60th IETF August 2004 - San Diego, CA

Message Authentication and

Signature Standards (MOSS) BOF

MTA Signatures Proposal – Brief Overview

Proposal details available at:
http://www.elan.net/~william/asrg/mta_signatures.htm

Presentation and Proposal by William Leibzon – william@elan.net

This presentation can be downloaded at
http://www.elan.net/~william/asrg/IETF60-MTA_Signatures-Brief.pdf

The following two slides are actually last slides in conclusion of presentation
http://www.elan.net/~william/asrg/SecuringEmailPath.pdf

Goals for Mail Server Added Signatures

1. Applicability from any MTA to any other MTA in email path
   Should provide security both end-end and from any one point in email path transmission to any other point
2. Compatibility with different scenarios in existing email path
   Should be adoptable to changes made to email message during transmission through more complex email path and should work with all common forwarding scenarios even if forwarding system does not support this security model and can not add its own signature
3. No upgrades or changes necessary for MUAs
   Should not require new mail client programs (MUAs) for either sender or recipient. New extensions should not cause problems and original email data should still be readable in all MUAs
4. Achieves verification and traceability of email
   The result should be that email message is fully traceable, i.e. it should be possible to confirm that email indeed came through each listed system (preferably by cryptographic means verifying signature with listed server). In case email was changed, its good if there was a way to tell which parts of the email were changed during the transmission .

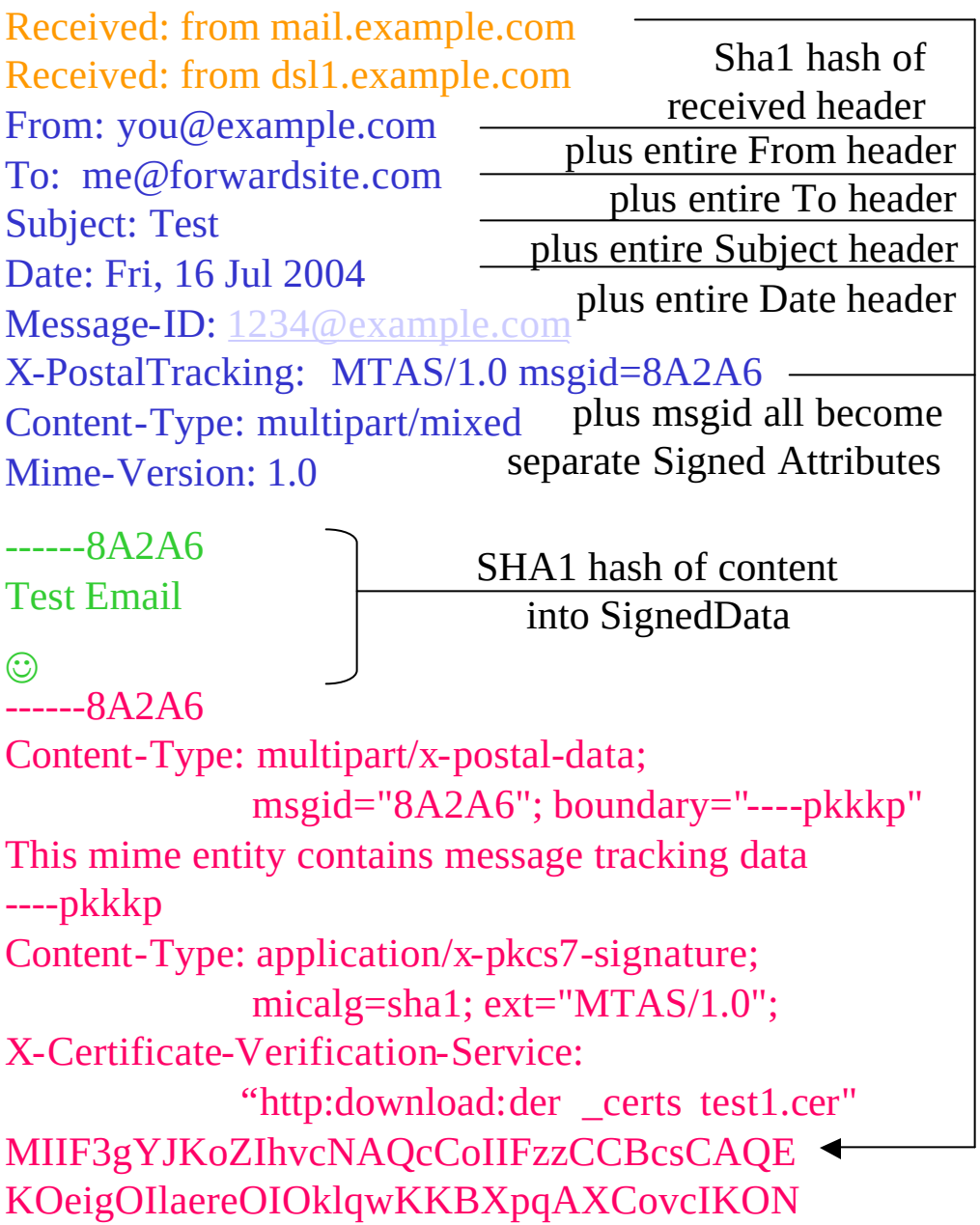
Additional implementation goals for Mail Server Added Signatures

