| | |
|---|---|
| Internet Engineering Task Force | P. Hallam-Baker |
| Internet-Draft | Comodo Group Inc. |
| Intended status: Standards Track | R. Stradling |
| Expires: April 22, 2013 | Comodo CA Ltd. |
| | October 19, 2012 |

TOC

# OCSP Digest Extension
# draft-hallambaker-ocspdigest-01


## Abstract

The OCSP digest extension creates a strong cryptographic binding between an OCSP token and the certificate it asserts a status value for. Support for the digest identifier extension permits a certificate issuer to employ a high assurance cryptographic digest function such as SHA2 to attest to the authenticity of their certificates in a fashion that is fully downwards compatible with legacy clients that only support SHA1.


## 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 http://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 April 22, 2013.

## Copyright Notice



---

## Table of Contents

## 1. Definitions

TOC

### 1.1. Requirements Language

TOC

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in **RFC 2119** [RFC2119].

## 2. Purpose

TOC

The OCSP digest identifier is provides a mechanism that permits a new cryptographic digest function to be used to authenticate an X.509v3 certificate in a manner that is fully backwards compatible with deployed browsers. This capability overcomes a 'deployment deadlock' condition that would otherwise make deployment of new cryptographic digest algorithms unacceptable to many certifcate users.

A second advantage of the OCSP digest identifier is to provide an affirmative demonstration that the OCSP responder had actual knowledge of the existence of the certificate whose status is being queried. This provides a transparency control on the operation of the Certificate Authority issuing the certificate. A Certificate Authority that has lost track of which certificates have been legitimately issued will be unable to determine if a response MUST or MUST NOT contain the digest identifier extension.

### 2.1. Digest Agility

TOC

Although the SSL Certificate industry has successfully completed a transition from use of the MD5 digest algorithm to SHA-1, this transition was a straightforward one as every Web browser that supported MD5 also provided support for SHA-1. Recent cryptanalytic work on the SHA-1 algorithm strongly suggest that while the use of SHA-1 in TLS should not be an immediate cause for concern it is prudent to ensure that there is a viable transition plan to use of SHA-2, preferably a plan that can be put into effect at short notice.

Although the X.509v3 certificate format has supported use of SHA-2 as a cryptographic digest since the algorithm was first published in 2001, there is currently no viable transition plan that permits SHA-2 to be deployed in a manner that will be acceptable to most operators of Web sites that use the certificates.

Merely adding support for a new cryptographic algorithm does little to improve the security of a system against attack. In general a reduction in risk will only be realized by withdrawing the old algorithm from use.

The TLS protocol and X.509v3 certificates are widely used to ensure the accountability, authenticity and confidentiality of Web transactions. One consequence of this widespead use is that the population of Web browsers has become highly hetrogeneous. While many Web users only use the latest Web browsers with the most up to date security features, a significant proportion of Web users do not. In particular there remains a significant number of Web users whose browsers are ten or more years old.

The use of older Web browsers has significant consequences for merchants using the Web to offer products and/or services. A merchant whose Web site is not accessible to 5% of the population of Web browsers risks losing 5% of their sales. Although most Web merchants are interested in offering their customers 'security', their motivation for doing so is to encourage them to do business with them. Thus a security feature that causes the merchant to lose more customers than it gains will be unacceptable to them.

Certificate Authorities will not issue certificates for which there is no market and browser providers cannot insist on the use of a credential format that no sites want and no Certificate Authority will issue. Deployment of SHA-2 has thus reached a deadlock condition in which none of the parties involved can or will act until all the other parties have acted first.

Although most Certificate issuers have the technical capability to offer digital certificates that use the SHA-2 algorithm, there is currently no demand for such certificates except for use in closed environments where the legacy browser constraints do not apply.

The OCSP digest identifier extension permits an OCSP response to identify the certificate whose status it reports using a cryptographic digest of the certificate. This provides a stronger binding between that OCSP token and the certificate to which it applies than the current protocol permits.

