Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: 2 September 2026

J. Reid
RTFM llp

1 March 2026

DNS Architecture Considerations for Digital Emblems
draft-reid-diem-dnsarch-00

Abstract

It is expected that the Domain Name System (DNS) will be used to publish and retrieve Digital Emblems. The objective of this Internet Draft is to propose an architecture on how the DNS could be used and outline the main challenges that will require work from the diem Working Group. Publication of this document is intended to provoke discussion and analysis of how digital emblems can be deployed in the DNS.

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 2 September 2026.

Copyright Notice

Table of Contents

1. Introduction

This content-free placeholder text should be replaced with something more appropriate when the time comes.

2. Requirements Language

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. Structuring the DIEM Name Space

There are essentially two approaches to organising the name space used for digital emblems. These are not necessarily mutually exclusive. Both may be acceptible because of how digital emblems are applied to different use cases.

One option would be to anchor these domain names under diem.arpa (say) and have that overseen by IANA, just like how IANA coordinates the in-addr.arpa and ip6.arpa domains for reverse lookups of IPv6 addresses. IANA delegates parts of these domains to the Regional

Internet Registries who manage the distribution of IP addresses. For digital emblems, IANA could delegate parts of diem.arpa to the appropriate authorities such as humanitarian organisations or international treaty bodies. Each of them would be responsible for the oversight of subsequent delegations: for instance to the national chapters of the ICRC or to ICAO member states.

An advantage of this approach is diem.arpa, a potential apex for these zones, would be notionally neutral and independent. Other top-level domains (TLDs) are in general either overseen by ICANN or the relevant country's government. The Internet Architecture Board is responsible for the .arpa top-level domain and IANA does not currently charge for operating the .arpa registry. Using .arpa would fit with the IAB guidelines that the top-level domain gets used for infrastructure resources [RFC3172]. Digital emblems could reasonably be viewed as infrastructure resources that should be anchored somewhere under the .arpa TLD.

One potential difficulty with using diem.arpa (say) is the administrative burden on IANA. It would need to identify, establish and maintain relationships with DIEM stakeholders: international humanitarian organisations and/or treaty bodies. These relationships would need to be documented and processes put in place to manage delegations in diem.arpa. There would probably need to be a hierarchical naming or numbering scheme to identify digital emblems so they can be easily mapped into domain names, This would require a global registry. It is currently unclear if such a registry exists, if one would be set up or who would have the authority to create one and pay for it.

The second approach would be for each participant in digital emblems to choose the domain name(s) that best suit and have each organisation manage these independently. As an example, ICRC could anchor its DIEM entries under diem.icrc.org and take care of managing any delegations under that domain name. It would also be advisable to use discrete domain names and DNS platforms for the organisation and those used to support digital emblems. Fate-sharing could have undesirable consequences, This is why large eyeball networks separate the IT infrastructure used to run their business from the one used to provide service to its customers.

This ad-hoc approach might not scale. It will also rely on DNS expertise that might not be readily available at some participants. That way well create otherwise avoidable instability and operational problems.

4. Discovery of DIEM domain names

It is not clear how clients would decide which domain names to use whenever they make DIEM-related DNS lookups. One possibility is a client has a priori knowledge of the relevant domain name, for instance from a URL. This would probably require a diem-specific template to be added to the existing URL naming scheme. Another option might be for a client to be specially configured to lookup the domain name, eg refugee-camp.disaster-zone.relief-agency.TLD. While that could work, it does present scaling problems,

This topic needs detailed analysis by the working group.

5. Provisioning and Managing DIEM domain names

Conventional domain name registrations generally follow the well-established registry-registrar-registrant model. The registry maintains a database of domain names and runs authoritative DNS servers to publish delegation information for those domain names. The registrar updates that database on behalf of the end user, the registrant. The registar often provides tools, typically a web-based GUI, so registrants can update the contents of their registered domain names. In practice, these arrangements are much more complicated. However that operational detail does not matter here and is only of concern to pedants.

As an example, the IETF is the registrant for the ietf.org domain name. It uses Cloudflare as the registrar to manage the registration data for that domain name in the .org registry which is operated by PIR.