5. Benefits to early adaptors with no risk of lost mail
   Should function in such a way as to provide full benefits to early adaptors located at both ends of the email path even if intermediate MTAs are not aware of new security model. At the same time early adaptors should not risk that some of their emails might not get delivered due to signatures
6. Fixed data size
   New data fields added to email message should be of fairly fixed size and this size should not be in direct proportion to the size email message but be primarily based on the level of security desired.
7. Extensibility for the future
   Protocol(s) should be extendable and it should be possible to create new versions and use new security protocols without breaking existing setup
8. Should be based on existing IETF work
   The system should be compliant with existing IETF protocols and it should try to base the work on existing IETF email security standards.
9. Use of existing libraries. No licensing requirements.
   The system should be patent free to allow everybody to implement it. Ability to reuse existing encryption libraries is also desired.

From S/MIME to MTA Signatures

- It is notable that there are existing standard methods to add cryptographic mail signatures by sender end-users – S/MIME and PGP. S/MIME is more extendable format, so it was decided to use that as basis
- Tests were done on how S/MIME like signature can be added to email so that MUAs do not confuse them with S/MIME. Two ways were found:
  - Making sure main mail message is not multipart/signed and adding signature use new mime type (that does not have “pkcs7-signature” as any part of its name) and having signature names add with extension other then .p7s
  - Having signature embedded as part of unknown multipart mime type (tests with 10 MUAs show that they ignore unknown multipart types)
- MTA Signatures initial draft has all signatures added as part of new “Multipart/Postal-Data” mime part, which is added at the end of existing email body and actual signed mail message part is everything above the Multipart/Postal-Data.

MTA Signatures Details



- Mail signatures are added into new mime entity of multipart type “postal-data”. This is entity is added below existing email body content.
- Mail signature is hash of content added into PKCS7 format (S/MIME like) data structure, signature is then put inside postal-data structure.
- MUA visible headers are signed by adding entire header into PKCS7 structure as signed attribute. Hash of received headers can also added.
- Hash of distinct MIME parts can be added as signed attributes and this allows to verify message even if some of its mime parts have been modified in transit (or deleted)
- Verification is supported through multiple methods which are listed at Certificate-Verification-Service mime header or CMS attribute

MTA Signature Verification

- Multiple signature verification services can be supported at the same time and new methods easy to define.These are listed in new MIME header (below) or through PKCS7 attributes:

  X-Certificate-Verification-Service: "domain:key:email _key1._certs;
  http:download:der _certs completewhois-com-test1.cer"

- Names of possible signature verification services:

http:download:der	https:download:der
ftp:download:der	tftp:download:der
domain:key:email	domain:cert:pkix
domain:txt:xml:_ep:keys	domain:txt:dk
http:scvp	http:dvcs
http:pgp-keyserver	ldap:smime-keyserver
http:soap:policyserv:email:cms	soap-beep:policyserv:email:cms

- Proposal paper defines two simplest to implement verification methods which can be used for initial testing:
  - http:download:der (and also https, ftp, tftp variations)
    Here entire certificate that signed MTA signature is made available for download by the signing system
  - domain:key:email
    Here public key is published by means of standard dns KEY record

Email Verification

- Proposal also specifies how signatures should be verified by MTAs and format for reporting the result of verification. These results are to be reported back by means of either MTAS-VerificationInfo header or signed attribute with same name (preferred if verifying MTA is going to resign the message).
- Additionally mail servers that add MTA signatures and mail senders (based on “From:” header) may provide policy information by means of SPF dns record on level of their support for MTA signatures using new SPF modifies MTAS which can have values "ignore", "test", "verify", "required".
- Based on the result of verification and policies coming from SPF records mail servers are able to make informed decision on if the email should be accepted or not.

Comparison to Goals

- The proposal has design such that any MTA in email path can verify signature of any other previous MTA and that intermediate systems that do not support new extensions do not cause problem if they add/reorder/remove headers or add additional content below existing one (all common changes to mail data during transport are covered).
- All data elements are signed and this is done in a way that would not cause loss of data (hash of content is signed plus headers added as signed attributes plus hash of received headers is added)
- Use of standard PKCS7 format that is well supported by many encryption libraries for use with S/MIME should make implementation easier
- Proposal supports multiple verification methods that use common protocols (dns, http) and allows for new verification methods to be defined in the future. Support for certificates signed by well known certification authorities allows to minimize lookups and offers easy way to support reputation services
- Other syntax is also very extensible as well as main format for signature itself (ASN.1)