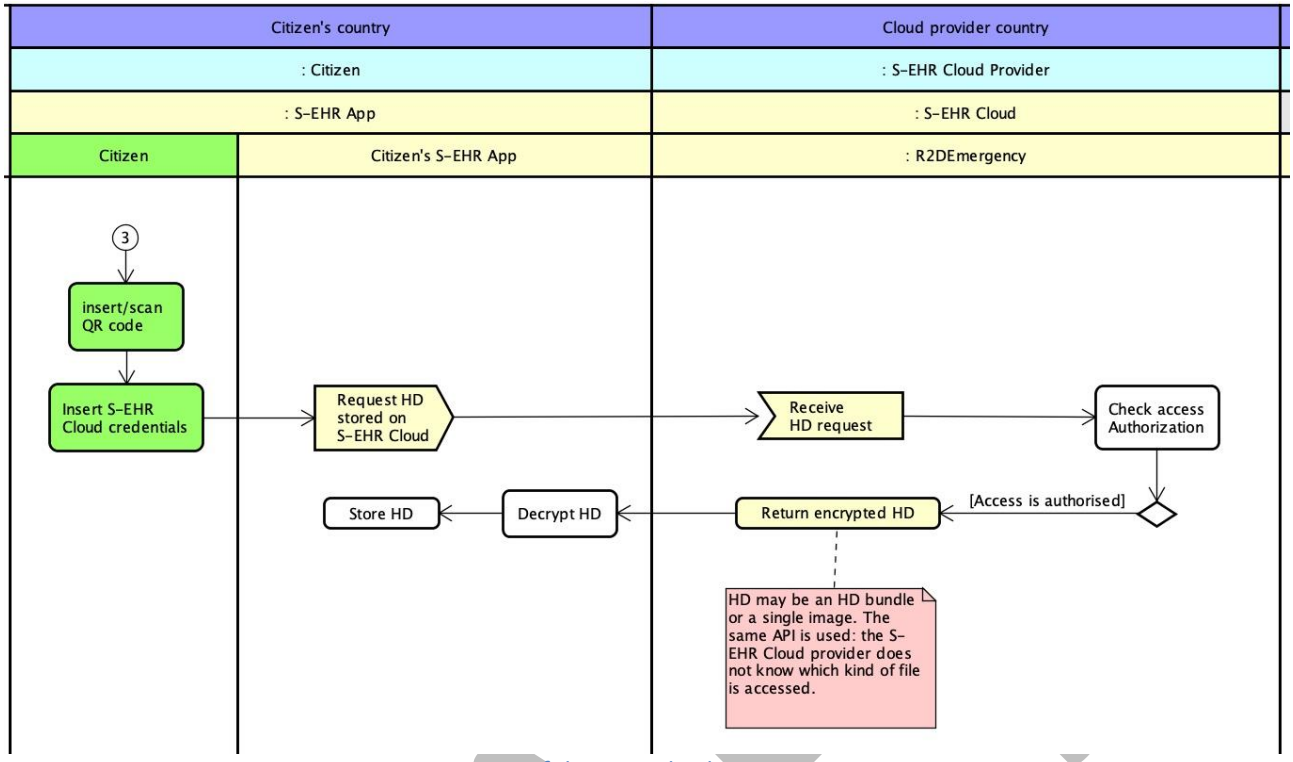

Figure 15 - Import of the S-EHR backup on a new S-EHR App

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, 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.

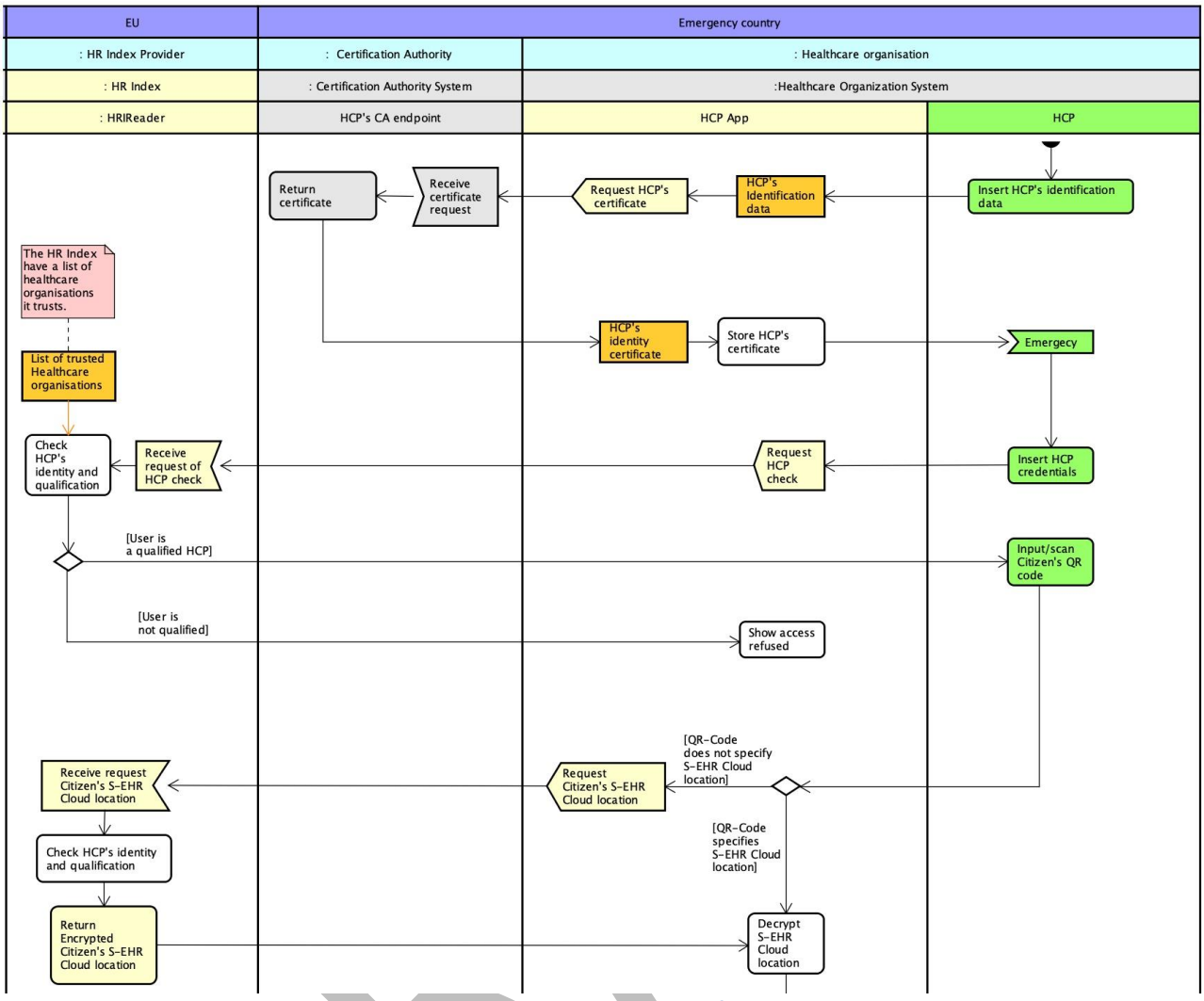

Figure 16 - Access to S-EHR Cloud by an HCP for emergency reasons

After determining the location of the S-EHR Cloud, the HCP App tries to invoke the interface R2DCloudEmergency offered by the S-EHR Cloud 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 allows 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 to allow the citizen to audit all accesses to her health data. The bundle is then decrypted from the S-EHR App using the HCP key provided by the QR code. The HCP will look at the initial bundle (containing the identification data of the Citizen, possibly including a Citizen's photo, and an index of all other available health data) and will decide whether to retrieve the bundles of related health data following steps similar to the previous ones. If possible, the HCP will try to check the identity of the patient looking at the Citizen's photo and other identifying data, before downloading the related health data.

In the case that the HCP asks to access a DICOM study that is not contained in but just referred to by the downloaded HD, the HCP app will invoke the interface R2DAccessDICOM exposed by the producer of the DICOM file, in order to retrieve it. To this end, the HCP App will forward to the producer HCO the Citizen consent for the access to the Citizen's health data in emergency.

