Texte français ci-dessous

Belangrijk :

Mededeling ivm de toepassing IAM/SecurityTokenService STS WS-TRUST

Tijdens onze major release R2024.1 van 12/05/2024 zal er een wijziging worden aangebracht aan de dienst STS WS-TRUST die het endpoint*/IAM/SecurityTokenService/v1* gebruikt.

Het betreft de upgrade van het foutenbeheer voor de dienst STS WS-TRUST. Vanaf R2024.1 zal het niet meer mogelijk zijn om meermaals hetzelfde attribuut ("claims") te gebruiken in eenzelfde STS-request.

Er werd een nieuwe cookbook STS WS-TRUST opgesteld; de beschrijving van deze wijziging vindt u in hoofdstuk *5.2.1.1.1 Claims* en is beschikbaar via deze link: ***https://www.ehealth.fgov.be/ehealthplatform/sts---ws-trust--cookbook-v1.1-dd-12012024***.

Indien u niets onderneemt, is het mogelijk dat u deze dienst niet meer correct zal kunnen gebruiken.

Hieronder een voorbeeld van request die niet meer aanvaard zal worden vanaf R2024.1.

Niet toegestane request (zie groene en rode kleur)

```
<wst:RequestSecurityToken Context="RC-${RequestId}" xmlns:wst="http://docs.oasis-open.org/ws-sx/wstrust/200512" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
xmlns:wsu="http://docs.oasisopen.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:wsse="http://docs.oasisopen.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile1.1#SAMLV1.1</wst:TokenType>
  STS – WS Trust - Cookbook v.1.1 dd 12/01/2024 14/26
  <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</wst:RequestType>
  <wst:Claims Dialect="http://docs.oasis-open.org/wsfed/authorization/200706/authclaims">
    <auth:ClaimType Uri="urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number">
      <auth:Value>71089914</auth:Value>
    </auth:ClaimType>
    <auth:ClaimType Uri="urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number">
      <auth:Value>71089914</auth:Value>
    </auth:ClaimType>
  </wst:Claims>
  <wst:Lifetime>
    <wsu:Created>2023-01-03T22:55:00.000Z</wsu:Created>
    <wsu:Expires>2023-01-03T23:55:00.000Z</wsu:Expires>
  </wst:Lifetime>
  <wst:KeyType>http://docs.oasis-open.org/ws-sx/wstrust/200512/PublicKey</wst:KeyType>
</wst:RequestSecurityToken>
```

Antwoord van de (foutieve) request (zie rood)

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <soapenv:Fault>
      <faultcode xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">wst:InvalidRequest</faultcode>
      <faultstring>The request was invalid or malformed</faultstring>
      <detail>
        <urn:BusinessError Id="_881d555eaaabbb66655dfd22d188d471" xmlns:urn="urn:be:fgov:ehealth:errors:soa:v1">
          <Origin>Client</Origin>
          <Code>wst:InvalidRequest</Code>
          <Message xml:lang="en">Message not properly encoded</Message>
          <Message xml:lang="en">Attribute urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number multiple times found.</Message>
          <urn:Environment>Integration</urn:Environment>
        </urn:BusinessError>
      </detail>
    </soapenv:Fault>
  </soapenv:Body>
</soapenv:Envelope>
```

Hieronder een voorbeeld van een **correcte** request vanaf R2024.1

```
<wst:RequestSecurityToken Context="RC-${RequestId}" xmlns:wst="http://docs.oasis-open.org/ws-sx/wstrust/200512" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
xmlns:wsu="http://docs.oasisopen.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:wsse="http://docs.oasisopen.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile1.1#SAMLV1.1</wst:TokenType>
    <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</wst:RequestType>
  <wst:Claims Dialect="http://docs.oasis-open.org/wsfed/authorization/200706/authclaims">
    <auth:ClaimType Uri="urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number">
      <auth:Value>71089914</auth:Value>
    </auth:ClaimType>
  </wst:Claims>
  <wst:Lifetime>
    <wsu:Created>2023-01-03T22:55:00.000Z</wsu:Created>
    <wsu:Expires>2023-01-03T23:55:00.000Z</wsu:Expires>
  </wst:Lifetime>
  <wst:KeyType>http://docs.oasis-open.org/ws-sx/wstrust/200512/PublicKey</wst:KeyType>
</wst:RequestSecurityToken>
```

Antwoord van de request

