# EHE Security

## Komercijalni opis

Verzija 5.1

# 1 Uvod

Electronic Healthcare Exchange (EHE) linija je proizvoda koji zadovoljavaju različite potrebe sustava eZdravstva, od temeljnih kao što su infrastruktura, sigurnost i integracija, preko upravljanja kliničkim dokumentima i povjerljivim medicinskim podacima te njihove razmjene, do naprednih funkcionalnosti kao što je podrška kliničkom odlučivanju. Rješenja sastavljena od različitih EHE proizvoda, samostojeća ili integrirana s postojećom infrastrukturom, podržavaju širok raspon procesa u zdravstvenom sustavu.

EHE Security je proizvod koji omogućava definiranje i provođenje sigurnosnih pravila pristupa te razmjene i pohrane informacija. Proizvod EHE Security može osigurati provođenje sigurnosnih pravila temeljeno na integracijskom profilu IHE IUA [1][2] i preporukama standarda HL7 FHIR (implementacijski profil SMART *on* FHIR *Backend Services*) [3][4] za komponente drugih proizvoda iz EHE portfelja ili za komponente koje su razvili Ericsson Nikola Tesla ili drugi proizvođači specifično za potrebe određenog projekta.

Proizvod omogućava autentikaciju i autorizaciju informacijskih sustava i krajnjih korisnika, pohranu revizijskih zapisa vezanih za sigurnosne aspekte korištenja usluga i podataka te neporecivost transakcija korištenjem digitalnog potpisa.

EHE Security se sastoji od sljedećih komponenti:

- pružatelj potvrde identiteta korisnika
- IHE ATNA (en. *Audit Trail and Node Authentication*) revizijski zapis
- upravljanje digitalnim potpisom.

# 2 Opis funkcionalnosti

U idućim potpoglavljima dan je opis komponenti koje čine EHE Security.

## 2.1 Pružatelj potvrde identiteta korisnika

Komponenta pružatelja potvrde identiteta omogućuje provjeru i potvrdu identiteta te autentikaciju korisnika (krajnjih korisnika i informacijskih sustava), zaštićenih usluga i aplikacija.

Kako bi se omogućila autentikacija i autorizacija krajnjih korisnika, oni moraju biti registrirani u repozitoriju korisnika te im moraju biti definirane uloge, odnosno, prava pristupa pojedinim aplikacijama i uslugama centralnog sustava. Krajnji korisnici se registriraju u repozitoriju korisnika ili putem sinkronizacije s nekim vanjskim, postojećim, repozitorijem korisnika (npr. *Lightweight Directory Access Protocol*, LDAP) ili se mogu ručno kreirati putem aplikacije za upravljanje korisnicima.

Kako bi se mogla provesti autentikacija i autorizacija vanjskih informacijskih sustava svaki informacijski sustav mora biti registriran te moraju biti definirani

njegovi sigurnosni parametri. Vanjski sustavi se registriraju korištenjem aplikacije za upravljanje vanjskim sustavima.

Ova komponenta je usklađena s interacijskim profilom IHE IUA i implementira komponentu *Autorization Server*. Prema navedenom integracijskom profilu komponenta implementira sljedeće transakcije:

- *Get Access Token* [ITI-71] – dohvat pristupnog tokena u skladu s OAuth2 specifikacijom za informacijske sustave, odnosno, OIDC specifikaciji za krajnje korisnike
- *Introspect Token* [ITI-102] – provjera tokena navedenog u zahtjevu.

Prema integracijskom profilu IHE IUA, informacijski sustavi koji samostalno koriste određene usluge rješenja ili aplikacije i informacijski sustavi koje koriste krajnji korisnici moraju implementirati komponentu *Authorization Client* integracijskog profila i transakciju *Incorporate Access Token* [ITI-72]. Ova transakcija definira da klijenti moraju u svaki zahtjev koji šalju prema zaštićenim resursima uključiti ili dobiveni token ili identifikator sesije na osnovi koje se može dohvatiti potreban token iz autorizacijskog servera.

## 2.2 IHE ATNA revizijski zapis

Ova komponenta omogućava pohranu i pregled revizijskih i sigurnosnih zapisa u skladu s integracijskim profilom IHE ATNA [5]. Revizijski zapisi koji se spremaju moraju biti usklađeni sa specifikacijom revizijskih zapisa pojedinog IHE integracijskog profila koji se koristi za kreiranje, dohvat i upravljanje podatcima.

U ovaj podsustav se spremaju sljedeći nužni revizijski podatci:

- pokretanje i zaustavljanje modula ili komponente u skladu s profilom IHE ATNA [5]
- pristup demografskim podatcima pacijenta u skladu s integracijskim profilima IHE PDQm [6] i IHE PIXm [7]
- izmjena demografskih podataka pacijenta u skladu s integracijskim profilom IHE PMIR [8]
- pristup medicinskim podatcima pacijenta u skladu s integracijskim profilom IHE QEDm [9]
- pristup, spremanje i upravljanje dokumentima pacijenta u skladu s integracijskim profilom IHE MHD [10]
- uspješna autentikacija i autorizacija korisnika (krajnjih korisnika i vanjskih informacijskih sustava)
- kreiranje posjeta i upravljanje podatcima o posjetama
- kreiranje slučajeva i upravljanje podatcima o slučajevima.

### 2.3 Upravljanje digitalnim potpisom

Ova komponenta omogućava provjeru digitalnog potpisa poruka i dokumenata koji se razmjenjuju s informacijskim sustavima u zdravstvu sukladno standardu HL7 FHIR i specifikacijama JWS (JSON *Web Signature*) [14].

