Digital Emblems
Internet-Draft
Intended status: Informational
Expires: 20 March 2026

C. Deccio
Brigham Young University
R. A. Fainchtein
JHU/APL
F. Linker

J. Reid
RTFM llp
A. Rosenberg
Veridigo
A. Mankin
Packet Clearing House
16 September 2025

Digital Emblems - Use Cases and Requirements
draft-fainchtein-diem-use-cases-00

Abstract

TODO Abstract

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://rahelFain.github.io/combined-diem-uses-reqs/draft-fainchtein-diem-use-cases.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-fainchtein-diem-use-cases/.

Discussion of this document takes place on the Digital Emblems Working Group mailing list (mailto:diem@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/diem. Subscribe at https://www.ietf.org/mailman/listinfo/diem/.

Source for this draft and an issue tracker can be found at https://github.com/rahelFain/combined-diem-uses-reqs.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

This Internet-Draft will expire on 20 March 2026.

Copyright Notice

Table of Contents

1. Introduction 3
2. Conventions and Definitions 3
3. Requirements 4
  3.1. Digital Emblem Requirements 4
    3.1.1. Digital Emblem Format 4
    3.1.2. Emblem Semantics 4
  3.2. Discovery Requirements 4
    3.2.1. Discovery 4
    3.2.2. Removable 4
    3.2.3. Undetectable Validation 5
  3.3. Validation Requirements 5
    3.3.1. Validation 5
    3.3.2. Authorization 5
  3.4. Other Requirements 5
    3.4.1. Extensibility 5
4. Extensions 5
  4.1. Data Formats 5
  4.2. Bearer Discovery 6
  4.3. Implicit Discovery 6
  4.4. Confidentiality 6

4.5. Proof of Presence 6
5. Use Cases 6
5.1. Basel Convention 7
5.2. Ramsar Convention on the Wetlands 7
5.3. International Atomic Energy Agency (IAEA) 7
5.4. International Humanitarian Law 7
5.5. Organization for the Prohibition of Chemical Weapons (OPCW) 8
5.6. Press 8
5.7. United Nations Economic and Social Council (ECOSOC) . . . 8
5.8. United Nations Peacekeepers 8
5.9. World Customs Organization (WCO) 8
5.10. World Health Organization (WHO) 8
5.11. United Nations Food and Agriculture Organization (FAO) . 9
5.12. World Intellectual Property Organization (WIPO) 9
5.13. International Civil Aviation Organization (ICAO) 9
6. Security Considerations 9
7. IANA Considerations 9
8. References 9
8.1. Normative References 9
8.2. Informative References 10
Acknowledgments 11
Authors' Addresses 11

1. Introduction

Digital emblems are a means for an asset to signal to validating entities that it should be protected or treated in a specific way, using some normative framework. The DIEM WG will define a set of standards for an architecture that enables discovery and validation of digital emblems. This document lists the requirements that the architecture must accommodate. These requirements were identified across different use cases. Not all use cases share all requirements. We envision an architecture system comprising multiple standards, which can be flexibly profiled for different use cases. We use the terms "(digital) emblem," "bearer," and "validation" in accordance with the DIEM charter as of writing [CHARTER].

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Requirements

The DIEM architecture will allow validators to discover and validate digital emblems that are associated with bearers. This section contains the requirements that this architecture will address. They are based on use cases identified thus far (see Section Use Cases), but note that not all use cases share all requirements. We categorize these requirements into: requirements on digital emblems and their format, on their discovery, on their validation, and other requirements.

3.1. Digital Emblem Requirements

3.1.1. Digital Emblem Format

Digital emblems MUST identify their bearer and their kind of digital emblem. Beyond that, digital emblems MAY include other data, for example, an issuer or a validity window. As of writing, the DIEM charter requires that digital emblems MUST explicitly identify their bearer by a Fully Qualified Domain Name (FQDN).

3.1.2. Emblem Semantics

Individual use cases MUST specify the semantics of the emblem and the bearer. It must be clearly stated how discovery and validation of a digital emblem should inform validator behavior.

3.2. Discovery Requirements

3.2.1. Discovery

Digital emblems MUST specify how validators can check for the presence of a digital emblem. That is, given a potential bearer a validator must be able to determine whether it has an associated emblem. For example, verifying whether a FQDN has an emblem associated with it could be realized by fetching digital emblem-associated records for said FQDN.

3.2.2. Removable

Digital emblems MAY require to be removable in that checking for the presence of an emblem associated with a bearer results in no emblem. Note that checking for emblem presence is independent of its validation. That is, emblems do not count as removed when they become invalid.

