White Paper

IPPC ePhyto Digital Signature
EU Requirements and GeNS Implementation

2nd -Sep-2021

Table of Contents

Acronyms

ePhyto	Electronic phytosanitary certification
GeNS	Generic National System
XML	Extensible Markup Language
SPS	Sanitary and Phytosanitary
IPPC	International Plant Protection Convention
OIE	Office International des Epizooties
eIDAS	electronic IDentification Authentication and Signature
XAdES	XML Advanced Electronic Signatures
ETSI	European Telecommunications Standards Institute
TSP	Trust service provider
TRACES NT	EU information system used to manage SPS certificates to and from the EU
ISPM	International Standards for Phytosanitary Measures

1 Summary

The purpose of this document is to describe how digital signature can be exchanged between National Systems as it has been implemented in the IPPC Generic ePhyto National System (GeNS) implementation [1].

Electronic phytosanitary certification (ePhyto) refers to digitalization of global trade transactions using electronic information lieu of traditionally a paper documentation. In other words, ePhyto is the electronic equivalent of a paper phytosanitary certificate (ISPM 12).

Digital signature (XML DSIG) is an electronic, encrypted data exchange which is part of ePhyto certificate security. To validate the authenticity and integrity of the information signed from the signer (exporter) was not altered in transmission. It provides the same legal value as a handwritten signature as long as it follows the requirements of the specific regulation.

2 From Paper to Electronic SPS Certification

SPS certification today is based largely on exchange of official papers. The format of these paper certificates is discussed and agreed during bilateral negotiations between exporting and importing countries. The paper is issued by the competent authorities of the exporting countries based on the model defined by the importing countries or international organizations, namely IPPC (International Plant Protection Convention) and OIE (Office International des Epizooties).

The paper on which the certificate is issued, is frequently using security features in order to limit the circulation of fraudulent certificates.

[1] GeNS Implementation Framework:
https://www.ephytoexchange.org/landing/assets/docs/ePhyto_GeNS_Implementation_Framework.pdf

More and more countries are implementing SPS electronic certification system. These systems have been initially designed to implement the import and export workflows of these certificates and print the paper-based certificate. However, relatively recent evolutions have seen countries started exchanging the electronic content of these certificates between national competent authorities' systems; these exchanges are implementing a pre-notification function and can as well allow the replacement of the paper by an electronic transaction.

A relatively recent EU legislation is defining uniformly for all EU Member States what can be considered as an official electronic document aiming to replace a paper-based official document; in simple terms, the electronic document should be properly signed /sealed digitally in accordance with the eIDAS Regulation1 (and its implementing provisions) which defines the digital signature levels needed to achieve this goal. Being an EU Regulation, this text applies completely and in a mandatory manner to all EU Member States and replaces pre-existing national laws in this domain. This is applicable to document produced outside the EU and intended for an administration of an EU Member State as in the case of SPS certificates.

3 EU Digital Signature requirements

All the technical requirements[2] and guidelines needed to implement such exchanges in relation to the EU certification system (IMSOC-TRACES) are available in the TRACES Toolkit website (access to this toolkit can be granted after sending a mail to SANTE-TRACES@ec.europa.eu).

3.1 Practical Implementation of Electronic Signature On an eCert XML

To replace a paper SPS certificate to be presented to an EU authority, an advanced or qualified signature will have to be applied on the XML materialising the SPS certificate. Please note that, contrary to the paper version requiring the signature of an officer and the stamp of the authority, the XML will require only a single electronic signature: either the one associated to the authority (called eSeal in EU eIDAS regulation terminology) or the one of an authorised person representing this authority. In order to identify the valid signature for an exporting country, an exchange of letter and/or digital certificate will have to occur before the start of the electronic transactions in order to identify the valid signature representing an authority.

3.1.1 General Principles of XML Signatures

XML Signature defines XML syntax for digital signatures and is defined by W3C recommendation XML Signature Syntax and Processing.

Three methods are supported:

- ***XML Embedded or Enveloped Signature***
  Using XML Signature to sign some parts of its containing document (called an embedded or enveloped signature).
  A signature block is embedded inside the XML and represents the signed "SPSCertificate" part of the body of the XML.