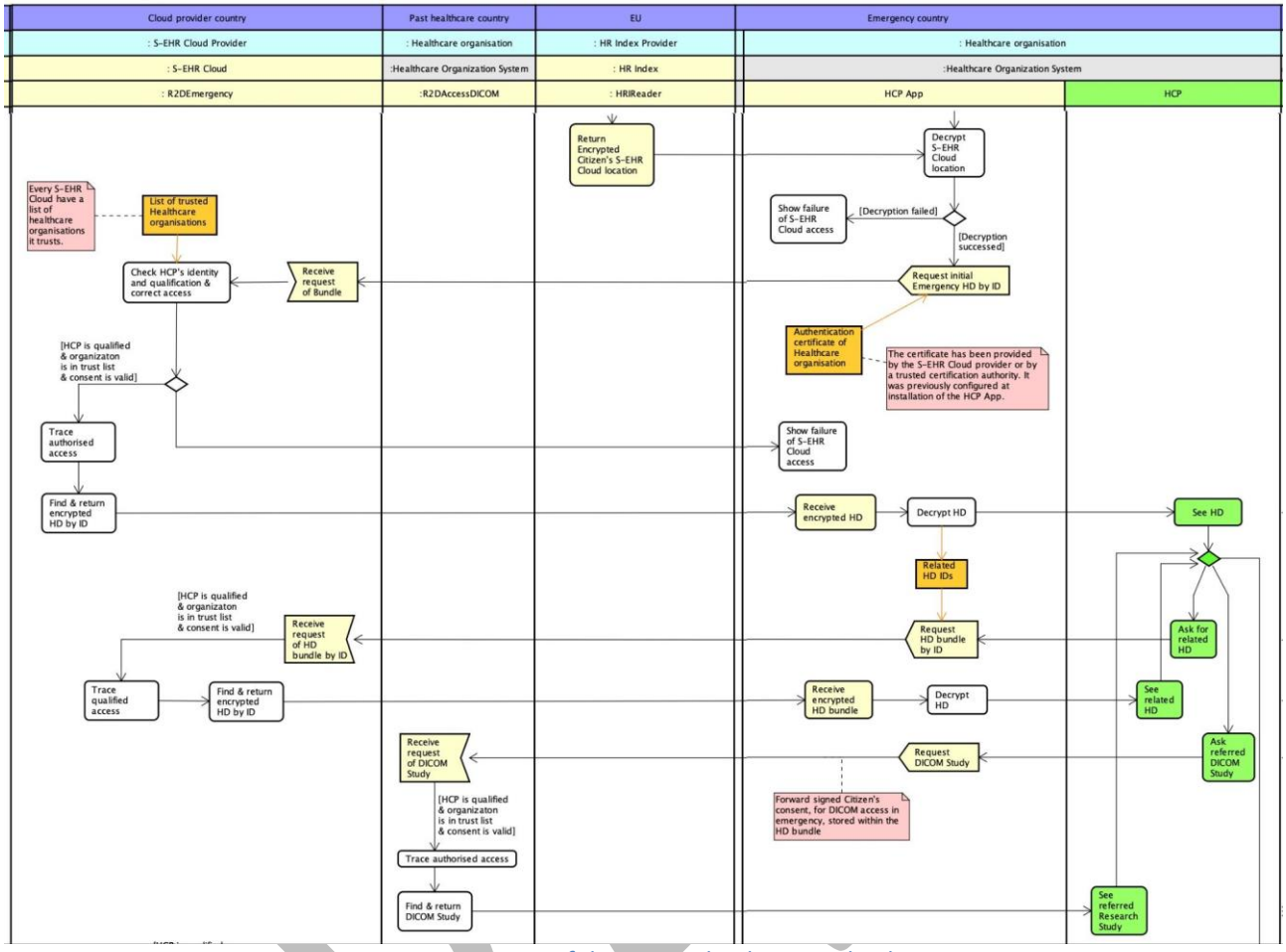

Figure 17 - Browsing of the S-EHR Cloud content by the HCP

Like the case of the medical visit, during the healthcare process in an emergency, the HCPs can produce new health data. For this reason, the interface R2DEmergency 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 R2DBackup 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).

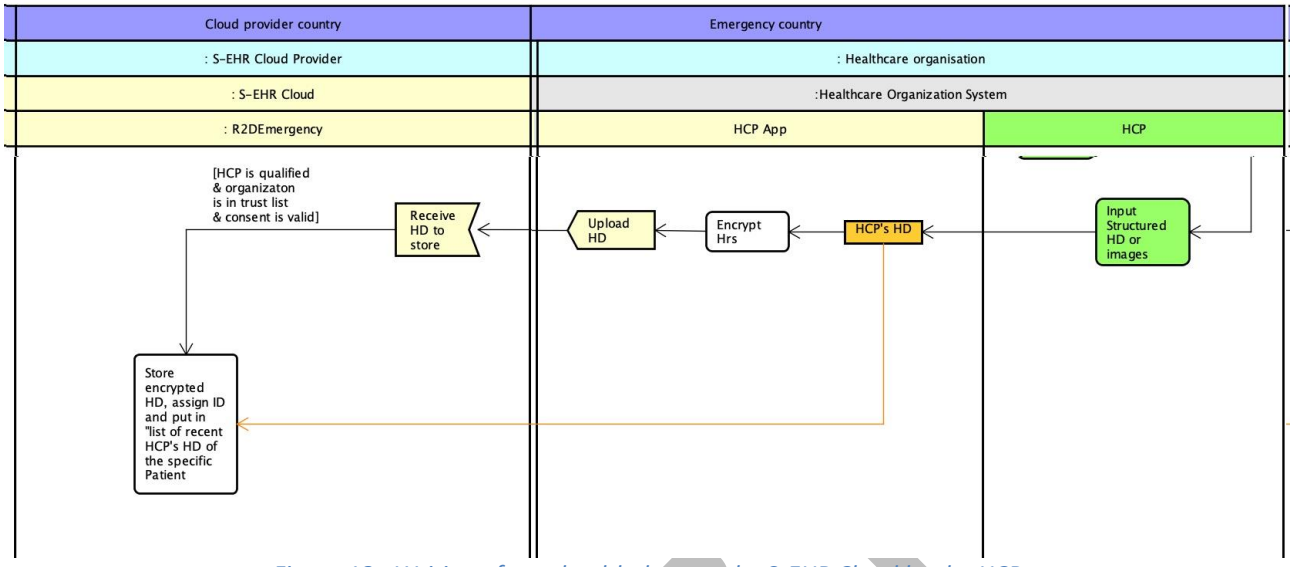

Figure 18 - Writing of new health data on the S-EHR Cloud by the HCP

The last figure below shows that the interface R2DBackup 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).

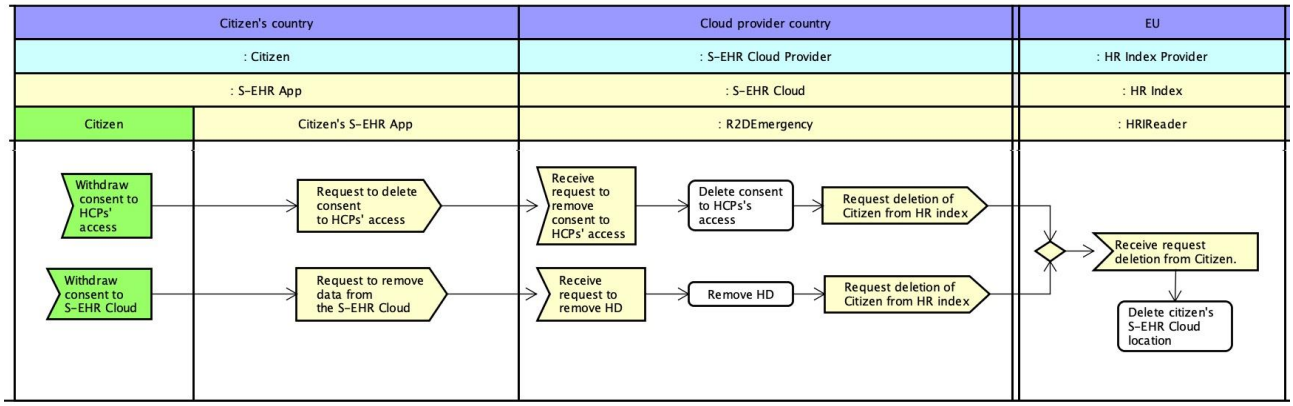

Figure 19 - Withdraw of consent to HCP access and/or to S-EHR Cloud usage

3.4 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 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.

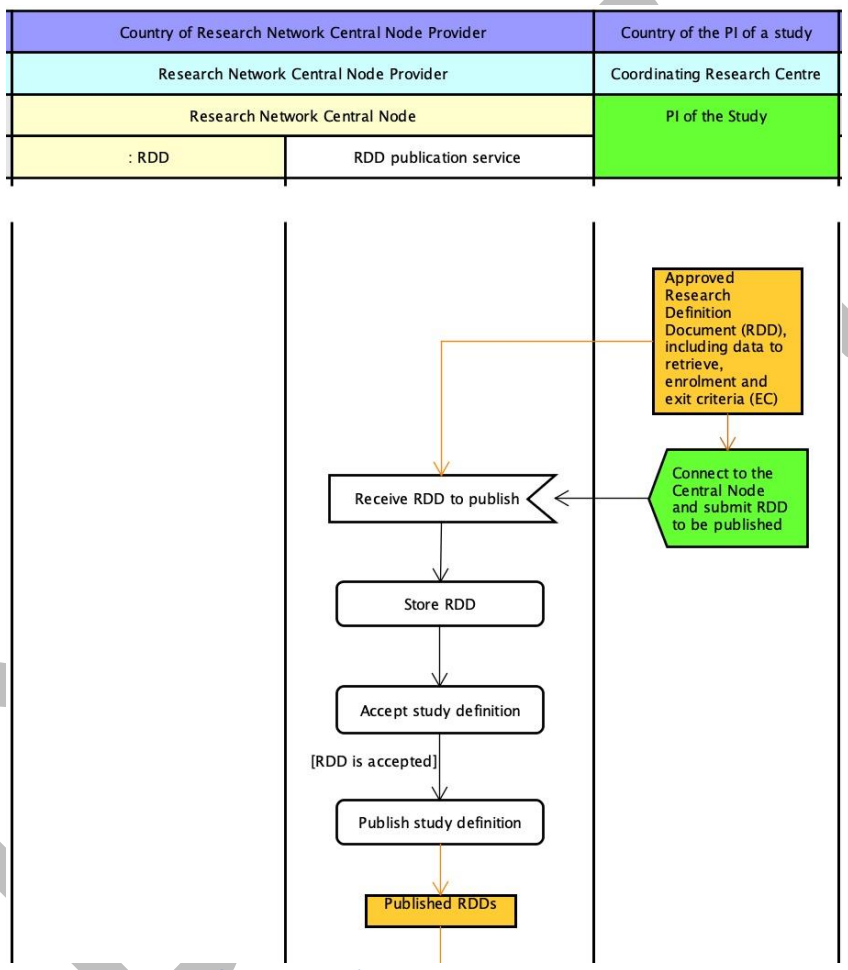

Figure 20 - Publication of a new RDD (required but not constrained by the RDS protocol)

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 user interface offered by a web application) that is specific to 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.

