Dokobit
By Signicat

SMS OTP signature creation policy

This document is for public use.

Dokobit
By Signicat

Table of Contents

Dokobit
By Signicat

1. Policy Information

Name	SMS OTP signature creation policy
Document Number	DKB-SP-09052023-1 v1.0
Policy OID	1.3.6.1.4.1.54720.2.7.1
Policy Owner	Dokobit, UAB
Version	1.0
Publish date	2023-09-05

Dokobit
By Signicat

2. Revisions

Date	Specification version	Change
2023-09-05	1.0	Initial version

Dokobit
By Signicat

3. Introduction

This signature policy defines requirements for signatures using SMS OTP as a verification mechanism. SMS OTP signatures are Simple Electronic Signatures as per eIDAS regulation and are linked to signer by including required evidences to prove signing action using specific phone number.

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 SMS OTP signatures (relying parties). The policy will help relying parties to better understand the information contained in an SMS OTP 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 SMS OTP signature.

Dokobit
By Signicat

8. Signature Creation Requirements

SMS OTP 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 confirms the intention to sign by entering a One Time Password that was sent by SMS using provided phone number. The TSP collects verification 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	2023-09-05T11:23:27+02:00	true
PolicyId	Policy ID that was used for creating the signature	1.3.6.1.4.1.54720.2.7.1	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	202309051550-d14c26a5e210a227e24ae2f10d062653bc336fc3	true
Signer Details			
Firstname	Signer firstname	Firstname	true
Lastname	Signer lastname	Lastname	true
Identifier	Unique signer identifier specifying code type, issuing country and code	+37060000000	true
CountryCode	Country code specifying in which country phone number was issued	lt	true
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	2023-09-05T11:23:27+02:00	true
User Action Details			
Method	Method used for authentication. Possible values: sms_otp.	sms_otp	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>2023-09-05T11:23:27+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>+37060000000</Identifier>
    <Code></Code>
    <CountryCode>lt</CountryCode>
  </SignerDetails>
  <UserActions>
    <UserAction>
      <Name>user-authentication</Name>
      <TimeStamp>2023-09-05T11:23:27+02:00</TimeStamp>
      <Data>
        <Method>sms_otp</Method>
        <TransactionId>7f22fd6a-3d46-4d5a-ae56-6de3c53e1873</TransactionId>
      </Data>
    </UserAction>
    <UserAction>
      <Name>document-view</Name>
      <TimeStamp>2023-09-05T11:23:27+02:00</TimeStamp>
    </UserAction>
    <UserAction>
      <Name>document-sign</Name>
      <TimeStamp>2023-09-05T11:23:27+02:00</TimeStamp>
    </UserAction>
  </UserActions>
</DokobitAuthenticationBasedSignature>
```

Dokobit
By Signicat

