Network Working Group
Internet-Draft
Intended status: Informational
Expires: 7 October 2026

S. Uimonen
Independent

April 2026

Verified Email Identity Framework (VEIF)
draft-uimonen-veif-01.txt

Abstract

This document defines the Verified Email Identity Framework (VEIF), a mechanism for associating a cryptographically verifiable real-world identity with an email message. VEIF complements existing email authentication technologies such as SPF, DKIM, and DMARC by providing a higher-level identity assurance layer.

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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at https://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at https://www.ietf.org/shadow.html

This Internet-Draft will expire on 7 October 2026.

Copyright Notice

Copyright (c) 2026 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

1. Introduction

Existing mechanisms such as DKIM [RFC6376] and DMARC [RFC7489] validate domains but do not establish a verified real-world identity.

VEIF introduces a cryptographic identity assertion layer bound to an email message.

2. Terminology

The key words "MUST", "SHOULD", and "MAY" in this document are to be interpreted as described in [RFC2119].

Verified Identity: A real-world entity validated by an IdP.

Identity Provider (IdP): Entity issuing identity assertions.

VIA: Signed structure binding identity to email.

Trust Anchor: Root used for validation.

3. Architecture

3.1 Overview

VEIF operates as an overlay to domain authentication.

3.2 Components

* Sending Domain
* Identity Provider (IdP)
* Receiving MTA/MUA
* Trust Anchor

3.3 Message Flow

1. Identity verified by IdP
2. VIA issued
3. Sender attaches VIA
4. Receiver validates DKIM [RFC6376] and DMARC [RFC7489]
5. Receiver validates VIA

4. Trust Model

4.1 Trust Anchors

Trust anchors MAY be distributed via:

* Pre-configured trust stores
* DNSSEC-protected records
* Public PKI

4.2 Identity Binding

The IdP MUST verify that the sender is authorized to use the claimed domain.

5. Key Distribution

Public keys for VIA validation MAY be obtained via:

* DNS (TXT or dedicated RR)
* HTTPS endpoints
* Certificate chains

6. Revocation

IdPs MUST provide a revocation mechanism.

Possible mechanisms include:

* CRL-style lists
* OCSP-like queries
* Short-lived assertions

7. VEIF Identity Header

7.1 Definition

```
VEIF-Identity = "VEIF-Identity:" veif-value

veif-value = "v=" 1*DIGIT ";"
             "org=" quoted-string ";"
             "regid=" quoted-string ";"
             "domain=" domain ";"
             "sig=" base64
```

7.2 Signature Requirements

The signature MUST:

* Cover selected headers and/or body
* Be bound to the IdP
* Be verifiable using published keys

8. Validation Procedure

Receiving systems MUST:

1. Validate DKIM [RFC6376]
2. Check DMARC alignment [RFC7489]
3. Extract VEIF-Identity
4. Resolve public key
5. Verify signature
6. Check revocation status
7. Evaluate trust anchor

If validation fails, the identity MUST be treated as unverified.

9. Security Considerations

Attacks include identity misbinding, replay, and trust anchor compromise.

10. Privacy Considerations

Implementations SHOULD minimize exposed personal data.

11. Deployment Considerations

VEIF can be deployed incrementally alongside DMARC.

12. IANA Considerations

Header field name: VEIF-Identity
Applicable protocol: mail
Status: provisional

13. References

13.1 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs..."

[RFC6376] DomainKeys Identified Mail (DKIM)

[RFC7489] Domain-based Message Authentication (DMARC)

Author’s Address

Seppo Uimonen
Finland
Email: me@seppo-uimonen.fi