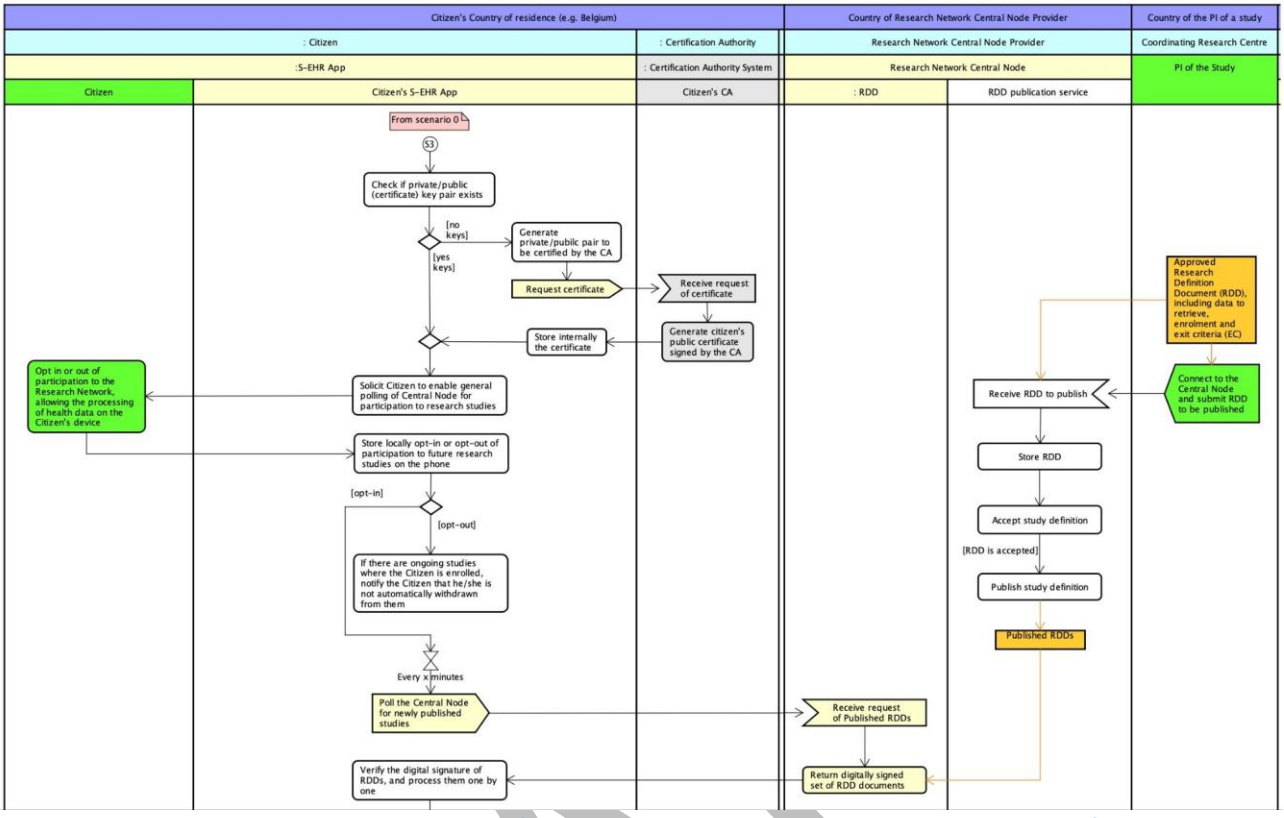

Figure 21 - Citizen opt out or opt in of participation to the Research Network and polling of RDDs

A prerequisite for participating in the Research Network is that the citizen owns a digital certificate, therefore the first steps of the diagram show the creation of the digital certificate (this is usually already done in the installation phase, as shown in the section on scenario S0). At the installation of the S-EHR App, or also in a successive moment if the citizen asked to be reminded, the app also 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 RDD 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 pseudonymization of data, a specific pseudonym or pseudo-identity is created, according to the indications of the RDD. The difference between the usage of a pseudonym and the usage of a pseudo-identity is that in the first case the Reference Research Centre does not know the real identity of the citizen associated with the pseudonym, while in the

second case it knows it. The pseudonym is created by invoking the remote API PP offered by the Pseudonym Provider, that will generate a random pseudonym having a high level of entropy. The pseudo-identity is instead created by asking it to the remote API RDS offered by the Reference Research Centre, which will generate an identifier following a pattern depending on the specific research study (usually characterised by a lower level of entropy with respect to a pseudonym).

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.

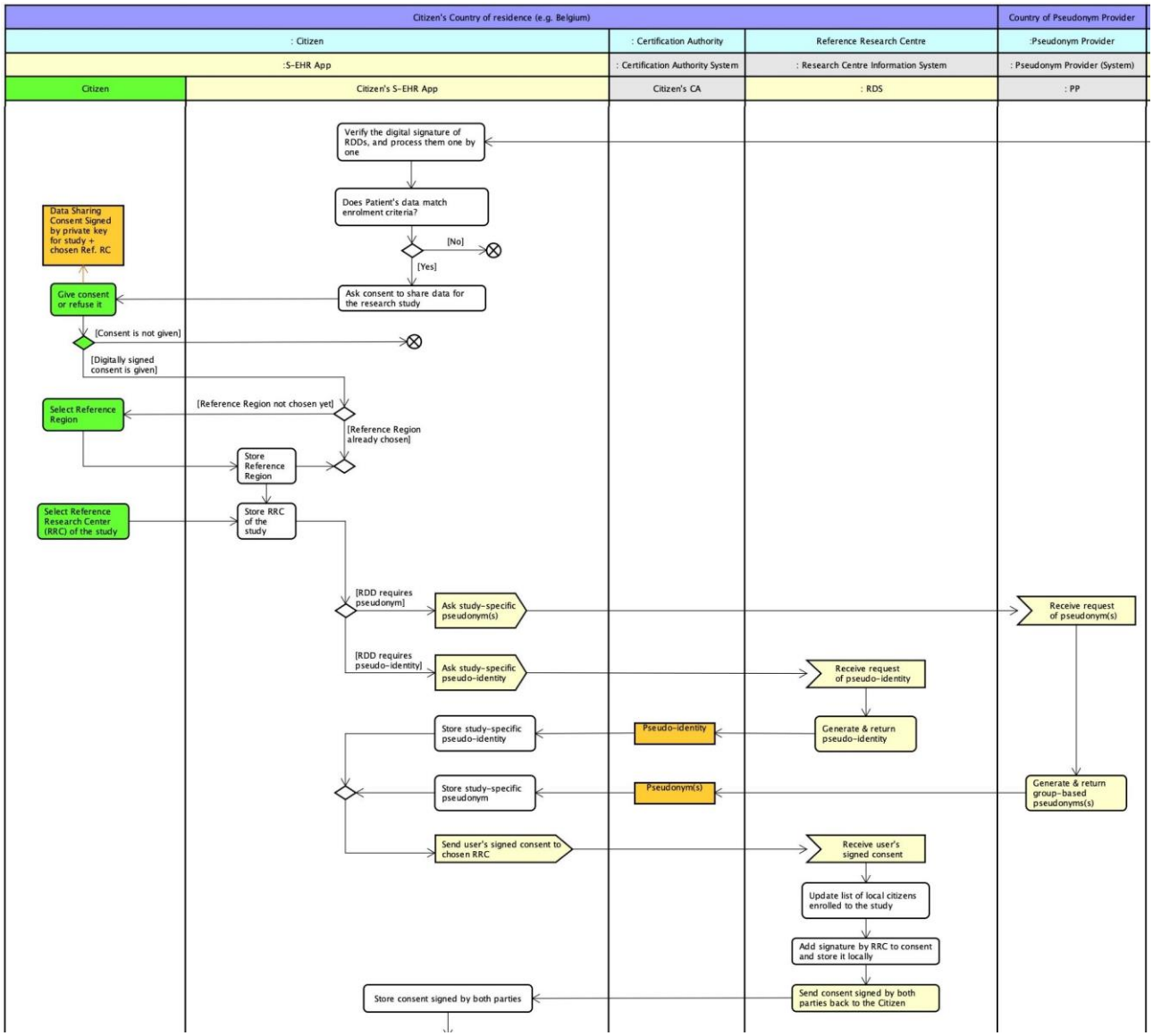

Figure 22 - Enrolment of a citizen in a research study

This is the first data that the S-EHR App shares. This step is performed by invoking the remote API RDS offered by the Reference Research Centre, which will add the citizen to the list of participants in 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 Figure 23 below.

At the time specified or condition specified by the RDD, the S-EHR App checks the health data stored on the mobile device. If the RDD requires the citizens to fill a questionnaire, the App asks them to do it.

Afterwards, it checks if the exit criteria expressed by the RDD are verified. In a positive case, the S-EHR App stops sending 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 matching data is then anonymised or pseudonymised, using the pseudonym or pseudo-identity previously assigned, and then the data is encrypted and sent to the Reference Research Centre, again by invoking an operation of the remote API RDS. If the Citizen asked for it, a notification is shown, informing that new health data has 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 the scope of the RDS protocol. In case the HD contains references to anonymised files not available on the S-EHR App, the Reference Research Centre may obtain them directly from the producer Healthcare Organisation by invoking the interface R2RAccessDICOM (in the case of anonymised DICOM files) or R2RAccess (in the case of other kind of data, such as anonymised PDF files). In order to obtain the referred data, the Reference Research Centre will be required to forward to the producer Healthcare Organisation both the ID of the required anonymised data and the electronic consent given by the Citizen to access the data. This request may potentially be done also by the PI, in this case the Citizen's consent has to authorize the specific PI.

