Digital Emblems
Internet-Draft
Intended status: Informational
Expires: 19 July 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

15 January 2026

Digital Emblems - Use Cases and Requirements
draft-ietf-diem-requirements-01

Abstract

Digital emblems are a means for digital assets to signal that they should be treated in a specific way by reference to some normative framework. This document lists the requirements and use cases that an architecture for digital emblems must accommodate.

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://ietf-wg-diem.github.io/diem-requirements/draft-ietf-diem-requirements.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-diem-requirements/.

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/ietf-wg-diem/diem-requirements.

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 19 July 2026.

Copyright Notice

Table of Contents

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 this writing [CHARTER]. These definitions have been reproduced in section Conventions and Definitions.

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.

The definitions for terms "(digital) emblem," "bearer," and "validation" are reproduced from the charter [CHARTER] as of this writing.

(Digital) Emblem: Emblems such as the Red Cross, Red Crescent, Red Crystal, and Blue Shield can be symbols of protection governed by International Humanitarian Law (IHL). Emblems can also be identified by other laws, agreements, or standards. There is a need to present emblems through digital communication channels. Emblems presented in such ways are called digital emblems. Digital emblems extend the range of identifying marks from the physical (visual and tactile) to the digital realm.

Asset: A digital resource, system, or service - such as a server, data repository, or networked device - that can display a digital emblem. An asset represents the digital equivalent of an object, installation, or service that would be designated by a physical emblem.

Emblem issuer: The entity that operates or controls an asset that bears a digital emblem. Depending on the applicable emblem, the issuer may have received authorization to issue emblems, and in such cases, emblem issuers are also called _authorized entities_. For example, emblem issuers could be a medical or humanitarian organization, a cultural institution, or an operator of installations containing dangerous forces, among others.

Authorizing entity: An entity competent to grant authorization for the use, by an authorized entity, of a digital emblem. The authorizing entity ensures that such authorization is issued and recorded in accordance with applicable legal requirements, enabling technical and operational verification. In certain specific cases, the authorizing entity is also the authorized entity.

Validator: An entity that queries, inspects, or otherwise interacts with assets to determine whether they are marked with a valid digital emblem. Validators may include technical systems, network operators, or other actors implementing protective or non-interference measures consistent with the emblem’s purpose.

Validation: "To validate an emblem" means to confirm the authenticity or legitimacy of a particular symbol or design, often by checking its details against a known standard or reference point. Validation may include ensuring that the emblem has not been forged, stolen, or tampered with.

3. Requirements

The DIEM architecture will allow validators to discover and validate digital emblems that are associated with assets. 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 the marked asset 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 the marked asset by a Fully Qualified Domain Name (FQDN).

3.1.2. Emblem Semantics

Individual use cases MUST specify the semantics of the emblem. 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 an asset 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 asset's emblems 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

A digital emblem MAY require that its discovery and validation is undetectable. This requirement is motivated by emblems that mark its asset as protected and ask validators to not disrupt the marked asset. If emblem discovery were detectable, malicious parties could misuse the digital emblem as an intrusion detection system.

For specific use cases and designs, it may be acceptable that certain parties can detect emblem discovery and validation, for example, when the validator can hide in a sufficiently large anonymity set, or it is acceptable that the given party could detect the discovery or validation. Concrete designs MUST specify a threat model for undetectable validation. This threat model must detail which parties can detect emblem discovery and validation, under which conditions, and to what extent.

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 asset. 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. Asset Identifier Discovery

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

4.3. Implicit Discovery

An alternative approach to the above problem would be to bind emblems implicitly to the marked asset. Implicit binding could identify the marked asset by the emblem’s location. For example, if emblems were distributed via NFC, the marked asset 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 asset, 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

5.4.1. Background

The Geneva Conventions and their Additional Protocols constitute the core of 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

However, these emblems can currently only be used to mark physical assets, and there is no way to mark digital, network-connected infrastructure that enjoys the same protections. A digital emblem using the DIEM architecture could address this gap, and we call such emblems digital emblems for IHL.

5.4.2. Domain Model and Stakeholders

In context of emblems under IHL, emblems will mark assets that are digital services and that solely serve protected purposes (for example, a medical unit, a cultural site, or an installation containing dangerous forces). Such emblems will be issued by the party controlling the marked service, and they signal that these assets must be respected and protected. Emblems must only be issued by entities that have been authorized to bear a digital emblem or other distinctive sign under international law. Such authorizations must be issued by a state, other party to an armed conflict, or other entity competent under international law.

For digital emblems under IHL, validators will typically be armed forces under the command of either state or non-state actors. In situations of armed conflict, all such actors are under an obligation to check whether assets subject to military activities bear an emblem. Similarly, other malicious ICT actors, whilst not necessarily obligated under IHL, may choose to respect assets bearing the emblem. Concretely, we can assume that they will typically first identify an asset that they plan to engage with and then check whether that asset bears an emblem.

5.4.3. Requirements

The purpose of a digital emblem is to prevent disruptions of assets by informing verifiers that marked assets enjoy protection under IHL. Digital emblems will only be able to do so when verifiers are willing to pay attention to them. As verifiers intend to attack assets that are not protected under IHL, this will only be the case they are confident that their targets cannot fake protection and that they do not alert their target about an imminent attack. Therefore, digital emblems under IHL require validation for authenticity (Section 3.3.1) that is undetectable (Section 3.2.3).

At the same time, digital emblems under IHL should fit well into the existing framework of IHL and not put emblem issuers at increased risk. First, IHL requires that, emblem issuers must seek authorization from a competent authority prior to applying them (see Section 3.3.2 and Section 5.4.2). The authorization must be decentralized, i.e., there must be no central authorities that govern the use or distribution of digital emblems. Second, bearing an emblem can increase the risk for targeted attacks. We require that emblem issuers must be able to individually assess that risk and remove emblems whenever they see the risks to outweigh the benefits, i.e., we require that digital emblems are removable (Section 3.2.2).

Beyond the DIEM architecture as described in this document, digital emblems under IHL would benefit from other discovery mechanisms than the DNS, as not all assets may have domain names associated with them.

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

Because this is a requirements document, it does not directly have security considerations. However, multiple of the defined requirements include security properties. The architecture and standards developed need to detail the security properties of validation and authorization especially. Use cases have threat models and discussion of mitigating specific threats is needed. For example, in a use case where removability (Section 3.2.2) is needed, there are security considerations such as the potential for replay of removed emblems.

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