eHealth Service management message 19/05/2025

Ce message est destiné aux intégrateurs des services de la plateforme eHealth qui utilisent la CryptoLIB.

Suite aux problèmes rencontrés par certains packages providers et partenaires, nous avons décidé de **reporter** cette intervention.
Une communication ultérieure suivra avec de nouvelles dates de mise en production.

Toutefois, nous vous conseillons vivement de ne pas mettre en pause les efforts que vous avez déjà réalisés concernant l'implémentation des changements pour prendre en charge la nouvelle méthode cryptographique ECC.
Vous devez donc continuer à implémenter et tester sans attendre la nouvelle communication.

Cryptolib Version
Les problèmes rencontrés sont principalement liés à des partenaires qui n'utilisent pas encore la dernière version **cryptolib** (version **2.3.0**) qui exige l'utilisation de **Java 8**.
C'est donc un point d'attention (et potentielle adaptation) que nous souhaitons vous rappeler par le biais de cette communication.

D'autrepart, nous avons conservé la possiblité de demander des certificats RSA, uniquement en acceptation, afin de ne pas vous bloquer dans vos développements et tests de non régresssion

Vous trouverez via le lien https://www.ehealth.fgov.be/ehealthplatform/fr/service-certificats-ehealth les URLS vers les versions RSA et ECC au niveau du paragraphe "Evolution du ETEE Certificate Manager (RSA - ECC)"

Changement de méthode cryptographique pour les certificats eHealth

Les acteurs des soins de santé peuvent obtenir via la Plate-forme eHealth des certificats eHealth (avec les paires de clés y associées). Ces certificats peuvent être utilisés pour authentifier des entités (personnes ou organisations). Une nouvelle méthode cryptographique a été choisie pour améliorer la sécurité et les performances, à savoir la **cryptographie à courbe elliptique** (**ECC**). ECC 384 remplacera prochainement l'approche actuelle RSA 2048. Les deux types de certificats (ECC & RSA) seront toujours utilisables en parallèle, mais les solutions pour obtenir de nouveaux certificats (Certificate Manager Requestor) ne généreront plus que des certificats ECC uniquement (les ETKs resteront RSA).

Nouvelle version de l'application de demandes de certificats (Certificate Manager Requestor) :
- Disponible à partir du 9 avril 2025 en ACCEPTATION
- Déploiement prévu en PRODUCTION (le 17 juin 2025 (2025.1.1)

PAS d'impact sur les certificats actuels et la procédure de demande
Tous les certificats eHealth existants, dans leur validité prévue, ne doivent PAS être remplacés de manière anticipative. Si vous disposez donc encore d'un certificat valide RSA, vous pouvez continuer

à l'utiliser durant la période de validité complète du certificat.
Il n'y a pas non plus de modifications dans la procédure de demande de certificats eHealth. Les informations utiles pour la demande d'un certificat eHealth par les prestataires de soins sont disponibles sur le portail de eHealth.
(Service de base certificats eHealth: ***https://www.ehealth.fgov.be/ehealthplatform/fr/service-certificats-ehealth*****)**