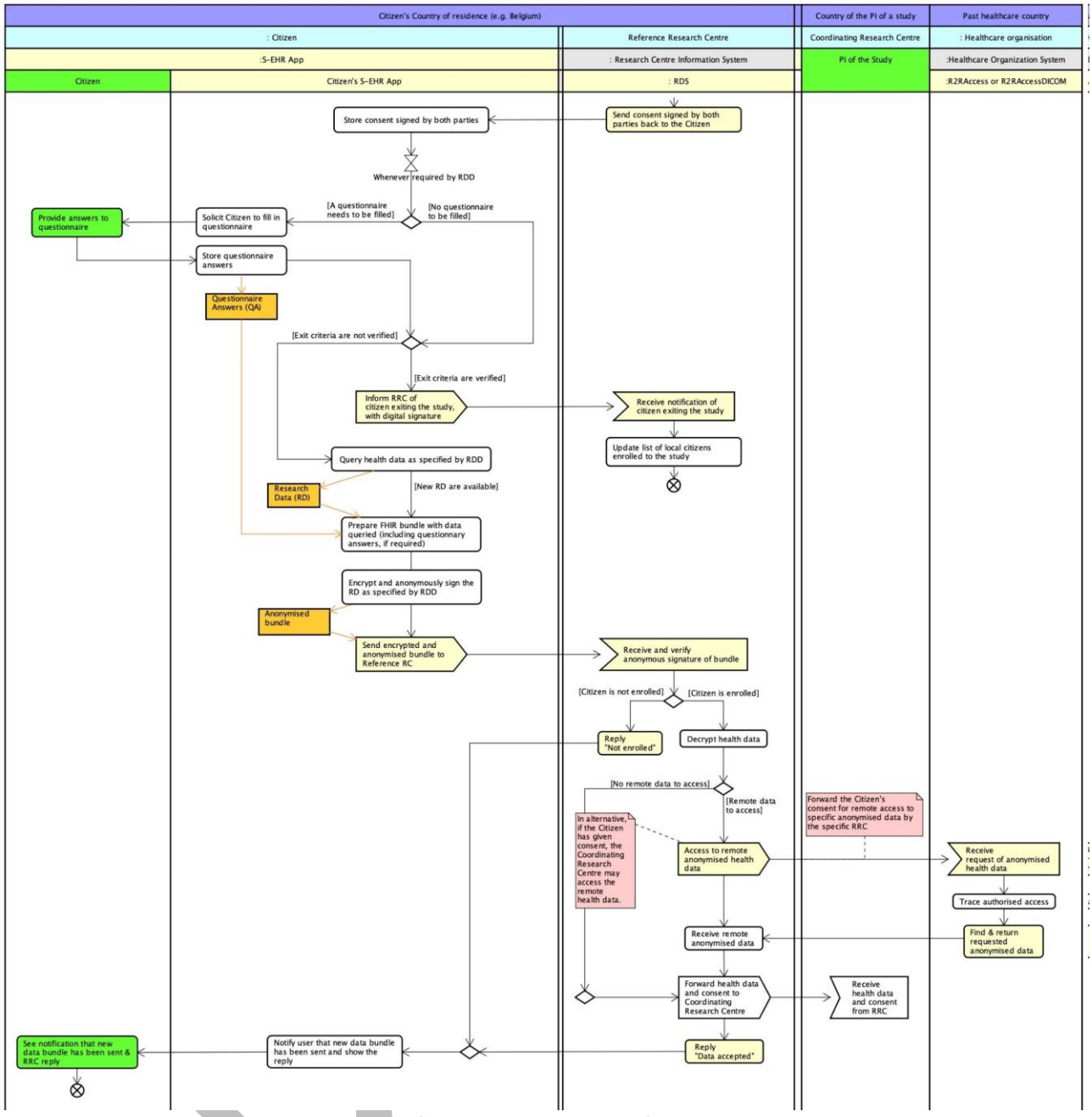

Figure 23 - Sharing of health data with the Reference Research Centre

The citizen may withdraw (Figure 24) at any moment from a research study. This is done by invoking another operation offered by the remote interface RDS, 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 non-repudiation of these contracts by means of encryption and digital signature.

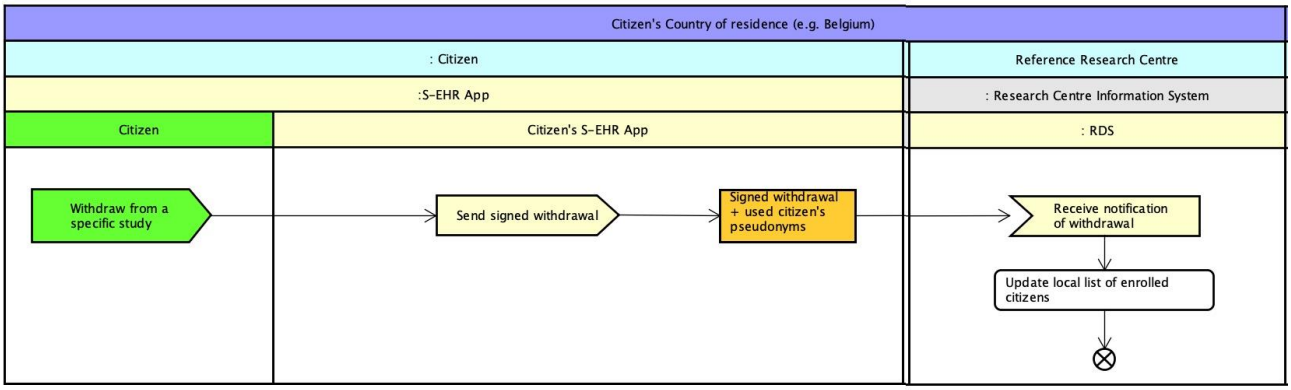

Figure 24 - Withdrawal from a research study

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 basis 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. The additional components support the conversion and translation of exchanged health data.

The following picture shows in an informal way the main 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 is 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).

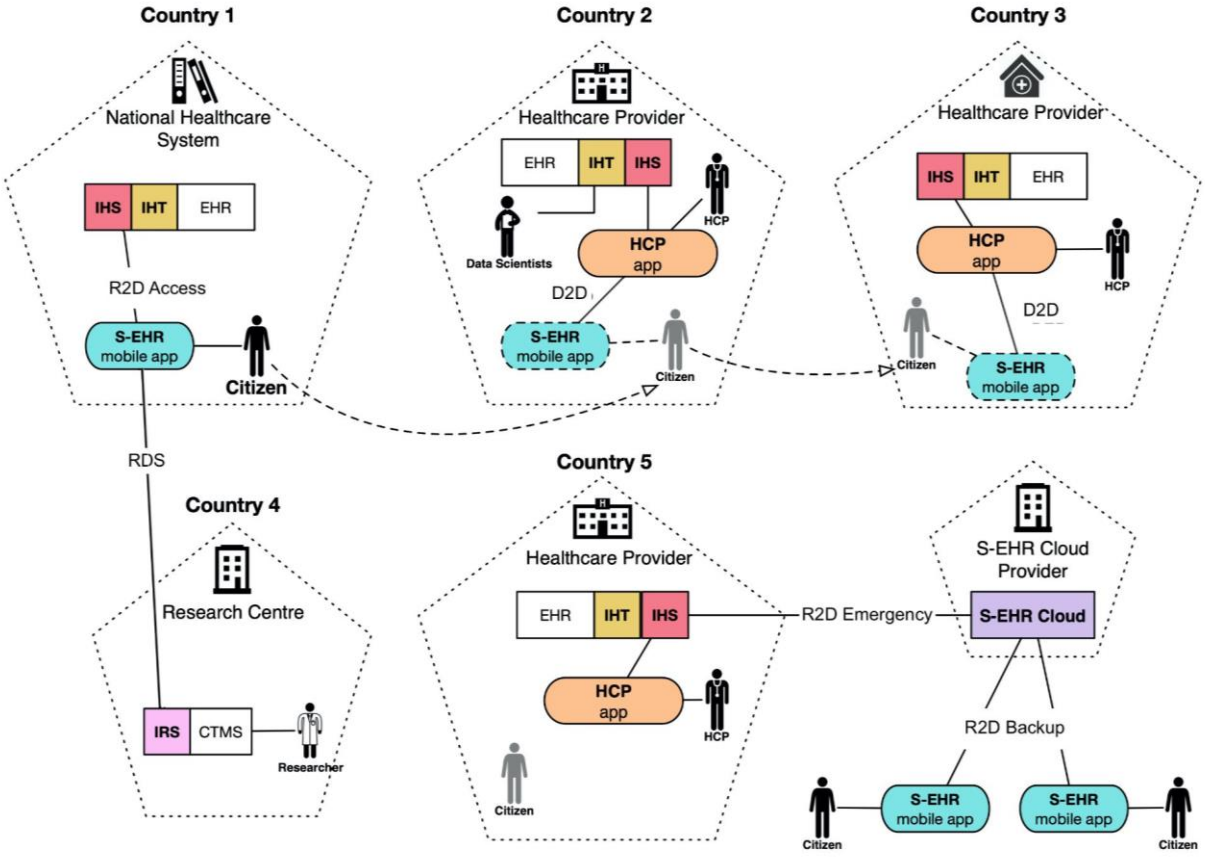

Figure 25 - Examples of health data exchange using the components offered by the InteropEHRate Framework

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.

Actors	Description
CN Administrator	A person responsible of approving the publication of new RDDs on the reference implementation of the Research Network Central Node.
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**[D2.3]** scenarios, it is also called "domain expert".

Table 4 - 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 5 - 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".

