Network Working Group
Internet-Draft
Intended status: Informational
Expires: 24 October 2026

J-I. Kadjo
Zenith Intelligence Technologies Inc.

22 April 2026

ZI2 Certified Email Server Attestation Protocol
draft-kadjo-zi2cert-00

Abstract

This document specifies the ZI2 Certified Email Server Attestation Protocol, a mechanism for cryptographic attestation of email origin at the mail server level. Unlike existing email authentication protocols (SPF, DKIM, DMARC), which operate at the domain level, ZI2 Certified operates at the server-instance level, enabling definitive identification of the specific server that dispatched a given email message. The protocol introduces two custom mail headers (X-ZI2-Certified and X-ZI2-Verified), a DNS TXT record publication format, a graduated trust model with four levels, and an integration interface for AI-based email classification systems. The protocol operates complementarily to existing email authentication infrastructure and does not require modification of SPF, DKIM, or DMARC.

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 24 October 2026.

Copyright Notice

Table of Contents

1. Introduction 2
1.1. Problem Statement 2
1.2. Scope 3
1.3. Relationship to Existing Protocols 3
2. Terminology 3
3. Protocol Specification 4
3.1. Cryptographic Primitives 4
3.2. Key Generation 4
3.3. Outbound Certification 4
3.4. Inbound Verification 5
4. Header Format 5
5. DNS Publication 5
6. Trust Levels 5
7. Security Considerations 5
8. IANA Considerations 6
9. References 6
9.1. Normative References 6
9.2. Informative References 6
Author's Address 7

1. Introduction

1.1. Problem Statement

The current email authentication ecosystem relies on three principal protocols: SPF [RFC7208], DKIM [RFC6376], and DMARC [RFC7489]. Each of these protocols operates at the domain level, answering questions about whether a domain authorized the sending of a message. None of these protocols, individually or in combination, answer a more fundamental question: "Did this specific server actually send this email?"

This distinction is critical in multi-tenant mail server environments, where a single server hosts multiple domains under a shared IP address and MTA process. In such environments, domain-level authentication cannot distinguish between legitimate email from one co-hosted domain and spoofed email purporting to originate from another co-hosted domain. An attacker who compromises one domain's DNS records or DKIM keys can forge emails that pass SPF, DKIM, and DMARC validation for any domain on the shared server.

1.2. Scope

This document specifies a server-level cryptographic attestation protocol that:

1. Generates a unique Ed25519 [RFC8032] key pair per server instance.
2. Signs outbound email with a server-specific attestation header.
3. Publishes the server’s public key via DNS TXT records, HTTPS well-known endpoints, and direct server-to-server exchange.
4. Verifies inbound email bearing the attestation header against the published public key.
5. Assigns graduated trust levels reflecting the strength of the verification method.
6. Integrates with AI-based email classification systems as a primary trust signal.

1.3. Relationship to Existing Protocols

ZI2 Certified does not modify, replace, or interfere with SPF, DKIM, DMARC, ARC [RFC8617], BIMI, MTA-STS, or DANE [RFC7671]. It operates as a complementary attestation layer that addresses the server-level authentication gap left by existing domain-level protocols. Existing protocols SHOULD continue to be deployed alongside ZI2 Certified.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] and [RFC8174].

Certification The process by which a sending mail server generates a cryptographic attestation of email origin and injects the attestation into the email as a structured header.

Verification The process by which a receiving mail server validates a certification header by retrieving the sender server’s public key and verifying the cryptographic signature.

Certifying Server A mail server that generates and injects ZI2 Certified headers on outbound email originating from its locally-hosted domains.

Verifying Server A mail server that validates ZI2 Certified headers on inbound email.

Trust Level A graduated integer value (0 through 3) representing the confidence in the verification result based on the method of public key retrieval.

Key Identifier (kid) A unique string identifying a specific public/private key pair, formatted as "zi2-cert-YYYY-MM".

Server Identifier (sid) The fully-qualified domain name (FQDN) of the certifying server.

Intra-Server Email Email transmitted between two domains hosted on the same physical or virtual server instance.

