EHE Security

Commercial Description

Version 5.1

1 Introduction

Electronic Healthcare Exchange (EHE) is a line of products fulfilling a variety of eHealth system needs, ranging from fundamental ones like infrastructure, security, and integration, over exchange and management of clinical documents and discrete medical information, to advanced functionalities like clinical decision support. Solutions made of different EHE products, alone or through integration with the existing infrastructure, support a wide range of processes in a healthcare system.

EHE Security is a product that enables the definition and implementation of security access rules and exchange and storage of information. The EHE Security product can ensure the enforcement of security rules based on the IHE IUA integration profile [1][2] and the recommendations of the HL7 FHIR standard (implementation profile SMART on FHIR Backend Services) [3], [4] for other components within the EHE product portfolio or for components that have been developed by Ericsson Nikola Tesla or other providers specifically for the needs of different projects.

The product enables the authentication and authorization of information systems and end users, the storage of audit records related to the security aspects of the use of services and data, and the non-repudiation of transactions using a digital signature.

EHE Security consists of the following components:

- user identity provider
- IHE ATNA (Audit Trail and Node Authentication) log
- digital signature management.

2 Functionality Description

The following chapters describe the components that make up EHE Security product.

2.1 User Identity Provider

The User Identity Provider component enables verification and confirmation of identity and authentication of users - end users and information systems – of protected services and applications.

To enable the authentication and authorization of end users, they must be registered in the user repository and their roles, i.e., access rights to individual applications and services of the central system, must be defined. End users are registered in the user repository either via synchronization with some external existing user repository (e.g. Lightweight Directory Access Protocol, LDAP) or can be manually created via a user management application.

To be able to carry out authentication and authorization of external information systems, each information system must be registered, and its security parameters must be defined. External systems are registered using the external systems management application.

This component conforms to the IHE IUA interaction profile and implements the Authorization Server component. According to the specified integration profile, the component implements the following transactions:

- Get Access Token [ITI-71] – access token retrieval in accordance with the OAuth2 specification for information systems, that is, the OIDC specification for end users
- Introspect Token [ITI-102] – verifying the token specified in the request.

According to the IHE IUA integration profile, information systems that independently use certain solution services or applications and information systems used by end users must implement the Authorization Client component of the integration profile and the Incorporate Access Token transaction [ITI-72]. The transaction defines that clients must include either the received token or the session identifier in every request they send to protected resources, based on which the required token can be retrieved from the authorization server.

2.2 ATNA Audit Log

This component enables the storage and review of audit and security records in accordance with the IHE ATNA integration profile [5]. The stored audit log records must comply with the audit log records specification of the individual IHE integration profile used to create, retrieve, and manage data.

The following required audit data is stored in this subsystem:

- starting and stopping the module or component according to the IHE ATNA [5]profile
- access to patient demographic data in accordance with IHE PDQm [6] and IHE PIXm [7] integration profiles
- changing the patient demographic data in accordance with the IHE PMIR [8] integration profile
- access to a patient's medical data in accordance with the IHE QEDm [9] integration profile
- access, storage, and management of patient documents in accordance with the IHE MHD [10] integration profile
- successful user authentication and authorization (end users and external information systems)

- creation of visits and management of visit data
- creating cases and managing case data.

2.3 Digital Signature Management

This component enables verification of the digital signature of messages and documents that are exchanged with information systems in healthcare in accordance with the HL7 FHIR standard and JWS (JSON Web Signature) specifications [14].

To ensure the non-repudiation of information and requests transmitted by documents and messages, each document and message must be signed with a digital certificate of the end user who is defined as the author of a certain message or document. To verify that documents and messages have not been altered after the application has been signed, modules use this component to verify the validity of the digital signature.

3 Interdependencies

EHE Security depends on the following components:

- EHE Infrastructure [11]
- EHE FHIR Repository [12][11] – it is also possible to use other providers' data repository compliant with the FHIR R4 standard
- EHE Terminology Services [13][12] – it is also possible to use other providers' terminology repository and terminology service provider that are compliant with the FHIR R4 standard and the IHE SVCM integration profile.

To implement the EHE Security product, it is necessary to provide a PostgreSQL or Oracle relational database and the Ubuntu Linux operating system.

EHE Security product components can be installed on physical servers, virtual machines, or containers.