3.2.3. Undetectable Validation

Digital emblem discovery MAY require that bearers, issuers, and authorizing parties be unable to detect when an emblem is being discovered or validated. This requirement is motivated by emblems that mark its bearer as protected and ask validators to not attack the bearer. If emblem discovery were detectable by the bearer, issuer, or by an authorizing party, malicious parties could misuse the digital emblem as an intrusion detection system.

3.3. Validation Requirements

3.3.1. Validation

Digital emblems MAY require validation. Validation MUST support verification of all the emblem's data and its context. In particular, validation MUST ensure that the emblem was issued for the respective bearer. Some use cases MAY use unverified digital emblems.

3.3.2. Authorization

Digital emblems MAY require authorization by third-parties. Any authorization mechanism MUST account for the possibility of compromise of cryptographic key material, for example, by specifying revocation mechanisms or using short-lived credentials. Individual profiles MUST standardize a trust model that describes how validators can discover authorities and how the system selects authorities.

3.4. Other Requirements

3.4.1. Extensibility

The digital emblem architecture should be extensible. The initial work should not preclude future extensions and individual standards should be designed as general as possible.

4. Extensions

In this section, we sketch how the digital emblem architecture could be extended by future standards to accommodate more use cases, but it is not a comprehensive list.

4.1. Data Formats

Emblems for additional use cases may be defined via new profiles in future standards, potentially including new types of atomic data elements requiring additional specification.

4.2. Bearer Discovery

It may be non-obvious for some use cases to identify the bearer that is associated with an asset, and thus impossible to fetch emblems associated with that asset. To accommodate for such use cases, one could specify means to discover bearers for different types of assets.

4.3. Implicit Discovery

An alternative approach to the above problem would be to bind emblems implicitly to their bearer. Implicit binding would identify the bearer by the emblem’s location. For example, if emblems were distributed via NFC, the bearer could be the asset to which the NFC chip was attached. As of this writing, the current charter scope requires that digital emblems explicitly identify their bearer, but such discovery mechanisms could be investigated in future WG work.

4.4. Confidentiality

Some use cases may contain confidential or sensitive data, and may require mechanisms to protect such data. For example, this could be realized with encryption of the general emblem data format that will be part of the architecture or by only serving emblems over channels with access control mechanisms.

4.5. Proof of Presence

For some emblems, it may be relevant to track that an emblem has been presented. This could be achieved, for example, by standardizing different distributions mechanisms, e.g., using decentralized authenticated data structures.

5. Use Cases

Different use cases have different requirements. The purpose of this document is to list the requirements that will be addressed with the initial architecture. The use cases overlap and would benefit from a DIEM architecture developed to provide the requirements listed above, though some may require additional extensions. We alphabetically list use cases here so that relevant stakeholders can provide input whether their use case would indeed benefit from a DIEM architecture, and invite participants to provide use cases or details that we have missed.

We provide auxiliary material under Informative References.

5.1. Basel Convention

Regulates the trans-boundary movement of hazardous wastes. Use cases are functionally identical to OPCW and IAEA.

5.2. Ramsar Convention on the Wetlands

The Convention on Wetlands of International Importance especially as Waterfowl Habitat "providees the single most global framework for intergovernmental cooperation on wetland issues" and it features a list of geographic areas designated by Member States. A digital emblem for the geographic areas potentially requires

* Indication of location
* Access to presence or absence of Ramsar designation of a specified location
* Textual description
* Ability to validate the presence or absence of Ramsar designation

5.3. International Atomic Energy Agency (IAEA)

IAEA administers several treaties, especially related to the controlled shipment of atomic fuels and wastes across borders. Similar use case as OPCW.

5.4. International Humanitarian Law

The Geneva Conventions and their Additional Protocols constitute the core of International Humanitarian Law (IHL). Some assets enjoy certain specific protections under IHL, including that they must not be attacked, and IHL codifies four types of protective emblems for armed conflict, which inform other parties that marked assets benefit from one or several of these specific protections:

* The emblems of the Red Cross, Red Crescent, and Red Crystal
* The Blue Shield emblem
* The emblem for the protection of civil defense marks
* The dangerous forces emblem

Digital emblems under IHL could be extended to digital, network-connected and network-addressable assets that enjoy aforementioned specific protections under IHL.

5.5. Organization for the Prohibition of Chemical Weapons (OPCW)

Requires protection of Schedule 1 chemicals in transit between signatory countries for research, medical, pharmaceutical, or protective purposes. Emblem would identify place, date, and volume of production, and the emblem can contain confidential data.

5.6. Press

Journalists in conflict zones use protective markings that indicate their status as a non-combatant. Digital assets belonging to the press could be digitally marked, and protective markings in conflict zones could be digitized.

