Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: 8 April 2026

S. Uimonen

7 October 2025

Verified Email Identity Framework (VEIF)
draft-uimonen-veif-00

Abstract

This document proposes the Verified Email Identity Framework (VEIF), a mechanism to ensure that every email address used for sending electronic mail is associated with a verifiable and accountable registrant. The goal is to significantly reduce spam, phishing, and identity abuse by introducing individual-level authentication in addition to existing domain-level controls such as SPF [RFC7208], DKIM [RFC6376], and DMARC [RFC7489].

1. Introduction

Despite the introduction of SPF [RFC7208], DKIM [RFC6376], and DMARC [RFC7489], spam and email-based fraud remain major global issues. While these mechanisms validate domain-level authorization and integrity, they do not authenticate or identify the individual sender

behind an email address.

Today, malicious actors can easily register domains and create thousands of email accounts without any real identity verification. These accounts are used to distribute phishing campaigns, fraud, and other malicious content. Victims often cannot trace the sender to a real-world identity.

The Verified Email Identity Framework (VEIF) aims to address this gap by requiring that every active email address be tied to a verified human or corporate identity.

2. Problem Statement

1. Domain-based authentication (SPF [RFC7208]/DKIM [RFC6376]/DMARC [RFC7489]) ensures only that an email is authorized to be sent from a given domain, not who the sender actually is.

2. Spammers and fraudsters can purchase or register domains freely and issue thousands of mailboxes, each capable of sending messages anonymously.

3. Email addresses and entire domain lists are traded and reused in criminal networks.

4. Current trust mechanisms are insufficient for receivers to block malicious or anonymous senders without also harming legitimate communication.

3. Proposed Framework: Verified Email Identity (VEIF)

The Verified Email Identity Framework introduces an additional layer of accountability by linking every email address to a verifiable identity.

Core principles:

* Each email address must be registered to an identifiable person or legal entity through a trusted identity provider (IDP).

* Identity providers may include government agencies, telecom operators, or accredited organizations capable of verifying legal identity.

* When an email is transmitted, the sending system attaches a cryptographic assertion (similar to DKIM) referencing a VEIF token issued by the identity provider.

* Receiving servers validate the token by checking its cryptographic authenticity and its current validity status from the issuing IDP.

* Receivers or mail clients may be configured to accept mail only from verified identities, similar to DMARC [RFC7489] domain enforcement.

The system can coexist with current standards. For example, SPF [RFC7208], DKIM [RFC6376], and DMARC [RFC7489] continue to verify domain authenticity, while VEIF adds sender identity verification at the user level.

4. Identity Model

* Individual Accounts - Identity is tied to a natural person via government-issued ID, strong digital signature, or similar proof.

* Corporate Accounts - Identity corresponds to an organization with named accountable representatives approved by management.

* Delegation and Privacy - A verified sender may delegate sending authority to systems or assistants but retains legal accountability.

5. Benefits

* Strong deterrent to spam and phishing.

* Easier law enforcement tracing and accountability.

* Enhanced trust in verified senders.

* Optional policy enforcement at receiver side (reject unverified mail).

6. Privacy and Security Considerations

VEIF must balance accountability with privacy. Identity verification does not require public disclosure of personal data. Verification tokens may be pseudonymous, revealing actual identity only under legal or authorized circumstances. End-to-end encryption and strict data minimization principles apply.

7. Backward Compatibility

VEIF is designed to complement, not replace, existing email security protocols. Adoption can be incremental. Non-verified mail continues to work unless recipients choose to enforce verification-only policies.

8. Next Steps

* Establish a dedicated IETF working group to explore identity-layer authentication for email.

* Define the VEIF token format and trust model.

* Develop reference implementations for mail servers and IDPs.

* Conduct interoperability testing with SPF [RFC7208]/DKIM [RFC6376]/DMARC [RFC7489] ecosystems.

9. IANA Considerations

This document makes no request of IANA at this time.

10. Security Considerations

Security considerations are discussed throughout this document, particularly in Section 6.

11. References

11.1. Normative References

[RFC7208] Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, DOI 10.17487/RFC7208, April 2014, <https://www.rfc-editor.org/info/rfc7208>.

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/info/rfc6376>.

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/info/rfc7489>.

Acknowledgements

The author thanks the IETF community for ongoing work on trusted internet communication.

Author’s Address

Seppo Uimonen
Finland

Email: me@seppo-uimonen.fi