Madame, Monsieur,

Nous tenons à vous informer des changements à venir au niveau des certificats numériques de confiance publique qui sont utilisés pour l'authentification des serveurs dans la couche TLS/SSL.
Le but est que cette communication soit diffusée auprès des équipes techniques responsables de la mise en place des connexions avec les services de la Plate-forme eHealth.

Actuellement, la durée de validité maximale des certificats utilisés pour l'authentification des serveurs dans la couche TLS/SSL s'élève à 1 an. Google a cependant annoncé qu'il comptait **ramener la durée de validité de ces certificats à 90 jours**.

Normalement, toute modification des règles applicables à ces certificats est soumise à une procédure de vote au sein d'un consortium industriel, à savoir le CA/Browser Forum qui est composé des autorités de certification (CA) et des fournisseurs de navigateurs.
Bien que la procédure de vote n'ait pas encore été entamée, il s'est avéré dans le passé que des entités influentes (telles que Google) peuvent exercer une influence considérable sur les décisions du CA/B Forum, indépendamment des résultats formels du vote. C'est une préoccupation que partagent les principales CA.

Dès lors, notre fournisseur d'infrastructure IT et toutes les CA estiment qu'il est fort probable que les modifications proposées par Google soient implémentées d'ici fin 2024. Comme vous pouvez l'imaginer, ceci aura un impact considérable sur notre business et nous nous voyons contraints de prendre des mesures afin de faire face à ce changement.

IMPACT

C'est pourquoi nous devons aligner nos procédures et automatiser le cycle de vie des certificats. Malheureusement, cela aura des conséquences pour certains use cases qui ne peuvent être alignés, ce qui obligera eHealth à mettre fin aux services suivants :

- Communication préalable à l'attention des utilisateurs finaux en ce qui concerne l'émission et l'installation de nouveaux certificats. Il en résulte que l'épinglage de certificats ne sera plus autorisé.
- L'utilisation de certificats TLS/SSL d'authentification du serveur en dehors du contexte prévu à cet effet (p.ex. utilisation du même certificat pour la signature d'assertions SAML2).

1. Addendum général eHealth

1.1 La Plate-forme eHealth publie actuellement le certificat SSL final pour le domaine '.ehealth.fgov.be' en ligne :

- sur le portail : ***https://www.ehealth.fgov.be/ehealthplatform/ehealth-chaining.zip***
- dans les métadonnées de nos services IAM AA, STS et IDP:
  - Lien vers AA : ***https://services.ehealth.fgov.be/IAM/Metadata/AA***
  - Lien vers STS : ***https://services.ehealth.fgov.be/IAM/Metadata/STS***
  - Lien vers IDP : ***https://www.ehealth.fgov.be/idp/profile/Metadata/SAML***

Tout renouvellement à ce niveau est communiqué.

1.2 Suite à l'automatisation du processus de renouvellement du certificat final, ce mode de travail va changer.

- Le certificat SSL final ne sera plus publié sur le portail ou dans les métadonnées en ligne.
- Les modifications ne seront plus communiquées. Vous pourrez partir du principe que le renouvellement a lieu automatiquement dans un délai de 90 jours.
- Seule une modification de la root CA (si d'application) sera encore communiquée préalablement.

1.3 Quel est l'impact attendu pour vos applications qui ont recours aux services eHealth ?

Si le certificat SSL final n'est défini nulle part dans vos configurations et que la confiance dans le certificat est simplement basée sur la validation de la chaîne de certificats jusqu'au certificat racine, vous ne subirez aucun impact.

Cependant, si le certificat SSL final est défini dans les configurations utilisées par votre logiciel, il faudra l'adapter de sorte à ce que la validation s'effectue dorénavant sur la base de la chaîne de certificats. Ceci est nécessaire afin que vos applications puissent rester connectées aux services eHealth sans interruption.