4 Free and Open Source Software

This product uses free and open source software (FOSS) components with the following licenses:

- Apache Software License 2.0 [15]
- MIT License [16]
- Eclipse Distribution License [17]

- Eclipse Public License [18]
- Creative Commons CC0 [19]
- BSD License (2 clause and 3 clause) [20]
- Bouncy Castle License [21]
- Common Development and Distribution License [22]
- GNU Library General Public License [23]
- Mozilla Public License (MPL) [24]
- Elastic license v2 [25].

5 Version

The current product version is 5.1.

6 References

[1] IHE (Integrating the Healthcare Enterprise) – This is a joint initiative of healthcare professionals and industry with the aim of improving the way in which information systems and applications in healthcare exchange information by defining integration profiles that determine standards to solve common integration tasks in healthcare (https://ihe.net).

[2] IHE IUA (Internet User Authorization) – integration profile that defines the authentication and authorization mechanisms of end users and information systems that access web services and/or applications of information systems in healthcare, specification available at https://profiles.ihe.net/ITI/IUA/index.html.

[3] HL7 FHIR - This is a standard that describes data formats and elements and an application programming interface for electronic health record exchange. It was created by Health Level Seven, an international health standards organization. Specification available at https://www.hl7.org/fhir/.

[4] SMART on FHIR Backend Services– implementation profile that defines the standard and mechanisms of authorization and authentication of applications and systems that use the HL7 FHIR standard for information exchange, specification available at https://hl7.org/fhir/uv/bulkdata/authorization/index.html

[5] IHE ATNA (Audit Trail and Node Authentication) – profile that defines the security/privacy model, specification available at https://wiki.ihe.net/index.php/Audit_Trail_and_Node_Authentication.

[6] IHE PDQm (Patient Demographics Query for Mobile) – profile defines a lightweight RESTful interface to a patient demographics supplier – specification available at https://profiles.ihe.net/ITI/PDQm/.

[7] IHE PIXm (Patient Identifier Cross-Reference for Mobile) – profile defines a lightweight RESTful interface to a Patient Identifier Cross-reference Manager, leveraging technologies readily available to mobile applications and lightweight browser based applications – specification available at https://profiles.ihe.net/ITI/PIXm/index.html.

[8] IHE PMIR (Patient Master Identity Registry) – profile provides a RESTful patient identity management – specification available at https://profiles.ihe.net/ITI/PMIR/.

[9] IHE QEDm (Query for Existing Data for Mobile) – profile that defines the search and retrieval of clinical data elements (FHIR resources such as Observation, Condition, Medication...) - specification available at https://wiki.ihe.net/index.php/Query_for_Existing_Data_for_Mobile_(QEDm).

[10] IHE MHD (Mobile access to Health Documents) – profile that defines a simple interface for document sharing – specification available at https://profiles.ihe.net/ITI/MHD/.

[11] EHE Infrastructure – standard Ericsson Nikola Tesla’s product which implements the functions necessary for the operation, internal communication, and monitoring of the components of the solution.

[12] EHE FHIR Repository - standard Ericsson Nikola Tesla’s product which enables data management and storage based on the HL7 FHIR standard.

[13] EHE Terminology Services – standard Ericsson Nikola Tesla’s product which enables the use of terminologies, terminological operations, and management of terminologies (code lists, concept groups, concept maps) based on the HL7 FHIR standard and the IHE SVCM integration profile.

[14] JWS (JSON Web Signature) https://www.rfc-editor.org/rfc/rfc7515

[15] Apache Software License 2.0 https://www.apache.org/licenses/LICENSE-2.0.txt

[16] MIT License https://opensource.org/licenses/MIT

[17] Eclipse Distribution License https://www.eclipse.org/org/documents/edl-v10.php

[18] Eclipse Public License https://www.eclipse.org/legal/epl-v10.html https://www.eclipse.org/legal/epl-2.0/

[19] Creative Commons CC0 https://creativecommons.org/publicdomain/zero/1.0/

[20] BSD License https://opensource.org/licenses/BSD-2-Clause https://opensource.org/licenses/BSD-3-Clause

[21] Bouncy Castle Licence https://www.bouncycastle.org/licence.html

[22] Common Development and Distribution License
https://opensource.org/licenses/CDDL-1.0

[23] GNU Library General Public License
https://www.gnu.org/licenses/old-licenses/lgpl-2.0.html

[24] Mozilla Public License (MPL)
https://www.mozilla.org/media/MPL/2.0/index.48a3fe23ed13.txt

[25] Elastic license
https://www.elastic.co/licensing/elastic-license