



Authentication-based signature creation policy for NemID

This document is for public use.

Table of Contents

1. Policy information.....	3
2. Revisions	4
3. Introduction	5
4. Terms and acronyms.....	6
5. Versioning and backwards compatibility	7
6. About Signature Policies	8
7. Scope and structure.....	9
8. Signature creation requirements	10
8.1 Evidence Structure.....	10
9. Signature validation requirements.....	14
10. Limitation of liability	15
11. Appendix A (normative): Certificates used for e-sealing PDF documents.....	16
11.1 Certificate in PEM format:	18

1. Policy Information

Name	Authentication-based signature creation policy for NemID
Document Number	DKB-SP-02282022-1 v1.0
Policy OID	1.3.6.1.4.1.54720.2.3.1
Policy Owner	Dokobit, UAB
Version	1.0
Publish date	2022-02-28

2. Revisions

Date	Specification version	Change
2022-02-15	1.0	Initial version

3. Introduction

This signature policy defines requirements for authentication-based signatures using NemID as authentication mechanism. Authentication-based signatures are Advanced Electronic Signatures as per eIDAS regulation and are uniquely linked to signer by including required evidences to prove signing action by specified signer.

4. Terms And Acronyms

Term	Explanation
IdP	Identity provider.
Seal	This is the Trust Service Provider's signature on the signed document. It is commonly referred to as the <i>Seal</i> .
Signing ceremony	A sequence of activities like presenting the document, asking for the signers consent and the signing itself. The signing ceremony shall be conducted in a way that it afterwards is clear that the signer has willingly signed the document.
TSP	Trust Service Provider - the entity implementing this policy by packaging the signature.
Evidences	Collected evidences from Signing ceremony that are added as an additional metadata in PDF document.
PADES	ETSI TS 103 172 V2.2.2 (2013-04) Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile.
RFC-3161	IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)".
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

5. Versioning And Backwards Compatibility

Signature policy version numbers consist of a major and a minor number, denoting major and minor versions.

A change of minor version is always backward compatible, and the new policy may be brought into effect without notifying relying parties.

A change of major version may introduce non-backward compatible changes.

6. About Signature Policies

The purpose of a signature policy is to specify requirements for the signing process including requirements for signature creation and verification process.

The primary users of this policy will be users using authentication-based signatures (relying parties). The policy will help relying parties to better understand the information contained in an authentication-based signature, and on what basis it can be trusted and used.

7. Scope And Structure

This signature policy defines requirements for creating and validating signature based on an arbitrary method of signer authentication.

The normative parts of the policy are:

General process requirement defines high-level requirements for the overall signing process.

1. **Signature creation requirements** defines requirements for the format used for the signature
2. **Validation requirements** defines the validation of authentication-based signature.

8. Signature Creation Requirements

Authentication-based signatures work in the following way:

1. A Trust Service Provider (TSP) arranges a signing ceremony: It presents the documents to be signed and collects the user's explicit consent/intention to sign the documents.
2. The user authenticates using NemID. The TSP collects authentication proof.
3. The TSP collects traces and context in audit logs.
4. The TSP adds collected evidence as a metadata in XML format to the original PDF document.
5. The TSP seals a PDF document with collected Evidences using TSP's Advanced Electronic Seal with Qualified Certificate.
6. The sealed PDF results as a document with user's signature.

8.1 Evidence Structure

The following information must be collected from Signing Ceremony:

Element/Attribute	Description	Example	Required
Global			
SigningIdentifier	Unique signature identifier in Dokobit system	5e00fb8febc7d2 532fce637ca560 79baaddc6780	true
SigningTime	Signing time in ISO 8601 full date and time format	2022-01-14T11:2 3:27+02:00	true
PolicyId	Policy ID that was used for creating the signature	1.3.6.1.4.1.5472 0.2.3.1	true
LiabilityTier	Liability tier for created signature	1	true
Client Environment			

UserAgent	User agent string representing client environment	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36	true
Ip	Signer IP address	127.0.0.1	true
Server Environment			
Dns	Server DNS address	app.dokobit.com	true
VersionIdentifier	Codebase version identifier	202201131550-d14c26a5e210a227e24ae2f10d062653bc336fc3	true
Signer Details			
Firstname	Signer firstname detected using authentication mechanism	Firstname	true
Lastname	Signer lastname detected using authentication mechanism	Lastname	true
Identifier	Unique signer identifier specifying code type, issuing country and code	PNODK-30101010101	true
Code	Signer code representing unique person in authentication mechanism scope	30101010101	true
CountryCode	Country code specifying in which country code was issued	dk	true
BirthDate	Signer birthdate	1990-01-14	false

