Workgroup:	Network Working Group				
Internet-Draft:	draft-haberman-digital-emblem-00				
Published:	29 March 2024				
Intended Status:	Standards Track				
Expires:	30 September 2024				
Authors:	B. Haberman, Ed.	A. Mankin	B. Woodcock	C. Deccio	A. DeSimone
	JHU APL	*PCH*	*PCH*	*BYU*	*JHU APL*

Digital Emblems Indicating Protections Under International Law

Abstract

International law defines a number of emblems, such as the blue helmets of United Nations peacekeeping forces, the blue and white shield of UNESCO, and the Red Cross of the International Committee of the Red Cross, as indicative of special protections under the Geneva Conventions. Similar protections attach to journalists who wear "Press" protective emblems on the battlefield, under Article 79 of Protocol I of the Geneva Conventions and Resolution 2222 of the United Nations Security Council. The emblems of national governments and inter-governmental organizations protect diplomatic pouches, couriers, and envoys under the Vienna Convention on Diplomatic Relations. Other marks enjoy protections against mis-use under the Paris Convention, the Madrid Protocol, and the Trade-Related Aspects of Intellectual Property Rights.

Such physical emblems have a number of weaknesses (e.g., no real-time evaluation of their authenticity) and do not translate to the digital realm. This document describes a digital emblem which addresses the shortcomings of the physical emblems and makes possible the indication of protections of digital assets under international law.

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 30 September 2024.

Copyright Notice

Table of Contents

1. Introduction

International law defines a number of emblems, such as the blue helmets of United Nations (UN) peacekeeping forces, the blue and white shield of UNESCO, and the Red Cross of the International Committee of the Red Cross (ICRC), as indicative of special protections under international law. Similar protections attach to journalists who wear "Press" protective emblems on the battlefield. The emblems of national governments and inter-governmental organizations protect diplomatic pouches, couriers, and envoys, and international law protects certain marks against counterfeiting.

Physical emblems suffer from a number of weaknesses:

- It is not possible to evaluate their authenticity in real-time,
- They cannot be seen in the dark,
- They may not be visible at a distance, at an oblique angle, or from the opposite side of an object,
- They may be subject to wear, obfuscation, or vandalism,
- No audit mechanism exists to prove that the presence of an emblem has been queried for,
- No mechanism exists to prevent replay attacks,
- No mechanism exists to prevent time-shifting attacks,
- No mechanism exists to prevent location-shifting attacks,
- No mechanism exists to correlate an emblem with a specific quantity of persons or items, or a physical extent,
- No mechanism exists to correlate the validity of an emblem with its use in a specific place or time,
- There is no centralized ability to revoke instances of emblems which have been compromised, are being abused, or are no longer relevant.

A digital emblem must meet certain criteria to perform its function of notification under law:

- It MUST provide a clearly detectable and unambiguous marking,
- They MUST be machine readability,
- The emblem MUST identify the authorizing party that issued it,
- The emblem MUST be robust against misuse,
- It MUST be possible to restrict the validity of an emblem by temporal or geographic scope,
- It MUST be possible to associate the emblem with a range or specific quantity of persons or items,
- It MUST be possible to associate the emblem with online services (e.g., websites, emails),
- It MUST be possible to associate the emblem with data in transit or at rest,
- It MUST be possible to associate the emblem with network-addressable equipment (e.g., routers, servers),
- It MUST be possible to associate the emblem with a physical object (e.g., building, vehicle),

- It MUST be possible to associate the emblem with a person or group of people,
- It SHOULD be possible to view an emblem in-band via a communications network, optically (e.g., QR code), or wirelessly (e.g., RFID),
- The digital emblem MUST be capable of carrying a visual representation of the emblem,
- The emblem MUST carry an unambiguous indication of the international law or laws conferring protection upon the entity marked with the emblem,
- The emblem MUST be capable of providing a reference to additional relevant information (e.g., photographs, unique identifiers) which can be used to corroborate the association of the digital emblem with the entity bearing it,
- Querying the existence of or validating a digital emblem MUST NOT impose undue risk or cost on any party to the transaction.

This document describes a protocol for the creation and publication of a digital emblem utilizing the Domain Name System (DNS) global infrastructure.

1.1. Conventions

The capitalized 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].

2. Protocol Overview

The objective of the protocol is to allow organizations to digitally signal that people, places, things, services, and data are entitled to protection under international law.

3. Digital Emblem Material in DNS

3.1. Signing Credentials

Entities generate, publish, and maintain valid digital signing certificates for attesting to a Digital Emblem (DEM). These signing certificates MUST be published in the DNS via DNS-based Authentication of Named Entities (DANE) TLSA Record [RFC6698].

All TLSA records MUST be protected by DNS Security Extensions (DNSSEC) [RFC4033][RFC4034][RFC4035].

