Dokobit
By Signicat

Authentication-based signature creation policy for Finnish Trust Network

This document is for public use.

Dokobit
By Signicat

Table of Contents

Dokobit
By Signicat

1. Policy information

Name	Authentication-based signature creation policy for Finnish Trust Network
Document Number	DKB-SP-02282022-3 v1.1
Policy OID	1.3.6.1.4.1.54720.2.5.1
Policy Owner	Dokobit, UAB
Version	1.1
Publish date	2025-05-20

Dokobit
By Signicat

2. Revisions

Date	Specification version	Change
2022-02-15	1.0	Initial version
2025-03-20	1.1	Updated list of certificates

Dokobit
By Signicat

3. Introduction

This signature policy defines requirements for authentication-based signatures using Finnish Trust Network 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.

Dokobit
By Signicat

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 *Seal*.
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.

Dokobit
By Signicat

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.

Dokobit
By Signicat

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.

Dokobit
By Signicat

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.

Dokobit
By Signicat

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 Finnish Trust Network. 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	5e00fb8febc7d2532fce637ca56079baaddc6780	true
SigningTime	Signing time in ISO 8601 full date and time format	2022-01-14T11:23:27+02:00	true
PolicyId	Policy ID that was used for creating the signature	1.3.6.1.4.1.54720.2.5.1	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	PNOFI-30101010101	true
Code	Signer code representing unique person in authentication mechanism scope	30101010101	true
CountryCode	Country code specifying in which country code was issued	fi	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: ftn.	ftn	Required only for action “user-authentication“
TransactionId	Transaction identifier in authentication system	7f22fd6a-3d46-4d5a-ae56-6de3c53e1873	Required only for action “user-authentication“

Dokobit
By Signicat

Example of evidence structure:

```
<?xml version="1.0" encoding="utf-8"?>
<DokobitAuthenticationBasedSignature xmlns="https://dokobit.com/authentication-based-
signatures" Version="1">
  <SigningIdentifier>5e00fb8febc7d2532fce637ca56079baaddc6780</SigningIdentifier>
  <SigningTime>2022-01-14T11:23:27+02:00</SigningTime>
  <PolicyId>1.3.6.1.4.1.54720.2.5.1</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>PNOFI-30101010101</Identifier>
    <Code>30101010101</Code>
    <CountryCode>fi</CountryCode>
    <BirthDate>1990-01-14</BirthDate>
  </SignerDetails>
  <UserActions>
    <UserAction>
      <Name>user-authentication</Name>
      <TimeStamp>2022-01-14T11:23:27+02:00</TimeStamp>
      <Data>
        <Method>ftn</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>
```

Dokobit
By Signicat

9. Signature validation requirements

Authenticaton-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.

Dokobit
By Signicat

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 Finnish Trust Network.

1. “Finnish Trust Network 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	6F 76 D0 47 09 FC 85 1F 62 16 39 B5 F0 B3 76 D6
Valid from	2022-02-23T13:35:52Z
Valid to	2025-03-24T13:35:52Z
Subject information	
Organization identifier	NTRLT-301549834
Serial number	301549834
Location	Vilnius
Country	LT
Organization	Dokobit, UAB
Common name	Finnish Trust Network Signature by Dokobit
Issuer information	