[2] Electronic signature for SPS certification: the EU requirements
https://circabc.europa.eu/ui/group/af5deeae-af5b-4ae7-9cd2-24df51e9fa72/library/fb14c756-e3dc-459f-bdbc-8f4e6d519b66/details

- **Signature in the XML Header**

  A signature block is added to the XML within “header” element and covers the content of the “body” element.

- **Detached Signature**

  Using XML Signature to sign a resource outside its containing XML document (called a detached signature). The signature is over content external to the Signature element, and can be identified via a URI or transform. Consequently, the signature is "detached" from the content it signs. This definition typically applies to separate data objects, but it also includes the instance where the Signature and data object reside within the same XML document but are sibling elements.

3.1.2 Specific Recommendations for SPS XML Signature

The signature we require on XML for SPS electronic certification is conform to these specifications but with the following specific recommendations:

- The proposed method will be XML Embedded/Enveloped signature because of the following reasons:
  - Do not risk to suffer from any removal/change in the XML Header (like in the IPPC ePHYTO HUB case)
  - Is producing a stand-alone XML file with content of the original SPSCertificate XML plus its signature inside a single file
  - Would look more simple to implement and understand than a Detached signature
- To preserve structurally the original SPSCertificate Object to its eCERT specifications, we recommend to encapsulate the SPSCertificate and Signature Objects into a root structure called SignedSPSCertificate.

See Appendix for a complete sample.

4 Digital Signature Implementation in GeNS

4.1 Sequence Diagram

In the following sequence diagram figure 1, the process starts in the GeNS exporting country. When the exporting country issues an ePhyto certificate (XML format), the GeNS check if the Digital Signature is configured and enabled for the country.

If that is the case, the XML document is signed (using the country private key and certificate) generating a cryptographic hash before it is being sent to the HUB. The cryptographic hash will be encrypted using the exporter's private key. Then the encrypted signature is sent to the import country as part of the ePhyto certificate.

After that, when the importing country receives the XML document through the National System, they have the option to validate the digital signature of the document.

For the validation process the receiving system can validate the incoming signature certificate using the identified trust store/provider, alternatively the national system will be able to ask HUB for the exporting country's certificate via secure connection to compare the incoming certificate with the one configured in the HUB.

Then the import country (recipient) decrypts the signature with the public key of the exporter. The import country uses same hash algorithm by the export country to re calculates the certificate digest. If both, the sent and the received certificates digests are identical, the import country can be sure that the certificate hasn't been tampered and valid. See a full sample of Signature content in the **Appendix-** Error! Reference source not found..

Finally, the certificate is used to validate the received XML document and update its status in importing country's database (See section **5. GeNS Digital Signature Status**).