It is likely this model would be adopted when identifying the roles for managing the registration of DIEM related domain names. However these roles can be combined. As a hypothetical example, ICRC might occupy the role as the registry for the domain name used for a field hospital, an official at that hospital serves as the registrant and also fills the registrar role by using some ICRC-supplied website or smartphone app to manage the DIEM data for that field hospital’s domain name. The main consideration for this document is the separation of roles and responsibilities and not the actual entities who provide those functions.

Appropriate controls may be needed on how DIEM data get published in the DNS: who is authorised to add/remove DIEM-related DNS resource records, checking these are being used correctly, how long these records stay in the DNS, change management procedures, audits and so on. Some digital emblems will have protected status in international law and therefore need to be handled carefully. These controls

should ensure these resource records are used correctly and the "registry" is aware who is using which DIEM-related DNS resource records and for how long. Discussion of these issues are probably out of scope for this DNS architecture document. However they should be explored by the working group.

6. The DIEM Resource Record

Digital emblems SHOULD be stored in the DNS in the as-yet undefined DIEM resource record type (RRtype). Once this is documented, the lightweight expert review process defined in Section 3.1 of [RFC6895] will be used to obtain a formal RRtypecode and update the appropriate IANA database.

Digital emblems SHOULD NOT be stored as TXT records because these are already widely used for a diverse range of purposes: SPF data, version control information, publishing DMARC policy, nonce challenge-response strings and so on. Overloading TXT records with yet another use case would be unwise because it adds undesirable complexity for DNS administrators and the tools used to manage zone files.

A lookup for a domain name’s TXT records would return all of these records, forcing the client to process all of them to find the one(s) which contain digital emblem data. An additional concern is the possibility of truncated DNS responses, forcing retried queries over TCP when the amount of data in those TXT records is "too large" for a standard UDP responseq. Using a dedicated RRtypecode for DIEM records is cleaner and simpler.

The content of the proposed DIEM resource record has still to be decided. It will probably be some blob of structured text in CBOR or JSON format. This would allow the content of DIEM records to be extended whenever elements get added, updated or removed without needing a new typecode allocation. The HHIT and BRID resource records described in DRIP Entity Tags [RFC9886] provide an example of this approach.

7. IANA Considerations

IANA will be expected to issue a DNS RRtype code for the currently undefined and undocumented DIEM record.

It may be necessary for IANA to operate a registry and the supporting DNS infrastructure for the diem.arpa domain as outlined above.

8. Security Considerations

The main security concerns for DNS-based digital emblems are data validation, data authentication and client anonymisation.

Validation issues can be addressed by using Secure DNS, DNSSEC [RFC4033] [RFC5155]. When DIEM resource records are signed, validating DNSSEC-aware resolving servers can check the signatures on these responses and detect spoofed or tampered replies. They can also detect failures caused by DNSSEC signing errors such as incorrect or out of date keys. In short, clients receiving DNSSEC-signed responses can verify the replies exactly contain the data sent by the authoritative name servers that publish DIEM records.

Secure DNS offers provable non-repudiation as well as validation of DNS data. Though this DNSSEC feature is not widely appreciated. The private key used to sign DNS data implicitly identifies the signer and there is a chain of trust which terminates at the private key used to sign the DNS root. In simple terms, the private key for the domain name a.b.c is signed by the private key for b.c which in turn is signed by the private key for c which is signed by the DNS root’s private key.

In principle, this means it can be proven who signed DIEM-related resource records. Provided the relevant private keys are kept secret, impostors and other bad actors cannot sign those resource records. Similarly, the identity of the entity who does sign these resource records can be proven and they cannot claim otherwise. ie It can be shown a DNSSEC-signed DIEM record for (say) some ICRC resource was signed by the genuine authority for that resource and it could not have been signed by anyone else. This would prove there was a chain of trust showing that ICRC had responsibility for issuing that DIEM record and its accompanying DNSSEC signature(s).

