Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 8, 2018

W. Chuang, Ed.
Google, Inc.
T. Loder, Ed.
Agari

May 7, 2018

Brand Indicator for Message Identification in X.509 certificates
draft-chuang-bimi-certificate-00

Abstract

This document defines a X.509 certificate profile to distinguish those carrying logotypes and using email domain based authentication from other usages.

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 November 8, 2018.

Copyright Notice

Internet-DrBrand Indicator for Message Identification in X.50 May 2018

Table of Contents

1. Introduction

[RFC5280] defines the Extended Key Usage extension to define different usages of X.509 certificates. These certificates may carry logotype as defined in [RFC3709] whose format is further refined in [RFC6170]. This document defines a new usage for these logotype carrying certificates to define an identify for Electronic Mail senders as defined in [RFC5321] and whose sending domain is authenticated by either Sender Policy Framework [RFC7208] or by Domain Key Identified Mail signatures [RFC6376]. This new profile distinguishes it from other certificate usages with electronic mail such as S/MIME [RFC5751].

2. Conventions Used in This Document

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 [RFC2119].

3. BIMI

This section describes non-normatively the Brand Indicator for Message Identification (BIMI) electronic mail profile here. Its intended that there will be a separate document that specifies the BIMI electronic mail sending and receiving protocol that describes the BIMI electronic mail headers, the sender validation process using domain authentication methods and the fetch of the BIMI certificates. BIMI follows the current practice of using domain based validation methods Sender Policy Framework [RFC7208] or by Domain Key Identified

Mail signatures [RFC6376]. When an electronic mail sender has been validated this way, and with the fetched BIMI certificate, the receiver can proceed to validate the BIMI certificate with the sender domain as described in this document. Upon successful validation, the receiver may choose to show the associated logotype and other

identifying information contained in the BIMI certificate. This document does not inform other uses of logotype with other email profiles such as S/MIME.

4. BIMI Certificate Validation

Before a BIMI certificate can be used to provide identification, the certificate path MUST be validated using the algorithm in [RFC5280]. The BIMI certificate MUST contain an extended key usage extension specified for id-kp-BrandIndicatorforMessageIdentification as defined in Section 5. It MUST also contain dnsName field of an X.509 Subject Alternative Name as specified in [RFC5280] and a subject LogoType as specified in [RFC3709]. The BIMI certificate domain name and the domain of the From or Sender header email address are compared. If they match using the method specified in [RFC5280]), then the certificate identifies the sender of the electron mail and the certificate subject information may be used to describe the sender.

5. BIMI Certificate Extension

This document describes a new Extended Key Usage OID for the BIMI use case id-kp-BrandIndicatorforMessageIdentification.

id-kp-BrandIndicatorforMessageIdentification OBJECT IDENTIFIER ::= { id-kp 31 }

6. Security Considerations

- SPF maybe spoofed. See considerations in [RFC7208].
- DKIM maybe spoofed. See considerations in [RFC6376].
- LogoTypes identities may be spoofed. See considerations in [RFC3709].

7. IANA Considerations

In Section 5 and the ASN.1 module identifier defined in Appendix A. 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).

8. Normative References

[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>.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <https://www.rfc-editor.org/info/rfc3629>.

[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>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[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>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008,

<https://www.rfc-editor.org/info/rfc5321>.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, DOI 10.17487/RFC5751, January 2010, <https://www.rfc-editor.org/info/rfc5751>.

[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>.

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/info/rfc6376>.

[RFC7208] Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, DOI 10.17487/RFC7208, April 2014, <https://www.rfc-editor.org/info/rfc7208>.

[RFC7299] Housley, R., "Object Identifier Registry for the PKIX Working Group", RFC 7299, DOI 10.17487/RFC7299, July 2014, <https://www.rfc-editor.org/info/rfc7299>.

Appendix A. ASN.1 Module

The following ASN.1 module normatively specifies the BIMI extended key usage name. This specification uses the ASN.1 definitions from [RFC7299].

```
LAMPS-BIMI-Certificate-2018
  { iso(1) identified-organization(3) dod(6)
    internet(1) security(5) mechanisms(5) pkix(7) id-kp(3)
    id-kp-BrandIndicatorforMessageIdentification(TBD) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

```
  IMPORTS
    id-pkix
    FROM PKIX1Explicit-2009
      { iso(1) identified-organization(3)
                dod(6) internet(1) security(5) mechanisms(5) pkix(7) } ;


  -- Extended key purpose identifiers
      id-kp   OBJECT IDENTIFIER ::= { id-pkix 3 }

    id-kp-BrandIndicatorforMessageIdentification OBJECT IDENTIFIER ::= { id-kp

  END
```

Appendix B. Acknowledgements

Thank you to Kefeng Chen and Kirk Hall for their help with the BIMI certificate profile. Thanks to the other document reviewers.

Authors' Addresses

Weihaw Chuang (editor)
Google, Inc.
1600 Amphitheater Parkway
Mountain View, CA 94043
US

Email: weihaw@google.com

Thede Loder (editor)
Agari
100 S. Ellsworth Ave
San Mateo, CA 94401
US

Email: tloder@agari.com