User Actions			
Name	Action made by user. Possible values: user-authentication, document-view, document-sign	user-authentication	true
TimeStamp	Action time in ISO 8601 full date and time format	2022-01-14T11:23:27+02:00	true
User Action Details			
Method	Method used for authentication. Possible values: dk_nemid.	dk_nemid	Required only for action "user-authentication"
TransactionId	Transaction identifier in authentication system	7f22fd6a-3d46-4d5a-ae56-6de3c53e1873	Required only for action "user-authentication"

Example of evidence structure:

```
<?xml version="1.0" encoding="utf-8"?>
<DokobitAuthenticationBasedSignature xmlns="https://dokobit.com/authentication-based-signatures" Version="1">
  <SigningIdentifier>5e00fb8feb7d2532fce637ca56079baaddc6780</SigningIdentifier>
  <SigningTime>2022-01-14T11:23:27+02:00</SigningTime>
  <PolicyId>1.3.6.1.4.1.54720.2.3.1</PolicyId>
  <LiabilityTier>1</LiabilityTier>
  <Environment>
    <Client>
      <UserAgent>Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36</UserAgent>
      <Ip>127.0.0.1</Ip>
    </Client>
    <Server>
      <Dns>app.dokobit.com</Dns>
      <VersionIdentifier>202201131550-d14c26a5e210a227e24ae2f10d062653bc336fc3</VersionIdentifier>
    </Server>
  </Environment>
  <SignerDetails>
    <Firstname>Firstname</Firstname>
    <Lastname>Lastname</Lastname>
    <Identifier>PNODK-30101010101</Identifier>
    <Code>30101010101</Code>
    <CountryCode>dk</CountryCode>
    <BirthDate>1990-01-14</BirthDate>
  </SignerDetails>
  <UserActions>
    <UserAction>
      <Name>user-authentication</Name>
      <TimeStamp>2022-01-14T11:23:27+02:00</TimeStamp>
      <Data>
        <Method>dk_nemid</Method>
        <TransactionId>7f22fd6a-3d46-4d5a-ae56-6de3c53e1873</TransactionId>
      </Data>
    </UserAction>
    <UserAction>
      <Name>document-view</Name>
      <TimeStamp>2022-01-14T11:23:27+02:00</TimeStamp>
    </UserAction>
    <UserAction>
      <Name>document-sign</Name>
      <TimeStamp>2022-01-14T11:23:27+02:00</TimeStamp>
    </UserAction>
  </UserActions>
</DokobitAuthenticationBasedSignature>
```

9. Signature Validation Requirements

Authentication-based signatures should be validated in the following way:

1. If a valid seal with any certificate that is specified in Appendix A is found in document, validation of authentication-based signature should continue, otherwise signature does not meet requirements of this policy.
2. Seal dictionary contains "Metadata" element which refers to Collected Evidences in PDF document.
3. Information that resides in Collected Evidences should be treated as a trusted information.

10. Limitation Of Liability

TSP assumes the liability only for the execution of the Signing ceremony and provides the services with two different limitations:

- Tier 1 (Basic Liability). This tier is for the documents that don't exceed the value of EUR 100 as Dokobit will be liable up to EUR 100 per signed document.
- Tier 2 (Advanced Liability). This tier is for the documents that don't exceed the value of EUR 10 000 as Dokobit will be liable up to EUR 10 000 per signed document.

11. Appendix A (Normative): Certificates Used For E-Sealing PDF Documents

The following certificates are used as a trust anchor for creation and validation of authentication-based signatures using NemID.

1. "NemID Signature by Dokobit" Qualified Certificate for Seal is issued by Qualified Trust Service Provider - SK ID Solutions - in accordance with SK ID Solutions Certification Practice Statement for KLASS3-SK - SK-CPS-KLASS3-v8.0 which is available at https://www.sk.ee/upload/files/SK-CPS-KLASS3-EN-v8_0_20190815.pdf.

Certificate details:

Key	Value
Serial number	20 8B B7 A5 D5 5B BA C4 62 16 3C B4 28 1A 78 7D
Valid from	2022-02-23T13:53:38Z
Valid to	2023-03-05T13:53:38Z
Subject information	
Organization identifier	NTRLT-301549834
Serial number	301549834
Location	Vilnius
Country	LT
Organization	Dokobit, UAB
Common name	NemID Signature by Dokobit
Issuer information	

Key	Value
Organization identifier	NTREE-10747013
Organizational unit	Sertifitseerimisteenused
Organization	AS Sertifitseerimiskeskus
Country	EE
Common name	KLASS3-SK 2016

