Beste,

We willen u informeren over aankomende veranderingen op het gebied van public trust digitale certificaten die worden gebruikt voor server authentication in de TLS/SSL-layer. Deze mededeling is bedoeld om te worden gedeeld met de technische teams die verantwoordelijk zijn voor het opzetten van connecties naar services van het eHealth-platform.

Momenteel is de maximale duur voor certificaten die worden gebruikt voor server authentication op de TLS/SSL-layer 1 jaar. Google heeft echter aangekondigd dat het van plan is om de **geldigheidsduur** van bovengenoemde **certificaten** terug te brengen naar **90 dagen**.

Normaal gesproken worden wijzigingen in de regels voor deze certificaten onderworpen aan een stemprocedure binnen een industrieconsortium, namelijk het CA/Browser Forum, dat bestaat uit Certification Authorities (CA's) en browserleveranciers. Hoewel de stemprocedure nog niet is begonnen, geven historische waarnemingen aan dat invloedrijke entiteiten (zoals Google) aanzienlijke invloed kunnen uitoefenen op de uitkomst van de beslissingen van het CA/B Forum, ongeacht de formele stemresultaten. Deze zorg wordt gedeeld door grote CA's.

Onze IT-infrastructuurleverancier en alle CA's achten het dan ook zeer waarschijnlijk dat de door Google voorgestelde wijzigingen eind 2024 zullen worden doorgevoerd. Zoals u zich kan voorstellen, zal dit een aanzienlijke impact hebben op onze business en zijn we genoodzaakt maatregelen te nemen om voorbereid te zijn op deze verandering.

Impact

Daarom moeten we onze procedures stroomlijnen en de levenscyclus van certificaten automatiseren. Dit zal gevolgen hebben voor bepaalde use cases die niet gestroomlijnd kunnen worden, waardoor eHealth de volgende diensten zal stopzetten:

- Voorafgaande communicatie naar eindgebruikers met betrekking tot de uitgifte en installatie van nieuwe certificaten. Als uitvloeisel hiervan wordt het gebruik van certificaatpinning nu niet meer toegestaan.
- Gebruik van server authentication TLS/SSL-certificaten buiten de daarvoor bestemde context (bijv. gebruik van hetzelfde certificaat om SAML2-asserties te ondertekenen).

1. Addendum algemeen eHealth

1.1 **Het eHealth-platform publiceert het eind ssl-certificaat voor het domein '.ehealth.fgov.be' momenteel online:**

- op het portaal : ***https://www.ehealth.fgov.be/ehealthplatform/ehealth-chaining.zip***
- in de metadata van onze IAM services AA, STS en IDP:
  - Link naar AA : ***https://services.ehealth.fgov.be/IAM/Metadata/AA***
  - Link naar STS : ***https://services.ehealth.fgov.be/IAM/Metadata/STS***
  - Link naar IDP : ***https://www.ehealth.fgov.be/idp/profile/Metadata/SAML***

Elke vernieuwing hiervan wordt gecommuniceerd.

1.2 **Met de noodzakelijke automatisatie van het vernieuwingsproces van het eindcertificaat zal deze werkwijze wijzigen.**

- Het eind SSL-certificaat zal niet meer gepubliceerd worden op het portaal of in de online metadata.
- Wijzigingen zullen ook niet langer gecommuniceerd worden.
  U zal er kunnen van uitgaan dat dit binnen de 90 dagen automatisch gebeurt.
- Enkel een wijziging van de root CA (indien van toepassing) zal nog op voorhand gecommuniceerd worden.

1.3 **Welke impact kunt u verwachten voor uw toepassingen die gebruik maken van eHealth services?**

Als het eind ssl-certificaat nergens in uw configuraties is gedefinieerd en het vertrouwen in dat certificaat louter gebaseerd is op validatie van de certificate chain tot aan de root ca, dan zal u geen impact ondervinden.

Als het eind ssl-certificaat wel gedefinieerd is in configuraties die door uw software gebruikt worden, zal dit moeten worden aangepast zodat validatie in de toekomst louter op basis van de certificate chain gebeurt. Dit is noodzakelijk opdat uw toepassingen zonder onderbreking geconnecteerd kunnen blijven met de eHealth services.

