kadaster

Signing Documenten Realisatie

het **XML-Pakket met Attachments:**

1) Verzoeken tot inschrijving,
tot in depotname en tot intrekking

het "Verzoek-Pakket"

2) Inschrijvings- en Kadastermededelingen
het "Mededeling-Pakket"

07 Juni 2020
Carmen Visinescu

Signing XML-Pakket [XML metadata – met attachments]

Signing van "***het Pakket XML***": de metadata met de attachments
Usecase SYVAS – het "Verzoek-XML-Pakket" en het "Mededeling-XML-Pakket" ondertekenen

***Het businessdoel is, h*et bewijs hebben voor:**

- **Data integriteit:**

  De ontvangen metadata (en essentialia in geval van een niet-KIK akte) en de attachments die naar het Kadaster gestuurd zijn vanuit de NSL of vanuit de SYVAS-GUI zijn niet aangepast.

- **Signer authentication en Non-repudiation**:

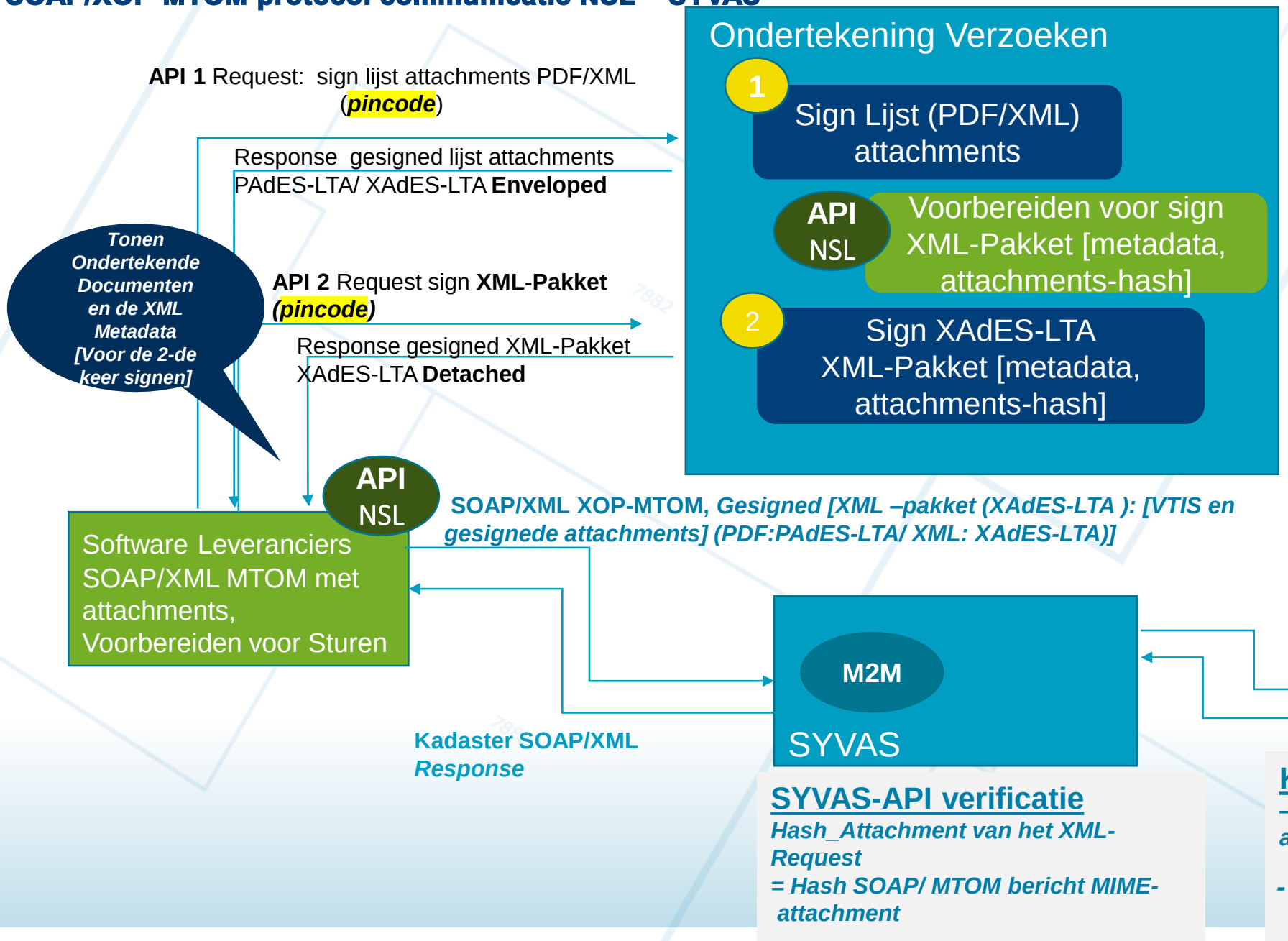
  Beveiliging wordt geboden door het gebruik maken van de digitale handtekeningen met de USB Token (lokale ondertekening)