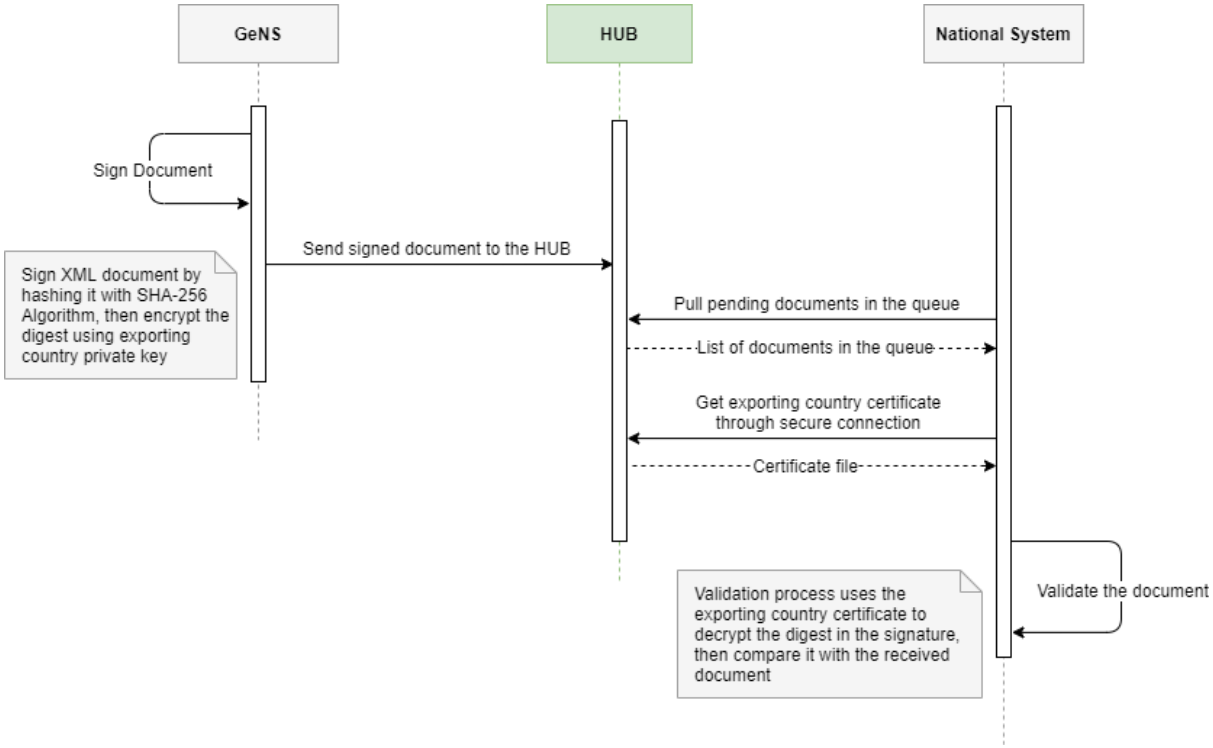


Figure 1: Digital Signature Sequence Diagram

4.2 Configuration

The GeNS Administrator can setup (add/update/delete) the following configuration for each instance:

FIELD	DESCRIPTION	EXAMPLE
DESTINATION COUNTRIES	Define countries which will receive the signed ePhyto	FR, IT, DE...
ACTIVE	Determine if digital signature is enabled for this country or not	True/False
ENABLE VALIDATION	Determine if GeNS do validate incoming certificates	True/False
CERTIFICATE	Destination country certificate file, it includes destination's public key, name, location, validity dates (from-to), and issuer information, CLR and OCSP validation	**Common Name**: GeNS LK **Organization**: United Nations International Computing Center **Organization Unit**: Applications Delivery **Country**: LK **Valid From**: June 26, 2020 **Valid To**: June 26, 2021 **Issuer**: GeNS, United Nations International Computing Center

To request or generate a certificate, the following information are needed:

- **Common Name:** the fully qualified name of the instance.

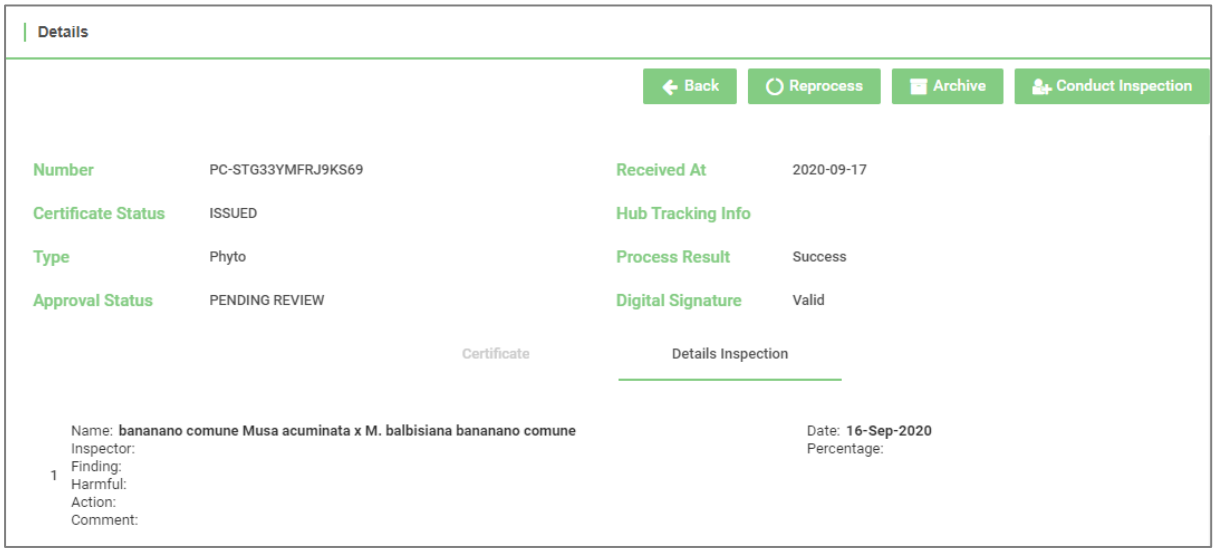
- **Organization**: the complete legal name of the organization.
- **Organization Unit**: the name of the division, department, or section in the organization that manages network security.
- **Locality or City**: the city where the organization is legally located.
- **State/Province**: the state or province where the organization is legally located.
- **Country**: the two-letter ISO abbreviation for the country.
- **Key Size**: 2048 Bits.

