Workgroup: Network
Internet-Draft:
draft-fetch-validation-vmc-wchuang-03
Published: 9 October 2022
Intended Status: Standards Track
Expires: 12 April 2023
Authors: W. Chuang Google
M. Bradshaw Fastmail
T. Loder Skyelogicworks
A. Brotman Comcast

Fetch and Validation of Verified Mark Certificates

Abstract

A description of how entities wishing to validate a Verified Mark Certificate (VMC) should retrieve and validate these documents. This document is a companion to BIMI core specification, which should be consulted alongside this document.

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 12 April 2023.

Table of Contents

1. Introduction

Brands Indicators or logos help people visually recognize products and services, and consequently their providers. In the context of email, it can help users understand who a sender is. Brand Indicators for Message Identification is a specification as described in [I-D.blank-ietf-bimi] for senders to associate and provide brand Indicators to email. As noted in that document's security considerations, the potential for abuse with brand indicators is high, and in particular a risk for look-alike domains and copycat indicators. One way to mitigate abuse is to validate brand ownership of some Indicators by some third-party and have that validation provably demonstrated through an X.509/PKIX [RFC5280] certificate as an evidence document [I-D.blank-ietf-bimi]. We call such certificates containing Indicators that meet the profile described later in this document Verified Mark Certificate (VMC). This document provides a specification on how email receivers working on behalf of email users can fetch VMC from the Internet and how they can validate the content of the VMC. With this, the email receiver can prove that the VMC was indeed issued by some trusted third-party such as a Certification Authority (CA).

2. Terminology

BIMI: Brand Indicators for Message Identification (BIMI) specification [I-D.blank-ietf-bimi] that combines DMARC-based message authentication with cryptographic methods to ensure the identity of a sender.

BIMI Evidence Document: A document published by a Mark Verifying Authority (MVA) which in the context of a Verified Mark Certificate (VMC) is a Certification Authority (CA) to assert evidence of verification.

Email Receivers: The entity or organization that receives and processes email. Mail Receivers operate one or more Internet facing Mail Transport Agents (MTAs).

End entity certificate: A non-CA certificate representing a user (or domain) of the PKI certificates.

Indicator: A brand indicator displayed on a Mail User Agent (MUA e.g., an email client) when the sender's email meets the BIMI specification requirements. The brand logo and other associated identity information is parsed from the Verified Mark Certificate. Immediate issuing CA certificate: A non-root CA certificate that issues end entity certificates.

Root certificate: A self-signed CA certificate issued by the root CA to identify itself and to facilitate verification of certificates issued by Subordinate CAs.

Verified Mark Certificate (VMC): An end entity certificate that meets the profile specified in this document and the Verified Mark Certificate Guideline document.

3. Fetch of Verified Mark Certificate

This section normatively describes the actions needed to receive and handle BIMI identified messages using Verified Mark Certificates that is built on the protocol described in the [I-D.blank-ietf-bimi]. Receivers use these specified processes to fetch Verified Mark Certificates securely, and then to validate the certificates and their embedded Indicators. If all requirements are met, receivers may then display the Indicators. Details of these steps are described below, and the indicator display procedure is described here.

3.1. BIMI Assertion Record

The sender declares associating BIMI to a domain via an Assertion record as normatively described by [I-D.blank-ietf-bimi]. That

record describes the BIMI policy and that policy may include a means to find the BIMI Indicator via the publication of evidence documents. The email receiver uses [RFC1035] to look for the publication of the Assertion record as well as the lack of publication when [RFC1035] returns NXDOMAIN. Assertion records containing the "a=" tag and associated populated value indicates that a sender has published a BIMI evidence document for use with that domain such a Verified Mark Certificate. The evidence document may be found at a hosting service specified by the URI in the value. The rest of this document describes the process for fetching and validating the Verified Mark Certificate with the clarification that other types of evidence document will have their own specification for fetch and validation.