Realisatie in de projecten:

- NSL met eigen signing oplossing
- KNB (CSS-signing-oplossing)
- SYVAS-GUI met SigningHub (Ascertia)
- SYVAS Backend met Kadaster Signing Server (Ascertia signing oplossing)

Elektronisch ondertekenen uitwisselberichten (XML) met bijlagen (XML/PDF)

SOAP/XOP-MTOM protocol communicatie NSL – SYVAS



Voordeel oplossing:

- ***De stap ondertekenen van het "XML-Verzoek-Pakket" heeft geen beperkingen meer w.b. de grootte en de aantal attachments.***

Het XAdES-Xml Signature wordt toegevoegd in de Soap-Envelop-Header van het SOAP-XML MTOM bericht, volgens de WS-Security standards.

- ***Geen SOAP ondertekening oplossing, afhankelijk van de frameworks implementatie nodig***
- ***Generieke oplossing voor het "XML – Pakket" (Verzoeken/ Mededelingen) voor het Kadaster en KNB(CSS)***

SYVAS-API verificatie

Hash_Attachment van het XML-Request
= Hash SOAP/ MTOM bericht MIME-attachment

KSS-API verificatie

– "signature-verificatie" van elke attachment (PDF/XML-Document)

- "signature-verificatie" van het XML-Pakket

Resultaat SOAP-Envelop XML/MTOM NSL bericht naar SYVAS sturen


```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header>
       <SOAP-SEC:Signature ...>

          <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

             <ds:SignedInfo>
                <ds:Reference Id="SignedDataObject_23763778485819" URI=" ID-VTIS ">
                   <ds:Transforms>
                         <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>4/KW6jx/di0YYPmyuj0mG1VbMYOYwHkWV0aWl31jE1Q=</ds:DigestValue>
                </ds:Reference>

                 <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#SignedProperties-1644729058">
                    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                    <ds:DigestValue>fnj0m7+azCbvwEwragazn+slJfA=</ds:DigestValue>
                 </ds:Reference>
           </ds:SignedInfo>
          .....................
          </ds:Signature>
       </SOAP-SEC:Signature>
  </SOAP-ENV:Header>

  <SOAP-ENV:Body >
    <AanbiedenVerzoekRequest xmlns="http://www.kadaster.nl/schemas/aanbiedenverzoek/service/v20191120">
      <vraag>
        <VerzoekTotInschrijvingProduct xmlns="http://www.kadaster.nl/schemas/aanbiedenverzoek/verzoektotinschrijvingproduct/v20191120" id = “ID-VTIS”>
        ...............
                      <sch4:TerInschrijvingAangebodenStuk>
                        <sch4:terInschrijvingAangebodenStukDocument>7f758b0b-6452-4177-9475-72a5e0d221fd</sch4:terInschrijvingAangebodenStukDocument>
                          <digestMethod>sha256</digestMethod>
                           <digestValue>fnj0m7+azCbvwEwragazn+slJfA</digestValue>
                      </sch4:TerInschrijvingAangebodenStuk>
        </VerzoekTotInschrijvingProduct>

          <av:attachments>
              <v204:Attachment>
                 <v204:referentie> 7f758b0b-6452-4177-9475-72a5e0d221fd 0</v204:referentie>
                 <v204:naam>FakeAkteRep268.pdf</v204:naam>
                 <v204:document>cid:926597255386</v204:document>
              </v204:Attachment>
          </av:attachments>
      </vraag>
    </AanbiedenVerzoekRequest>

   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

------=_Part_60_1645142674.1587899337315
Content-Type: application/pdf
Content-Transfer-Encoding: binary
Content-ID: <926597255386>
Content-Disposition: attachment; name="SyvasTestEchtePdf.pdf"

%PDF-1.7
%µµµµ
```

Stap 1)

- Verzoeken attachments documenten PDF/XML worden ondertekend

(*PDF documenten zijn stuk, evt. bijlage(n), evt. bewijsstuk(ken) en XML-document is KIK-data ingeval van een KIK-akte*)

- Mededeling – attachments documenten PDF worden ondertekend

PDF document(en) is/zijn de mededeling en voor bepaalde mededelingen ook het ingeschreven stuk

Request: Lijst Documenten (PDF/XML) te ondertekenen

Response: Lijst Documenten PAdES-LTA ondertekend

XAdES – LTA-Enveloped ondertekend (Enveloped – signing de hele KIK.xml bestand)

Stap 2) het **“pakket xml”** met ondertekende documenten ondertekenen

Dat kan gerealiseerd worden met een **XML digital XAdES –LTA Detached signature** van een deel XML element van het SOAP/MTOM XML bericht,

Het XML element kan via een URI (ID) of transformatie (XPath / Filter) geïdentificeerd worden.