Que devez-vous faire?
Assurez-vous que les certificats ECC délivrés soient approuvés ("trustés") par vos systèmes (le "certificate chain" doit être approuvé ("trusted")).
Vous devez donc ajouter les certificats ainsi que la chaînes de certificats liées ('certificate chain'), de cette autorité de certification, à votre liste de certificats CA de confiance.
Vous trouverez via ces liens ci-dessous les certificats root et émetteurs pour l'acceptation.
ACCEPTATION :
Pour l'autorité intermédiaire "UAT ZetesConfidens Private Trust PKI - eHealth issuing CA 002":
http://crt-eh-ptpki-uat.confidens.zetes.com/ZCPTPKIeHIssCA002.crt
http://crl-eh-ptpki-uat.confidens.zetes.com/ZCPTPKIeHIssCA002.crl
http://ocsp-eh-ptpki-uat.confidens.zetes.com
Pour l'autorité intermédiaire "UAT ZetesConfidens Private Trust PKI - eHealth issuing CA 003":
http://crt-eh-ptpki-uat.confidens.zetes.com/ZCPTPKIeHIssCA003.crt
http://crl-eh-ptpki-uat.confidens.zetes.com/ZCPTPKIeHIssCA003.crl
Pour l'autorité racine (issued by "UAT ZetesConfidens Private Trust PKI - root CA 002"):
http://crt-ptpki-uat.confidens.zetes.com/ZCPTPKIROOTCA002.crt
http://crl-ptpki-uat.confidens.zetes.com/ZCPTPKIROOTCA002.crl
http://ocsp-ptpki-uat.confidens.zetes.com
PRODUCTION :
Pour l'autorité racine "ZetesConfidens Private Trust PKI - root CA 002":
Certificat: http://crt-ptpki.confidens.zetes.com/ZCPTPKIROOTCA002.crt
CRL: http://crl-ptpki.confidens.zetes.com/ZCPTPKIROOTCA002.crl
OCSP: http://ocsp-ptpki.confidens.zetes.com
Pour l'autorité intermédiaire "Zetes Confidens Private Trust PKI eHealth Issuing CA 002":
Certificat: http://crt-eh-ptpki.confidens.zetes.com/ZCEHPTPKICA002.crt
CRL: http://crl-eh-ptpki.confidens.zetes.com/ZCEHPTPKICA002.crl
OCSP: http://ocsp-eh-ptpki.confidens.zetes.com
Si vous ne suivez pas ces consignes, il se peut que votre logiciel ne fasse pas confiance dans les nouveaux certificats eHealth !

En cas de questions, n'hésitez pas à contacter le **CENTRE DE CONTACT** via le courriel ***support@ehealth.fgov.be*** ou au numéro **02/788 51 55** (chaque jour ouvrable de 7h à 20h)

****
****
****

Goedendag,

Dit bericht is bestemd voor de dienstenintegratoren van het eHealth-platform die de CryptoLIB gebruiken.

Naar aanleiding van de problemen die sommige softwareleveranciers en partners hebben ondervonden, hebben we beslist om deze interventie **uit te stellen.**
Er volgt een nieuwe communicatie met nieuwe datums voor een inproductiestelling.

We raden u echter aan om uw inspanningen voor het implementeren van de noodzakelijke wijzigingen voor de nieuwe cryptografische techniek ECC niet te pauzeren.
U moet de nieuwe communicatie dus onverwijld verder implementeren en uittesten.

Cryptolib Version
De vastgestelde problemen hebben hoofdzakelijk betrekking op de partners die de laatste versie van **cryptolib** (versie **2.3.0**) nog niet gebruiken waarvoor het gebruik van **Java 8** is vereist.
Bij deze communicatie willen wij u dus herinneren aan dit aandachtspunt (en de mogelijke aanpassing).

Bovendien hebben we de mogelijkheid behouden om RSA-certificaten aan te vragen, weliswaar enkel in acceptatie, zodat u niet geblokkeerd geraakt in uw ontwikkelingen en non-regressietesten.

Via de link https://www.ehealth.fgov.be/ehealthplatform/nl/service-ehealth-certificaten vindt u de URL's naar de versies RSA en ECC op het niveau van de paragraaf "Evolutie van de ETEE Certificate Manager (RSA - ECC)".

<u>Wijziging van cryptografietechniek voor de eHealth-certificaten</u>

Via het eHealth-platform kunnen de actoren in de gezondheidszorg eHealth-certificaten met bijbehorende sleutelparen verkrijgen. Deze certificaten kunnen worden gebruikt voor het authentiseren van entiteiten (personen of organisaties). Er werd geopteerd voor een nieuwe cryptografietechniek om de veiligheid en het prestatievermogen te verbeteren, namelijk de **elliptische curve cryptografie** (**ECC**). De ECC 384 zal binnenkort de huidige methode RSA-2048 vervangen. Beide types certificaten (ECC & RSA) zullen nog steeds in parallel gebruikt kunnen worden maar de oplossingen voor het verkrijgen van nieuwe certificaten (Certificate Manager Requestor) zullen enkel nog ECC-certificaten genereren (ETK's blijven RSA).

