Change certificates to ECC

Wijziging van cryptografietechniek voor de eHealth-certificaten

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.

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 ACC.

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-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).