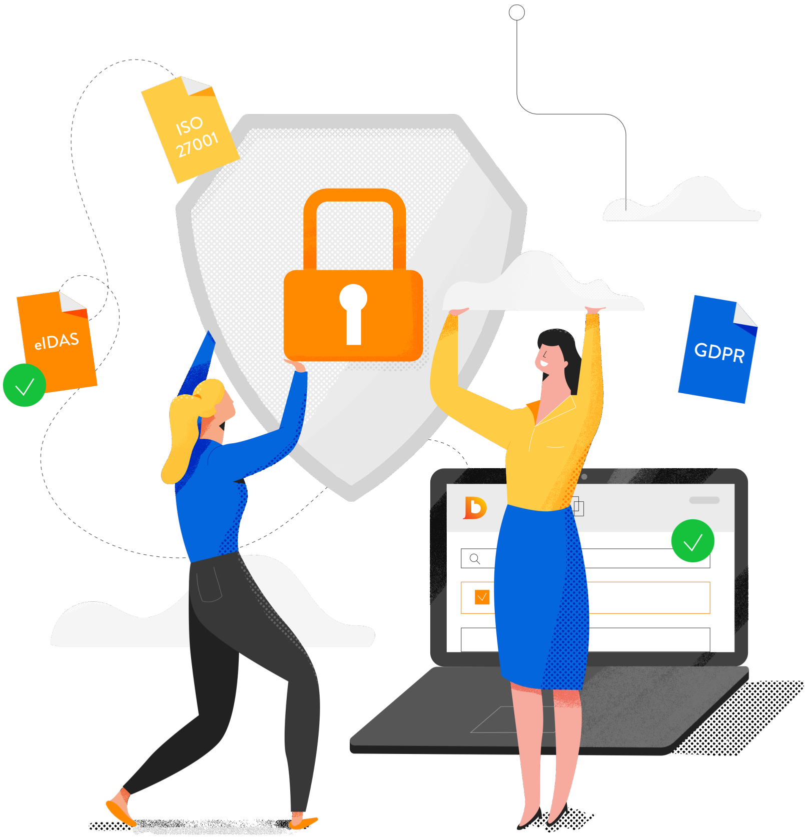
Dokobit
Part of Signicat



Authentication-based signature creation policy for iDIN

This document is for public use.

https://www.dokobit.com

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 iDIN
Document Number	DKB-SP-02282022-4 v1.0
Policy OID	1.3.6.1.4.1.54720.2.6.1
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 iDIN 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 *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.

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 iDIN. 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	1.3.6.1.4.1.54720.2.6.1	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	PNONL-30101010101	true
Code	Signer code representing unique person in authentication mechanism scope	30101010101	true
CountryCode	Country code specifying in which country code was issued	nl	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: idin.	idin	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>5e00fb8febc7d2532fce637ca56079baaddc6780</SigningIdentifier>
  <SigningTime>2022-01-14T11:23:27+02:00</SigningTime>
  <PolicyId>1.3.6.1.4.1.54720.2.6.1</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>PNONL-30101010101</Identifier>
    <Code>30101010101</Code>
    <CountryCode>nl</CountryCode>
    <BirthDate>1990-01-14</BirthDate>
  </SignerDetails>
  <UserActions>
    <UserAction>
      <Name>user-authentication</Name>
      <TimeStamp>2022-01-14T11:23:27+02:00</TimeStamp>
      <Data>
        <Method>idin</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

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.

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 iDIN.

