Network Working Group
Internet Draft
<draft-ietf-dkim-rfc4871-errata-01>
Intended status: Standards Track
Expires: July 2009

D. Crocker, Editor
Brandenburg InternetWorking
January 2009

RFC 4871 DomainKeys Identified Mail (DKIM) Signatures -- Errata

draft-ietf-dkim-rfc4871-errata-01

Status of this Memo

CONFORMANCE UNDEFINED.

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 <http://www.ietf.org/ietf/1id-abstracts.txt>.

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

This Internet-Draft will expire in July 2009.

Abstract

This documents and resolves errata for RFC 4871, DomainKeys Identified Mail (DKIM) Signatures. Specifically the document clarifies the nature, roles and relationship of the two DKIM identifier tag values that are candidates for payload delivery to a receiving processing module.

Errata Contact Fields

Name: Dave Crocker

Email: dcrocker@bbiw.net

Type

Technical

Table of Contents

1. Introduction

About the purpose for DKIM, [RFC4871] states:

> The ultimate goal of this framework is to permit a signing domain to assert responsibility for a message, thus protecting message signer identity...

Hence, DKIM has a signer that produces a signed message, a verifier that confirms the signature and an assessor that consumes the validated signing domain. so the simple purpose of DKIM is to communicate an identifier to a receive-side assessor module. The identifier is in the form of a domain name that refers to a responsible identity. For DKIM to be interoperable and useful, signer and assessor must share the same understanding of the details about the identifier.

However the specification defines two, potentially different identifiers that are carried in the DKIM-Signature: header field and might be delivered to a receiving processing module that consumes validated payload. The DKIM specification fails to clearly define what is "payload" to be delivered to a consuming module, versus what is internal and merely in support of achieving payload delivery.

This currently leaves signers and assessors with the potential for having differing -- and therefore non-interoperable -- interpretations of how DKIM operates.

This erratum resolves this confusion. It defines new labels for the two values, clarifies their nature, and specifies and their relationship.

2. RFC 4871 Abstract

Original Text: The ultimate goal of this framework is to permit a signing domain to assert responsibility

Corrected Text: The ultimate goal of this framework is to permit a person, role or organization that owns the signing domain to assert responsibility

3. RFC4871 Section 1. Introduction

Original Text: permitting a signing domain to claim responsibility

Corrected Text: permitting a person, role or organization that owns the signing domain to claim responsibility

4. RFC4871 Section 2.7 Identity

A person, role or organization.

Original Text: (None. Additional text.)

Corrected Text: A person, role or organization.

5. RFC4871 Section 2.8 Identifier

Original Text: (None. Additional text.)

Corrected Text: A label that refers to an identity.

6. RFC4871 Section 2.9 Signing Domain Identifier (SDID)

Original Text: (None. Additional text.)

Corrected Text: A single, opaque value that is the mandatory payload output of DKIM and that refers to the identity claiming responsibility for the introduction of a message into the mail stream. Within the scope of the DKIM Signing specification, the conventions and semantics used by a signer to create and use a specific SDID are outside the scope of the DKIM Signing specification, as is any use of those conventions and semantics.

7. RFC4871 Section 2.10 User Agent Identifier (UAID)

Original Text: (None. Additional text.)

Corrected Text: A single, opaque value that is the optional, additional payload output of DKIM and that identifies the user or agent on behalf of whom the SDID has taken responsibility. The conventions and semantics used by a signer to create and use a specific UAID are outside the scope of the DKIM Signing specification, as is any use of those conventions and semantics.

8. RFC4871 Section 2.11 Identity Assessor

Original Text: (None. Additional text.)

Corrected Text: The name of the module that consumes DKIM's primary payload, the responsible Signing Domain Identifier (SDID). It can optionally consume the User Agent Identifier (UAID) value, if provided to the module. The conventions and semantics used by a signer to create and use a specific SDID or UAID are outside the scope of the DKIM Signing specification, as is any use of those conventions and semantics.

9. RFC4871 Section 3.9 Relationship Between SDID and UAID

Original Text: (None. This is an addition.)

Corrected Text: DKIM's primary task is to communicate from the Signer to a recipient-side Identity Assessor a single, Signing Domain Identifier (SDID) that identifies a responsible identity. The SDID MUST be the value of the d= tag. DKIM MAY optionally provide a single responsible User Agent Identifier (UAID); if the UAID is present, it MUST be the value of the i= tag.

The SDID MUST correspond to a valid DNS name under which the DKIM key record is published.

The UAID is specified as having the same syntax as an email address, but is not required to have the same semantics. Notably, the domain name is not required to be registered in the DNS -- so it might not resolve in a query -- and the Local-part MAY be drawn from a namespace that does not contain the user's mailbox. The details of the structure and semantics for the namespace are determined by the Signer. Any knowledge or use of those details by verifiers or assessors is outside the scope of the DKIM Signing specification. The Signer MAY choose to use the same namespace for its UAIDs as its users' email addresses, or MAY choose other means of representing its users. However, the signer SHOULD use the same UAID for each message intended to be evaluated as being within the same sphere of responsibility, if it wishes to offer receivers the option of using the UAID as a finer grained, stable identifier than the SDID.

