Workgroup:	Network Working Group				
Internet-Draft:	draft-haberman-digital-emblem-00				
Published:	14 March 2024				
Intended Status:	Standards Track				
Expires:	15 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 15 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 are not amenable to machine readability,
- 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,
- 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 remaining sections and text are placefolders based on the early prototype work

The objective of the protocol is to allow organizations to digitally signal that assets are entitled to protection from attack under law. These assets include both physical and virtual resources (servers, virtual machines, etc.) and network traffic associated with those resources. This is accomplished by associating a digital emblem attribute with the DNS domain name, or sub-domain, and/or with the IP address(es) associated with those resource(s).

The following sub-sections describe the three parties associated with the digital emblem and their roles in creating an emblem.

2.1. Actors

2.1.1. Approvers

An Approver is an organization empowered to authorize the use of the emblem. Each member of the United Nations has an identified organization tasked with fulfilling this role. All Approvers, or an organization operating on their behalf, generate and maintain digital signing credentials in TLSA records published in the DNS (Section Section 3.1). An Approver receives requests for use of

the digital emblem from Requestors. If the request satisfies all necessary requirements, the Approver generates the necessary cryptographic material and returns it to the Requestor (Section Section 3.2.1).

2.1.2. Requestors

A Requestor is any organization wishing to use the digital emblem to protect the digital assets associated with its humanitarian mission. The Requestor sends the necessary DNS resource information to an Approver. If the Approver approves the use of the digital emblem for the identified resources, the Requestor publishes the returned cryptographic material in a Digital Emblem Record (Section Section 3.2.2).

2.1.3. Observers

An Observer is any entity that wishes to assess the claim of protection under the digital emblem. This is accomplished by obtaining both the Digital Emblem Record associated with a target system (domain name or IP address) published by the Requestor and the signing certificate associated with the Approver that is identified in the Digital Emblem Record. An Observer then uses the key material in the signing certificate to verify the cryptographic material published in the target's Digital Emblem Record (Section Section 3.3).

3. Digital Emblem Material in DNS

3.1. Approver Credentials

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

TODO : Add text on the generation of the key material and signing certificate

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

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

3.2. Digital Emblem Record

3.2.1. Approver Generated Material

Once an Approver has deemed a request to be satisfactory, it generates two pieces of cryptographic material. First, the Approver generates a pseudo-random number (i.e., nonce) using a secure random number generator (TBD: need additional details on the characteristics of the nonce). Second, the Approver generates a digital signature (FIPS.186-5?) using its private key associated with its signing certificate (published in a DNS TLSA record) over the nonce and the identifying material (e.g., domain name) provided by the Requestor.

After generating the above material, the Approver returns the nonce, the digital signature, and a reference to its DNS TLSA record containing the corresponding signing certificate.

3.2.2. Digital Emblem Record

A Digital Emblem Record (DER) is a DNS record that declares that a host is protected under IHL. The DER is expressed as a single string of text found in the RDATA of a single DNS TXT resource record. Multiple DER records MAY exist for the same name. This occurs if the Requestor has received authorization from multiple Approvers. Each DER is placed in the DNS tree at the owner name to which it pertains. Given that TXT records serve multiple purposes, publishers need to be mindful of size limitations.

TODO : Need to consider the creation of a new DNS RR type for DER

A notional DER string is as follows:

```
de=c517d02d6554a9add49b emblem.example.org e5d391930ac48dd482810fed
```

The fields in the DER are as follows:

- de - indentifies the DER string
- nonce - A pseudo random number generated by the Approver
- reference - The DNS name of the endpoint approving the use of the digital emblem
- signature - Digital signature generated by the Approver

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

TODO : Integrate underscored naming indicator per [RFC8552].

The publication of a DER under a domain name indicates protection for that name under IHL. Protection for IP addresses is accomplished through the use of the DNS reverse zone. If protection under IHL is requested for an IP address, the Requestor MUST:

- Obtain a proper IP address delegation
- Publish a reverse zone mapping the target IP addresses to domain names
- Requests approval for use of the digital emblem from an Approver for the target domain names

3.3. Digital Emblem Verification

Any entity can act as an Observer and verify the existence and validity of a digital emblem associated with a target system. An Observer performs the following tasks:

1. Perform a DNS lookup for a TXT record associated with the target system.
2. If a TXT record exists, parse it for a DER. Otherwise, terminate process.
3. If a DER exists, extract the nonce, reference, and signature. Otherwise, terminate process.

4. Perform a DNS lookup for the TLSA record associated with the reference.
5. If the TLSA exists, extract the key material. Otherwise, terminate process.
6. Using the retrieved key material, nonce, and target domain name, verify the signature.

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

4. IANA Considerations

5. Security Considerations

6. Contributors

7. Acknowledgments

8. References

8.1. 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>.

8.2. 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