```
<wst:RequestSecurityTokenResponse Context="RC-a55c3420-6ae3-4d17-bebe-e70daf1f557c"
xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
  <wst:RequestedSecurityToken>
    <Assertion AssertionID="_444b70688b525e6c19f582e282855c48" IssueInstant="2023-01-
11T13:20:46.160Z" Issuer="urn:be:fgov:ehealth:sts:1_0" MajorVersion="1" MinorVersion="1"
xmlns="urn:oasis:names:tc:SAML:1.0:assertion">
      <Conditions NotBefore="2023-01-03T22:55:00.000Z" NotOnOrAfter="2023-01-04T23:00:00.000Z"/>
      <AuthenticationStatement AuthenticationInstant="2023-01-11T13:20:46.160Z"
AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:X509-PKI">
        <Subject>
          <NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"
NameQualifier=${SUBJECT-CA2}>${SUBJECT3}</NameIdentifier>
          <SubjectConfirmation>
            <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:holder-ofkey</ConfirmationMethod>
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
              <ds:X509Data>
                <ds:X509Certificate>${certificate}</ds:X509Certificate>
              </ds:X509Data>
            </ds:KeyInfo>
          </SubjectConfirmation>
        </Subject>
      </AuthenticationStatement>
      <AttributeStatement>
        <Subject>
          <NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"
NameQualifier=${Subject-CA2}>${Subject3}</NameIdentifier>
        </Subject>
        <Attribute AttributeName="urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihiinumber"
AttributeNamespace="urn:be:fgov:identification-namespace">
          <AttributeValue>71089914</AttributeValue>
        </Attribute>
      </AttributeStatement>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
          <ds:Reference URI="#_444b70688b525e6c19f582e282855c48">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#envelopedsignature"/>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>

            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
            <ds:DigestValue>zhPBGtUjR4PPRgJmEMQBflbiCGI4QZSf5KBYodo7qd4=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>ZXyW...h9WbOw==</ds:SignatureValue>
        <ds:KeyInfo>
```

```
            <ds:X509Data>
               <ds:X509Certificate>${certificate}</ds:X509Certificate>
            </ds:X509Data>
         </ds:KeyInfo>
      </ds:Signature>
   </Assertion>
</wst:RequestedSecurityToken>
</wst:RequestSecurityTokenResponse>
```

Bij vragen kan u contact opnemen met het contactcenter via support@ehealth.fgov.be of op het nummer 02 788 51.55 (alle werkdagen van 7 tot 20 uur)

Important:

Communication au sujet du service IAM/SecurityTokenService STS WS-TRUST

Lors de notre majeur R2024.1 du 12/05/2024 une modification sera apporté au service STS WS-TRUST qui utilise l'endpoint */IAM/SecurityTokenService/v1.*

Celle-ci concerne la mise à jour de la gestion des erreurs pour le service STS WS-TRUST. A partir de R2024.1, il ne sera plus possible d'utiliser plusieurs fois le même attribut ("claims") dans une seule et même requête STS.

Un nouveau cookbook STS WS-TRUST a été produit avec la description de ce changement décris via ce lien : ***https://www.ehealth.fgov.be/ehealthplatform/sts---ws-trust--cookbook-v1.1-dd-12012024*** dans la section *5.2.1.1.1 Claims*

Si vous ne prenez aucune action, il est possible que vous ne puissiez plus utiliser correctement ce service.

Voici un exemple de requête qui ne sera plus admise à partir de R2024.1

Requête non authorisé (voir couleur verte et rouge)

