

Deze mededeling heeft betrekking op de SOAP-aanroepen, zowel voor de eenvoudig beveiligde webservices X509 als voor de webservices die door een SAML-token worden beveiligd.

Gelieve deze mail aandachtig te lezen. Zo niet kan er een impact zijn op uw gebruik van de SOAP webservices van het eHealth-platform.

Mevrouw, Mijnheer,

Om de veiligheid van onze toepassingen en van de gegevensuitwisselingen tussen de verschillende actoren in de gezondheidszorg te garanderen, herziet het eHealth-platform permanent zijn minimale veiligheidsnormen.

Deze mail wordt u toegestuurd omdat u momenteel als gebruiker van onze SOAP webservices bent gekend.

Tenzij wij ons vergissen, stellen we vast dat u nog steeds het hashalgoritme SHA-1 gebruikt.

Ter herinnering, dit veiligheidsniveau is niet meer voldoende. Het gebruik ervan moet absoluut worden vermeden in het kader van de elektronische handtekening.

Het hash- en handtekeningsalgoritme dat door het eHealth-platform wordt aanbevolen is SHA-256.

Deze wijziging gaat effectief in productie in oktober 2023 (eHealth release 2023.2).

U moet voor die datum iets ondernemen omdat we op dat ogenblik de strikte verificatie van de algoritmen SHA-256 implementeren.

Indien u niets onderneemt, zal uw integratie op de SOAP-webservices van het eHealth-platform niet meer werken.

- Acceptatie 21-08-2023
- Productie 15-10-2023

Indien u geen gebruiker bent van de eHealth Connector

Via deze mail wordt u verzocht om 2 gelijktijdige migraties te verrichten:

1. **De overschakeling naar een nieuwe versie van de STS (indien nodig)**

De volgende URL van de STS wordt buiten gebruik genomen: /IAM/Saml11TokenService/v1

Indien u deze nog gebruikt, wordt u verzocht het nodige te doen om **de nieuwe versie van de SecurityTokenService (WS-Trust)** te gebruiken die de meest recente algoritmes voor hashing (SHA-256) en ondertekening (RSA-SHA-256 / ECDSA-SHA-256) ondersteunt in overeenstemming met de huidige veiligheidsnormen.

- [/IAM/SecurityTokenService/v1](#)
- [/IAM/SecurityTokenService/v1](#)

Voor meer technische informatie over de SecurityTokenService ([cookbook](#))

1. Het gebruik van de nieuwe algoritmen voor hashing/ondertekening

Gelieve ervoor te zorgen dat uw **handtekening WS-Security op de SOAP business services tevens migreert naar SHA-256**. Deze veranderen niet van endpoint, en ondersteunen momenteel zowel de SHA-1 als de SHA-256-handtekeningen.

Deze opmerking geldt voor elk beroep op de SOAP, zowel voor de eenvoudig beveiligde webservices X509 als voor de via een SAML-token beveiligde webservices (de token zal vervolgens worden bezorgd door de nieuwe versie van de SecurityTokenService, vermeld in punt 1 hierboven).

Voor meer informatie over de beveiliging van de webservices: ([cookbook](#))

Indien u de eHealth Connector gebruikt

Gelieve over te schakelen naar een nieuwe versie van de connector, minimaal naar versie 4.1.2. Vanaf die versie van de technische connector (en de verschillende business connectoren) is het mogelijk om over te schakelen naar de nieuwe versie van de SecurityTokenService en de algoritmen voor hashing/ondertekening in SHA-256 te wijzigen voor de oproepen op de verschillende business-diensten door de `be.ehealth.technicalconnector.properties` aan te passen.

De vereiste configuratie die in uw systeem moet worden gewijzigd, is de volgende

```
default.rsa.digest.method.algorithm=(Link)
```

```
default.rsa.signature.method.algorithm=(Link)
```

```
service.sts.class=be.ehealth.technicalconnector.service.sts.impl.STSServiceWsTrustImpl
```

De nieuwe versie van de connector 4.2.x zal standaard evolueren naar deze waarden SHA-256 en STS WS-Trust.

Met deze versie is het dus mogelijk om terug te keren naar de vorige standaardwaarden, dit wordt wel niet aanbevolen:

```
default.rsa.digest.method.algorithm=(Link)
```

default.rsa.signature.method.algorithm=([Link](#))

service.sts.class=be.ehealth.technicalconnector.service.sts.impl.STSServiceImpl

Indien u niet de persoon bent die verantwoordelijk is voor deze wijzigingen, gelieve deze informatie door te sturen naar uw informaticadienst.

Voor bijkomende informatie, aarzel niet om contact op te nemen met onze ondersteuningsdienst via het volgende mailadres: support@ehealth.fgov.be