Nieuwe versie van de toepassing voor de aanvraag van certificaten (Certificate Manager Requestor) :
- Beschikbaar vanaf 9 april 2025 in ACCEPTATIE
- Uitrol in PRODUCTIE voorzien op 17 juni 2025 (2025.1.1)

GEEN impact op de huidige certificaten en de aanvraagprocedure
Alle bestaande eHealth-certificaten met hun huidige geldigheid moeten niet proactief worden vervangen. Indien u dus nog over een geldig RSA-certificaat beschikt, mag u die verder gebruiken tijdens de volledige geldigheidsperiode van het certificaat.

Er is ook geen wijziging in de aanvraagprocedure van de eHealth-certificaten. De nuttige informatie voor de aanvraag van een eHealth-certificaat door de zorgverleners is beschikbaar op het eHealth-portaal.
(Basisdienst eHealth-certificaten: ***https://www.ehealth.fgov.be/ehealthplatform/nl/service-ehealth-certificaten*****)**

Wat moet u doen?
Zorg ervoor dat de uitgereikte ECC-certificaten goedgekeurd ("trusted") worden door uw systemen (de "certificate chain" moet worden goedgekeurd ("trusted")).
U moet dus de certificaten en de betreffende certificatenreeks ('certificate chain') van die certificatie-autoriteit toevoegen aan uw lijst van betrouwbare CA-certificaten.
U vindt via de linken hierna de rootcertificaten en verzenders voor acceptatie.

ACCEPTATIE
Voor de intermediaire autoriteit "UAT ZetesConfidens Private Trust PKI - eHealth issuing CA 002":
http://crt-eh-ptpki-uat.confidens.zetes.com/ZCPTPKIeHIssCA002.crt
http://crl-eh-ptpki-uat.confidens.zetes.com/ZCPTPKIeHIssCA002.crl
http://ocsp-eh-ptpki-uat.confidens.zetes.com
Voor de intermediaire autoriteit "UAT ZetesConfidens Private Trust PKI - eHealth issuing CA 003":
http://crt-eh-ptpki-uat.confidens.zetes.com/ZCPTPKIeHIssCA003.crt
http://crl-eh-ptpki-uat.confidens.zetes.com/ZCPTPKIeHIssCA003.crl
Voor de intermediaire autoriteit Timestamp "UAT ZetesConfidens Private Trust PKI - eHealth TimeStamp CA 002":
http://crt-eh-ptpki-uat.confidens.zetes.com/ZCPTPKIeHTSCA002.crt
http://crl-eh-ptpki-uat.confidens.zetes.com/ZCPTPKIeHTSCA002.crl
Voor de root-autoriteit (issued by "UAT ZetesConfidens Private Trust PKI - root CA 002"):
http://crt-ptpki-uat.confidens.zetes.com/ZCPTPKIROOTCA002.crt
http://crl-ptpki-uat.confidens.zetes.com/ZCPTPKIROOTCA002.crl
http://ocsp-ptpki-uat.confidens.zetes.com

Productie:
Voor de root-autoriteit "ZetesConfidens Private Trust PKI - root CA 002":
Certificaat http://crt-ptpki.confidens.zetes.com/ZCPTPKIROOTCA002.crt
CRL: http://crl-ptpki.confidens.zetes.com/ZCPTPKIROOTCA002.crl
OCSP: http://ocsp-ptpki.confidens.zetes.com
Voor de intermediaire autoriteit "Zetes Confidens Private Trust PKI eHealth Issuing CA 002":
Certificaat http://crt-eh-ptpki.confidens.zetes.com/ZCEHPTPKICA002.crt
CRL: http://crl-eh-ptpki.confidens.zetes.com/ZCEHPTPKICA002.crl
OCSP: http://ocsp-eh-ptpki.confidens.zetes.com

Indien u deze instructies niet volgt, is het mogelijk dat uw softwarepakket de nieuwe eHealth-certificaten niet vertrouwt.

Bij vragen aarzel niet om contact op te nemen met het **CONTACTCENTER** via mail aan ***support@ehealth.fgov.be*** of op het **02/788 51 55** (elke werkdag tussen 7 en 20 uur).