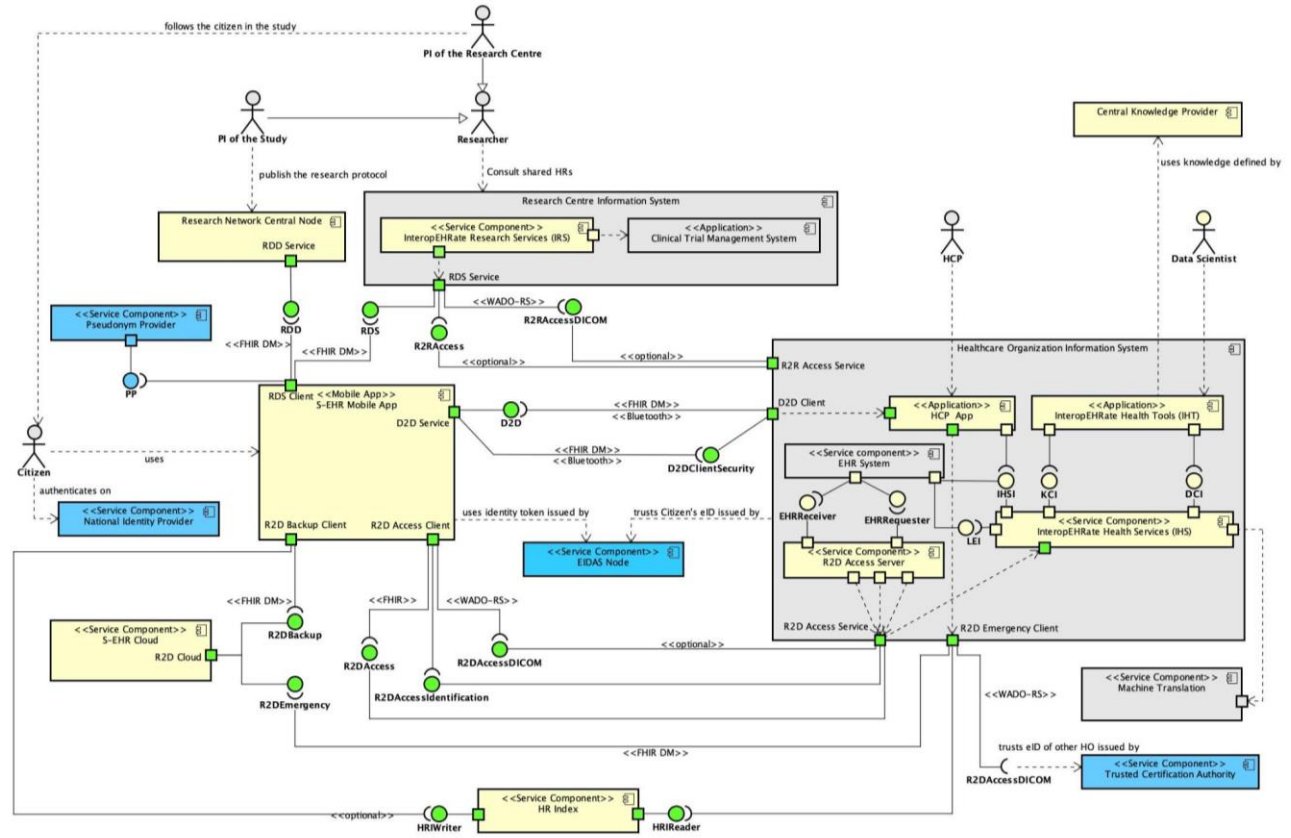

Figure 26 - Architecture of the InteropEHRate framework

The "InteropEHRate Framework'', is composed of different systems, one usable independently of the others. These systems are in turn composed of reusable libraries, each one representing a reference implementation of 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].
- **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 interfaces that a Research Centre has to implement to support the RDS protocol. It allows the scientists to engage voluntary citizens at a 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 IHSI and LEI interfaces, which allow the conversion and translation of health data retrieved 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.

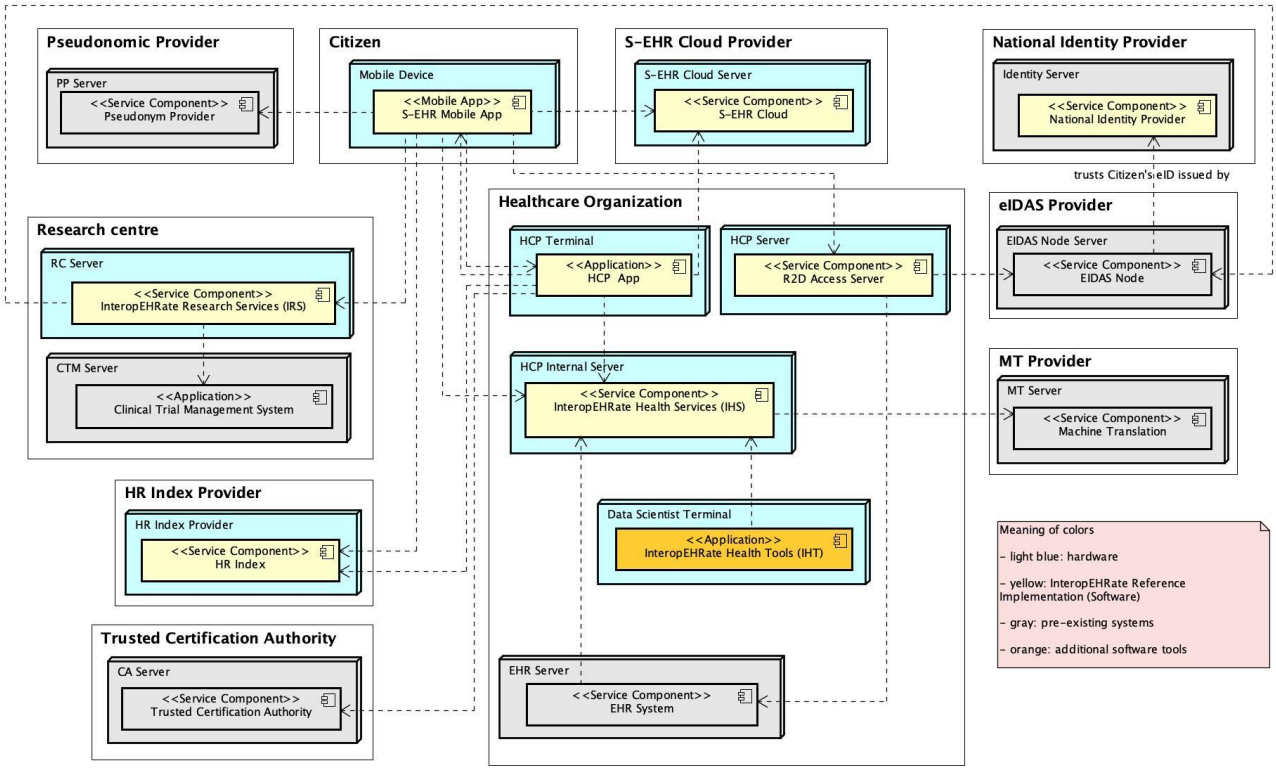

Figure 27 - Deployment view of the InteropEHRate framework

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, 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 of 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 protocols. 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" **[D3.2]**.
- **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 **[D3.11]**.

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 protocols for the exchange of health data on the Internet **[D4.3]** . 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 **[D4.3]** . They are used respectively for mobile applications and desktop applications.
- Mobile R2D Backup: This library offers the implementation of the R2D Backup protocol from the S-EHR Application side and allows the exchange of encrypted health data with the S-EHR Cloud.
- Terminal R2D Emergency: This library offers the implementation of the R2D Emergency protocol from the HCP Application side and allows an authorized HCP to gain access to the health data of a citizen during an emergency as well as allowing them to upload encrypted health data to the S-EHR Cloud.

Details on the design of libraries for D2D and R2D protocols may be found in the upcoming report **[D4.6]** .

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 **[D4.9]**. 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 [D4.18].

4.6 S-EHR Mobile App RI

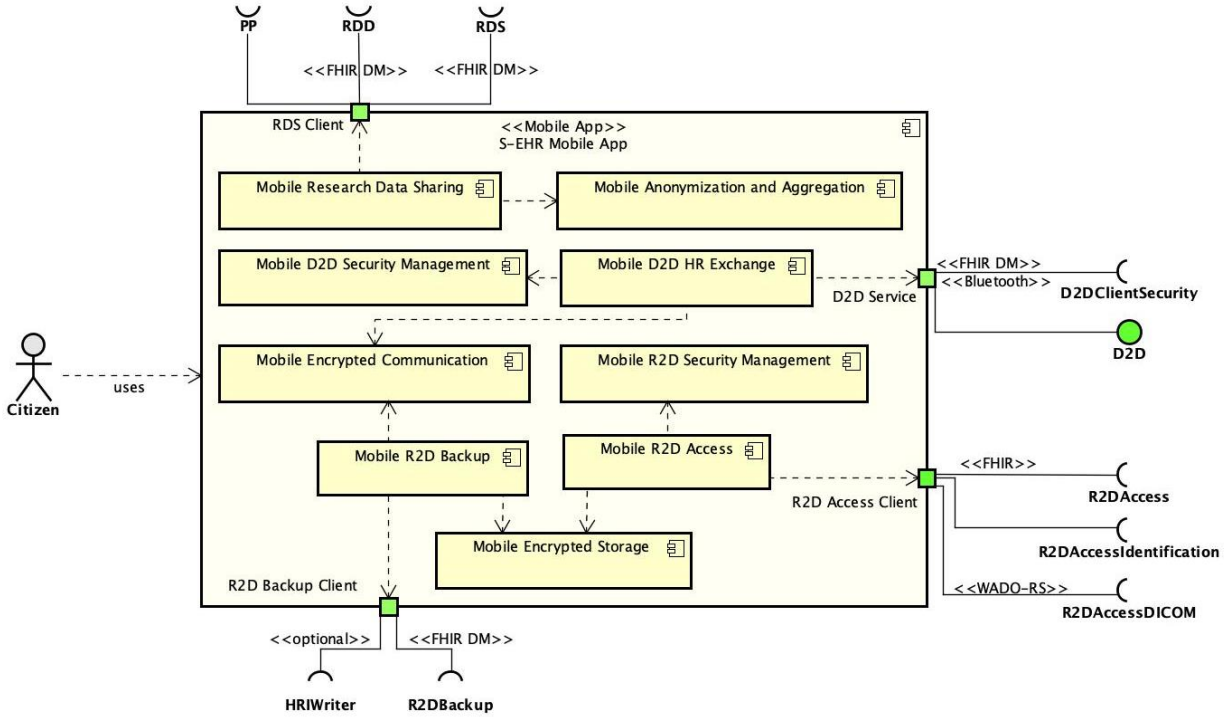

Figure 28 - S-EHR Mobile App internal view

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 **[D3.2]**. 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 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 Access" for importing health data through the Internet.
- "Mobile R2D Backup" for the back of health data on (and restore from) the S-EHR Cloud.

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 final version of the S-EHR Mobile App RI is in particular used to:

- retrieve health data from a remote healthcare organisation by means of R2D-Access;

- collect and transmit patient's consent and health data by means of D2D;
- collect and display to patient data produced by HCPs and shared by the InteropEHRate protocols and by the legacy A7 protocol;
- save personal health data on S-EHR Cloud by means of R2D-Backup;
- retrieve personal health data from S-EHR cloud by means of R2D-Backup;
- give access to backed up data on S-EHR Cloud to HCP to enable R2D-Emergency;
- import research studies from research network by means of RDS;
- determine if a Citizen is eligible to be enrolled in a research study;
- register a citizen to a research centre by means of RDS;
- collect, anonymise and transmit patient data to the reference research centre by means of RDS.