3.2. Verified Mark Certificate Fetch

Verified Mark Certificates, in this specification, are published by the sender's web hosting service. The service MUST use HTTPS protocol and SHOULD use TLS version v1.2 [RFC5246] or newer to avoid protocol security bugs with earlier versions of TLS. That secure TLS connection MUST be established by using the protocol specified in [RFC8446]. The TLS certificate MUST have a valid issuance path to some client trusted server root CA certificate using the procedures in [RFC5280].

3.3. Fetch Format

Certificates fetched from the hosting service MUST be in PEM encoding [RFC7468]. To facilitate X.509/PKIX certificate issuance validation, the full issuance chain up to and optionally including the root CA certificate, MUST be present. The downloaded file SHOULD be ordered by starting with the Verified Mark Certificate, followed by its issuer CA certificate and potential successive issuers all the way to the optional root CA certificate. If the certificates appear out of issuance order, contain duplicates or more than one VMC, the receiver may choose to reject the validation. The filename specified of the BIMI Assertion record "a=" tag URI SHOULD have a ".pem" file name extension. Email receivers MAY cache the certificates and other evidence documents, and if so the receivers SHOULD set a Time-To-Live (TTL) on the cache entries as well as index by URI. This document intentionally does not specify what that TTL value is. If the sender wants force a certificate update, the sender MAY change the URI to a new unique location that will "bust the cache".

4. Verified Mark Certificate Profile

The profile describes the metadata contained within the Verified Mark Certificate. This section normatively describes a subset of the

Verified Mark Certificate profile that pertains to the certificate issuance and validity verification. The remaining content of the VMC profile is defined via guidance documents from the Authindicators (aka BIMI) Working Group, and in particular the process for obtaining that content (with some overlap). For example, while this section defines a requirement for the VMC to contain the Logotype extension, the Authindicators' VMC Guidelines document defines the content of the logotype extension. The following section describes the VMC profile checks using the profile described here as part of the VMC validation process.

4.1. Logotype Extension

Verified Mark Certificates MUST use logotype extension to carry the Indicators in the certificate as specified in [RFC3709]. That RFC uses secure URIs to specify the Indicators, and this specification calls for the Indicators to be embedded directly in the certificate via a DATA URI as defined by [RFC6170] and [RFC2397].

4.2. SVG Indicators

The Indicators image format MUST be SVG (an open W3C specification) as this helps with supporting different display resolutions that likely change in the future as SVG is a vectorized (meaning dimensionless) format. We believe that constraining the Indicators to a single image type will help with interoperability. This SVG MUST use the secure profile as defined by [RFC6170]. Non-normatively, to reiterate the secure profile defined there, it is summarized as:

- *Use SVG Tiny profile
- *No script
- *No external resource references

Additionally this document normatively specifies additional security restrictions on the SVG formatting as defined in [I-D.svg-tiny-ps-abrotman]. The SVG MUST be compressed to be space efficient, and base64 encoded for the DATA URI encoding as defined by [RFC6170] and [RFC2397].

4.3. BIMI Domain

A Verified Mark Certificate MUST define one or more Subject Alternative Name (SAN) extension dNSName domain as defined by [RFC5280] that identifies the location of the BIMI Assertion record that was used to fetch the VMC. There may be stronger properties that can be said about the relationship between the VMC and the Assertion record depending on the validation done on dNSName, but

that is outside the scope of this document. The domain name may either be the author or organizational name as defined in [I-D.blank-ietf-bimi] i.e. the Assertion record domain without the BIMI header selector or "default" selector and without the "*bimi" well-known label, meaning that it matches against any BIMI header selector including "default". Alternatively the domain name may specify also the BIMI header selector or "default" selector along with the* "bimi" well-known label, and will only match against that specific selector. If the domain is internationalized, it MUST follow canonicalization procedure specified in section 7.2 of [RFC5280].

4.4. BIMI Extended Key Usage

This document describes a new [RFC5280] Extended Key Usage OID that identifies Verified Mark Certificate as id-kp-BrandIndicatorforMessageIdentification. Certificates conforming to the Verified Mark Certificate profile is distinguished by using this extended key usage.

```
id-kp-BrandIndicatorforMessageIdentification OBJECT IDENTIFIER ::= {id-kp 31 } OID.
```

Verified Mark Certificates MUST contain an Extended Key Usage extension with the id-kp-BrandIndicatorforMessageIdentification OID. Also the CA certificate representing the immediate issuer of Verified Mark Certificates MUST also contain an Extended Key Usage extension with the id-kp-BrandIndicatorforMessageIdentification OID designating its usage.