2. Addendum voor toepassingen die gehost worden door partners met gebruik van Shibboleth SP

2.1 Als u een Shibboleth SP gebruikt om uw toepassing(en) te hosten en te beveiligen, dan maakt u normaal gezien gebruik van een xml-bestand (saml 2.0 metadata) voor het vastleggen van identifiers, URL's en te vertrouwen certificaten van onze IDP. eHealth publiceert daarvoor sinds vele jaren een bestand online, de idp metadata:
https://www.ehealth.fgov.be/idp/profile/Metadata/SAML

Shibboleth SP ondersteunt een automatische update van uw lokaal xml-bestand, op basis van online metadata. Indien u dat nog niet doet, wordt dat ten zeerste aangeraden. Meer info op:
https://shibboleth.atlassian.net/wiki/spaces/pages/2063696005/XMLMetadataProvider

2.2 De eHealth idp metadata bevat momenteel minstens 2 certificaten: het SSL-certificaat voor het domein .ehealth.fgov.be en het IAM-certificaat voor het signeren van SAML berichten. Van elk van deze twee kunnen 2 opeenvolgende versies gepubliceerd zijn om een key-roll-over te ondersteunen wanneer een oud certificaat door een nieuw moet worden vervangen zonder onderbrekingen.

Binnenkort zullen wij het SSL-certificaat verwijderen uit deze online metadata (momenteel gedefinieerd in KeyDescriptor-elementen). Ter vervanging zal de root ca van het SSL-certificaat toegevoegd worden (gedefinieerd in een KeyAuthority-element).

De elementen KeyDescriptor die overblijven, zullen zijn voor het IAM-certificaat, gebruikt om de SAML-berichten te signeren.

Zie afbeelding op de volgende pagina

2.3 Shibboleth SP ondersteunt standaard beide werkwijzen:

- vertrouwen op basis van expliciete sleutel (i.e. het eindcertificaat, ExplicitKey)
- vertrouwen op basis van een certificate chain (i.e. tot aan de root ca, PKIX).

Dit mechanisme wordt reeds vele versies van Shibboleth SP ondersteund. Momenteel is de laatste versie 3.4.1.

Als u een oudere versie gebruikt of u de configuratie defaults hebt aangepast, kan het zijn dat dit niet out-of-the-box gaat blijven werken.

Als dat het geval is, zal u de configuratie moeten aanpassen om de PKIX trustengine te ondersteunen of upgraden naar de laatste versie, wat sowieso aangeraden wordt.

Meer info op

https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2063695951/TrustEngine

https://shibboleth.atlassian.net/wiki/spaces/SP3/overview

2.4 Op volgende data zullen de metadata online aangepast worden.

- **Acceptatie: 19/02/2024**
- **Productie: 8/10/2024 (R2024.2)**

Vernieuwde metadata

3. Te ondernemen acties

3.1 **Gelieve vanaf 19/02/2024 grondige tests in acceptatie in te plannen om u ervan te verzekeren dat uw applicatie nog steeds correct** functioneert en dat er geen foutberichten verschijnen die verband houden met de “trust” van het SSL-certificaat.

3.2 **Stuur via mail feedback** over de resultaten van uw testen (zowel positief als negatief) aan ***eHealth_Service_Management@ehealth.fgov.be***.

3.3 Bijlage A geeft u de lijst van toepassingen die een verbinding maken met onze IDP voor authenticatie.
Als uw toepassing niet meer gebruikt wordt, gelieve een mail te sturen naar ***eHealth_Service_Management@ehealth.fgov.be*** zodat we deze kunnen schrappen.

In de loop van de maand maart wordt een communicatie verstuurd met de uitnodiging om het SSL-certificaat te vernieuwen (geldigheid van 12 maanden).

Deze communicatie zal de laatste zijn want de SSL-certificaten krijgen een geldigheid van 90 dagen ingevolge de beslissing van het CA/B Forum.

Wij nodigen u dus uit om werk te maken van de implementatie van dit nieuwe “trust”-mechanisme zoals hierboven uitgelegd.

Deadline: 7 oktober 2024.

Indien u tegen dan het mechanisme niet geïmplementeerd hebt, riskeert u om na deze datum geen toegang meer te hebben tot uw applicaties.