11.1 Certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGYzCCBEugAwIBAgIQIiU3pdVbusRiFjy0KBp4fTANBgkqhkiG9w0BAQsFADCB
hjELMAkGA1UEBhMCRUUxIjAgBgNVBAoMGUFTIFNlcnRpZml0c2VlcmVtaXRzXNlbnR
dXMxITAfBgNVBAsMGFNlcnRpZml0c2VlcmVtaXRzXN0ZWVudXNlZDEXMBUGA1UEYQW0
TLRSRUUtMTA3NDcwMTMxZjZAVBgNVBAMMDktMQVNTMy1TSyAyMDE2MB4XDTIyMDIy
MzEzNTMzOFoXDTIzMDMwNTEzNTMzOFowZSsxGDAWBgNVBGEMD05UUkxULTMwMTU0
OTgzNDESMBAGA1UEBRMjMzAxNTQ5ODM0MRAwDgYDVQIDAdWawXuaXVzMRAwDgYD
VQOHDAAdWawXuaXVzMQswCQYDVQGEwJMVDEVMBMGA1UECgwMRG9rb2JpdCwgVUFC
MSMwIQYDVQDDb0Zw1JRCBTAWduYXR1cmUgYnkRG9rb2JpdDCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAJ6EOPx39nZZLT3q3E/AznpH6yYJqjDSGuXy
U5k0UE669F2f7ooTzrIM7Yy55Q77KZu/ZF/nuXFDnu31hkUxGwjGQ2L/EQS4RjF3
43Ez3k59UU0oBe9aNe6cW8e07t1kJYFaOeRkXHXl+KpmyQZ5idf7Kkn4+xdmfVQJ
W3eZ9HSeLrdGRtDMHfG6WkQ0iR3CWNrPzEyXrZnWan22YyGzq3XUShXvfgAaSdH+
knbaki4qCxDnRimQTVx6dLl8ot7C1vsKNMmcbk6Wukh2TM471XkCIHjVoMmoVysh
ulosrc9RCNJmN6EnVbU4dzHi+uMRu0GVyzVY0pruN5T9aADZ/WcCAwEABa0CABQw
ggGwMAkGA1UdEwQCMAAwUwYDVROGBEwwSjAwBgkrBgEEAc4fBwMwIzAhBggrBgEF
BQcCARYVaHR0cHM6Ly93d3cuc2suZWUvY3BzMAkGBWQAi+xAQQEwCwYJKwYBBAHO
HwkBMB8GA1UdIwQYMBaFAFK5eWPXy8tnBjtnvTgfbdcPQ4ocAMA4GA1UdDwEB/wQE
AwIGQDAdBgNVHQ4EFgQURlwkfmwcmBUK4ZSoyjnmIV90DQ8wewYIKwYBBQUHAQEE
bzBtMCGCCsGAQUFBzABHxodHR0Oi8vYwVhLnNrLmVlL2tsYXNzMy0yMDE2MEEG
CCsGAQUFBzACHjVodHRwczovL2Muc2suZWUvS0xBU1MzLVNlXzIwMTZFRUVDQ1JD
QV9TSEEzODQuZGVyLmNydDCBgAYIKwYBBQUHAQMEdDBYMAgGBGQAjkyBATATBgYE
AI5GAQYwCQYHBAcORgEgAajBRBgYEAI5GAQUwRzBFFj9odHRwczovL3NrLmVlL2Vu
L3JlcG9zaXRvcnkVY29uZGl0aW9ucy1mb3ItZXNlLW9mLWlnLnRlcnRpZmljYXRlc3R
AkVOMA0GCSqGSIb3DQEBwUAA4ICAQB5NNBFWBLDKKnw8QJ20o60pjylDdBHEIT1
JlW6W1G88Kwa/Fs2+KzJbcl+n1yKmzeFeDam3o54JQc2yjMV88HrLF8ss/mfjxLg
2vM+N1fHP+3qkBN45lZymv1H8hezAJbHUBN/6/nKGE7SJXh6gd6cUa33aYNIiINX
B4L05BBNgmiWJDuwqGR3ZrrTHI9puVj90fw2dkYoZYFd1RS25WejCe/cLcQdnkh1
QkGHepKDPDM90FRWTIavAdfRHc1pzODzblX8eyVsnUK40jPJ4t1BVpFskQyinazb
0Pj1pi/P8/GTHJg1IYE4wm0WicM03A96ufnmTp5RARgSk7GTsNqDLV4C5cKWuSYP
Tom7pVup000Zk/bZ0by6XdPbWbUzgSG3pyW+3VZLI8XIO02cvMkXQF/tPm97MQyp
q/g19pivuca5L726Ca7vtyfV8gqjglsn2WfnrHWDzNtFo7SQF0izrVexAr53QAZn
Nz5LS79F7BgrHhmvX7mSU4W/PVuRjL2nK/vCLVyfMkrE6XB8D4p/3iGxhIGRnB9m
GXM8Ssq/IzPkoym+wZllI5VY48XXxUGLpWxYNrdr+L4Mfu040sojbrYu/SzIw+Hn
ehUPc+8iPqomZrFEDSdxhFhoPhaQA8lMgdNPKfgWdKt/C7Mi9fYfsYOR5kwNxAC+
eKUqoJjozA==
-----END CERTIFICATE-----
```