2. Addendum pour les applications hébergées par des partenaires qui ont recours à Shibboleth SP

2.1 Si vous utilisez Shibboleth SP pour héberger et sécuriser vos applications, vous avez normalement recours à un fichier xml (métadonnées saml 2.0) pour déterminer les identifiants, URL et les certificats de confiance de notre IDP. Depuis de nombreuses années, eHealth publie à cet effet un fichier en ligne, les métadonnées IDP :
https://www.ehealth.fgov.be/idp/profile/Metadata/SAML

Shibboleth SP supporte une mise à jour automatique de votre fichier xml local sur la base de métadonnées en ligne. Si vous ne le faites pas encore, ceci est fortement recommandé. Vous trouverez davantage d'informations sur
https://shibboleth.atlassian.net/wiki/spaces/pages/2063696005/XMLMetadataProvider

2.2 Les métadonnées ehealth idp contiennent actuellement au moins 2 certificats : le certificat SSL pour le domaine .ehealth.fgov.be et le certificat IAM pour la signature des messages SAML. Pour chacun de ces certificats, il est possible que 2 versions successives soient publiées afin de permettre un « key-roll-over » lorsqu'un ancien certificat doit être remplacé par un nouveau sans interruption.

Nous supprimerons bientôt le certificat SSL de ces métadonnées en ligne (actuellement défini dans des éléments KeyDescriptor). En remplacement, la « root ca » du certificat SSL sera ajoutée (définie dans un élément KeyAuthority).

Les éléments KeyDescriptor restants seront pour le certificat IAM, utilisé pour signer les messages SAML.

Voir image à la page suivante.

2.3 Par défaut, Shibboleth SP supporte les deux approches :

- la confiance basée sur une clé explicite (c'est-à-dire le certificat final, ExplicitKey)
- une chaîne de certificats (c'est-à-dire jusqu'à la « root CA », PKIX).

Ce mécanisme est déjà supporté depuis de nombreuses versions de Shibboleth SP.

Actuellement, la dernière version est la version 3.4.1.

Si vous utilisez une version plus ancienne ou si vous avez adapté la configuration par défaut, il se peut que ça ne continue pas à fonctionner.

Si tel est le cas, vous devrez adapter la configuration afin de supporter le PKIX trustengine ou passer à la version la plus récente, ce qui est de toute façon recommandé.

Plus d'informations sur

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

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

2.4 Nous adapterons les métadonnées en ligne aux dates suivantes :

- **Acceptation 19/02/2024**
- **Production: 08/10/2024 (R2024.2)**

Métadonnées renouvelées

3. Actions à entreprendre

3.1 **Veuillez planifier des tests approfondis en acceptation à partir du 19/02/2024 afin de vous assurer que votre application fonctionne toujours correctement** et qu'aucun message d'erreur n'est lié au "trust" du certificat SSL.

3.2 Nous aimerions que **vous nous informiez des résultats de vos tests** (tant positif que négatif) via e-mail à ***eHealth_Service_Management@ehealth.fgov.be***

3.3 Vous trouverez en annexe A la liste des applications qui se connectent à notre IDP pour l'authentification.
Si votre application n'est plus utilisée, merci de nous en faire part via mail à ***eHealth_Service_Management@ehealth.fgov.be*** afin que nous puissions la décommissionner.

Dans le courant du mois de mars nous vous enverrons une communication vous invitant à renouveler le certificat SSL (validité 12 mois).

Cette communication sera la dernière car les certificats SSL auront une validité de 90 jours suite à la décision du CA/B Forum.

Nous vous invitons donc à ne pas perdre de temps pour mettre en place ce nouveau mécanisme de "trust" comme expliqué ci-dessus.

Deadline : le 7 octobre 2024.

Passé ce délai, si vous n'avez pas mis ce mécanisme en place, vous risquez de ne plus avoir accès à vos applicatifs.

Si vous avez encore des questions, vous pouvez faire appel au contact center via support@ehealth.fgov.be ou au numéro 02 788 51.55 (tous les jours ouvrables de 7 h à 20 h)

Annexe 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