The DNS provides serveral mechanisms to anonymise the source of DNS queries. However there is an unavoidable limitation. The client making the query usually sends the fully qualified domain name (FQDN) to its resolving DNS server. So that resolving server is aware which clients query for specific FQDNs. A client could make label-by-label iterative queries. Though this is unlikely. It wouldn’t help anonymisation because the resolving server would still in principle be able to assemble the FQDN from that client’s iterative queries.

Query minimisation [RFC9156] improves privacy for DNS clients and is widely supported in resolving servers. When this is used, the resolving server does label-by-label iterative queries instead of sending the FQDN for each step of the resolution. ie Instead of sending the FQDN a.b.c.d to the authoritative servers for the d, c.d

and b.c.d domains, the resolver sends a query for c.d to the authoritative servers for d, then a query for b.c.d to c.d's authoritative servers and then queries b.c.d's authoritative servers for a.b.c.d. Thus, the FQDN is ony visible to the resolving server and the authoritative server(s) for the b.c.d domain.

It should be noted that most resolving servers support Client Subnet in DNS Queries [RFC7871]. This discloses details about the source IP address of a DNS client to authoritative servers. [The rationale was so authoritative servers for a CDN could respond with the IP address of the CDN node that was optimal for the client making the initial query.] Clearly, this can have unfortunate privacy implications. When this feature is used, authoritative DNS servers may be able to identify the initiating client or at least get a reasonable indication of that client's identity.

Encrypted DNS transports provide a degree of anonimity, mostly by preventing eavesdropping and traffic interception. DNS over TLS [RFC7858], DNS over HTTPS [RFC8484] and DNS over QUIC [RFC9250] all use Transaction Layer Security to encrypt DNS queries and responses between clients and servers.

Oblivious DNS [RFC9230] is another possibility for improving client anonimity. This introduces a proxy which forwards encrypted DNS messages between a client and server. The proxy has no visibility of these messages and the server only receives the query and the source IP address of the query.

Choosing between these DNS capabilities and features is out of scope for this document because those are largely policy-based decisions that will depend on the prevailing local circumstances.

9. References

9.1. 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>.

[RFC3172] Huston, G., Ed., "Management Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain ("arpa")", BCP 52, RFC 3172, DOI 10.17487/RFC3172, September 2001, <https://www.rfc-editor.org/info/rfc3172>.

[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>.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, DOI 10.17487/RFC5155, March 2008, <https://www.rfc-editor.org/info/rfc5155>.

[RFC6895] Eastlake 3rd, D., "Domain Name System (DNS) IANA Considerations", BCP 42, RFC 6895, DOI 10.17487/RFC6895, April 2013, <https://www.rfc-editor.org/info/rfc6895>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC7871] Contavalli, C., van der Gaast, W., Lawrence, D., and W. Kumari, "Client Subnet in DNS Queries", RFC 7871, DOI 10.17487/RFC7871, May 2016, <https://www.rfc-editor.org/info/rfc7871>.

[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/info/rfc8174>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

[RFC9156] Bortzmeyer, S., Dolmans, R., and P. Hoffman, "DNS Query Name Minimisation to Improve Privacy", RFC 9156, DOI 10.17487/RFC9156, November 2021, <https://www.rfc-editor.org/info/rfc9156>.

[RFC9230] Kinnear, E., McManus, P., Pauly, T., Verma, T., and C.A. Wood, "Oblivious DNS over HTTPS", RFC 9230, DOI 10.17487/RFC9230, June 2022, <https://www.rfc-editor.org/info/rfc9230>.

[RFC9250] Huitema, C., Dickinson, S., and A. Mankin, "DNS over Dedicated QUIC Connections", RFC 9250, DOI 10.17487/RFC9250, May 2022, <https://www.rfc-editor.org/info/rfc9250>.

[RFC9886] Wiethuechter, A., Ed. and J. Reid, "DRIP Entity Tags (DETs) in the Domain Name System", RFC 9886, DOI 10.17487/RFC9886, December 2025, <https://www.rfc-editor.org/info/rfc9886>.

Acknowledgements

Fill this in when anyone needs to be acknowledged

Author’s Address

Jim Reid
RTFM llp
St Andrews House
Glasgow
South Georgia and the South Sandwich Islands
Email: jim@rfc1035.com