4.5. Validity

A Verified Mark Certificate MUST specify a certificate validity period using the notBefore and notAfter fields. It MUST also define a location to check for certificate revocation using a Certificate Revocation List (CRL) Distribution Point and that is encoded in the VMC as a [RFC5280] cRLDistributionPoints extension.

4.6. Certificate Transparency

CT as specified provides transparency for the issued certificates. The Verified Mark Certificate MUST be logged to a set of Certificate Transparency (CT) logs, and the proof of that logging must be present in the certificate as a [RFC6962] SCT extension. The SCT extension MUST contain one or more SCTs.

5. Validation of Verified Mark Certificate

Verified Mark Certificates provide the means to securely authenticate as well as identify the third-party Mark Verifying Authority which in this case is a Certification Authority by verifying the issuance chain. It also provides the means to associate the Verified Mark Certificate to the BIMI Assertion record. This section concludes with a BIMI validation procedure for determining whether the VMC is valid or not. This should be used as part of a procedure in determining whether to display a BIMI Indicator based on a VMC.

5.1. Issuance and Profile Verification

To ensure the correctness of that certificate information, the receiver verifies the authenticity of the certificate, its validity and that it is a Verified Mark Certificate. After the certificate is downloaded, the receiver MUST validate the certificate with the following procedure:

1. Validate the authenticity of the certificate by checking the certificate signatures, that the end-entity certificate issuance chain leads back to some BIMI root CA certificate, and confirm membership of the root CA certificate in the receiver's trusted BIMI root set following the path validation procedures specified in section 6.1 of [RFC5280]. The downloaded certificates MUST contain all intermediate CA certificates up to but not necessarily including the root certificates.

2. Check the validity of the certificates in the certificate chain using the procedures in section 4.1.2.5 of [RFC5280].

3. Check that the certificates in the certificate chain are not revoked using the procedures in section 6.3 of [RFC5280]. The end-entity certificate MUST identify the CRL by a cRLDistributionPoints extension.

4. Validate the proof of CT logging. The receiver MUST find one or more SCTs, and validate that they are signed by a CT log recognized by the receiver using the procedures in [RFC6962].

5. Verify that the end-entity certificate is a Verified Mark Certificate. The certificate MUST contain an Extended-Key-Usage extension, and that it contains extended-key-usage is id-kp-BrandIndicatorforMessageIdentification. The entity certificate must contain a logotype extension, and that it contains a SVG as described in [#svg_indicators].

5.2. VMC Domain Verification

Next the receiver checks VMC SAN dNSName domain name relationship to the Assertion Record domain name, to demonstrate that they mutually identify each other. The following procedure allows the dNSName to either specify and thus match against the Assertion Record's domain name only, or selector + domain name. To do this, the receiver creates two domain name sets: 1) selector-set and 2) domain-set. The receiver iterates over the VMC SAN dNSName domain names and adds them to the domain name sets as follows.

- If the domain name contains "*bimi" i.e. prefixed with the labels <selector>.*bimi, add to selector-set.

- Otherwise add the domain name to domain-set.

Then check if the Assertion record domain matches by checking the following:

- Check if the Assertion record author or organizational domain names as defined in [draft-blank-ietf-bimi-01], which includes the <selector>._bimi prefix, is present in the selector-set. If found, the VMC Domain Verification is considered to match.

- Check if the remaining Assertion record author or organizational domain name is present in the domain-set. If found, the VMC Domain Verification is considered to match.

If internationalization is present, the receiver MUST canonicalize the domain names using the internationalization procedures specified in section 7.2 of [RFC5280].

5.3. Validation of VMC Evidence Document

The following procedure combines the above steps to determine whether a VMC contains a valid BIMI Evidence Document. This should be a part of a larger receiver defined procedure to determine whether to display a BIMI Indicator that may take into account other receiver specific signals such as reputation.

