Cette communication se réfère à tout appel SOAP, que ce soit pour les webservices sécurisés en simple X509, que pour les webservices sécurisés par un token SAML.

Merci de lire ce mail attentivement sinon un impact pourrait être prévu sur votre utilisation des webservices SOAP de la Plateforme eHealth.

Madame, Monsieur,

Afin de garantir la sécurité de nos applications et des échanges de données réalisés entre les différents acteurs en soins de santé, la Plateforme eHealth revoit continuellement ses normes minimales en terme de sécurité.

Ce mail vous parvient car vous êtes actuellement connu comme utilisateur au niveau nos webservices SOAP.

Sauf erreur de notre part nous constatons que vous utilisez toujours l'algorithme de hashage SHA-1.

Pour rappel, ce niveau de sécurité n'est plus suffisant et son utilisation doit absolument être évitée dans le contexte de la signature électronique.

L'algorithme de hashage et signature actuellement recommandé par la Plateforme eHealth est SHA-256.

Cette modification sera effectif en production en Octobre 2023 (eHealth release 2023.2).

Vous êtes tenu d'agir avant cette date, car nous mettrons à ce moment en œuvre la vérification stricte des algorithmes SHA-256.

Sans action de votre part, votre intégration avec les webservices SOAP de la Plateforme eHealth ne fonctionnera plus.

- Acceptance 21-08-2023
- Production 15-10-2023

Si vous n'êtes pas un utilisateur du eHealth Connector

Par ce mail on vous demande 2 migrations simultanées:

1. **Le passage à un nouvelle version du STS (si besoin)**

L'URL suivante de STS est en phase de décommissionnement: /IAM/Saml11TokenService/v1

Si vous utilisez encore celle-ci, nous vous prions de faire le nécessaire afin d'utiliser **la nouvelle version du SecurityTokenService (WS-Trust)** supportant les derniers algorithmes de hashage (SHA-256) et signature (RSA-SHA-256) conformes aux normes de sécurité actuelles.

- /IAM/SecurityTokenService/v1
- /IAM/SecurityTokenService/v1

Plus d'informations techniques sur le SecurityTokenService (Cookbook)

1. **L'utilisation des nouveaux algorithmes de hashage/signature**

Veuillez faire de sorte que votre **signature WS-Security sur les services SOAP business migre également vers du SHA-256**. Ceux-ci ne changent pas de endpoint, et supportent actuellement autant les signatures SHA-1 et SHA-256.

Cette remarque est valide pour tout appel SOAP, que ce soit pour les webservices sécurisés en simple X509, que pour les webservices sécurisés par un token SAML (le token alors délivré par la nouvelle version du SecurityTokenService, mentionné ci-dessus dans le point 1.).

Plus d'informations techniques sur la sécurisation des services web: (Cookbook)

Si vous êtes un utilisateur du eHealth Connector

Veuillez passer à une nouvelle version du connecteur, au moins en version 4.1.2.
A partir de cette version du connecteur technique (et des différents connecteurs business), il est possible de basculer vers la nouvelle version du SecurityTokenService et de modifier les algorithmes de hashage/signature en SHA-256 sur les appels vers les différents services business en modifiant le be.ehealth.technicalconnector.properties.

La configuration requise et donc à modifier dans votre système est la suivante

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

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

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

La nouvelle version du connecteur 4.2.x passera à ces valeurs SHA-256 et STS WS-Trust par défaut.

Avec cette version - ceci n'est donc pas recommandé - il sera alors possible de revenir aux valeurs par défaut précédentes:

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

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

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

Si vous n’êtes pas responsable de ces changements, veuillez transmettre ces informations à votre service informatique.

Pour toute demande d’informations complémentaires, veuillez contacter notre équipe de support via l'adresse mail : support@ehealth.fgov.be