Systeem voor end-to-endversleuteling

Wat is de dienst End to End Encryption van het eHealth-platform?

De dienst End to End Encryption (ETEE) (ook wel versleutelings- of encryptiedienst genoemd) van het eHealth-platform is een reeks diensten die toelaten berichten gericht aan zorgverleners (individuele zorgverleners of instellingen) te versleutelen. Deze diensten zijn toegankelijk voor individuele zorgverleners en instellingen en in sommige gevallen ook voor patiënten.

De versleutelingsdiensten worden onder meer toegepast in het kader van het gebruik van de eHealthBox-dienst of de elektronische voorschriften (Recip-e).

De ETEE-diensten zijn de volgende:

- ETKDepot (SOAP & REST) en KeyDepot (REST) voor de versleuteling naar een gekende bestemmeling
- KGSS(SOAP & REST) voor de versleuteling naar een niet-gekende bestemmeling

De ETEE-diensten zijn beschikbaar als webservices (toegankelijk via een medisch softwarepakket of via een externe toepassing).

Welke functionaliteiten biedt de dienst End to End Encryption?

De webservice ETKDepot is toegankelijk voor iedereen en biedt de volgende functionaliteiten:

- de opzoeking van een ETK, dit wil zeggen de publieke sleutel die verbonden is aan het eHealthcertificaat van een zorgverlener of een instelling waarvan de identificatienummers (INSZ, RIZIV-nummer, KBO-nummer) gekend zijn. Aan de hand van de REST-dienst kan tevens de certificaathouder worden achterhaald.

    - eens verkregen, laat die ETK toe om een bericht te versleutelen ter attentie van een gekende bestemmeling (de zorgverlener of instelling).

De webservice KGSS (Key Generation and Storage System) is toegankelijk voor iedereen en biedt de volgende functionaliteiten:

- de aanmaak van een symmetrische encryptiesleutel die opgeslagen zal worden door het eHealth-platform en die toegankelijk zal zijn volgens de voorwaarden van degene die de sleutel heeft aangemaakt;
- het ophalen van een bestaande sleutel, op voorwaarde dat het identificatienummer van de sleutel gekend is en de toegangsvoorwaarden die vastgesteld werden bij de aanmaak van de sleutel voldaan zijn (bijvoorbeeld: geauthenticeerd zijn als apotheker erkend door het eHealth-platform).
- dankzij de REST-dienst is het tevens mogelijk voor de houder om een bestaande sleutel te verwijderen

Deze functionaliteiten laten toe de dienst KGSS te gebruiken indien de identiteit van de bestemmeling van het versleutelde bericht niet op voorhand gekend is, maar dat bepaalde voorwaarden voldaan moeten zijn om de encryptiesleutel te verkrijgen.

De webservice KeyDepot is voor alle doelgroepen toegankelijk en biedt de volgende functies:

- De aanmaak van een sleutelpaar; de openbare sleutel zal door het eHealth-platform worden opgeslagen en voor alle doelgroepen toegankelijk zijn
- De toevoeging van informatie voor een reeds bestaande openbare sleutel door de houder ervan
- De opzoeking van een openbare sleutel
- De verwijdering van openbare sleutels door de houder ervan
- De opzoeking van alle openbare sleutels met betrekking tot een persoon
- De opzoeking van het 'attestation object' met betrekking tot een openbare sleutel
- De opzoeking van informatie over de houder van een sleutel

In de praktijk

Afhankelijkheden, aanbevelingen en waarschuwingen

Om gebruik te maken van de webservice ETKDepot of de webservice KGSS, dient de zorgverlener of de patiënt te beschikken over een medisch softwarepakket waarin deze dienst geïntegreerd is. Beide diensten zijn ook geïntegreerd in globalere oplossingen zoals Recip-e, Hoofdstuk IV, eHealthBox.

Er is een technische bibliotheek beschikbaar ter ondersteuning van uw versleutelingsbewerkingen.

Wat zijn de voorwaarden voor de integratie van de dienst End to End Encryption van het eHealth-platform?

- Neem contact op met de verantwoordelijke projectleider binnen het eHealth-platform Kris Van Aken en schets duidelijk de context, het doeleinde en het geschatte volume van uw project.

Stuur een e-mail om meer informatie te vragen