As a preamble, consider if the receiver supports VMC validation and an Assertion Record is found which has BIMI VMC location in the "a=" tag value. If so then validate the VMC using the following algorithm:

1. Use the mechanism in the "a=" tag location to retrieve the VMC, this MUST be a URI with HTTPS transport.

2. If the TLS connection setup as described in [#verified*mark*certificate_fetch] fails, then validation returns with an error.

3. If the evidence document does not contain a single valid VMC certificate chain then validation returns with an error.

4. Validate the VMC path validation procedure described in [#issuance*and*profile_verification]. If path validation fails then validation returns with an error.

5. Validate the VMC Domain relationship to the Assertion record as described in [#VMC*domain*verification] i.e. matches. If the VMC Domain is not related to the Assertion record, then validation returns with an error.

6. Retrieve the SVG Indicator from the [Logotype] Extension (oid 1.3.6.1.5.5.7.1.12) of the validated VMC.

7. Optionally, the receiver MAY choose to retrieve the SVG Indicator from the URI specified in the l= tag location of the Assertion Record and compare this to the SVG Indicator embedded within the VMC. The receiver MAY fail validation if these Indicators differ.

8. Validate the certificate meets the remaining profile specification of the VMC as described in [#verified*mark*certificate_profile], otherwise validation returns with an error.

9. Proceed to the Indicator Validation as described in section 8.6 in [I-D.blank-ietf-bimi].

6. Appendix

6.1. IANA Considerations

IANA is kindly requested to reserve the following assignments for:

*The LAMPS-Bimi-Certificate-2018 ASN.1 module in the "SMI Security for PKIX Extended Key Purpose" registry (1.3.6.1.5.5.7.3).

*The BIMI certificate extended key usage (1.3.6.1.5.5.7.3.31).

7. Normative References

[I-D.blank-ietf-bimi] Blank, S., Goldstein, P., Loder, T., Zink, T., and M. Bradshaw, "Brand Indicators for Message Identification (BIMI)", Work in Progress, Internet-Draft,

draft-blank-ietf-bimi-02, 9 March 2021, <https://www.ietf.org/archive/id/draft-blank-ietf-bimi-02.txt>.

[I-D.svg-tiny-ps-abrotman] Brotman, A. and T. Adams, "SVG Tiny Portable/Secure", Work in Progress, Internet-Draft, draft-svg-tiny-ps-abrotman-03, 10 April 2022, <https://www.ietf.org/archive/id/draft-svg-tiny-ps-abrotman-03.txt>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC2397] Masinter, L., "The "data" URL scheme", RFC 2397, DOI 10.17487/RFC2397, August 1998, <https://www.rfc-editor.org/info/rfc2397>.

[RFC3709] Santesson, S., Housley, R., and T. Freeman, "Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates", RFC 3709, DOI 10.17487/RFC3709, February 2004, <https://www.rfc-editor.org/info/rfc3709>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

[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>.

[RFC6170] Santesson, S., Housley, R., Bajaj, S., and L. Rosenthol, "Internet X.509 Public Key Infrastructure -- Certificate Image", RFC 6170, DOI 10.17487/RFC6170, May 2011, <https://www.rfc-editor.org/info/rfc6170>.

[RFC6962] Laurie, B., Langley, A., and E. Kasper, "Certificate Transparency", RFC 6962, DOI 10.17487/RFC6962, June 2013, <https://www.rfc-editor.org/info/rfc6962>.

[RFC7468] Josefsson, S. and S. Leonard, "Textual Encodings of PKIX, PKCS, and CMS Structures", RFC 7468, DOI 10.17487/RFC7468, April 2015, <https://www.rfc-editor.org/info/rfc7468>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

Authors' Addresses

Weihaw Chuang
Google

Email: weihaw@google.com

Marc Bradshaw
Fastmail

Email: marc@fastmailteam.com

Thede Loder
Skyelogicworks

Email: thede@skyelogicworks.com

Alex Brotman (ed)
Comcast

Email: alex_brotman@comcast.com