Gebruik maken van de SHA256 algoritme, eIDAS compliant QES

Signing XML-Pakket [XML metadata – met attachments]
XAdES- Detached met Referentie-URI = XML-Element-ID *(ID van de XML-element is verplicht)*

Ondertekende Request XML- Element wordt geïdentificeerd op basis van ID

```
<vtip:VerzoekTotInschrijvingProduct id="ID-VTIS">
    <vtip:bevat>
      <i:VerzoekTotInschrijvingStuk>
          <i:klD>958a24dc-f97c-11e9-8f0b-362b9e155667</i:klD>
                ……..
           <sch4:TerInschrijvingAangebodenStuk>
                <sch4:terInschrijvingAangebodenStukDocument>Ref-ID
                </sch4:terInschrijvingAangebodenStukDocument>
                <digestMethod>sha256</digestMethod>
                <digestValue>fnj0m7+azCbvwEwragazn+slJfA</digestValue>
           </sch4:TerInschrijvingAangebodenStuk>
          </i:VerzoekTotInschrijvingStuk>
    </vtip:bevat>
  </vtip:VerzoekTotInschrijvingProduct>
```

Signature XML-Pakket: XML-XAdES-LTA – Detached

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature_23763778485819">
  <ds:SignedInfo Id="SignedInfo_23763778485819">
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
    <ds:Reference Id="SignedProperties-Reference_23763778485819"
          Type="http://uri.etsi.org/01903#SignedProperties" URI="#SignedProperties_23763778485819"
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>hWGQyW73F3VxGp3c9Cqx8RcORGWE2nIkkd/4TCtiJxY=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference Id="SignedDataObject_23763778485819" URI=" ID-VTIS ">
      <ds:Transforms>
        <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>4/KW6jx/di0YYPmyuj0mG1VbMYOYwHkWV0aWl31jE1Q=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue Id="SignatureValue_23763778485819">
    YSSyfxCHy8BkiiBp9RMFO5saI0IskH0H83hq7lgmt0ftSzZMTkprJNw3mnwotl96
    GitkMKS32XM6RObmPwR0o3RepjrD4Q23KbJMsvuBgFvbnu+ugkhL2u5vYNLnTBH8
    /rG6E1eKplYyVEq6l24drc2bhnq4+yo6a2dh3sYjX8WNUhEDg7MelIJcqGm6dKzI

……..
</ds:Signature>
```

Signing XML-Pakket [XML metadata – met attachments]
KSS-Kadaster Signing voor het Pakket Mededelingen – met XPath van een XML- Element

Input Request XML- Element geïdentificeerd op basis van XPath van een XML- Element

```
<vtip:MededelingProduct>
    <vtip:bevat>
      <i:Mededeling>
          <i:kID>958a24dc-f97c-11e9-8f0b-362b9e155667</i:kID>
                ……..
            <digestMethod>sha256</digestMethod>
             <digestValue>fnJ0m7+azCbvwEwragazn+sIJfA</digestValue>

          </i: Mededeling >
    </vtip:bevat>
</vtip:MededelingProduct >
```

Resultaat XML-XAdES – Detached Signature:

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature_23763778485819">
  <ds:SignedInfo Id="SignedInfo_23763778485819">
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
    <ds:Reference Id="SignedProperties-Reference_23763778485819"
          Type="http://uri.etsi.org/01903#SignedProperties" URI="#SignedProperties_23763778485819
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>hWGQyW73F3VxGp3c9Cqx8RcORGWE2nIkkd/4TCtiJxY=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference Id="SignedDataObject_23763778485819" URI="">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
          <XPath xmlns="http://www.w3.org/2002/06/xmldsig-filter2" Filter="intersect">
              //*[local-name()= MededelingProduct ']

          </XPath>
        </ds:Transform>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>4/KW6jx/di0YYPmyuj0mG1VbMYOYwHkWV0aWl31jE1Q=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue Id="SignatureValue_23763778485819">
    YSSyfxCHy8BkiiBp9RMFO5saI0IskH0H83hq7lgmt0ftSzZMTkprJNw3mnwotl96
    GitkMKS32XM6RObmPwR0o3RepjrD4Q23KbJMsvuBgFvbnu+ugkhL2u5vYNLnTBH8
    /rG6E1eKplYyVEq6l24drc2bhnq4+yo6a2dh3sYjX8WNUhEDg7MelIJcqGm6dKzI
```