```
<wst:RequestSecurityToken Context="RC-${RequestId}" xmlns:wst="http://docs.oasis-open.org/ws-sx/wstrust/200512" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
xmlns:wsu="http://docs.oasisopen.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:wsse="http://docs.oasisopen.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile1.1#SAMLV1.1</wst:TokenType>
  STS – WS Trust - Cookbook v.1.1 dd 12/01/2024 14/26
  <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</wst:RequestType>
  <wst:Claims Dialect="http://docs.oasis-open.org/wsfed/authorization/200706/authclaims">
    <auth:ClaimType Uri="urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number">
      <auth:Value>71089914</auth:Value>
    </auth:ClaimType>
    <auth:ClaimType Uri="urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number">
      <auth:Value>71089914</auth:Value>
    </auth:ClaimType>
  </wst:Claims>
  <wst:Lifetime>
    <wsu:Created>2023-01-03T22:55:00.000Z</wsu:Created>
    <wsu:Expires>2023-01-03T23:55:00.000Z</wsu:Expires>
  </wst:Lifetime>
  <wst:KeyType>http://docs.oasis-open.org/ws-sx/wstrust/200512/PublicKey</wst:KeyType>
</wst:RequestSecurityToken>
```

Réponse de la requête en erreur (voir en rouge)

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Body>
<soapenv:Fault>
<faultcode xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">wst:InvalidRequest</faultcode>
<faultstring>The request was invalid or malformed</faultstring>
<detail>
<urn:BusinessError Id="_881d555eaaabbb66655dfd22d188d471" xmlns:urn="urn:be:fgov:ehealth:errors:soa:v1">
<Origin>Client</Origin>
<Code>wst:InvalidRequest</Code>
<Message xml:lang="en">Message not properly encoded</Message>
<Message xml:lang="en">Attribute urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number multiple times found.</Message>
<urn:Environment>Integration</urn:Environment>
</urn:BusinessError>
</detail>
</soapenv:Fault>
</soapenv:Body>
</soapenv:Envelope>

Voici un exemple de requête **correcte** partir de R2024.1

<wst:RequestSecurityToken Context="RC-${RequestId}" xmlns:wst="http://docs.oasis-open.org/ws-sx/wstrust/200512" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706" xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:wsu="http://docs.oasisopen.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:wsse="http://docs.oasisopen.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile1.1#SAMLV1.1</wst:TokenType>
<wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</wst:RequestType>
<wst:Claims Dialect="http://docs.oasis-open.org/wsfed/authorization/200706/authclaims">
<auth:ClaimType Uri="urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihii-number">
<auth:Value>71089914</auth:Value>
</auth:ClaimType>
</wst:Claims>
<wst:Lifetime>
<wsu:Created>2023-01-03T22:55:00.000Z</wsu:Created>
<wsu:Expires>2023-01-03T23:55:00.000Z</wsu:Expires>
</wst:Lifetime>
<wst:KeyType>http://docs.oasis-open.org/ws-sx/wstrust/200512/PublicKey</wst:KeyType>
</wst:RequestSecurityToken>

Réponse de la requête

```
<wst:RequestSecurityTokenResponse Context="RC-a55c3420-6ae3-4d17-bebe-e70daf1f557c"
xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512">
  <wst:RequestedSecurityToken>
    <Assertion AssertionID="_444b70688b525e6c19f582e282855c48" IssueInstant="2023-01-
11T13:20:46.160Z" Issuer="urn:be:fgov:ehealth:sts:1_0" MajorVersion="1" MinorVersion="1"
xmlns="urn:oasis:names:tc:SAML:1.0:assertion">
      <Conditions NotBefore="2023-01-03T22:55:00.000Z" NotOnOrAfter="2023-01-04T23:00:00.000Z"/>
      <AuthenticationStatement AuthenticationInstant="2023-01-11T13:20:46.160Z"
AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:X509-PKI">
        <Subject>
          <NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"
NameQualifier=${SUBJECT-CA2}>${SUBJECT3}</NameIdentifier>
          <SubjectConfirmation>
            <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:holder-ofkey</ConfirmationMethod>
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
              <ds:X509Data>
                <ds:X509Certificate>${certificate}</ds:X509Certificate>
              </ds:X509Data>
            </ds:KeyInfo>
          </SubjectConfirmation>
        </Subject>
      </AuthenticationStatement>
      <AttributeStatement>
        <Subject>
          <NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"
NameQualifier=${Subject-CA2}>${Subject3}</NameIdentifier>
        </Subject>
        <Attribute AttributeName="urn:be:fgov:ehealth:1.0:certificateholder:hospital:nihiinumber"
AttributeNamespace="urn:be:fgov:identification-namespace">
          <AttributeValue>71089914</AttributeValue>
        </Attribute>
      </AttributeStatement>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
          <ds:Reference URI="#_444b70688b525e6c19f582e282855c48">
            <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#envelopedsignature"/>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>

            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
            <ds:DigestValue>zhPBGtUjR4PPRgJmEMQBflbiCGI4QZSf5KBYodo7qd4=</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>ZXyW...h9WbOw==</ds:SignatureValue>
        <ds:KeyInfo>
```

```
            <ds:X509Data>
               <ds:X509Certificate>${certificate}</ds:X509Certificate>
            </ds:X509Data>
         </ds:KeyInfo>
      </ds:Signature>
   </Assertion>
</wst:RequestedSecurityToken>
</wst:RequestSecurityTokenResponse>
```

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)