3. Protocol Specification

3.1. Cryptographic Primitives

The protocol uses Ed25519 [RFC8032] for signing (approximately 128 bits of security, deterministic signatures, 32-byte public keys, 64-byte signatures), SHA-256 [RFC6234] for body hash computation, and Base64 [RFC4648] for encoding.

3.2. Key Generation

Upon initial deployment, the certifying server MUST generate an Ed25519 key pair. The private key MUST be stored with restricted filesystem permissions and MUST NOT be transmitted outside the server boundary. The key identifier MUST follow the format "zi2-cert-YYYY-MM".

3.3. Outbound Certification

The certifying server MUST construct a canonical certification payload containing: protocol version, lowercase sender address, lowercase recipient address, Unix timestamp, Message-ID, server hostname, Base64 SHA-256 hash of the complete message body, and Base64 128-bit random nonce. The payload MUST be signed with Ed25519 and injected as the X-ZI2-Certified header.

3.4. Inbound Verification

The verifying server MUST check for the X-ZI2-Certified header, retrieve the public key (from local store, trust store cache, direct exchange, DNS TXT, or HTTPS endpoint), reconstruct the canonical payload, and verify the Ed25519 signature. Additional checks include timestamp freshness (24-hour window), body hash integrity (SHA-256 of complete body), and optional nonce uniqueness.

4. Header Format

The X-ZI2-Certified header uses tag=value format: v (version), t (timestamp), sid (server ID), bh (body hash), n (nonce), sig (Ed25519 signature), kid (key identifier). All tags are REQUIRED.

The X-ZI2-Verified header uses: result (pass/fail/missing/expired/tampered), level (0-3), reason (machine-readable code), sid, ts (verification timestamp).

5. DNS Publication

A certifying server MUST publish a DNS TXT record at _zi2cert.<domain> for each hosted domain. Format: "v=ZI2CERT1; k=ed25519; p=<base64_key>; kid=<key_id>". All domains on the same server share the same public key because attestation is server-level. During key rotation, two records MAY coexist.

6. Trust Levels

Level 3 (ABSOLUTE): Intra-server verification using local key store. Level 2 (VERIFIED): Key obtained via direct server-to-server exchange. Level 1 (DNS): Key obtained via DNS TXT record. Level 0 (UNKNOWN): No certification present or verification failed.

Level 3 is unique to this protocol. When both sender and recipient domains are co-hosted, verification uses the same key pair that generated the certification, providing mathematical certainty with no external dependencies.

7. Security Considerations

Key compromise impact is bounded by the 24-hour freshness window and key rotation interval. DNS poisoning affects Trust Level 1 only; DNSSEC [RFC4033] SHOULD be deployed. Header injection is mitigated by Ed25519 signature verification. Replay attacks are mitigated by nonce, timestamp, and Message-ID binding. Body modification by intermediaries causes body hash mismatch. Ed25519 is vulnerable to quantum computing; post-quantum algorithms may be adopted via the

version and algorithm tags.

8. IANA Considerations

This document requests registration of header fields X-ZI2-Certified and X-ZI2-Verified, DNS underscore label _zi2cert, and well-known URI zi2-cert.json.

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>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/info/rfc4648>.

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, DOI 10.17487/RFC6234, May 2011, <https://www.rfc-editor.org/info/rfc6234>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <https://www.rfc-editor.org/info/rfc8032>.

[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>.

9.2. Informative References

[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>.

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/info/rfc6376>.

[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>.

[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>.

[RFC7671] Dukhovni, V. and W. Hardaker, "The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance", RFC 7671, DOI 10.17487/RFC7671, October 2015, <https://www.rfc-editor.org/info/rfc7671>.

[RFC8617] Andersen, K., Long, B., Ed., Blank, S., Ed., and M. Kucherawy, Ed., "The Authenticated Received Chain (ARC) Protocol", RFC 8617, DOI 10.17487/RFC8617, July 2019, <https://www.rfc-editor.org/info/rfc8617>.

Author’s Address

Joseph-Israel Kadjo
Zenith Intelligence Technologies Inc.
Hagerstown, MD 21740
United States of America
Email: dev@zi2.app
URI: https://zi2.app