

Network Working Group  
Internet Draft  
January 2005  
Expires in six months

R. Housley  
Vigil Security

## Security Review of Two MASS Proposals

<[draft-housley-mass-sec-review-00.txt](#)>

### Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, or will be disclosed, and any of which I become aware will be disclosed, in accordance with [RFC 3668](#).

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/lid-abstracts.txt>.

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

### Abstract

A small group conducted a speedy security review of two MASS proposals: DomainKeys and Identified Internet Mail (IIM). This short document provides the findings.

Internet Draft [draft-housley-mass-sec-review-00.txt](#)

January 2005

## [1.](#) Introduction

The MASS effort began with many proposed solutions at the first MASS BoF held at IETF 60. Discussions on the mail list have trimmed the number of proposals considerably. The leading contenders are now DomainKeys [[Delany](#)] and Identified Internet Mail (IIM) [[Fenton](#)].

A small group was gathered by the Security Area Director to conduct a speedy security review of DomainKeys and Identified Internet Mail (IIM). The group included (in alphabetical order):

- Steve Bellovin (Columbia University)
- Matt Fanto (NIST)
- Sam Hartman (MIT)
- Russ Housley (Vigil Security)
- Blake Ramsdell (Sendmail)
- Neil Rerup (EDS)
- Jim Schaad (Soaring Hawk)
- Sam Weiler (SPARTA)

## [2.](#) Security Review

The DomainKeys and IIM specifications are both in good shape. They represent a lot of work. This review could not have been conducted without well written specifications as an input. While the syntax and semantics could use some further clarification, the basic intent is clear.

The MASS effort, if it goes forward in the IETF, will specify mechanisms to support the automated reduction of Phishing attacks and Spam. The idea is that the email message can be automatically filtered if the advertised source of the message is not associated with the domain that signed the message.

### [2.1.](#) Spamming Phishing, Authentication, and Privacy

Steve Bellovin published an article in the Communication of the ACM [[Bellovin](#)] That takes the position that authentication is probably not going to be a silver bullet that solves this problem. The review team agrees; however, Phishing and Spam have reached epidemic proportions, and they demand the attention of the IETF and other

Internet-related groups. Further, authentication will provide A valuable input to automated filtering, which could eventually aid all email users.

## [2.2.](#) S/MIME and OpenPGP

DomainKeys and IIM claim to be much simpler than S/MIME or OpenPGP. The security review team agrees with this assessment. Since the problem trying to be solved is somewhat simpler than previous efforts, the problem domain is restricted and the solution is simpler. However, we must be careful that requirements are not added during the development process. If this happens, the final outcome could be just as complex (or even more so) than S/MIME and OpenPGP.

## [2.3.](#) Public Key Infrastructure

Neither DomainKeys nor IIM makes use of certificates. The goal is to start with something simple; something that does not depend on the deployment of an infrastructure. The question is: what is simple enough? The solution needs to be complex enough to support the evolution to a supporting infrastructure; however, there are also concerns with incrementally adding things. One must ensure that the final architecture is not more complex than deploying an infrastructure from the beginning.

The solution space is discontinuous. Both DomainKeys and IIM seem to have decided that existing certificate-based technologies are too complicated. That is, Certification Authorities (CAs) and certificate revocation are not required by either proposal. They only include a placeholder for the future use of X.509 certificates.

This decision may be reasonable. If a mechanism to deal with revocation is added to the architecture several years after deployment, then the Internet community can probably live with some duplication of effort. However, if two weeks before the MASS RFC is published, the Internet community decides that a revocation mechanism is needed, then everyone will be wondering why [RFC 3280](#) and the other outputs of the PKIX working group were not employed. Such a transition will be very difficult.

Overall complexity must be considered. Enhanced deployment may be a reasonable justification for incrementally developing technology. Minimizing specification time at the cost of deployment complexity is not such a justification.

Since a transition to X.509 certificates is considered, [RFC 2538](#) should at least be considered.

### [3.](#) Cryptography

Neither DomainKeys nor IIM does a good job specifying the Cryptographic algorithms. Both require RSA (probably the PKCS#1 version 1.5 variant) and SHA-1. This is a fine choice, but the specification needs to handle other algorithms too. It is not clear how one would migrate to ECDSA with SHA-256, for example.

The key sizes specified for use with this system are different than those specified in other IETF applications. No justification is provided. RSA with a key size smaller than 1024 bits clearly needs justification. Migration to an RSA key size of 2048 bits should be expected.

No mechanism to facilitate the transition from one signature algorithm to another is included. One approach might be the support for multiple signatures to appear in a message.

### [4.](#) Potential Security Concerns

#### [4.1.](#) Replay Attacks

One of the MASS goals is to prevent ISPs from having from their addresses forged by spammers. This service would support the construction of a reputation system. Neither DomainKeys nor IIM prevent source address masquerade. It is fairly easy to send Spam with a valid isp.example.com signature by simply getting an account

from that ISP and use it to send a Spam message to another account served by another ISP. The received message contains a valid signature for the Spam message. The message can be duplicated and resent to any recipients, and the ISPs signature will be valid.