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

4.7 S-EHR Cloud RI

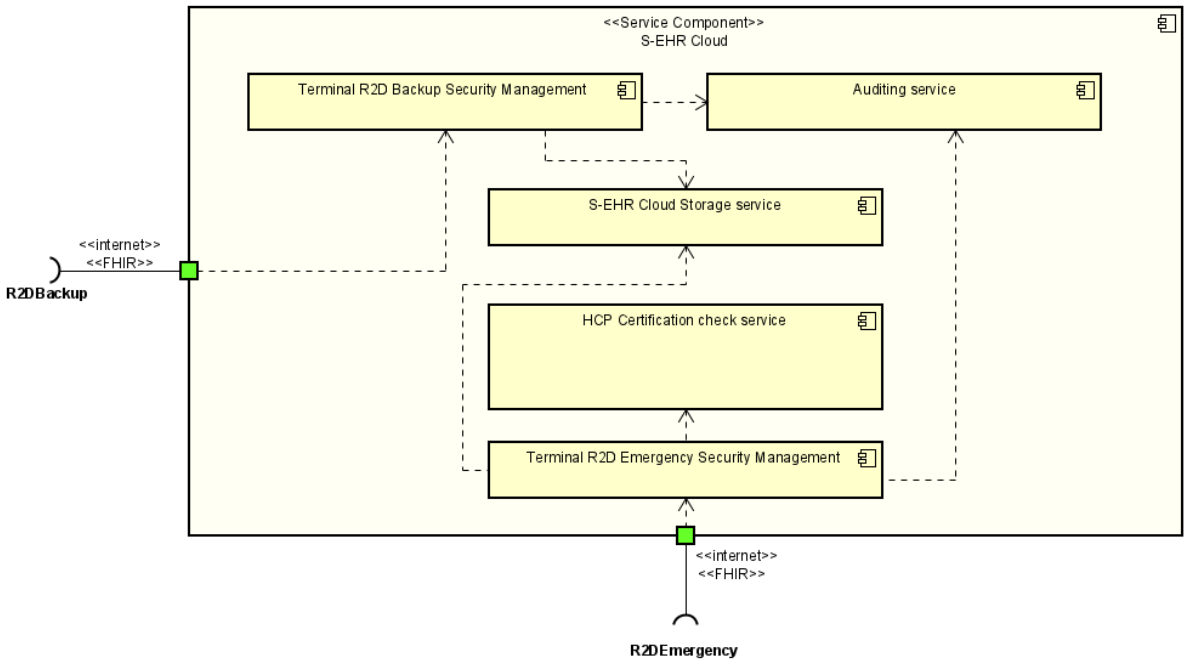

Figure 29 - S-EHR Cloud RI Internal view

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. All communication from both the S-EHR Mobile App and the HCP App is managed by the reusable libraries of the R2D Backup and R2D Emergency protocols as defined in the section 4.5. 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
- Terminal R2D EmergencyBackup Security Management: This component ensures that the communication between the S-EHR Cloud RI and the HCP App RI is encrypted.
- **Storage** service**:** This component is used to safely store the citizen's encrypted 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 third-party trusted certification authority as an HCP of a trusted healthcare organization. Only if this authentication is successful, the HCP gains access to the citizen's content.

More information regarding the design of the S-EHR Cloud service is reported in the report **[D6.7]**.

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 has 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 and upload them back using the R2D Emergency protocol;
- importing health data from an EHR located within the healthcare organisation;
- transferring health data from an HCP app instance to another HCP app instance.

Considering the overall architecture, user requirements specified in **[D2.3]** and technical solutions available at the moment, the HCP App is developed using web technologies. According to **[D4.3]** 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 [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 R2D in order to retrieve a patient's EHR for emergency cases.

Hcp-app-hospital-services is the component used by the HCP App instances from a hospital to transfer between them the EHRs of a patient during a medical visit, in case it is necessary to be consulted by several HCPs. This component is not part of the HCP App architecture, being a centralized service at the hospital level. The complete flow of the functionality is described in more details in [D5.14] at Chapter 3.3.4.

The HCP application integrates the D2D library that is capable of transferring information from the S-EHR App to the HCP App in a request-response approach, HCP App sends requests, S-EHR responds to requests.

[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 the 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.

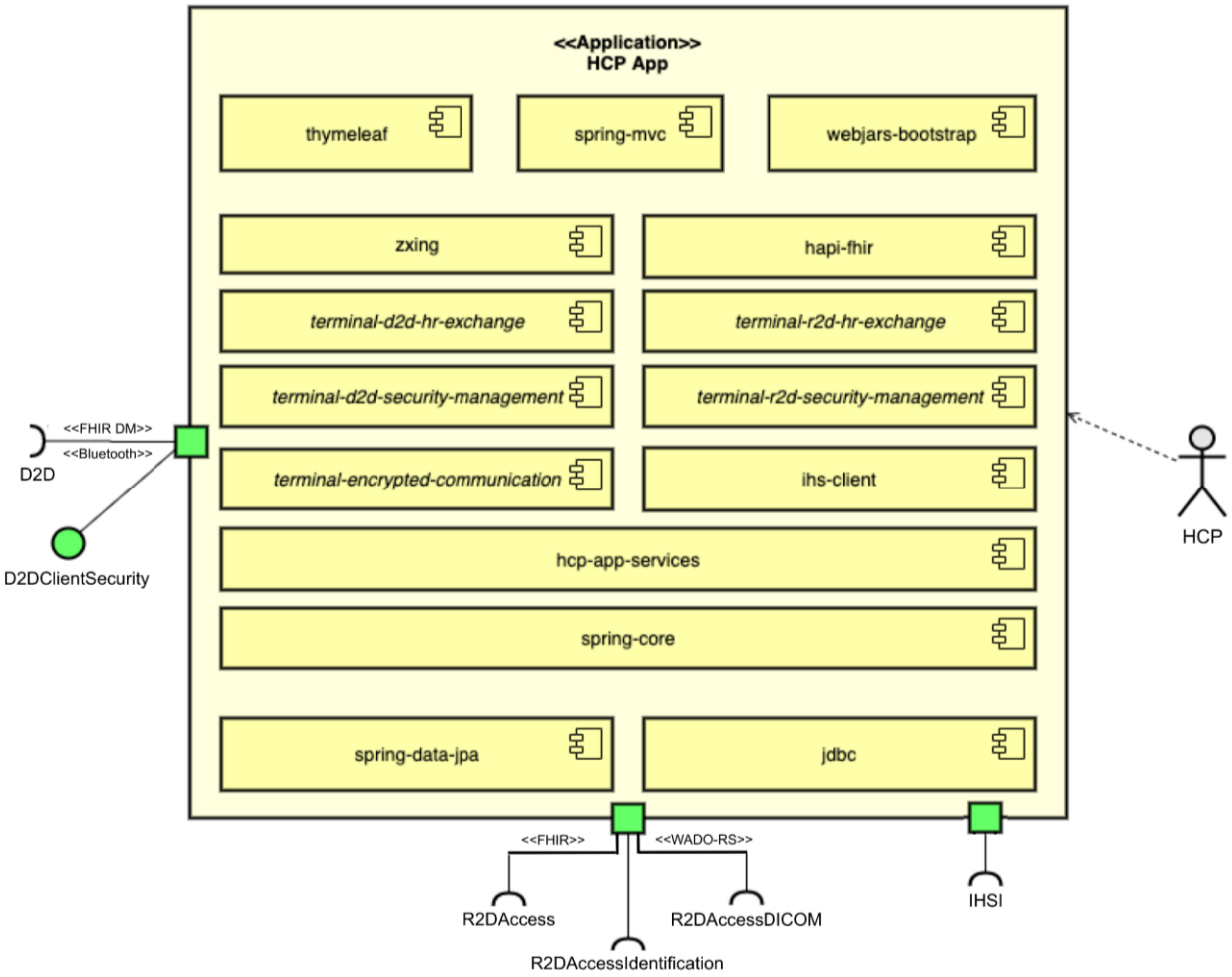

Figure 30 - HCP app internal view

The HCP App will be distributed as a microservice with all components included, and the installation on the Healthcare professional's terminal will consist of copying a single file.

4.9 R2D Access Server

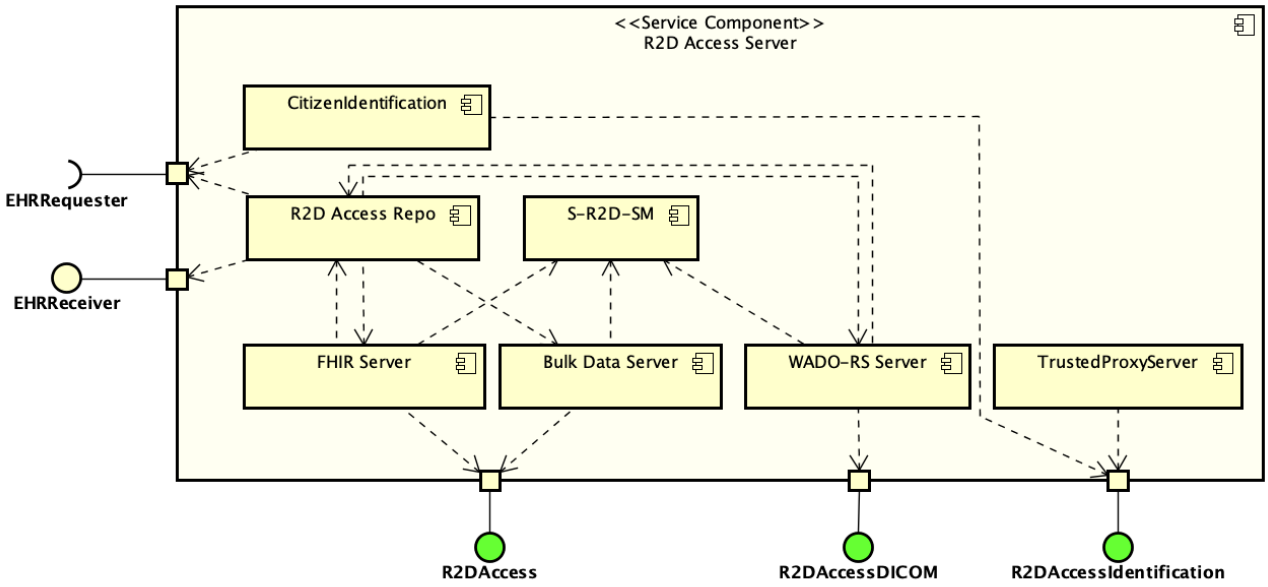

Figure 31 - IRS internal view

The R2D Access Server is the component of the InteropEHRate Framework that offers a reference implementation of the R2D Access Service. It implements the three interfaces of the R2D Access protocol and an additional interface (EHR Receiver) to interact with the EHR of the Healthcare Organisation. The remote Interface R2DAccessIdentification is partially implemented by the nested component called TrustedProxyServer and partially implemented by the next component called CitizenIdentification. The TrustedProxyServer implements the portion of the interface related to the interaction with eIDAS, while CitizenIdentification manages the requests of additional identification attributes that an healthcare organisation may ask to a citizen, as described in previous sections. It interacts with the healthcare organisation by means of the interface EHRRequester, in order to request the authentication of the Citizen on the EHR system.

