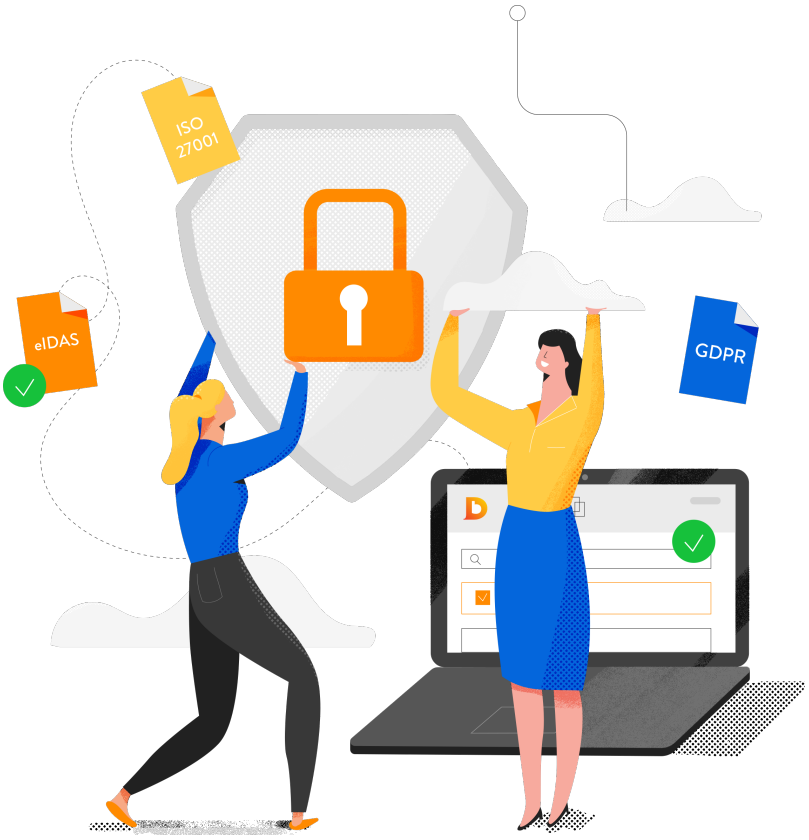
Dokobit
Part of Signicat



Authentication-based signature creation policy for Swedish BankID

This document is for public use.

Table of Contents

1. Policy Information

Name	Authentication-based signature creation policy for Swedish BankID
Document Number	DKB-SP-02152022 v1.0
Policy OID	1.3.6.1.4.1.54720.2.2.1
Policy Owner	Dokobit, UAB
Version	1.0
Publish date	2022-02-15

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 Swedish BankID 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 Swedish BankID. 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	1.3.6.1.4.1.54720.2.2.1	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	PNOSE-30101010101	true
Code	Signer code representing unique person in authentication mechanism scope	30101010101	true
CountryCode	Country code specifying in which country code was issued	se	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: se_bankid.	se_bankid	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>1.3.6.1.4.1.54720.2.2.1</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>PNOSE-30101010101</Identifier>
    <Code>30101010101</Code>
    <CountryCode>se</CountryCode>
    <BirthDate>1990-01-14</BirthDate>
  </SignerDetails>
  <UserActions>
    <UserAction>
      <Name>user-authentication</Name>
      <TimeStamp>2022-01-14T11:23:27+02:00</TimeStamp>
      <Data>
        <Method>se_bankid</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 Swedish BankID.