In a typical deployment scenario, the certificate itself would be signed using a SHA-1 digest to ensure backwards compatibility with legacy browsers and the OCSP token would contain a digest identifier extension that uses the SHA-2 algorithm or better. This approach

---

TOC

## 2.2. Transparency Requirement

A transparency requirement is a constraint on the operation of a service that may be verified by through access to public information alone.

A transparency requirement is thus a stronger criteria than an audit requirement that may require privileged access to verify.

The digest identifier extension MAY be used to enforce a transparency requirement that an OCSP responder mantain a complete and accurate log of all certificates issued and accurately reports the existence status of the certificate(s) for which OCSP requests are made.

Such a transparency requirement would typically be placed on an OCSP service that is operated by a Certification Authority to provide transparency with respect to compliance with a breach notification requirement.

---

TOC

## 2.3. The Current OCSP Protocol

The OCSP protocol defines an online service that reports the status of an issued X.509v3 certificate. The original protocol permitted an OCSP response to specify the certificate it reported status of by means of a CertID structure specified as follows:

```
CertID          ::=     SEQUENCE {
    hashAlgorithm       AlgorithmIdentifier,
    issuerNameHash      OCTET STRING, -- Hash of Issuer's DN
    issuerKeyHash       OCTET STRING, -- Hash of Issuers public key
    serialNumber        CertificateSerialNumber }
```

While the issuerNameHash and serialNumber should be unique, this is a matter of convention rather than a cryptographic guarantee, a convention that an attacker might be able to subvert in the case that a CA was breached.

The original justification made for only supporting a weak binding to the certificate in the

CertID structure was that it should be possible to operate an OCSP service from information contained in CRLs alone

This particular requirement is rejected. A protocol specification should not attempt to enforce a lowest common denominator for security. Services that have additional information available should not be unable to deliver it to clients merely because other services might not have that information.

It is certainly legitimate for a relying party making use of an OCSP responder to consider a service that reports the status 'good' for a certificate that has never been issued to be defective. An accomodation made in a specification to permit a certain level of service to be offered by constrained services should not prevent other services that are not limited from offering a greater degree of security.

In this case a purpose of the specification is precisely to determine whether the OCSP responder has actual knowledge of the certificates issued.

---

TOC

## 3. Syntax

The digest identifier extension MAY be used in CRLs or OCSP requests and responses. The extension has the following format:

```
cabf-ocsp-digest OBJECT IDENTIFIER ::=  { cabf 2 }

DigestData ::= SEQUENCE {
       hashAlgorithm        AlgorithmIdentifier,
       CertHash             OCTET STRING}
```

The CertHash contains the digest value of the certificate to which the enclosing status assertion or request applies.

---

TOC

### 3.1. OCSP Request

When specified in an OCSP request as a singleRequestExtensions entry, the Digest Identifier extension provides an additional means of identifying the certificate whose status is being queried rather than a replacement for the existing CertID structure.

Should an OCSP responder detect an inconsistency between the contents of the CertID structure and the Digest Identifier extension, there are three possible explanations:

- The discrepancy is due to an unintentional software error in either the client software or the CA infrastructure
- The discrepancy is due to an OCSP request being intentionally misformed.
- The digest algorithm that was originally used to sign the digital certificate has been compromised and the OCSP request was made by client software that recieved a compromised certificate.

An OCSP responder that is able to do so SHOULD take approrpiate steps to determine the cause of such discrepancies.

---

TOC

### 3.2. OCSP Response

When specified in an OCSP request as a singleExtensions entry, the Digest Identifier extension provides an additional means of identifying the certificate whose status is being reported.

If the contents of either the CertID or the Digest Identifier extension are inconsistent with the

certificate being querried, the response entry SHOULD be rejected as not matching the specified certificate.

If no matching response entries are present in a response, a client SHOULD consider the status of the certificate to be unknown.

