Development, Deployment & Operations

IETF 73

Dave Crocker, Tony Hansen,
Phillip Hallam-Baker, Ellen Siegel

Reorganization

- Turned inside out
  - Activity oriented
  - development, deployment and operations information placed within activities
- Refocus on domain-specific information
  - Move tutorial information to appendices and external references
- Work in progress
- Intend to have WGLC before San Francisco

New Organization

1. Introduction

2. Using DKIM as part of Trust Assessment
3. DKIM Key Generation, Storage, and Management
4. DKIM Signing
5. DKIM Verifying
6. DKIM Deployment Considerations for Email Agents
7. Migrating from DomainKeys to DKIM
8. DKIM Example Uses

9. Author Domain Signing Practices (ADSP)

Appendices

2. Using DKIM as part of Trust Assessment

2.1. A systems view of trust assessment

2.2. Considerations in choosing signing names

- 2.2.1 Segmentation of traffic streams
- 2.2.2. d= vs. i=
- 2.2.3. Flexibility vs. utility – what will receivers use?

2.3 Recipient-based Assessments

- 2.3.1 Third-party Reputation and Accreditation Services

Trust assessment is different from Mis-trust assessment.

What do people believe this means?

3. DKIM Key Generation, Storage, and Management

3.1 Key Generation and Storage

- 3.1.1 Assignment of Selectors
- 3.1.2 Third Party Key Management
- 3.1.3 Storing Public Keys: DNS Server Software Considerations
- 3.1.4 Private Key Management: Deployment and Ongoing Operations

3.2 DNS Signature Record Deployment and Maintenance Considerations

- 3.2.1 Time Basis and Security Considerations
- 3.2.2 Deploying New Selectors
- 3.2.3 Subdomain Considerations
- 3.2.4 Delegating Signing Authority to a Third party

Nothing contentious here?

4. DKIM Signing

4.1 Deployment

- 4.1.1 DNS Records
- 4.1.2 Signing Module
- 4.1.3 DKIM Signing Software Development
- 4.1.4 Operational Constraint Affects on Signing Practices

4.2 Mailing Lists

- 4.2.1 Mailing List Manager Actions

4.3 Signature Transition Strategy

- 4.3.1 Signer transition strategy
- 4.3.2 Verifier transition strategy

What issues about mailing lists should we cover?

5. DKIM Verifying

5.1 Verifier

5.2 DNS Client

5.3 Boundary Enforcement

5.4 Filtering Software

Nothing contentious here?

6. DKIM Deployment Considerations for Email Agents

6.1 Email Infrastructure Agents

6.2 Mail User Agent

What issues/concerns do people want us to cover?

7. Migrating from DomainKeys to DKIM

7.1 Signing

7.2 Verifying

7.3 DNS Key Record Differences

Any other areas we wish to cover?

8. DKIM Example Uses

8.1 Protection of Internal Mail

8.2 DKIM Support in the Client

8.3 Per user signing

8.4 Using Trusted 3rd-party senders

Send descriptions/details of additional examples to the list

9. Author DSP

9.1 Overview

9.2 Publishing ADSP Records

9.3 Using ADSP Information

9.4 Examples Using ADSP

What value add can we put in this document above & beyond what is in ADSP RFC?

What particular concerns do people want covered?