1. “BankID 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	4E 8C 83 1B CA 43 22 6A 62 13 7C 52 B3 D3 A6 9F
Valid from	2022-02-21T11:48:00Z
Valid to	2025-03-22T11:48:00Z
Subject information	
Organization identifier	NTRLT-301549834
Serial number	301549834
Location	Vilnius
Country	LT
Organization	Dokobit, UAB
Common name	BankID 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-----
MIIGZDCCBEygAwIBAgIQToyDG8pDImpiE3xSs9OmnzANBgkqhkiG9w0BAQsFADCB
hjELMAkGA1UEBhMCRUUxIjAgBgNVBAoMGUFTIFNlcnRpZml0c2VlcmltaXNrZXNr
dXMxITAfBgNVBAsMGFNlcnRpZml0c2VlcmltaXN0ZWVudXNlZDEXMBUGA1UEYQwO
TlRSRUUtMTA3NDcwMTMxFzAVBgNVBAMMDktMQVNTMy1TSyAyMDE2MB4XDTIyMDIy
MTExNDgwMFoXDTI1MDMyMjExNDgwMFowgZwxGDAWBgNVBGEMD05UUkxULTMwMTU0
OTgzNDESMBAGA1UEBRMJMzAxNTQ5ODM0MRAwDgYDVQQIDAdWaWxuaXVzMRAwDgYD
VQQHDAdWaWxuaXVzMQswCQYDVQQGEwJMVDEVMBMGA1UECgwMRG9rb2JpdCwgVUFC
MSQwIgYDVQQDDBtCYW5rSUQgU2lnbmF0dXJlIGJ5IERva29iaXQwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC0/OTEpSpMn239+g9ADn86tNA6ZYAJhDWy
c2AvjJQHsfD7tN9nVnFXBFHkPllp5F6Yzu2kq0PyA44bl2shd6AnJLzaJa6QmVUF
5dCcqTEq3lMFOq5kJqWMJXcpXDARkRXy8w4ZItAUKJs9h9trMklWNB8OA92+Rav1
Zw9qocQnxrQ6DpsVMBm9iOvSXNpJiQ6mlAFj4LyMEagjEcH7oG2ikII5JcGjeSW+
4g6g2T3mt8nrLxR68eh2E5dDdL84uEl3sKbx0wO4Nop4ehB48dWWvYLx5NCkiHIV
oDThEnIuK7uMl/yi9uEThr+3FnlzQ2Mn7oQse3cLKqVChkqtj/dnAgMBAAWjggG0
MIIBsDAJBgNVHRMEAjAAMFMGA1UdIARMMEowMAYJKwYBBAHOHwcDMCMwIQYIKwYB
BQUHAgEWFWh0dHBzOi8vd3d3LnNrLmVlL2NwczAJBgcEAIvsQAEBMAsGCSsGAQQB
zh8JATAfBgNVHSMEGDAWgBSuXlj18vLZwY7Z704H23XKUOKHADAOBgNVHQ8BAf8E
BAMCBkAwHQYDVR0OBBYEFAyXUeuI7bWXgUbf5GRUHHPkNOwUMHsGCCsGAQUFBwEB
BG8wbTAoBggrBgEFBQcwAYYcaHR0cDovL2FpYS5zay5lZS9rbGFzczMtMjAxNjBB
BggrBgEFBQcwAoY1aHR0cHM6Ly9jLnNrLmVlL0tMQVNTMy1TS18yMDE2X0VFQ0NS
Q0FfU0hBMzg0LmRlci5jcnQwgYAGCCsGAQUFBwEDBHQwcjAIBgYEAI5GAQEwEwYG
BACORgEGMAkGBwQAjkYBBgIwUQYGBACORgEFMEcwRRY/aHR0cHM6Ly9zay5lZS9l
bi9yZXBvc2l0b3J5L2NvbmRpdGlvbnMtZm9yLXVzZS1vZi1jZXJ0aWZpY2F0ZXMv
EwJFTjANBgkqhkiG9w0BAQsFAAOCAgEAGKWXVLDLce1ZfVJ61odOl0EtuIWXF6fT
ORVtb6j9JdfDodnRD7ZbUNdd+cQzNy3cYWQyscEfiyoa98SLFtAJsTvKjYNu7vdC
/ghiTTPBth5LWBjtnngFAFqsrv05TNcB9jX03r1c1uEwjpvBE6aI0RkzjBqnRgCE
NHd/Bagq9M9zm+o7ozsLNR/3WCZLvyy/G0vRQyx8AZBSbEDYSZcf0rORE534Ofq2
bv31ErRfTnG7DWMH7a3zh5uB0m7ZCM9Xxp7xxs/h1cNjnnFGzj+fvN3W5usyoqit
WQlCNUrIDa6uhR05a3Uv5eL56jELYIW5tP7Zs3FXr7wsehbX63uOMkQxYl02t2eB
ODtUaT5k47EkLkZjS1MHLynWeQcALSFtn4WoOOZPB/U9FEE6k0teb7euBVcuWYud
LXHzLFPDLJAZyNhpJSZYjOd1RJOl7DYrMVoPiW452aKec/JEZm4Af2+z1Tw1Ako8
CEG/MIY+HwfaKbpNYG6bro7jaCh44t2rZifktDSce/pax8k1Y4bAQcM7/XEvijS5
0neZ/JYReQWhb6jAnknh7b3Pu1/yObEnf37fGRgDH1ms2B6JqvPzlAQvMX59Eyg/
YgWkSKx96kAv0L1fOmjXg7m3qY2ZHtOPyRoo1uvIhTqI3WxAW6vUs13oBWGVxODb
Zk/iNBjWGew=
-----END CERTIFICATE-----
```