---

TOC

### 3.2.1. Transparency requirement

An OCSP responder MUST NOT present a digest identifier extension as a singleExtensions entry unless it has actual knowledge that the corresponding certificate exists.

An external policy MAY verify compliance with the transparency requirement by generating a sequence of queries for certificates that are known to exist and dummy queries for certificates that are known not to exist.

to pass the transparency requirement, an OCSP responder MUST return the appropriate response to each type of query:

- If the certificate exists: A response with a digest identifier extension.
- Otherwise: A response that indicates an invalid status for the certificate and does not contain a digest identifier extension.

Note that it is possible for a third party to determine compliance with the transparency requirement on a statistical basis even if the OCSP request discloses the digest identifier of the corresponding certificate in some way.

---

TOC

## 4. Acknowledgements

[List of CABForum and PKIX contributors]

---

TOC

## 5. Security Considerations

---

TOC

### 5.1. Disclosing non existence of certificates

The deployed OCSP infrastructure only permits a client to determine that a certificate has not been revoked. Some OCSP responders return the OCSP status 'good' in cases where the status of the certificate is not known. Some OCSP clients have identical behavior in the case that the returned status is 'good' and 'unknown'.

Consistent use of the digest identifier permits a client to distinguish these cases.

---

TOC

### 5.2. Client disclosure of certificate digest identifier

A client may disclose the digest identifier of an issued certificate in an OCSP request, thus providing the service with the information necessary to form a response in the case that it is not entitled to do so by reason of not having actual knowledge of the existence of the certificate.

---

TOC

### 5.3. Client detection of service compromise

Steps that a client should take in the event that a service compromise is detected are outside the scope of this document.

## 5.4. Verifying service compliance

A third party may verify the compliance of an OCSP service with the transparency requirement by following the process specified in section **Section 3.2.1**.

## 6. For discussion.

[RFC EDITOR: DELETE PRIOR TO PUBLICATION]

Does the OCSP Request use make any sense at all? It does provide the starting point for an early detection system for bad crypto but that is all. Also it is quite possible that TLS OCSP stapling will render the need for the request moot by the time a digest breach occurs.

If the request extension use was removed it would mean that the responder was providing an effective proof that the status source had specific knowledge of the certificate whose status was being queried. (This proof would be further strengthened by use of a MAC)

Such proof would be relevant in determining if a responder had actual knowledge of the certificates it reported the status of. If a query is made for a certificate that is known does not or should not exist, the responder should respond with a generic 'unknown' error response. If the responder attempts to return a digest value in such cases, the responses are clearly spurious.

This scheme could be further strengthened by adding an extension OID to the certificate to specify that the OCSP responder will always return the digest identifier extension. This enables a relying application to reject any non conformant responses as spurious.

## 7. IANA Considerations

No action by IANA is required.

## 8. Normative References


**[RFC1035]** Mockapetris, P., "**Domain names - implementation and specification**," STD 13, RFC 1035, November 1987 (**TXT**).

**[RFC2119]** **Bradner, S.**, "**Key words for use in RFCs to Indicate Requirement Levels**," BCP 14, RFC 2119, March 1997 (**TXT**, **HTML**, **XML**).

**[RFC4366]** Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, "**Transport Layer Security (TLS) Extensions**," RFC 4366, April 2006 (**TXT**).

**[X.509]** International Telecommunication Union, "**ITU-T Recommendation X.509 (11/2008): Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks**," ITU-T Recommendation X.509, November 2008.

**[X.680]** International Telecommunication Union, "**ITU-T Recommendation X.680 (11/2008): Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation**," ITU-T Recommendation X.680, November 2008.


## Authors' Addresses


Phillip Hallam-Baker
Comodo Group Inc.
**Email:** **philliph@comodo.com**

Rob Stradling
Comodo CA Ltd.
**Email:** **rob.stradling@comodo.com**