5 GeNS Digital Signature Status

In this section, we show how ePhytos will looks like in three different cases: Valid Document, Invalid Document, and Not Signed Document

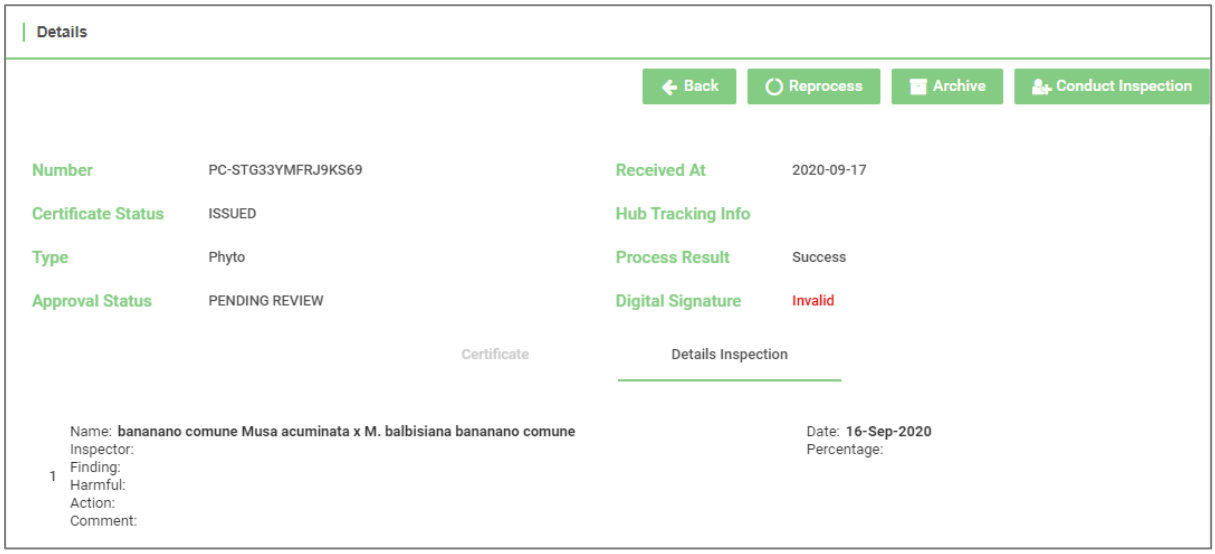
5.1 Valid Document

When an instance receives signed ePhyto, and there is no change on its content, it will appear like this:



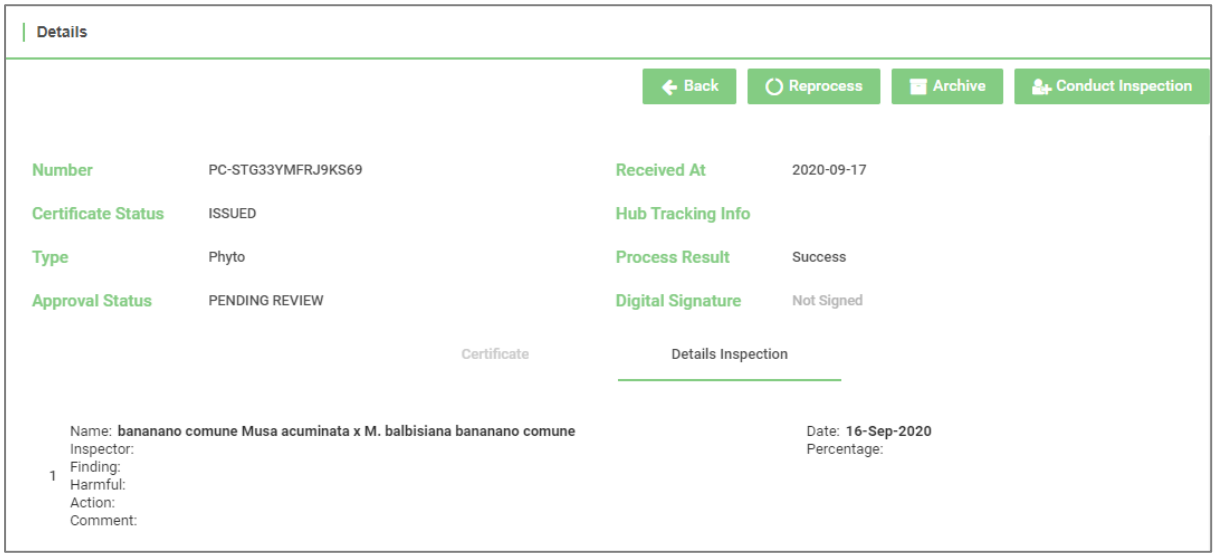
5.2 Invalid Document

In case when ePhyto document is altered while sending/receiving the envelope, GeNS will detect the invalid document and it will appear like in the following:



5.3 Not Signed Document

When the document is sent without digital signature, it will look like the following image when delivered to destination country:



6 Appendix

6.1 References

- https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature
- https://github.com/esig/dss

6.2 Digital Signature Sample

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="id-
ab518763b287d34797a983f809c85e08">
    <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 Id="r-id-ab518763b287d34797a983f809c85e08-1" URI="">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-
19991116">
                    <ds:XPath>not(ancestor-or-self::ds:Signature)
                    </ds:XPath>
                </ds:Transform>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha25
6"/>
            <ds:DigestValue>fv2SLuFhadiBPgPUce5karFUoJaNXuI0rC/nHzu6iCQ=
            </ds:DigestValue>
        </ds:Reference>
        <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#
xades-id-ab518763b287d34797a983f809c85e08">
            <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#sha25
6"/>
            <ds:DigestValue>EJWsWr2P6CfgeX5o7jZRQPQUDET5Vy0WVnu66fLKJ60=
            </ds:DigestValue>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue Id="value-id-ab518763b287d34797a983f809c85e08">
        Yeo+zSbZD7jKKE+Gr+4Kq4p0PbGZbbCHKcYOtNuPPg3izwHdwNAamoqoZ/ewJIr2fNtccV
ycdPikWS08u834kNlL+YOm0fX6lmjzMLyw/lhRewwIbJzyKKBCvW8rbjcfz7kqeGv7EZzVKc4hXuTD
/pTx8z5Zu4xGafLK4LdthNGyQBHQujPB2c2cx2s+hpG9TEJXmda0RF3gRG6bv6Z32QvaSWAJtnfXnT
```