The Interface R2DAccess is partially implemented by the nested FHIR Server and partially by the Bulk Data Server. The FHIR Server implements the standard FHIR REST API of the R2D Access protocol. It internally accesses the health by means of the component R2D Access Repo. This component requests health data to the EHR by means of the interface EHRRequester and receives health data from the EHR by means of the interface EHRReceiver and manages the files that the S-EHR App may download. The Bulk Data Server implements the portion of the FHIR HTTP API of R2D Access to download health data files (called Bulk data) asked by means of asynchronous requests.

Finally the R2D Access server may be extended with a WADO-RS Server to implement the interface R2DAccessDICOM. Similarly to the FHIR Server, the WADO-RS Server obtains the actual DICOM files by means of the mediation of R2D Access Repo.

The FHIR Server, the Bulk Data Server and the WADO-RS Server, all exploit the reusable library S-R2D-SM to check the eIDAs identity of the requester citizen and assure the security of the communication.

4.10 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, quantities, and names from the natural-language text contained in health data and expressed in multiple European languages.

The IHS component supports *semantic interoperability* where, beyond conversion to FHIR data schemas, data values in the 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 and interfaces of the IHS.

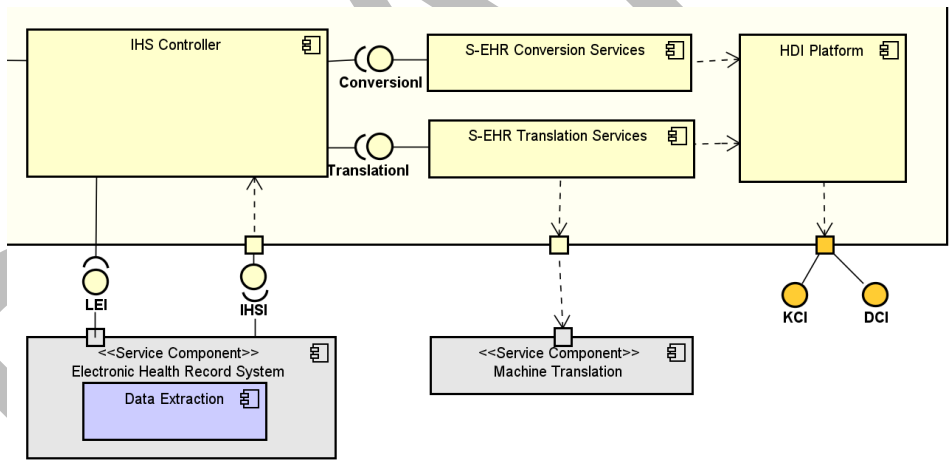

Figure 32 - IHS internal view

4.10.1 Health Data 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 6 - Conversion and Translation service functionalities

The Translation Service adopts two different methods to translate health data content, 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 thus operate on different kinds of data. 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 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.

4.10.2 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*.

4.10.3 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 the *IHS Interface (IHSI)*and the *Legacy EHR Interface (LEI)*, the latter 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 a supported format defined in [D5.8];
- 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", decomposing them into lower-level conversion and translation operations;
- serving requests to remote devices requesting patient data over the Internet;
- adapting the InteropEHRate Health Services to the local context and needs of the healthcare organisation, such as local language or local data formats.

4.11 Research Network Central Node RI

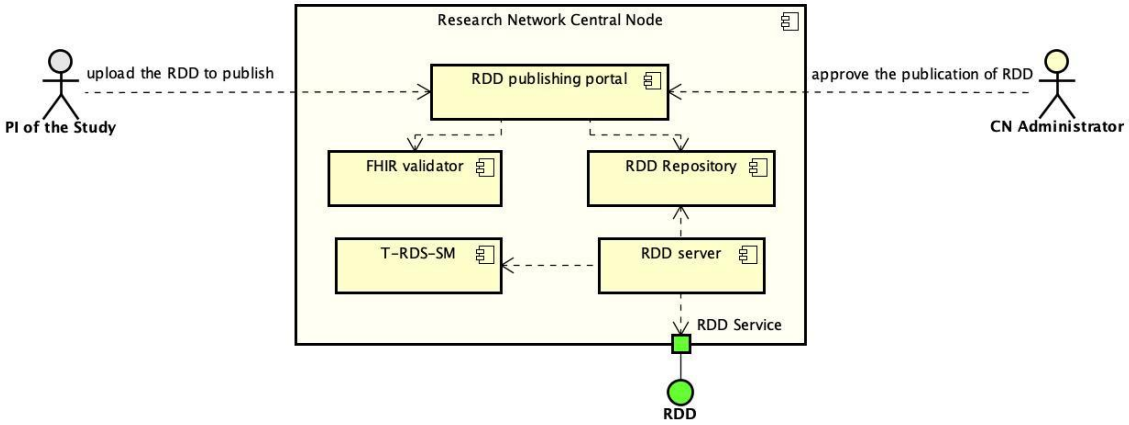

Figure 33 - IRS internal view

The *Research Network Central Node RI* is the reference implementation of a Research Network Central Node System (see section 2.5.7). It allows new studies to be published on the Research Network. The component is used by actors covering two different roles, the *PI of the Study*, that can upload the definition of a new research study (RDD), and the *CN Administrator*, in charge of approving the studies uploaded by the PI, and effectively publishing them on the Research Network.

The *PI of the Study* can upload the definition of a new study using a web portal provided by the CN, called RDD Publishing Portal, which offers a UI to upload and visualize the RDDs handled through the CN.

When a new RDD is uploaded, the component validates the FHIR structure and the content of the relative Research Definition Document (RDD), using a *FHIR validator* like shown in fig. 33. In case the RDD doesn't respect the InteropEHRate FHIR standard profile and/or the RDD content is not properly defined (i.e., using wrong data types), the FHIR validator will reject the upload of the RDD, providing the error to the RDD publishing portal, which will inform the PI about the upload failure. If the study upload succeeds, the relative RDD is saved internally in the CN within the *RDD Repository*. Once the RDD has been correctly uploaded, the *CN Administrator* can approve (or deny) the publication of that RDD through dedicated functionalities offered by the RDD publishing portal.

Once an RDD is published, it can be retrieved by any S-EHR App through the remote interface also called RDD. Such a service is served backend by the *RDD Server*, that is responsible for retrieving the published RDDs from the *RDD Repository*, and providing them to the requester S-EHR App. To maintain the trustability of the RDDs downloaded by the SEHR application, the *RDD Server* signs the data transmitted with a digital signature produced using the internal *T-RDS-SM* security library.

4.12 InteropEHRate Research Services (IRS)

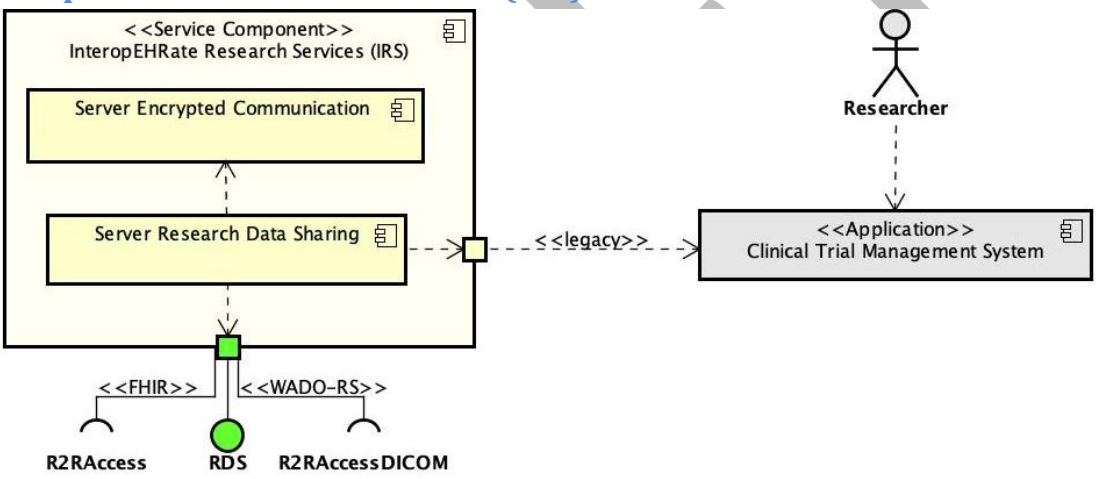

Figure 34 - IRS internal view

The component called *InteropEHRate Research Services (IRS)* provides the reference implementation of services exposed by Research Centres to enable the RDS protocol, as described in section 2.4.7. It implements 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. retrieving large anonymised health data files directly from citizens' healthcare organisations for research purposes, in case the files cannot be obtained from the mobile device;

5. forwarding citizen data to the requestor Research Centre.

4.13 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.