1. “iDIN 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	5D 70 B0 11 09 EB F0 52 62 16 3B E4 FE 80 82 A7
Valid from	2022-02-23T13:50:14Z
Valid to	2025-03-24T13:50:14Z
Subject information	
Organization identifier	NTRLT-301549834
Serial number	301549834
Location	Vilnius
Country	LT
Organization	Dokobit, UAB
Common name	iDIN 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-----
MIIGYjCCBEqgAwIBAgIQXXCwEQnr8FJiFjvk/oCCpzANBgkqhkiG9w0BAQsFADCB
hjELMAkGA1UEBhMCRUUxIjAgBgNVBAoMGUFTIFNlcnRpZml0c2VlcmltaXNrZXNr
dXMxITAfBgNVBAsMGFNlcnRpZml0c2VlcmltaXN0ZWVudXNlZDEXMBUGA1UEYQwO
TlRSRUUtMTA3NDcwMTMxFzAVBgNVBAMMDktMQVNTMy1TSyAyMDE2MB4XDTIyMDIy
MzEzNTAxNFoXDTI1MDMyNDEzNTAxNFowgZoxGDAWBgNVBGEMD05UUkxULTMwMTU0
OTgzNDESMBAGA1UEBRMJMzAxNTQ5ODM0MRAwDgYDVQQIDAdWaWxuaXVzMRAwDgYD
VQQHDAdWaWxuaXVzMQswCQYDVQQGEwJMVDEVMBMGA1UECgwMRG9rb2JpdCwgVUFC
MSIwIAYDVQQDDBlpRElOIFNpZ25hdHVyZSBieSBEb2tvYml0MIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyUuGcjnnlw3IM8gmIj0ZsdJ5s/qL/dz1+siG
Cto+9TwOqLAk5OlByVEf9OxaThoQW5mVaxnC8PJ+xemFZQ/qPPs00cIb5rwZVy5c
m35d0b+fJgTr0aQc3bHCaXlwIrJ59VdWjcwhYop6Az04Qy+Av6imHvdfD36BDibU
Reuf36wuKgw2X0jvDwkL0JUYlx3dFNsxvOZweJLfU15hlzoW/PeMAhtPWAKpT1+U
qIBmo0Iy1oRltLD9+1XaBxaw2UzSeNe4+D4IeTmVOh3wnHzXlkTTRTMnXMILftZD
r90Jmfgpp+7N690Pv3XYE1sqzZw1mWD/WbKmCCP7gzT9GX7s6QIDAQAFo4IBtDCC
AbAwCQYDVR0TBAIwADBTBgNVHSAETDBKMDAGCSsGAQQBzh8HAzAjMCEGCCsGAQUF
BwIBFhVodHRwczovL3d3dy5zay5lZS9jcHMwCQYHBACL7EABATALBgkrBgEEAc4f
CQEwHwYDVR0jBBgwFoAUrl5Y9fLy2cGO2e9OB9t1ylDihwAwDgYDVR0PAQH/BAQD
AgZAMB0GA1UdDgQWBBQAo/3eOVetvHVcsdxWXQEwMzMgJzB7BggrBgEFBQcBAQRv
MG0wKAYIKwYBBQUHMAGGHGh0dHA6Ly9haWEuc2suZWUva2xhc3MzLTIwMTYwQQYI
KwYBBQUHMAKGNWh0dHBzOi8vYy5zay5lZS9LTEFTUzMtU0tfMjAxNl9FRUNDUkNB
X1NIQTM4NC5kZXIuY3J0MIGABggrBgEFBQcBAwR0MHIwCAYGBACORgEBMBMGBgQA
jkYBBjAJBgcEAI5GAQYCMFEGBgQAjkYBBTBHMEUWP2h0dHBzOi8vc2suZWUvZW4v
cmVwb3NpdG9yeS9jb25kaXRpb25zLWZvci11c2Utb2YtY2VydGlmaWNhdGVzLxMC
RU4wDQYJKoZIhvcNAQELBQADggIBAGa05tDmmwicBcOBcgcN3qv370fATYnDBKAA
ej5HpTAWRkmBKEYwpt8XAndgdkKmmAQfvNM2n1E/E/A7ofmox5jG1vg1YlFYyRwI
h5KmPDj5l1PyZ0I20gFnObzlnufNgLAwbbkHNXy922IafkZ+4Vi7/SyRDxE5eZHp
YCW5kYtnqAXIDyqSLFRMjWaoZrWASk3b71iR8UTZfHdnZnB84ZRPHOWzS8+6V1Qi
yHHj0Elh7gUaDQnJ5TAygcqXswLGYxPoSRXvTyb6A9r2//UEzsLOSPGmMFm4axqs
+8DClMBdq/YOejIDCK7V09s3bxQZ3ZUv2oKwOqOOACTam5a/gmkZ/HL4lpnFlzJy
lXj8TOM8ZvJaaY3xHOFNO+ATfgApGqQce0Irh+CT5xYAz4HQys8nylfn8QNCXlme
Hqb8q/JZrGtp60r9cdXZxUVMtka+3vu9JZqcU0D+S4vfu1t8SOylu+hw2wVpIBMq
I0dAYXTSNyT25QhELEqrjw7g52AsqMbTrCEoeXgRjaeZi6Byq7+46Lv9Qp1XZaYx
PXkyGt42b4nY4vFxU/cvF8MGR/FkoeTN9hBC6VzB9ckuVlsTBZ05Y0lNRXCm6J8J
MiSuMXgkOH/wj9+kjcF5mDDYxFK0y6gJLUJzU4p/aeWAOunqkogx1SxJ2sE4J1zn
I4SowqCc
-----END CERTIFICATE-----
```