```
Uj3RZS8Y/tw3Tm3Vcvj+/1vaKcyFqEVlpk63X8HthJqAr87o+p304Por2Zi0cU0JBoSJBs/1Ds3h1E
3NkB67uyt06jfnC81rNdW1/2L1DuyqW8DACC1A==
    </ds:SignatureValue>
    <ds:KeyInfo>
        <ds:X509Data>
            <ds:X509Certificate>
                MIID6zCCAtOgAwIBAgIETl0ACDANBgkqhkiG9w0BAQsFADCBpTELMAkGA1UEBh
MCSVQxEDAOBgNVBAgTB1Vua25vd24xETAPBgNVBAcTCEJyaW5kaXNpMTYwNAYDVQQKEy1Vbml0ZWQg
TmF0aW9ucyBJbnRlcm5hdGlvbmFsIENvbXB1dGluZyBDZW50ZXIxIjAgBgNVBAsTGUFwcGxpY2F0aW
9uIERlbGl2ZXJ5IFVuaXQxFTATBgNVBAMTDEJlbGFsIFNoYmFpcjAeFw0yMDA5MjQxMTA4MTdaFw0y
MDEyMjMxMTA4MTdaMIGlMQswCQYDVQQGEwJJVDEQMA4GA1UECBMHVW5rbm93bjERMA8GA1UEBxMIQn
JpbmRpc2kxNjA0BgNVBAoTLVVuaXRlZCBOYXRpb25zIEludGVybmF0aW9uYWwgQ29tcHV0aW5nIENl
bnRlcjEiMCAGA1UECxMZQXBwbGljYXRpb24gRGVsaXZlcnkgVW5pdDEVMBMGA1UEAxMMQmVsYWwgU2
hiYWlyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA225UnC/KtuLAOT0AXXeqib5AluBS
j0tBt5OMWQUVqKf6hbJRQRVe29o2fYo7VMrWFVnykDulnDUq3wFqKhbYD0rvHZWdkYLEC5OdpP6vqI
FAS98UEvmYpoUmPBDrtT8z9kCRiU/viC79efLJEVNj7q0Cv/i6STkwLMzNhIk4Hqs0m/GjNC2evVJq
aBodBAQh1wrHIXXAnrWpzNvsbexhPmNI7sNPeicZHWe/adaTcW3yzIbmyP5VkNcco+ruEWMD99oK2x
SVVA0fwGk+kCJhZfdLsCQdEI1saQDkHIkvAkr42epSlNic0Xfb7MJDjFASZTzNdeOFmTDA8y0ypaMi
wwIDAQABoyEwHzAdBgNVHQ4EFgQUttwRShpyDeYoi+5OgOUx6YFoAVcwDQYJKoZIhvcNAQELBQADgg
EBAIqVsg5ImHBQLq8iCKC3NHarYvgOKY+O7Tn01bnfRfdaqAn0dy9QAO5/reSRslu6/qD5THfpg35n
AkNiRP8wt2CF5tabYOlka5oxPm+7ujZfqIJlB0FXuqnBP5JDKVSjBhsD6TWdCwMtgcKtumobgBXmCT
QWTHCxcyIhZsDW2TYrHtjwWfhypSNkC8TaqgXN8oY0T9XzvajQHSylf6aOpwrW0hr/opGyLDw8ajZu
vzC9c5NZT5OvikiCH7lIv4v4Z9D1Dh4QWhCibaQqFZHAGmbPDFW3WUFlIyunkTD9BNYtrGLA1uqQRE
T951flxFTTEX/i2cLgFZAQLk+MKWfQE2o=
            </ds:X509Certificate>
        </ds:X509Data>
    </ds:KeyInfo>
    <ds:Object>
        <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.
3.2#" Target="#id-ab518763b287d34797a983f809c85e08">
            <xades:SignedProperties Id="xades-id-
ab518763b287d34797a983f809c85e08">
                <xades:SignedSignatureProperties>
                    <xades:SigningTime>2020-09-24T11:14:55Z
                    </xades:SigningTime>
                    <xades:SigningCertificateV2>
                        <xades:Cert>
                            <xades:CertDigest>
                                <ds:DigestMethod Algorithm="http://www.w3.org/
2001/04/xmlenc#sha512"/>
                                <ds:DigestValue>F0IDcZIh8YleZLKYCFjydOaynq8qvf
6j/OltJjqK+MbWtr2zQNXQ5BRCr4KCP3F45fzmWIUs17u8XR4c2d66bg==
                                </ds:DigestValue>
                            </xades:CertDigest>
                            <xades:IssuerSerialV2>MIG0MIGrpIGoMIGlMQswCQYDVQQG
EwJJVDEQMA4GA1UECBMHVW5rbm93bjERMA8GA1UEBxMIQnJpbmRpc2kxNjA0BgNVBAoTLVVuaXRlZC
BOYXRpb25zIEludGVybmF0aW9uYWwgQ29tcHV0aW5nIENlbnRlcjEiMCAGA1UECxMZQXBwbGljYXRp
b24gRGVsaXZlcnkgVW5pdDEVMBMGA1UEAxMMQmVsYWwgU2hiYWlyAgROXQAI
                            </xades:IssuerSerialV2>
```

```
                        </xades:Cert>
                    </xades:SigningCertificateV2>
                </xades:SignedSignatureProperties>
                <xades:SignedDataObjectProperties>
                    <xades:DataObjectFormat ObjectReference="#r-id-
ab518763b287d34797a983f809c85e08-1">
                        <xades:MimeType>text/xml
                        </xades:MimeType>
                    </xades:DataObjectFormat>
                </xades:SignedDataObjectProperties>
            </xades:SignedProperties>
        </xades:QualifyingProperties>
    </ds:Object>
</ds:Signature>
```