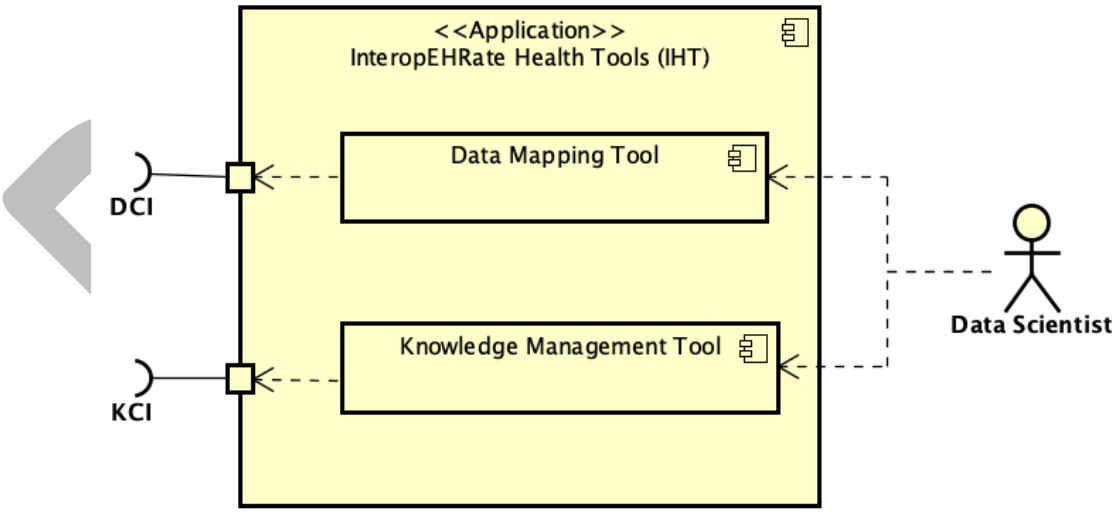

Figure 35 - IHT internal view

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 health data 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 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 local 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 health records. 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.

5 CONCLUSIONS AND NEXT STEPS

This report described the third and final version of the InteropEHRate standard architecture and of its reference implementation, the InteropEHRate framework. With respect to the previous version, the final version has been updated to satisfy the last version of user requirements and usage scenarios specified by the deliverable **[D2.3]**.

The main novelty of this last version is a better alignment between the different InteropEHRate protocols. While each one of the InteropEHRate protocols may be used individually, without requiring the other ones, a better synergy can be obtained by their combination. To simplify the adoption of the different protocols their specifications have been aligned so that, where it makes sense, similar operations may be performed with the different protocols. Now, all the protocols allow access to the health data in an incremental way, so as to limit the amount of data exchange and improve the performances of final applications for a better user experience. Both the D2D and the R2D Access protocol allows access to specific kinds of health data or to specific data items, giving more control to the applications and the users. A novelty of the last version of the specifications is also the combination with the WADO-RS protocol for supporting the remote access to DICOM files that have not been transmitted to the S-EHR App. The alignment of the specifications of the different protocols is expected to also allow a more consistent implementation of the libraries that are released as part of the InteropEHRate Framework.

Moreover, specific improvements have been applied to single protocols. The D2D protocol now includes the possibility to simplify the establishing of a secure Bluetooth connection when the same S-EHR app has to interact with different HCP Apps during the same medical visit, avoiding asking the citizen to scan a new QRCode for every terminal. The protocol R2D Access now supports asynchronous interactions to cover use cases where the availability of health data of the citizen is not immediate. Moreover, it includes a procedure to associate the legacy identity of patients to the eIDAS identity, to simplify the adoption of the protocol by healthcare organisations that never collected and stored the eIDAS identity for their patients. The specification of the protocols R2D Backup and R2D Emergency has been completely separated from the specification of R2D Access and enriched with specific audit capabilities. The new version of the protocol R2D Emergency exploits attribute-based Encryption (ABE) allowing controlled decryption depending on the attributes exhibited by the data requesters and also to provide better performance. The new specification of the RDS protocol now also covers security aspects that were not specified in the first version. Moreover, RDS now includes the possibility to collect questionnaire answers and supports both pseudonyms and pseudo-identity, offering different levels of anonymisation.

All the component diagrams and activity diagrams presented in this report have been updated to give evidence of the new capabilities of the protocols and to give better evidence of how the different libraries provided by the Framework are exploited by the S-EHR App, the HCP App and the S-EHR Cloud. The next activities of the InteropEHRate project will now focus on the implementation and validation of the portion of architecture that is required by the project pilots, that include almost all new specified features, with the exception of the interfaces R2DAccessDICOM and R2RAccessDICOM. They are not required by the pilots, as all DICOM images and signals involved in the pilots will be directly stored on the S-EHR App. While the specification of protocols is closed, some minor research activity is still envisioned, such as, in the case of D2D, to find a way to prioritize the data to be provided to the requesting party based on the HCP's medical specialty and historical data, and also to improve the exchange of large data sets with better lossless compression algorithms. In that way, the overall interaction and data transmission times will be reduced, without however affecting the overall data quality.

6 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	Purposes and methodology specified to collect and process a dataset of health and

Protocol	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 defining 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	The interface offered by the HealthCare organisation to support the R2D-Acccess

Interface	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 storing 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

- **[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

- **[BOYD 2003]** *Boyd, Colin and Mathuria, Anish. Protocols for Authentication and Key Establishment. 2003. Springer-Verlag Berlin Heidelberg. 10.1007/978-3-662-09527-0*

- **[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*

- **[D2.3]** InteropEHRate Consortium, D2.3*: User Requirements for cross-border HR integration - V3*, 2021 . www.interopehrate.eu/resources/#dels

- **[D2.9]** InteropEHRate Consortium, D2.9*: FHIR profile for EHR interoperability - V3*. Note that D2.9, final version of interoperability profiles, is due at December 2021. The previous version, D2.8-FHIR profile for EHR interoperability – V2, 2020, can be found at https://www.interopehrate.eu/resources/#dels

- **[D3.2]** InteropEHRate Consortium, D3.2*: Specification of S-EHR mobile privacy and security conformance levels - V2*. Note that D3.2, second version of *Specification of S-EHR mobile privacy and security conformance levels,* is due at December 2021. The previous version, D3.1 - *Specification of S-EHR mobile privacy and security conformance levels V1, 2020,* can be found at www.interopehrate.eu/resources/#dels

- **[D3.11]** InteropEHRate Consortium, D3.11-*Design of libraries for HR security and privacy services - V3*. Note that D3.11, third and final version of *Design of libraries for HR security and privacy services,* is due at December 2021. The previous version, D3.10 - *Design of libraries for HR security and privacy services V2, 2021,* can be found at www.interopehrate.eu/resources/#dels

- **[D4.3]** InteropEHRate Consortium, *D4.3-Specification of remote and D2D protocol and APIs for HR exchange - V3*, 2021. www.interopehrate.eu/resources/#dels

- **[D4.6]** InteropEHRate Consortium, D4.6-*Design of libraries for remote and D2D HR exchange - V3*. Note that D4.6, third and final version of *Design of libraries for remote and D2D HR exchange,* is due at December 2021. The previous version, D4.5 - *Design of libraries for remote and D2D HR exchange V2, 2021,* can be found at www.interopehrate.eu/resources/#dels

- **[D4.9]** InteropEHRate Consortium, *D4.9: Specification of protocol and APIs for research health data sharing - V2, 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)*, 2021 www.interopehrate.eu/resources/#dels

- **[DURGIN 2002]** *N. Durgin, J. Mitchell and D. Pavlovic, "A compositional logic for protocol correctness," in Proceedings 14th IEEE Computer Security Foundations Workshop, 2001., Cape Breton, Novia Scotia, Canada, 2001, doi: 10.1109/CSFW.2001.930150*
- **[ENISA 2020]** *ENISA. "Minimum Security Measures for Operators of Essentials Services". (2020).*
- **[eIDAS2018]** eIDAS-Node National IdP and SP Integration Guide, Version 2.1, 2018.
- **[EU CB ANNEX]** ANNEX to the Commission Recommendation of 6.2.2019 on a European Electronic Health Record exchange format
- **[GS]** *J. Camenisch and J. Groth."Group signatures: Better efficiency and new theoretical aspects", in: Security in Communication Networks. Springer, 2005, pp. 120-133.*
- **[HL7 FHIR]** HL7 Fast Healthcare Interoperability Resources Specification. http://hl7.org/fhir/
- **[ISO/IEC 2382:2015]** *ISO/IEC 2382:2015 Information technology — Vocabulary — Part 8: Security, 1998*
- **[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).
- **[NIST 2003]** National Institute of Standards and Technology. NIST SP 800-59, Guideline for Identifying an Information System as a National Security System, 2003 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf
- **[NIST 2014]** *National Institute of Standards and Technology. NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, 2014 https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf*
- **[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.*
- **[SCHIEDERMEIER 2019]** *M. Schiedermeier, O. Hasan, T. Mayer, L. Brunie, H. Kosch, A transparent referendum protocol with immutable proceedings and verifiable outcome for trustless networks, 2019, arXiv:1909.06462v1*
- **[SSPEAR 2014]** *S. Gisdakis, T. Giannetsos, and P. Papadimitratos. 2014. SPPEAR: security & privacy-preserving architecture for participatory-sensing applications. In Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks (WiSec '14). Association for Computing Machinery, New York, NY, USA, 39–50. DOI:https://doi.org/10.1145/2627393.2627402*

- **[WADO-RS]** Web Access to DICOM Objects by RESTful Services, http://dicom.nema.org/medical/dicom/current/output/html/part18.html#sect_10.4 https://www.dicomstandard.org/dicomweb/retrieve-wado-rs-and-wado-uri
- **[WBA]** Web Bluetooth Draft Community Group Report, 17 May 2021. https://webBluetoothcg.github.io/web-Bluetooth/
- **[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.*
- **[Zwingelberg 2011]** *Harald Zwingelberg, Marit Hansen. Privacy Protection Goals and Their Implications for eID Systems. PrimeLife. 2011: 245-260*
- [D5.8] InteropEHRate Consortium, *D5.8-Design of the data integration platform - V2*, 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
- [D5.14] InteropEHRate Consortium, *D5.14 - HCP Web App - V2,* 2021. www.interopehrate.eu/resources/#dels
- [D4.7] InteropEHRate Consortium, *D4.7 - Design of Health Record Index*, 2021. www.interopehrate.eu/resources/#dels
- [D4.18] InteropEHRate Consortium, D4.18 Libraries for research health data sharing - V2. This deliverable is due in March 2022 and will be available at www.interopehrate.eu/resources/#dels