Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: 22 August 2025

SC. Chin, Ed.
D3 Global Inc

18 February 2025

DNS to Web3 Wallet Mapping
draft-chins-dnsop-web3-wallet-mapping-02

Abstract

This document proposes a implementation standard for mapping wallets to domain names using the new WALLET RRType, allowing for TXT record fallback while the WALLET RRType propagates through DNS providers. The goal is to provide a secure and scalable and unbiased way to associate wallets with domain names, enabling seamless lookup as well as suggesting required authentication mechanism. The proposal relies on DNSSEC or security successors to ensure trust and security.

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 22 August 2025.

Table of Contents

1. Introduction

There is fragmentation in the mapping of Web3 Wallets to Domain Names [RFC1034]. This document is putting forth a implementation standard to map Web3 Wallet addresses to Domain Names and investigates the associated security and technical concerns.

As the use of digital wallets and online services grows, the need for a standardized way to lookup wallet addresses in an human readable format becomes increasingly important. This proposal aims to provide a solution that is easy to implement, scalable, unbiased, standardized and secure.

The proposed Notational Implementation involves using the DNS WALLET RRtype [WALLET-IANA-RRTYPE] to map a domain name on the Global DNS system to wallet address information. The WALLET record will contain a object that maps the wallet address to the registered coin type

token [SLIP-0044]. It will also handles multiple wallet addresses and chain, defaults and defines a heirarchy to deterministicly be able to find the appropriate wallet address. It is assumed that the record will be part of a DNSSEC [RFC4033] [RFC9364] signed zonefile, or its security successors, and that users of this service will verify the signatures to ensure that the record has been returned without alteration in flight. This implementation proposal is evolutionary to the the description in [WALLET-IANA-RRTYPE] because it defines standards for coin names, defaults, and conditions for rejection, in order to have consistant usages.

We also propose a fallback TXT record "_w3addr" which will be a backup for the WALLET RRtype and CAN duplicate the WALLET RRtype entries. This is intended to be a temporary measure while DNS Provider UIs support this type [RFC3597].

1.1. 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.

2. Terminology

This document will refer to Domain Name terminology [RFC9499].

3. Domain to Wallet Mapping

3.1. Record Format

The WALLET or TXT record SHALL have the following format:

```
    @ IN WALLET "coin1:address1"
    @ IN TXT    "coin1:address1"
```

@
: is the address

IN
: is the class of the record

WALLET / TXT
: is the type of the record

coin1:address1
: is the value of the record, containing a comma-separated list of coin:address pairs

3.2. Grammar for the record in EBNF format

```
item = (coin_name) ":" address
coin_name = (letter | digit | "_")
address = (letter | digit)+
letter = "A" | "B" | "C" | "D" | "E" | "F" | "G"
       | "H" | "I" | "J" | "K" | "L" | "M" | "N"
       | "O" | "P" | "Q" | "R" | "S" | "T" | "U"
       | "V" | "W" | "X" | "Y" | "Z" | "a" | "b"
       | "c" | "d" | "e" | "f" | "g" | "h" | "i"
       | "j" | "k" | "l" | "m" | "n" | "o" | "p"
       | "q" | "r" | "s" | "t" | "u" | "v" | "w"
       | "x" | "y" | "z"
digit = "0" | "1" | "2" | "3" | "4" | "5" | "6" | "7" | "8" | "9"
```

item
: represents a coin_name-address pair

coin_name
: represents the Symbol of a Coin Type represented in [SLIP-0044]. This is not case sensitive.

address
: represents the public wallet address associated with a coin (e.g., "0xabcdefg", "0x12345", etc.)

This grammar can be used to parse the input string and extract the chain identifier and addresses.

3.3. Example

Suppose a user wants to map their wallet with the public keys to the domain example.com using the registered coin type tokens BTC, SOL and ETH. The WALLET record would be:

```
@ IN WALLET "BTC:0x1234567890abcd"
@ IN WALLET "SOL:0x567890123456789"
@ IN WALLET "ETH:0x987654321098765"
```

3.4. TXT Record Example

Suppose a user wants to map their wallet with the public keys to the domain example.com using the registered coin type tokens BTC, SOL and ETH using a TXT record. The TXT record would be:

```
_waddr IN TXT "BTC:0x1234567890abcd"
_waddr IN TXT "SOL:0x567890123456789"
_waddr IN TXT "ETH:0x987654321098765"
```

3.5. Multiple Records

To support multiple coins, multiple coin:address pairs will each be represented by a WALLET record. There is no guarantees on ordering the records so overlapping records MAY be ordered at the resolver's discretion. In the event of duplicate coin types it is RECOMMENDED that multiple records be returned deduplicated for identical addresses.

3.6. Implementation

Wallet resolver implementations of this RFC SHALL:

1. Support the creation and retrieval of WALLET records for any given level of the DNS system.

2. Validate the records as being properly signed by DNSSEC or its successors.

3. Provide the wallet's address for a human readable domain name.

4. Provide an authoritative NXADDR if no address can be found.

4. Security Considerations

To ensure the security of the mapping, the following measures will be taken:

1. The WALLET RRtype record SHALL BE stored in a secure location, such as a DNSSEC-signed zone.

2. The WALLET RRtype might not be available throughout entire end to end DNS infrastructure.

3. The implementation SHALL validate the DNSSEC record or its IETF approved successors.

4. The wallet record SHALL be protected from replay attacks via DNSSEC time invalidation (or approved successors).

If the source of the DNS zone is compromised, the wallet address mapping is compromised. It is imperative that this not occur for both DNS stability, as well as wallet mapping Notationaly using DNS.

5. IANA Considerations

This proposal does not require IANA changes.

6. References

6.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[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>.

[RFC3597] Gustafsson, A., "Handling of Unknown DNS Resource Record (RR) Types", RFC 3597, DOI 10.17487/RFC3597, September 2003, <https://www.rfc-editor.org/info/rfc3597>.

[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>.

[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>.

[RFC9364] Hoffman, P., "DNS Security Extensions (DNSSEC)", BCP 237, RFC 9364, DOI 10.17487/RFC9364, February 2023, <https://www.rfc-editor.org/info/rfc9364>.

[RFC9499] Hoffman, P. and K. Fujiwara, "DNS Terminology", BCP 219, RFC 9499, DOI 10.17487/RFC9499, March 2024, <https://www.rfc-editor.org/info/rfc9499>.

6.2. Informational References

[SLIP-0044] "Registered coin types for BIP-0044", <https://raw.githubusercontent.com/satoshilabs/slips/master/slip-0044.md>.

[WALLET-IANA-RRTYPE]
"Wallet Completed Template", 2024-06-24,
<https://www.iana.org/assignments/dns-parameters/WALLET/wallet-completed-template>.

Appendix A. Appendix 1: Example code

Here is an example of how to create and retrieve a WALLET records using the domain name:

```
import dns.resolver.wallet
# Retrieve the WALLET record
record = dns.resolveWallet("example.com", "BTC")

print(record.value)  # Output: "0x1234567890abcdef"
xs
```

Contributors

Thanks to all of the contributors for contributions to security and clarity.

Yevhenii Andrushchak
Email: yevhenii@d3.email

Kai Sung
Email: kai@d3.email

Acknowledgements

Reviewed by:

Jothan Frakes
Email: jothan@frakes.com

Author’s Address

Shay Chin (editor)
D3 Global Inc
Email: shay@d3.email