Change certificates to 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.

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 chaîne de certificats liée ('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 ACC.

ACCEPTATION

Pour l'autorité intermédiaire "UAT ZetesConfidens Private Trust PKI - eHealth issuing CA 002" :

- <http://crt-eh-tpki-uat.confidens.zetes.com/ZCPTPKIeHlssCA002.crt>
- <http://crl-eh-tpki-uat.confidens.zetes.com/ZCPTPKIeHlssCA002.crl>
- <http://ocsp-eh-tpki-uat.confidens.zetes.com>

Change certificates to ECC

Pour l'autorité intermédiaire "UAT ZetesConfidens Private Trust PKI - eHealth issuing CA 003":

- <http://crt-eh-tpki-uat.confidens.zetes.com/ZCPTPKIeHlssCA003.crt>
- <http://crl-eh-tpki-uat.confidens.zetes.com/ZCPTPKIeHlssCA003.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-tpki.confidens.zetes.com/ZCEHPTPKICA002.crt>
- CRL: <http://crl-eh-tpki.confidens.zetes.com/ZCEHPTPKICA002.crl>
- OCSP: <http://ocsp-eh-tpki.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)