Hence, DKIM delivers to receive-side Identity Assessors responsible Identifiers that are individual, opaque values. Their sub-structures and particular semantics are not publicly defined and, therefore, cannot be assumed by an Identity Assessor.

A receive-side DKIM verifier MUST communicate the Signing Domain Identifier (d=) to a consuming Identity Assessor module and MAY communicate the User Agent Identifier (i=) if present.

To the extent that a receiver attempts to intuit any structured semantics for either of the identifiers, this is a heuristic function that is outside the scope of DKIM's specification and semantics. Hence it is relegated to a higher-level service, such as a delivery handling filter that integrates a variety of inputs and performs heuristic analysis of them.

10. RFC4871 Section 3.5 The DKIM-Signature Header Field

Original Text: d= The domain of the signing entity.

Corrected Text: d= Specifies the SDID claiming responsibility for an introduction of a message into the mail stream.

11. RFC4871 Section 3.5 The DKIM-Signature Header Field

Original Text: i= Identity of the user or agent (e.g., a mailing list manager) on behalf of which this message is signed

Corrected Text: i= The responsible User Agent Identifier (UAID) on behalf of which the SDID is taking responsibility.

12. RFC4871 Section 3.8. Signing by Parent Domains

the section where the error appears

Original Text: e.g., a key record for the domain example.com can be used to verify messages where the signing identity ("i=" tag of the signature) is sub.example.com, or even sub1.sub2.example.com. In order to limit the capability of such keys when this is not intended, the "s" flag may be set in the "t=" tag of the key record to constrain the validity of the record to exactly the domain of the signing identity. If the referenced key record contains the "s" flag as part of the "t=" tag, the domain of the signing identity ("i=" flag) MUST be the same as that of the d= domain. If this flag is absent, the domain of the signing identity MUST be the same as, or a subdomain of, the d=

Corrected Text: For example, a key record for the domain example.com can be used to verify messages where the UAID ("i=" tag of the signature) is sub.example.com, or even sub1.sub2.example.com. In order to limit the capability of such keys when this is not intended, the "s" flag MAY be set in the "t=" tag of the key record, to constrain the validity of the domain of the UAID. If the referenced key record contains the "s" flag as part of the "t=" tag, the domain of the UAID ("i=" flag) MUST be the same as that of the SDID (d=) domain. If this flag is absent, the domain of the UAID MUST be the same as, or a subdomain of, the SDID.

13. RFC4871 Section 6.3. Interpret Results/Apply Local Policy

Original Text: It is beyond the scope of this specification to describe what actions a verifier system should make, but an authenticated email presents an opportunity to a receiving system that unauthenticated email cannot. Specifically, an authenticated email creates a predictable identifier by which other decisions can reliably be managed, such as trust and reputation.

Corrected Text: It is beyond the scope of this specification to describe what actions an Identity Assessor can make, but mail carrying a validated SDID presents an opportunity to an Identity Assessor that unauthenticated email does not Specifically, an authenticated email creates a predictable identifier by which other decisions can reliably be managed, such as trust and reputation.

14. RFC4871 Section 6.3. Interpret Results/Apply Local Policy

Original Text: Once the signature has been verified, that information MUST be conveyed to higher-level systems (such as explicit allow/whitelists and reputation systems) and/or to the end user. If the message is signed on behalf of any address other than that in the From: header field, the mail system SHOULD take pains to ensure that the actual signing identity is clear to the reader.

Corrected Text: Once the signature has been verified, that information MUST be conveyed to the Identity Assessor (such as an explicit allow/whitelist and reputation system) and/or to the end user. If the SDID is not the same as the address in the From: header field, the mail system SHOULD take pains to ensure that the actual SDID is clear to the reader.

15. RFC4871 Appendix D. MUA Considerations

Original Text: The tendency is to have the MUA highlight the address associated with this signing identity in some way, in an attempt to show the user the address from which the mail was sent.

Corrected Text: The tendency is to have the MUA highlight the SDID, in an attempt to show the user the identity that is claiming responsibility for the message.

16. Security Considerations

This Errata document clarifies core details about DKIM's payload. As such it affects interoperability, semantic characterization, and the expectations for the identifiers carried with a DKIM signature. Clarification of these details is likely to limit misinterpretation of DKIM's semantics. Since DKIM is fundamentally a security protocol, this should improve its security characteristics.

17 Normative References

[RFC4871] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures", RFC 4871, May 2007.

Author's Address

D. Crocker (editor)
Brandenburg InternetWorking
Phone: +1.408.246.8253
EMail: dcrocker@bbiw.net

A. Acknowledgements

This document was initially formulated by an ad hoc design team, comprising: Jon Callas, J D Falk, Jim Fenton, Tony Hansen, Murray Kucherawy, John Levine, Michael Hammer, Jeff Macdonald, Ellen Siegel, Wietse Venema. It represents a rough consensus of that effort, although the final wording of the submitted draft is the sole responsibility (d=) of the listed author.

Full Copyright Statement

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org [1].

[1] mailto:ietf-ipr@ietf.org