Indien u vragen hebt, aarzel niet om contact op te nemen met het contactcenter via support@ehealth.fgov.be of op het nummer 02 788 51.55 (elke werkdag van 7u tot 20u)

Bijlage A

ServiceName FR	***ServiceName NL***
Neuro-Pain Platform	Neuro-Pain Platform
eBirth	eBirth
UZA@HOME	UZA@HOME
BelRAI V2	BelRAI V2
eCare Qermid Endoprotheses	eCare Qermid Endoprothesis
eCare Qermid Cardio	eCare Qermid Cardio
eCare Qermid Pacemakers	eCare Qermid Pacemakers
eCare Tool for Administrative Reimbursment Drugs Information Sharing	eCare Tool for Administrative Reimbursment Drugs Information Sharing
eCare Qermid Tuteur coronaire	eCare Qermid Tuteur coronaire
eCare Qermid ORTHOpride	eCare Qermid ORTHOpride
Treatment Demand Indicator Register (TDI)	Treatment Demand Indicator Register (TDI)
Web Security Log Consultation for eHealth CORE	Web Security Log Consultation for eHealth CORE
eHealth Frontdesk Access Support Tool	eHealth Frontdesk Access Support Tool
Chapter IV Agreement Requesting System	Chapter IV Agreement Requesting System
Contributions	Contributions
Source Authentique des Dispositifs Médicaux	Authentieke Bron Medische Hulmiddelen
Source Authentique des Distributeurs Notifiés	Authentieke Bron van de Genotificeerde Distributeurs
Autocontrôle	Autocontrol
Portail MEDSEIP	Portaal MEDSEIP
Source Authentique des Acteurs	Authentieke Bron van Actoren
Source Authentique des Activités et Classes	Authentieke Bron van Activiteiten en Klassen
Source authentique des Représentants Autorisés	Authentieke Bron van Gemachtigde Vertegenwoordigers
Registre Central de Traçabilité	Centraal traceringsregister
CIVICS	CIVICS
Register Inspection points	Register Inspection points
RETAM Labo	RETAM Labo
eTCT	eTCT

Orgadon	Orgadon
CONCERTO	CONCERTO
RAAS	RAAS
Invalidity Data Electronic System - IDES	Elektronisch uitkeringsdossier - IDES
Eunom-e	Eunom-e
Elections pour les dispensateurs de soins de santé	Verkiezingen voor zorgverstrekkers
Communication Prestataires de soins/INAMI	Communicatie Zorgverstrekkers/RIZIV
Accréditation - formation continue	Accreditering - continu vorming
INAMI - UAG	RIZIV - UAG
Demande de primes (INAMI)	Premieaanvragen (RIZIV)
Conventionnement (INAMI)	Overeenkomst (RIZIV)
Honoraires de disponibilité (INAMI)	Beschikbaarheidshonoraria (RIZIV)
Mes données légales et de contacts (INAMI)	Mijn wettelijke en contactgegevens (RIZIV)
Données administratives (INAMI)	Administratieve gegevens (RIZIV)
Mes documents (INAMI)	Mijn documenten (RIZIV)
Données financières et fiscales (INAMI)	Financiële en fiscale gegevens (RIZIV)
Portail ProSanté	Portaal ProGezondheid
Statut social INAMI	RIZIV sociaal statuut
eCarmed - Consultation des cartes médicales	eCarmed - Raadpleging van medische kaart
PACSonWEB	PACSonWEB
SCIENSANO – HD-APPS	SCIENSANO – HD-APPS
Wetenschappelijk Instituut Volksgezondheid - Healthdata for Primary Care	Institut Scientifique de Santé Publique - Healthdata for Primary Care
Institut Scientifique de Santé Publique - service healthdata	Wetenschappelijk Instituut Volksgezondheid - dienst healthdata
Enregistrement du cancer	Kanker Registratie
Heracles: Centre de la détection du cancer	Heracles: Centrum voor KankerOpsporing vzw
Catalogue de la Tumorothèque Virtuelle Belge	Catalogus van de Belgische Virtuele Tumorbank
Module d'enregistrement de la Tumorothèque Virtuelle Belge	Registratiemodule van de Belgische Virtuele Tumorbank
Web Security Log Consultation for eHealth VAS	Web Security Log Consultation for eHealth VAS
Moduledatabank	Moduledatabank
Vitalink Administratie Interface	Vitalink Administratie Interface

