Certificate Management

This form applies to the following situations and target groups

When a public key of the certificate needs to be renewed with:

- IAM Connect users:
    - Confidential clients working with signed JWT (access token) without using the eHealth JWKS URL (JSON Web Key Set)
    - Not applicable to
        - Public clients
        - Confidential clients using the eHealth JWKS URL
- Partners using IAM AA (Attribute Authority)
- Partners using IAM STS (Secure Token Service)
    - Only for WSC (Web Service Consumers) using IAM STS SAML Sender Voucher (the application itself provides the electronic signature of the message)
- Partners using IAM IDP (Identity Provider)
- Partners using IAM eXchange
    - Only for clients (trusted platform) using:
        - POST /iam/v1/protocol/oauth/tokenExchange Operation
        - Or /iam/v2/protocol/oauth/tokenExchange
- Partners using SEALS

Same process applies to both new requests and renewals of the public key of the certificate.

Renewal of the public key

To renew the public key of a certificate, you must submit this form. We ask you to gather all the necessary information so that the eHealth platform can make the necessary adjustments to its systems in good time.

Send this form (fully completed) at least:

- 8 weeks before the expiry of the certificate for the production environment;
- 2 weeks before the expiry of the certificate for the acceptance environment.

If the information is communicated late or is incomplete, the eHealth platform cannot be held liable for the unavailability of the services for which this certificate is required.

Please send the completed form to: eHealth_Service_Management@ehealth.fgov.be

Public key renewal form

Public key renewal form (You will be informed of the ticket reference and the corresponding schedule)

General information

Field name	**To be completed by partner**
Organisation/Institution	
Contact person	
Email address	
Date of request	

Certificate information

Field name	**To be completed by partner**
Certificate type	☐ SSL ☐ eHealth-certificate ☐ Self-signed ☐ Other, namely:
Old public key	☐ Paste here ☐ Attached as appendix
New public key	☐ Pasted here ☐ Attached as appendix
Validity date of the current certificate	

Desired implementation date for the new certificate	
Environment (*Multiple choices allowed)*	☐ INT[1] ☐ ACC[2] ☐ PRD[3]

eHealth certificate

Components used by the certificate	**Details**
Update certificate for issuer in IAM AA	• Issuer[4]:
Update certificate for issuer in IAM STS	• Issuer[5]:
Update certificate for trusted SP (Service Provider) in IAM IDP	• EntityID[6]:

[1] INT = Integration environment
[2] ACC = Acceptation environment
[3] PRD = Production environment
[4] See Attribute Authority WS Cookbook Version, p. 10.

[5] This section only concerns WSC (Web Service Consumers) using IAM STS Saml Sender Vouches.

Pay attention:

- WSC might require an update of the encryption certificate;
- this certificate can be different that the signing certificate.

This form does not allow to mention this encryption certificate.

[6] See IAM Federation Metadata , section 3.

Update certificate for client using token eXchange/ IAM eXchange	• ClientID[7]: ☐
Update certificate for IAM Connect	• ClientID[8] + associated realms[9] ☐
Update certificate for services using Seals	• ApplicationName: ☐ Select the desired option[10]: ☐ encode ☐ decode

[7] This field only concerns clients (trusted platform) using:
- the operation POST */iam/v1/protocol/oauth/tokenExchange;*
- *or /iam/v2/protocol/oauth/tokenExchange.*

[8] Does **not** apply to public clients or confidential clients using eHealth JWKS URL.
Does apply to confidential clients using signed JWT **without** eHealth JWKS URL.

[9] Multiple entries are possible. Use one line per combination.

There is no key rollover mechanism. Once the certificate has been modified, the old certificate can no longer be used. If the partner does not modify its side, the client will no longer be usable. The change must be implemented simultaneously (synchronously).

[10] Multiple options may apply.