Workgroup: Network Working Group
Internet-Draft: draft-santesson-svt-pdf-03
Published: 21 March 2022
Intended Status: Informational
Expires: 22 September 2022
Authors: S. Santesson R. Housley
IDsec Solutions Vigil Security

PDF Signature Validation Token

Abstract

This document defines a PDF profile for the Signature Validation Token defined in [SVT].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 22 September 2022.

Table of Contents

1. Introduction

The "Signature Validation Token" specification [SVT] defines a basic token to support signature validation in a way that can significantly extend the lifetime of a signature.

This specification defines a profile for implementing SVT with a signed PDF document, and defines the following aspects of SVT usage:

- How to include reference data related to PDF signatures and PDF documents in an SVT.

- How to add an SVT token to a PDF document.

PDF document signatures are added as incremental updates to the signed PDF document and signs all data of the PDF document up until the current signature. When more than one signature is added to a PDF document the previous signature is signed by the next signature and can not be updated with additional data after this event.

To minimize the impact on PDF documents with multiple signatures and to stay backwards compatible with PDF software that do not understand SVT, PDF documents add one SVT token for all signatures of the PDF as an extension to a document timestamp added to the signed PDF as an incremental update. This SVT covers all signatures of the signed PDF.

2. Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The definitions in [SVT] apply also to this document.

3. SVT in PDF Documents

The SVT for a signed PDF document MAY provide signature validation information about any of the present signatures in the PDF. The SVT MUST contain a separate "sig" claim (Signature object) for each signature on the PDF that is covered by the SVT.

An SVT added to a signed PDF document MUST be added to a document timestamp accordance with ISO 32000-2:2017 [ISOPDF2].

The document timestamp contains an [RFC3161] timestamp token (TSTInfo) in EncapsulatedContentInfo of the CMS signature. The SVT MUST be added to the timestamp token (TSTInfo) as an Extension object as defined in Section 3.1.

3.1. SVT Extension to Timestamp Tokens

The SVT extension is an Extension suitable to be included in TSTInfo as defined by [RFC3161].

The SVT extension is identified by the Object Identifier (OID) 1.2.752.201.5.2

Editors note: This is the current used OID. Consider assigning an IETF extension OID.

This extension data (OCTET STRING) holds the bytes of SVT JWT, represented as a UTF-8 encoded string.

This extension MUST NOT be marked critical.

Note: Extensions in timestamp tokens according to [RFC3161] are imported from the definition of the X.509 certificate extensions defined in [RFC5280].

4. SVT Claims

4.1. Profile Identifer

When this profile is used the SigValidation object MUST contain a "profile" claim with the value "PDF".

4.2. Signature Reference Data

The SVT Signature object MUST contain a "sig_ref" claim (SigReference object) with the following elements:

* "id" -- Absent or a Null value.

* "sig_hash" -- The hash over the signature value bytes.

*"sb_hash" -- The hash over the DER encoded SignedAttributes in SignerInfo.

4.3. Signed Data Reference Data

The SVT Signature object MUST contain one instance of the "sig_data" claim (SignedData object) with the following elements:

*"ref" -- The string representation of the ByteRange value of the PDF signature dictionary of the target signature. This is a sequence of integers separated by space where each integer pair specifies the start index and length of a byte range.

*"hash" -- The hash of all bytes identified by the ByteRange value. This is the concatenation of all byte ranges identified by the ByteRange value.

4.4. Signer Certificate References

The SVT Signature object MUST contain a "signer_cert_ref" claim (CertReference object). The "type" parameter of the "signer_cert_ref" claim MUST be either "chain" or "chain_hash".

*The "chain" type MUST be used when signature validation was performed using one or more certificates where some or all of the certificates in the chain are not present in the target signature.

*The "chain_hash" type MUST be used when signature validation was performed using one or more certificates where all of the certificates are present in the target signature.

Note: The referenced signer certificate MUST match any certificates referenced using ESSCertID or ESSCertIDv2 from [RFC5035].

5. JOSE Header

5.1. SVT Signing Key Reference

The SVT JOSE header must contain one of the following header parameters in accordance with [RFC7515], for storing a reference to the public key used to verify the signature on the SVT:

*"x5c" -- Holds an X.509 certificate [RFC5280] or a chain of certificates. The certificate holding the public key that verifies the signature on the SVT MUST be the first certificate in the chain.

*"kid" -- A key identifier holding the Base64 encoded hash value of the certificate that can verify the signature on the SVT. The

hash algorithm MUST be the same hash algorithm used when signing the SVT as specified by the alg header parameter. The referenced certificate SHOULD be the same certificate that was used to sign the document timestamp that contains the SVT.

6. IANA Considerations

This document has no IANA actions.

7. Security Considerations

The security considerations of [SVT] applies also to this document.

8. Normative References

[ISOPDF2] ISO, "Document management -- Portable document format -- Part 2: PDF 2.0", ISO 32000-2, July 2017.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3161] Adams, C., Cain, P., Pinkas, D., and R. Zuccherato, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", RFC 3161, DOI 10.17487/RFC3161, August 2001, <https://www.rfc-editor.org/info/rfc3161>.

[RFC5035] Schaad, J., "Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility", RFC 5035, DOI 10.17487/RFC5035, August 2007, <https://www.rfc-editor.org/info/rfc5035>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/info/rfc7515>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[SVT] Santesson, S. and R. Housley, "Signature Validation Token", IETF draft-santesson-svt-02, September 2021.

Authors' Addresses

Stefan Santesson
IDsec Solutions AB
Forskningsbyn Ideon
SE-223 70 Lund
Sweden

Email: sts@aaa-sec.com

Russ Housley
Vigil Security, LLC
516 Dranesville Road
Herndon, VA, 20170
United States of America

Email: housley@vigilsec.com