Cadastre des institutions de soins en Flandre	Gemeenschappelijk KlantenBestand
Portail d'accès intersectoral	INformatica Systeem Inter Sectorale TOegangspoort
VSB Operation Control Center	VSB Operation Control Center
VESTA	VESTA
CIRRO	CIRRO
SCIENSANO – Covid19-APPS	SCIENSANO – Covid19-APPS
Osimis (Lify)	Osimis (Lify)
Elearning platform Inami-Riziv	Elearning platform Inami-Riziv
Amaron I.AM LaboPlatform	Amaron I.AM LaboPlatform
E-guichet Soins et Santé	E-loket Zorg en Gezondheid
Elearning platform eSanté Wallonie	Elearning platform eSanté Wallonie
Institut Scientifique de Santé Publique - Healthdata for Data Providers	Wetenschappelijk Instituut Volksgezondheid - Healthdata for Data Providers
Elearning platform Inami-Riziv	Elearning platform Inami-Riziv
CEBAM Digital Library for Health	CEBAM Digital Library for Health
UMM infectieziekten	UMM infectieziekten
Extranet Mutualité Chrétienne	Extranet Christelijke Mutualiteit
RAAS	RAAS
Invalidity Data Electronic System - IDES	Elektronisch uitkeringsdossier - IDES
Elections pour les dispensateurs de soins de santé	Verkiezingen voor zorgverstrekkers
Communication Prestataires de soins/INAMI	Communicatie Zorgverstrekkers/RIZIV
Accréditation - formation continue	Accreditering - continu vorming
Demande de primes (INAMI)	Premieaanvragen (RIZIV)
Conventionnement (INAMI)	Overeenkomst (RIZIV)
Honoraires de disponibilité (INAMI)	Beschikbaarheidshonoraria (RIZIV)
Mes données légales et de contacts (INAMI)	Mijn wettelijke en contactgegevens (RIZIV)
Données administratives (INAMI)	Administratieve gegevens (RIZIV)
Données administratives (INAMI)	Administratieve gegevens (RIZIV)
Mes documents (INAMI)	Mijn documenten (RIZIV)
Données financières et fiscales (INAMI)	Financiële en fiscale gegevens (RIZIV)
Portail ProSanté	Portaal ProGezondheid

Statut social INAMI	RIZIV sociaal statuut
POEMA (DAMO – eServices)	POEMA (DAMO – eServices)
Eunom-e	Eunom-e
HospiSup (INAMI)	HospiSup (RIZIV)
Application web d'administration du Policy Administration Point	Webtoepassing om het Policy Administration Point te beheren
Application web de validation de certificats eHealth pour étrangers non-résidents	eHealth certificaten voor niet-ingezeten buitenlanders validatie webtoepassing
Etee Registration Authority Tool	Etee Registration Authority Tool
Medic-e	Medic-e
VONS	VONS
	Vlaamse Persoonlijke Medische Gegevens
UZ Gent Portail Employé	UZ Gent Medewerkersportaal
Attest112	Attest112
INAMI - Soins intégrés	RIZIV - Geïntegreerde zorg
MHC	MHC
INAMI - Soins intégrés	RIZIV - Geïntegreerde zorg
	GZAZNA portaal
Mijn AZ Sint-Lucas	Mijn AZ Sint-Lucas
MijnMariaMiddelares	MijnMariaMiddelares
Online Declaration Euthanasia Agreement	Online Declaration Euthanasia Agreement
Pharmastatut	Farmastatus
INAMI - pré-authentification	RIZIV - pre-authenticatie
Statistique Jongerenwelzijn	Statistiek JongerenWelzijn
TeleCovid	TeleCovid
eVIPA	eVIPA
DOMINO	DOMINO
MedAttest	MedAttest
Extranet Mutualité Chrétienne	Extranet Christelijke Mutualiteit
Hospital Network Antwerp - Electronic Care Trails	Ziekenhuisnetwerk Antwerpen - Elektronische Zorgtrajecten