5.7. United Nations Economic and Social Council (ECOSOC)

UN Model Regulations [UNMODELREGS] includes "Recommendations on the Transport of Dangerous Goods." This includes labeling of items with a four digit "UN Number" that indicates the comounds contained within, such as chemicals, explosives, flammable liquids, etc. For example, items containing lithium-based batteries are labeled with 3480 or 3481 and accompanied by a specific "battery mark" emblem.

5.8. United Nations Peacekeepers

UN Peacekeepers use protective markings in theater as well as facilities associated with the mission.

5.9. World Customs Organization (WCO)

Specifies "Harmonized Systems" codes [HARMONIZED] that classify items such as livestock, arms and ammunition, chemicals, plastics, machinery, foodstuffs, etc. They also provide a system for labeling origin of items and valuation of items, all enforced by numerous international trade agreements between individual nations and groups of nations.

5.10. World Health Organization (WHO)

Similar to the use case of the Red Cross, Red Crystal, and Red Crescent.

5.11. United Nations Food and Agriculture Organization (FAO)

Among other things is responsible for the International Plant Protection Convention (IPPC) and International Standards for Phytosanitary Measures standards including ISPM 15 that requires wood packaging materials (pallets, crates, dunnages) to be debarked, heat-treated or fumigated with methyl-bromide, and stamped or branded with a compliance mark known as a "wheat stamp."

5.12. World Intellectual Property Organization (WIPO)

WIPO administers 26+ treaties with different protections for different things. Brands that are protected under international law (e.g., Madrid Protocol) can mark their shipments with an emblem allowing customs agents to positively identify legitimate products.

5.13. International Civil Aviation Organization (ICAO)

Requires protection of civil aviation flights and the ability to assert that they are not dual-use (i.e., not carrying military cargo). Digital emblem would carry a geographic description of the flight plan, its current location, and an indicator of its identity (i.e., tail number). Potential need for the emblem to reference a limited or partially redacted flight manifest.

6. Security Considerations

TODO Security

7. IANA Considerations

This document has no IANA actions.

8. References

8.1. Normative References

[CHARTER] "Digital Emblems", 27 May 2025, <https://datatracker.ietf.org/doc/charter-ietf-diem/01/>.

[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/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

8.2. Informative References

[BLUEHELMET]
Doctors Without Borders, "The Practical Guide to Humanitarian Law", n.d., <https://guide-humanitarian-law.org/content/article/3/peacekeeping/>.

[BLUESHIELD]
United Nations Educational, Scientific and Cultural Organization, "Enhanced Protection - Cultural Property of Highest Importance to Humanity", n.d., <https://www.unesco.org/en/heritage-armed-conflicts/enhanced-protection-cultural-property-highest-importance-humanity>.

[DIPLOMAT] Cornell Law School - Legal Information Institute, "Personnel of Foreign Governments and International Organizations and Special Treatment for Returning Individuals", n.d., <https://www.law.cornell.edu/cfr/text/19/148.83>.

[HARMONIZED]
World Customs Organization, "Harmonized System", n.d., <https://www.wcotradetools.org/en/harmonized-system>.

[ISPM15] International Plant Protection Convention, Food and Agriculture Organization of the United Nations, "International Standards for Phytosanitary Measures No. 15: Regulation of Wood Packaging Material in International Trade", n.d., <https://www.ippc.int/static/media/files/publication/en/2019/02/ISPM_15_2018_En_WoodPackaging_Post-CPM13_Rev_Annex1and2_Fixed_2019-02-01.pdf>.

[PRESS] Reporters Without Borders, "RSF Resource for Journalists' Safety", n.d., <https://safety.rsf.org/appendix-i-protection-of-journalists-in-war-zones/>.

[RAMSAR] Convention on Wetlands Secretariat, "The Convention on Wetlands", n.d., <https://www.ramsar.org>.

[REDCROSS] International Committee of the Red Cross, "The Protection of the Red Cross / Red Crescent Emblems", n.d., <https://www.icrc.org/en/doc/assets/files/other/protection_emblems.pdf>.

[UNMODELREGS]
United Nations Economic and Social Council, "UN Model Regulations on the Transport of Dangerous Goods", n.d., <https://unece.org/transport/dangerous-goods/un-model-regulations-rev-23>.

Acknowledgments

Authors' Addresses

Casey Deccio
Brigham Young University
Email: casey@byu.edu

Rahel A. Fainchtein
JHU/APL
Email: rahel.fainchtein@jhuapl.edu

Felix Linker
Email: linkerfelix@gmail.com

Jim Reid
RTFM llp
Email: jim@rfc1035.com

Alex Rosenberg
Veridigo
Email: alexr@veridigo.com

Allison Mankin
Packet Clearing House
Email: allison@pch.net