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

Dokobit
By Signicat

11.1 Certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIGczCCBFugAwIBAgIQb3bQRwn8hR9iFjm18LN21jANBgkqhkiG9w0BAQsFADCB
hjELMAkGA1UEBhMCRUUxIjAgBgNVBAoMGUFTIFNlcnRpZml0c2VlcmltaXNrZXNr
dXMxITAfBgNVBAsMGFNlcnRpZml0c2VlcmltaXN0ZWVudXNlZDEXMBUGA1UEYQwO
TlRSRUUtMTA3NDcwMTMxFzAVBgNVBAMMDktMQVNTMy1TSyAyMDE2MB4XDTIyMDIy
MzEzMzU1MloXDTI1MDMyNDEzMzU1MlowgasxGDAWBgNVBGEMD05UUkxULTMwMTU0
OTgzNDESMBAGA1UEBRMJMzAxNTQ5ODM0MRAwDgYDVQQIDAdWaWxuaXVzMRAwDgYD
VQQHDAdWaWxuaXVzMQswCQYDVQQGEwJMVDEVMBMGA1UECgwMRG9rb2JpdCwgVUFC
MTMwMQYDVQQDDCpGaW5uaXNoIFRydXN0IE5ldHdvcmsgU2lnbmF0dXJlIGJ5IERv
a29iaXQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDfww/+xabGDcn4
btGyG88Ist2lAxGI7mPxWtT3cW30FG6smhcIc/oZ2kinngMzWe3CMQmQ9t5Iem3N
hQMU84/7yCQV0vi7GeP4mu3MmDUnXiumfYyANbwkwOLgbWfD44T35jcwZJutTAO3
Q8aS09O8niclHvGcWQa7ZNPUh5SKD0LpOhtOIs+d49GjMpBKuK0Bzy5s4toHYGZi
ZIPf7Y4r/vCA0teZqYjO0FxozALSUhI5WRB2AItx0wFj1+VO1OP3bbJkDz2gURKo
aQUj1N4wt7O3WCyEX6geBoMXLbbp+OSawychosTZjB1p6nIZYuxGApAKI+KXi+Y+
fMEiSVATAgMBAAWjggG0MIIBsDAJBgNVHRMEAjAAMFMGA1UdIARMMEowMAYJKwYB
BAHOHwcDMCMwIQYIKwYBBQUHAgEWFWh0dHBzOi8vd3d3LnNrLmVlL2NwczAJBgcE
AIvsQAEBMAsGCSsGAQQBzh8JATAfBgNVHSMEGDAWgBSuXlj18vLZwY7Z704H23XK
UOKHADAOBgNVHQ8BAf8EBAMCBkAwHQYDVR0OBBYEFFbYi1vmmoF146ANFMHZFEhD
n5dDMHsGCCsGAQUFBwEBBG8wbTAoBggrBgEFBQcwAYYcaHR0cDovL2FpYS5zay5l
ZS9rbGFzczMtMjAxNjBBBggrBgEFBQcwAoY1aHR0cHM6Ly9jLnNrLmVlL0tMQVNT
My1TS18yMDE2X0VFQ0NSQ0FfU0hBMzg0LmRlci5jcnQwgYAGCCsGAQUFBwEDBHQw
cjAIBgYEAI5GAQEwEwYGBACORgEGMAkGBwQAjkYBBgIwUQYGBACORgEFMEcwRRY/
aHR0cHM6Ly9zay5lZS9lbi9yZXBvc2l0b3J5L2NvbmRpdGlvbnMtZm9yLXVzZS1v
Zi1jZXJ0aWZpY2F0ZXMvEwJFTjANBgkqhkiG9w0BAQsFAAOCAgEAY0aRiOBiSu6u
Wa2DaCqSX3JZLyLWTElG7AZtuv1W3TwJkScYL99jJQAJr1unXXKA3nLaniLhQlYl
hqjWbevqJt5rPaEplttWxDNZuhlz1RGemeO+2poUUzfH/xGw8XB3v9XhFUQ6wdm1
3IYug//UMK/zP+CComVbzyzGJ8oyoX2f21I7+OJMpHLnZKfjxnFVAxJIei75ewa+
G4QYOnYV08u7RNMUb4L7RIsLth5lE8ge7xmYFy9kJSKaioKCwaW8kXlbA9TBolBi
G0Uk8d/uL0aUzDhAQcPtpp9ePWhkmucdXBc6J5L486CrjMlVxkgCiXJGPY1+Jx0B
F7+9mQTUzuWG7iw7UZ9Fv/txNed1WloYP+RWTPTEgMecEB+8mavY6yl5s/4fW0ZM
ADIFIQFVudKy7slbzRx0XarhIsuwQWzWwN9g2c4hMi+5BFQJW0GTqcJQkOI3kATb
ZGdsK/K2n4xpspl9HDkyc55lhhZm/0jLJgADbFCoTiS+W58WbqGlhpKs+ZMULYJe
ZeX2KmXdt34emjKxCdHWEIsW2e5A/Abk+OKLTRuHwdiuusAVJU2sqyd76o1cDK1s
00NlraspxsPiQF2X1gQxy+eNuM+NhXIsXGLPWkdvY4JM/EoWgffJrn4QlXuD8r33
JzgyJUR0BjgMSZ/R4eAWobH2eAenwsI=
-----END CERTIFICATE-----
```

2. “Finnish Trust Network 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 organisation certificates which is available at *https://www.skidsolutions.eu/wp-content/uploads/2025/01/SK-CPS-Organisation_Certificates-EN-v14_0_20250303.pdf*.

Certificate details:

Key	Value
Serial number	16 69 39 FB 77 5C B6 BC C3 F9 F5 67 64 B3 3C 52
Valid from	2025-03-20T11:46:34Z
Valid to	2028-04-18T11:46:33Z
Subject information	
Organization identifier	NTRLT-301549834
Serial number	301549834
Location	Vilnius
Country	LT
Organization	Dokobit, UAB
Common name	Finnish Trust Network Signature by Dokobit
Issuer information	
Organization identifier	NTREE-10747013
Organization	SK ID Solutions AS
Country	EE
Common name	SK ID Solutions ORG 2021E

Dokobit
By Signicat

11.2 Certificate in PEM format:

```
-----BEGIN CERTIFICATE-----
MIIFADCCBIagAwIBAgIQFmk5+3dctrzD+fVnZLM8UjAKBggqhkjOPQQDAzBnMQsw
CQYDVQQGEwJFRTEbMBkGA1UECgwSU0sgSUQgU29sdXRpb25zIEFTMRcwFQYDVQRh
DA5OVFJFRS0xMDc0NzAxMzEiMCAGA1UEAwwZU0sgSUQgU29sdXRpb25zIE9SRyAy
MDIxRTAeFw0yNTAzMjAxMTQ2MzRaFw0yODA0MTgxMTQ2MzNaMIGrMTMwMQYDVQQD
DCpGaW5uaXNoIFRydXN0IE5ldHdvcmsgU2lnbmF0dXJlIGJ5IERva29iaXQxEjAQ
BgNVBAUTCTMwMTU0OTgzNDEYMBYGA1UEYQwPTlRSTFQtMzAxNTQ5ODM0MRUwEwYD
VQQKDAxEb2tvYml0LCBVQUIxEDAOBgNVBAcMB1ZpbG5pdXMxEDAOBgNVBAgMB1Zp
bG5pdXMxCzAJBgNVBAYTAkxUMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAu5AGw3jGMYZF8u16QKMMEJxAHYn6GkYWnLv93PG4mWo5meij0kd4pwaq9Pw4
YNP7YF6aeWx6HRwZEs3yizK/R+HbP/FBuI0gZM4sv0Fsi5EnxcjexuYxP3RheDK2
1lE3Z+w2M8vm077K39WMCecV3O3RW/hIwgfsRTpVkCNmEZSQyiaeU9hTYYtAO6pO
4hPRByfPb3N6ta7jS+1/E6w2v159Zh/oZH/y0S3CvdzyYE+/g1BLMXo+hqg6nK3s
oAVK5yIn1X66p/woE4iH6N/XXHdnAljMRrVffjJfzsd7mO7rXLznJAjuqUsl7fd5
tjWsYMhk2jPeaoBh9sFmwLXSdQIDAQAFo4ICAjCCAf4wCQYDVR0TBAIwADAfBgNV
HSMEGDAWgBT8ief8Q3j/7CzDhKijgOMjSBrUKDBjBggrBgEFBQcBAQRXMFUwLAYI
KwYBBQUHMAKGIGh0dHA6Ly9jLnNrLmVlL09SR18yMDIxRS5kZXIuY3J0MCUGCCsG
AQUFBzABhhlodHRwOi8vYWlhLnNrLmVlL29yZzIwMjFlMIGGBgNVHSAEfzB9MAkG
BwQAi+xAAQEwCwYJKwYBBAHOHwkBMGMGCSsGAQQBzh8HAzBWMFQGCCsGAQUFBwIB
FkhodHRwczovL3d3dy5za2lkc29sdXRpb25zLmV1L3Jlc291cmNlcy9jZXJ0aWZp
Y2F0aW9uLXByYWN0aWNlLXN0YXRlbWVudC8wgYAGCCsGAQUFBwEDBHQwcjAIBgYE
AI5GAQEwEwYGBACORgEGMAkGBwQAjkYBBgIwUQYGBACORgEFMEcwRRY/aHR0cHM6
Ly9zay5lZS9lbi9yZXBvc2l0b3J5L2NvbmRpdGlvbnMtZm9yLXVzZS1vZi1jZXJ0
aWZpY2F0ZXMvEwJlbjAwBgNVHR8EKTAnMCWgI6Ahhh9odHRwOi8vYy5zay5lZS9z
a19vcmdfMjAyMWUuY3JsMB0GA1UdDgQWBBSBeip1rLMYJToh0xVSP/MT0ZAejAO
BgNVHQ8BAf8EBAMCBkAwCgYIKoZIzj0EAwMDaAAwZQIwDsXqWMlilO68QBNcx31Z
zug6JIFuxxe894/Zy/VXZdI5B3b4BrUHf0sqwc5WCOD9AjEAtvsZKITSDU80K7Cu
E9aqsSrko8qY+YUIMKxVrbZ+c/r7svGblglzbZ8HJ0ZQ5GdY
-----END CERTIFICATE-----
```