3.2. Digital Emblems

3.2.1. Digital Emblem Record

A DEM Record is a DNS record that declares use of a digital emblem. It is used to publish the certificate attesting to protection under international law. The DEM Record is a new DNS Resource Record Type. Multiple records MAY exist for the same name. Each DEM Record is placed in the DNS tree at the name to which it pertains.

3.2.1.1. DEM RDATA Wire Format

```
                        1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | Cert. Usage   |    Selector   | Matching Type |               /
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+               /
   /                                                               /
   /                 Certificate Association Data                  /
   /                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

3.2.1.1.1. Certificate Usage Field

A one-octet field where the value is selected from IANA's TLSA Certificate Usages registry [RFC6698].

3.2.1.1.2. Selector Field

A one-octet field where the value is selected from IANA's TLSA Selectors registry [RFC6698].

3.2.1.1.3. Matching Type Field

A one-octet field where the value is selected from IANA's TLSA Matching Types registry [RFC6698].

3.2.1.1.4. Certificate Association Data Field

This field contains either raw data (either the full certificate or its public key information) or the hash of the raw data.

3.2.2. DEM RR Presentation Format

TBD

Publication of a DEM follows all the rules for publishing DNS resource records described in [RFC1035]. The DEM MUST be protected by DNSSEC.

3.3. Digital Emblem Verification

Any entity can verify the existence and validity of a digital emblem. Anyone can perform the following tasks:

1. Perform a DNS lookup for a DEM Record.
2. If a DEM does not exist, terminate process.
3. Extract the certificate.
4. Perform a DNS lookup for the TLSA record associated with the Issuer.
5. If the TLSA exists, extract the key material. Otherwise, terminate process.
6. Using the retrieved key material, verify the signature on the DEM certificate.

If the signature verifies, the target system has protection from the digital emblem. In all other cases, it does not.

4. To Do List

Add text on necessary DANE TLSA parameters for use with the Digital Emblem per [RFC7671]

Integrate underscored naming indicator per [RFC8552].

Presentation format

Intermediate certificates.

DEM certficate fields and usages (e.g., SANs).

Investigate use of an updated LOC record.

DEP, QTY, and TIME RRType usage.

in-addr.foo.int, ip6.foo.int, and asn.foo.int namespace use.

Signaling protection of IP addresses via reverse DNS.

Legal/Policy considerations.

5. IANA Considerations

Two new IANA registries are required by this protocol.

- Digital Emblem Registry - The principal key in this registry is the name of a digital emblem using organization, followed by the principal jurisdiction of incorporation, followed by any necessary locational disambiguation (in case there are multiple organizations of the same name incorporated within the same jurisdiction), followed by a list of domain apexes which MAY contain digital emblem records, each of which which MUST be under the control of the same named entity, followed by a field which encodes a list of numeric references to the bodies of international protective law embodied in the emblem, sorted by order of importance or relevance as deemed by the Digital Emblem's registrant. These codes should be drawn from a separate table, which may be seeded with the following values, with a canonical URL for each: Hague Conventions, Geneva Conventions, Third Geneva Convention, Fourth Geneva Convention, Geneva Protocol I, Geneva Protocol II, Geneva Protocol III, Rome Statute, Madrid Protocol, Vienna Convention on Diplomatic Relations of 1961.
- ASN.ARPA Registry - This is a new delegation within .ARPA, to be managed jointly by the RIRs, or the NRO, in which RIRs may delegate NS and DS records to PTR RRs associated with Autonomous System Number assignments, analogous to the way they delegate the in-addr.arpa and ip6.arpa domains.

6. Security Considerations

7. Contributors

8. Acknowledgments

9. References

9.1. Normative References

[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>.

[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>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <https://www.rfc-editor.org/info/rfc4034>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <https://www.rfc-editor.org/info/rfc4035>.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August 2012, <https://www.rfc-editor.org/info/rfc6698>.

[RFC7671] Dukhovni, V. and W. Hardaker, "The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance", RFC 7671, DOI 10.17487/RFC7671, October 2015, <https://www.rfc-editor.org/info/rfc7671>.

[RFC8552] Crocker, D., "Scoped Interpretation of DNS Resource Records through "Underscored" Naming of Attribute Leaves", BCP 222, RFC 8552, DOI 10.17487/RFC8552, March 2019, <https://www.rfc-editor.org/info/rfc8552>.

9.2. Informative References

[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>.

Authors' Addresses

Brian Haberman (EDITOR)
Johns Hopkins University Applied Physics Lab
Email: brian@innovationslab.net

Allison Mankin
Packet Clearing House
Email: amankin@gmail.com

Bill Woodcock
Packet Clearing House
Email: woody@pch.net

Casey Deccio
Brigham Young University
Email: casey@deccio.net

Antonio DeSimone
Johns Hopkins University Applied Physics Lab
Email: antonio.desinome@jhuapl.edu