According to the IIM authors, they discuss this attack and some solutions. The solutions all had undesirable properties.

In security terms, this is a replay attack. Without replay protection DomainKeys and IIM fail to provide the authentication that being advertised.

#### 4.2. Denial of Service Attacks

Much more attention needs to be given to denial of service issues. Note that a large number of bogus messages can overload the CPU of a verifier. We have already seen CPU attacks by spammers against anti-spam systems.

### 5. Security Differences

#### 5.1. Key Registration Server

IIM includes the Key Registration Server (KRS). This provides significant flexibility, without requiring every domain name to deploy a server. This separate server has many properties in common with an OCSP server used in some PKI deployments.

It is not as easy to distribute KRS servers as is claimed; they are not serving up simple static pages.

The granularity of control offered by the KRS is desirable. However, the complexity raises questions. If this complexity is necessary, what complexity associated with a PKI is really being avoided?

The DomainKeys proposal depends entirely on DNS. Of course, the DNS has well known security issues. DNS responses are essentially unauthenticated. Some day, DNSsec will be deployed, but we should not depend on that security solution for the MASS effort. Note that this threat also needs to be discussed in the Security Considerations

section. At a minimum, mention DNSsec and point to [RFC 3833](#).

The type of DNS attacks that would allow arbitrary public key substitution are claimed to be "uneconomical." This assertion is completely unsupported. The spammers have shown great willingness to engage in many different forms of attack against anti-spam services.

KRS involves a reference from the DNS to the KRS server, which is accessed with HTTP. One can either accept a lack of security or provided by DNS as seems to be suggested, or TLS can be used to protect HTTP. However, the use of TLS involve the use of PKI to authenticate the KRS server. This leads to a very big question: which trust anchors are appropriate for use in this application? The answer involves infrastructure deployment.

## [5.2](#). DomainKeys Signature

Crucial semantics are specified in the DomainKey-Signature: line, but it is not covered by the signature. Can an attacker change the one-way hash function (h= portion of the header line)?

The document should require the signature algorithm (the default is a=rsa-sha1) to be present in the header line.

## [6](#). Open Email Issues

The DomainKeys and IIM documents employ the same canonicalization approaches. These need further review by the email community. The digital signature processing of DomainKeys and IIM has many similarities with digital signing XML. The canonicalization is very simple, much simpler than MIME. The MIME documents explain mail-mangling quite well, so justification for the simpler canonicalization needed.

Several header lines need further investigation. For example, "Resent-\*" and the myriad ways that mailing lists mangle email. Mailman, for example, can prepend text to a message as well as append text to a message, but only the latter case is discussed. Also, many mailing list systems modify the Subject: line, which will break

signature verification of any messages that covers the Subject: line. Anti-virus and anti-spam packages also make changes to messages.

Another mail-related issue is the existence of user+something@example.com Addresses. Are the wildcards proposed for per-user keys sufficient for these addresses? Should the canonicalization algorithm handle this in a special way?

## 7. Deployment Concerns

DomainKeys and IIM specify opt-in mechanisms. Therefore, when a specific domain goes on a black list, a Spammer can simply change domains. If the solution does not achieve full deployment, it is not clear that it will meet the stated objectives.

Deployment requires MUAs to be updated; however, updating to accept S/MIME or OpenPGP mail is considered to be too difficult. Since there is already a lot of software for S/MIME and OpenPGP, justification is needed.

ISPs need to update all POP/IMAP mail servers to perform signature verification; however, these same servers have not been updated to remove constraints on 7-bit mail. What will make this different?

ISPs need to update all mail submission points to generate the signature and authenticate the originator. Yet, many ISPs cannot or will not deploy TLS to protect passwords. What will make this different?

## 8. Security Considerations

This document provides a security review of DomainKeys and IIM. The review team hopes that the information here will improve the output of the MASS effort, if a working group is chartered to pursue this work.

## 9. IPR Considerations

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, or will be disclosed, and any of which I become aware will be disclosed, in accordance with [RFC 3668](#).

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](mailto:ietf-ipr@ietf.org).

## 10. Informative References



- [Bellovin] S. Bellovin. "Spamming, Phishing, Authentication, and Privacy", Communication of the ACM, 47(12):144, 2004.
- [Delany] M. Delany. Domain-based Email Authentication Using Public-Keys Advertised in the DNS (DomainKeys). August 2004. <[draft-delany-domainkeys-base](#)>, work in progress.
- [Fenton] J. Fenton and M. Thomas. Identified Internet Mail. October 2004. <[draft-fenton-identified-mail](#)>, work in progress.

## 11. Authors' Address

Russell Housley  
Vigil Security, LLC  
918 Spring Knoll Drive  
Herndon, VA 20170  
Phone: +1 703-435-1775  
Email: housley@vigilsec.com

## 12. Full Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED,

INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE  
INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED  
WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