Kako bi se osigurala neporecivost informacija i zahtjeva koji se prenose dokumentima i porukama svaki dokument i poruka moraju biti potpisani digitalnim certifikatom krajnjeg korisnika koji je definiran kao autor određene poruke, odnosno, dokumenta. Kako bi se provjerilo da dokumenti i poruke nisu promijenjeni nakon potpisa aplikacije, moduli koriste ovu komponentu kako bi se provjerila ispravnost digitalnog potpisa.

## 3 Međuovisnosti

EHE Security ovisi o sljedećim komponentama:

- EHE Infrastructure [11]
- EHE FHIR Repository [12] – moguće je koristiti i repozitorij podataka drugih proizvođača usklađen sa standardom FHIR R4
- EHE Terminology Services [13] – moguće je koristiti i repozitorij terminologija i pružatelj terminoloških usluga drugih proizvođača koji su usklađeni sa standardom FHIR R4 i integracijskim profilom IHE SVCM.

Za implementaciju proizvoda EHE Security potrebno je osigurati relacijsku bazu podataka PostgreSQL ili Oracle i operativni sustav Ubuntu Linux.

Komponente proizvoda EHE Security moguće je instalirati na fizičke poslužitelje, u virtualne mašine ili kontejnere.

## 4 Komponente otvorenog koda

Ovaj proizvod koristi komponente otvorenog koda (en. *Free and Open Source Software, FOSS*) sa sljedećim licencama:

- 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 Licence [21]
- Common Development and Distribution License [22]
- GNU Library General Public License [23]
- Mozilla Public License (MPL) [24]
- Elastic license v2 [25].

# 5 Verzija

Aktualna verzija proizvoda je 5.1.

# 6 Reference

[1] IHE (en. Integrating the Healthcare Enterprise) – Zajednička je inicijativa zdravstvenih profesionalaca i industrije s ciljem unapređenja načina na koji informacijski sustavi i aplikacije u zdravstvu razmjenjuju informacije. Taj cilj se postiže putem definiranja integracijskih profila koji određuju standarde za rješavanje uobičajenih integracijskih zadataka u zdravstvu (https://ihe.net).

[2] IHE IUA (*Internet User Authorization*) – integracijski profil koji definira mehanizme autentikacije i autorizacije krajnjih korisnika i informacijskih sustava koji pristupaju *web* uslugama i/ili aplikacijama informacijskih sustava u zdravstvu – specifikacija dostupna na https://profiles.ihe.net/ITI/IUA/index.html.

[3] HL7 FHIR – Ovo je standard koji opisuje formate podataka i elemente te sučelje za programiranje aplikacija za razmjenu elektroničkih zdravstvenih zapisa. Kreirala ga je Health Level Seven organizacija za međunarodne zdravstvene standarde. Specifikacija dostupna na https://www.hl7.org/fhir/.

[4] SMART *on* FHIR *Backend Services*– implementacijski profil koji definira standard i mehanizme autorizacije i autentikacije aplikacija i sustava koji koriste HL7 FHIR standard za razmjenu informacija, specifikacija dostupna na https://hl7.org/fhir/uv/bulkdata/authorization/index.html

[5] IHE ATNA (*Audit Trail and Node Authentication*) – profil koji definira model sigurnosti/privatnosti, specifikacija dostupna na https://wiki.ihe.net/index.php/Audit_Trail_and_Node_Authentication

[6] IHE PDQm (en. *Patient Demographics Query for Mobile*) – profil koji definira jednostavno RESTful sučelje prema pacijentovim demografskim podacima – specifikacija dostupna na https://profiles.ihe.net/ITI/PDQm/.

[7] IHE PIXm (en. *Patient Identifier Cross-Reference for Mobile*) – profil koji definira jednostavno RESTful sučelje za dohvaćanje pacijentovih identifikatora u različitim domenama – specifikacija dostupna na https://profiles.ihe.net/ITI/PIXm/index.html.

[8] IHE PMIR (en. *Patient Master Identity Registry*) – profil koji podržava kreiranje i ažuriranje podataka pacijenta koristeći HL7 FHIR resurse i RESTful transakcije – specifikacija dostupna na https://profiles.ihe.net/ITI/PMIR/.

[9] IHE QEDm (en. *Query for Existing Data for Mobile*) – profil koji definira pretragu i dohvaćanje kliničkih podatkovnih elemenata (FHIR resursi poput *Observation*, *Condition*, *Medication*…) – specifikacija dostupna na https://wiki.ihe.net/index.php/Query_for_Existing_Data_for_Mobile_(QEDm).

[10] IHE MHD (en. *Mobile access to Health Documents*) – profil koji definira jednostavno sučelje za dijeljenje dokumenata – specifikacija dostupna na https://profiles.ihe.net/ITI/MHD/.

[11] EHE Infrastructure – standardni proizvod tvrtke Ericsson Nikola Tesla d.d. koji implementira funkcije potrebne za rad, internu komunikaciju i nadzor komponenti rješenja.

[12] EHE FHIR Repository - standardni proizvod tvrtke Ericsson Nikola Tesla d.d. koji omogućava upravljanje i pohranu podataka temeljenu na HL7 FHIR standardu.

[13] EHE Terminology Services – standardni proizvod tvrtke Ericsson Nikola Tesla d.d. koji omogućava korištenje terminologija, terminoloških operacija i upravljanje terminologijama (kodnih listi, skupina koncepata, mapa koncepata) temeljeno na standardu HL7 FHIR i integracijskom profilu IHE SVCM.

[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