Kadaster maakt gebruik van ADSS-ascertia pakket, en dat kan de signature met XPath realiseren

Resultaat SOAP-Envelop XML/MTOM bericht Kadaster (Mededeling-XML-Pakket) - naar NSL – (ophalen-Mededeling – XML Pakket)

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header>
       <SOAP-SEC:Signature ...>
          <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
              <ds:SignedInfo>
                      <ds:Reference Id="SignedDataObject_23763778485819" URI="">
                          <ds:Transforms>
                             <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                             <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                                 <XPath xmlns="http://www.w3.org/2002/06/xmldsig-filter2" Filter="intersect">//*[local-name()= MededelingProduct ']</XPath>
                             </ds:Transform>
                            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                            <ds:DigestValue>bIfV8igkOP+xen9yt8UhfQ++oL8=</ds:DigestValue>
                      </ds:Reference>
                      <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#SignedProperties-1644729058">
                         <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                          <ds:DigestValue>fnj0m7+azCbvwEwragazn+slJfA=</ds:DigestValue>
                     </ds:Reference>
               </ds:SignedInfo>
          .....
   </SOAP-SEC:Signature>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body >
   <MededelingRequest xmlns="http://www.kadaster.nl/schemas/ophalenmededeling/service/v20191120">
     <vraag>
       <MededelingProduct xmlns=http://www.kadaster.nl/schemas/aanbiedenverzoek/mededelingproduct/v20191120>
              <Mededeling>
                    <referentie>958a24dc-f97c-11e9-8f0b-362b9e155667</i:kID>
                     <digestMethod>sha256</digestMethod>
                      <digestValue>fnj0m7+azCbvwEwragazn+slJfA</digestValue>
              </i: Mededeling >
      ..............
       </ MededelingProduct >
        <av:attachments>
            <v204:Attachment>
              <v204:referentie>10000000-0000-0000-0000-000000000000</v204:referentie>
             <v204:naam>mededeling.pdf</v204:naam>
             <v204:document>cid:926597255386</v204:document>
           </v204:Attachment>
       </av:attachments>
     </vraag>
    </ MededelingRequest >

</SOAP-ENV:Body>
</SOAP-ENV:Envelope>

------=_Part_60_1645142674.1587899337315
Content-Type: application/pdf
Content-Transfer-Encoding: binary
Content-ID: <926597255386>
Content-Disposition: attachment; name=" mededeling.pdf"

%PDF-1.7
%µµµµ
```

KIK.XML - Signing XML (Root) XAdES-LTA, Signing XML-Enveloped met URI = “”

Input Kik.xml

```
<KIKRoot>
      <bevat>
      ……..
      </bevat>
 </KIKRoot >
```

Resultaat XML-XAdES – signature KIK.XML:

```
<KIKRoot>

      <bevat>
      ……..
      </bevat>

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signature_23763778485819">
   <ds:SignedInfo Id="SignedInfo_23763778485819">
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <ds:Reference Id="SignedProperties-Reference_23763778485819"
               Type="http://uri.etsi.org/01903#SignedProperties" URI="#SignedProperties_23763778485819">
         <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
         <ds:DigestValue>hWGQyW73F3VxGp3c9Cqx8RcORGWE2nIkkd/4TCtiJxY=</ds:DigestValue>
      </ds:Reference>
      <ds:Reference Id="SignedDataObject_23763778485819" URI="">
         <ds:Transforms>
            <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>4/KW6jx/di0YYPmyuj0mG1VbMYOYwHkWV0aWl31jE1Q=</ds:DigestValue>
      </ds:Reference>
   </ds:SignedInfo>
   <ds:SignatureValue Id="SignatureValue_23763778485819">
      YSSyfxCHy8BkiiBp9RMFO5saI0IskH0H83hq7lgmt0ftSzZMTkprJNw3mnwotl96
      GitkMKS32XM6RObmPwR0o3RepjrD4Q23KbJMsvuBgFvbnu+ugkhL2u5vYNLnTBH8
      /rG6E1eKplYyVEq6l24drc2bhnq4+yo6a2dh3sYjX8WNUhEDg7MelIJcqGm6dKzI

  </KIKRoot >
```

Lokaal Signing Flow diagram Notaris –GUI Applicatie