9. Signature Validation Requirements

SMS OTP 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 SMS OTP 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.

Dokobit
By Signicat

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 SMS OTP signatures.

1. “SMS OTP 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	5F EB 32 AA 26 0E AF 1A 64 E3 10 0E AF 20 53 78
Valid from	2023-08-21T07:18:40Z
Valid to	2026-09-19T07:18:40Z
Subject information	
Organization identifier	NTRLT-301549834
Serial number	301549834
Location	Vilnius
Country	LT
Organization	Dokobit, UAB
Common name	SMS OTP 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-----
MIIGZTCCBE2gAwIBAgIQX+syqiYOrxpk4xAOryBTeDANBgkqhkiG9w0BAQsFADCB
hjELMAkGA1UEBhMCRUUxIjAgBgNVBAoMGUFTIFNlcnRpZml0c2VlcmltaXNrZXNr
dXMxITAfBgNVBAsMGFNlcnRpZml0c2VlcmltaXN0ZWVudXNlZDEXMBUGA1UEYQwO
TlRSRUUtMTA3NDcwMTMxFzAVBgNVBAMMDktMQVNTMy1TSyAyMDE2MB4XDTIzMDgy
MTA3MTg0MFoXDTI2MDkxOTA3MTg0MFowgZ0xGDAWBgNVBGEMD05UUkxULTMwMTU0
OTgzNDESMBAGA1UEBRMJMzAxNTQ5ODM0MRAwDgYDVQQIDAdWaWxuaXVzMRAwDgYD
VQQHDAdWaWxuaXVzMQswCQYDVQQGEwJMVDEVMBMGA1UECgwMRG9rb2JpdCwgVUFC
MSUwIwYDVQQDDBxTTVMgT1RQIFNpZ25hdHVyZSBieSBEb2tvYml0MIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsQXK29avkfP2AcLpAWf3FLqeB2JG2zB6
QkYNVsQBUkgJfs453amswVFOUFcu5QP65oVYbco+h8oco4hqAKcU1vVo5IJsSRbN
657yUR/UGV9N1ciXgkfYNTjEoWvFbZ3DHqZjOOMtZErOuA1/1pTR9R9fM42jMQRO
H9XVbd7D4l6tgl+ns3Zdc5wbyyJnM6tozDvrVR0F2CaKAqSx2juBtjCZz7x+cGMn
PZe+G1O58VuwcUMNFrnVlRO92GCxqUlziPMqPh9JQhvzcnzmd9Q3PDgRD+HtO5SH
3RT+S2G4ZU35KxGfqo1YNYrkfgwe3QOWCyGFNGY1XIQtsw29lmLhtQIDAQAFo4IB
tDCCAbAwCQYDVR0TBAIwADBTBgNVHSAETDBKMDAGCSsGAQQBzh8HAzAjMCEGCCsG
AQUFBwIBFhVodHRwczovL3d3dy5zay5lZS9jcHMwCQYHBACL7EABATALBgkrBgEE
Ac4fCQEwHwYDVR0jBBgwFoAUrl5Y9fLy2cGO2e9OB9t1ylDihwAwDgYDVR0PAQH/
BAQDAgZAMB0GA1UdDgQWBBRp16ie87XrM6ZWHmaNRWwGkzd/cTB7BggrBgEFBQcB
AQRvMG0wKAYIKwYBBQUHMAGGHGh0dHA6Ly9haWEuc2suZWUva2xhc3MzLTIwMTYw
QQYIKwYBBQUHMAKGNWh0dHBzOi8vYy5zay5lZS9LTEFTUzMtU0tfMjAxNl9FRUND
UkNBX1NIQTM4NC5kZXIuY3J0MIGABggrBgEFBQcBAwR0MHIwCAYGBACORgEBMBMG
BgQAjkYBBjAJBgcEAI5GAQYCMFEGBgQAjkYBBTBHMEUWP2h0dHBzOi8vc2suZWUv
ZW4vcmVwb3NpdG9yeS9jb25kaXRpb25zLWZvci11c2Utb2YtY2VydGlmaWNhdGVz
LxMCRU4wDQYJKoZIhvcNAQELBQADggIBAF3HV3FcB8OHwWAa4AvU7y3H0SjOwm44
GFuxxkB+Royt1U+GHuWHaqNHmrMUB9QAvsx625ERdIXD7FgNPqW5g2L+r6anTrw+
iuP+CQsloJ/6Jpa2VPV21XGkhqOkEvPTY+2G9+XARJQr9hUWscILZ6GdU7fABOPD
oOGOnTZzMCBmaNYyHloED6padbTExqVwdkgpylMJ7pusvhTbjArkZ0YkvrqBA4W0
n2+IOBVMruLIyvbjjllxbFXoTD9lm0eFzmG5+8S/W0f3h8l+DxdymEm2MvTdK+zd
VWXvtWS9IyTvKK0wSRwRImW5ewQ9U+1O4kOcsk7aPJ7+7HRnMVu8mTvUOsXmp0Bq
5gLjI+n3oFvdS4JcL1TWJ/sriPfQRVU4BiajmHkP4OnrNLeXecF2m2kffui2W1cE
omzU4tseILvkMFZhITtId4QPIpFO43THaXMN1MGw6zxsgGUoZO1aB55+VSfClq63
GBue7nd4k3tGY7h8LhVbnqTOR8VvUUaj41qnecHsHSpQKEC892Y1/MdzhiGuoOwX
WdYztp1onCHP0CVqFZB/vncp4ClEBVoPK0EcfK/hInCm82Tc9PKdzOBkBMTgM7tw
Fm8bp1Ivrk3Zp65Zr0HOp25xtFfxHcIRGnpJ7q/d5RgGX6KXPc8F44KyOV2JLVhF
EAoAGSvNAhkk
-----END CERTIFICATE-----
```