Mailing lists and DKIM

Mailing lists and DKIM

DKIM will benefit to internet users if most emails are signed using DKIM. Many of the emails everyone received are coming from LS (List Server), that's why we propose DDX group to experiment DKIM on LS. Naturally, Sympa LS software which is used by internet2 should be the LS used for this. Sympa author's team (CRU) will introduce DKIM technologies into Sympa, but first, we must discuss the way LS should use DKIM and agree on a set of specifications for Sympa LS.

This document is intended to explain the issues and discuss them.

DKIM and MLM general issues

There are various questions about what a LS (list server) should do with DKIM signed messages. A simple answer "keep original message unchanged" may not be a sufficient answer for various reasons :

- One of the initial goal is to be able to check the message origin against white list, black list or reputation services. This requires message origin verification, that's why a signing technology is needed. In the LS case, the LS reputation could be checked, not only the original sender reputation.
- Most of existing LS modify some parts of the distributed messages and alter the original DKIM signature thereby. It is not the goal of the DKIM WG to specify what kind of message modification is unwanted or not. There is an agreement that we don't expect LS implementations to give away message customization ; they are related to features of interest for LS users.

The goal is to specify a clear way for a LS to implement DKIM and tell in which situations a List Server MAY/MUST/SHOULD remove an existing DKIM signature and add its own signature. ietf-dkim mailing list archive can help. There are a lot of discussion about LS, unfortunately there is a poor number of conclusions. One of the threads can introduce you to the question to solve. It's quite old (2006) but still up to date. Stephen Farrell submitted an overview of the discussion that could be read first. Unfortunately this summary covers only half of the discussion, there were lots of comments after it was sent 😒

Simple LS

Sometimes LS do not modify a message before it is distributed, so the initial DKIM signature is preserved. This depends on each LS software but also on the initial message : if the initial signature included SMTP headers fields that were modified by the LS (Return-Path, List-id, etc). Even when it is feasible to preserve the initial DKIM message signature, some says it's better to remove it because spreading the signature may ease the replay attack.

LS modifying messages

Most LS modify messages in some way : summary of modification made by LS
The open issue is : what to do when a message is modified before it is distributed?
It seems there is an agreement that **the original DKIM signature should be removed**.

Should the LS sign the message ? Not sure !

- it may depend on the DKIM Sender Signing Policy (SSP) of the sender : the SSP must be checked before applying a signature at the LS level because the SSP may forbid third party DKIM signature. In such case the message should be rejected (not because the original signature is altered but because the message can't be distributed according to the SSP). Have a look at Hector Santos position.
- but remember the initial goal : *be able to check LS origin against reputation services* .
- there is still an open issue about the semantic of a signature added by a LS. Wietse Venema says *"I am concerned that the FROM: address is becoming a conceptual bottle neck, and would like to see a solution that allows mailing lists and other forwarders to sign mail ("as I forwarded this") without implied claims about the authenticity of the FROM: address. That is, the possibility of a mailing list etc. DKIM signature that just authenticates the list or forwarder."* Other contributors agreed with him, proposing various solutions that do not sign the message itself but just sign a part of it with the semantic that proves which service did forward the message. This seems a good solution for any forwarder **but I could not identify a conclusion**.

Sympa and DKIM

This is a short description of the development planned in Sympa project for DKIM support. Many question are still open and **every point may be discussed with the DDX group**.

I love the following sentence that John Levine published in a post post about mailing lists and DKIM in his blog :

> **"One thing I can definitely promise is that people will have religious beliefs as deep and irrational as the ones they have about Reply-To: headers, so no matter what you do, you can be sure that someone will tell you that you are an idiot for not doing it his way."**

We will focus on :

- How existing DKIM signature can be tested for incoming messages
- Should Sympa sign outgoing services messages (welcome message, etc.)?
- Should Sympa sign messages brodcasted to list subscribers?

Authentication of incoming messages

Sympa apply 3 different authentication levels for incoming messages.

- **signed messages** : applied to message with a valid S/MIME Signature (PGP could also be checked)
- **basic authentication** : applied if an email challenge or a password have been used
- **smtp authentication** : this is not really an authentication, sympa just trusts the "From:" SMTP header field.

Using DKIM in order to trust the From: header field

Sympa could apply *__basic authentication__* if the incoming message includes a valid DKIM signature and :

- *From:* is part of signed headers
- the optional "'i=" tag ((identity of the user or agent on behalf of which this message is signed)) from "'*DKIM-Signature:*" header is present
- *"i=*"tag value match the "From:" including the local part of the address.

the description of "*i=*" tag in RFC 4871 (page 21) includes an informative discussion section that recommends to strictly limit this usage. In addition, we doubt that the optional "*i=*" tag is used many users overall with a local part.

Sympa DKIM signature verification module could add a new variable to its Message object so as to tell if the DKIM signature is present or not, verified success fully or not and says if the signer entity :

- is an authorized third party signer
- matches the sender domain
- matches the sender address including local part

Sympa could use those message properties within its authorization scenario mecanism.

Using DKIM in order to reject unwanted messages

Could Sympa use DKIM signature in order to reject or drop unwanted messages? This depends on the SSP (Sender Signing Policy) information about the domain. As long as SSP is a draft it is difficult to decide what to do with it. Anyhow, if the SSP requires a valid signature for the domain of the sender, Sympa could drop or reject incoming message that do not satisfy it .

Send Sympa service messages

In a virtual host based configuration, Sympa should be able to sign each automatic answer, notification and alarm that are issued by Sympa himself. In such case the configuration should allow to specify :

- if this category of messages must be signed or not
- the "*d=*" tag, default matches the robot name
- the private key file location (no default)
- the selector to be used (no default)
- the "*i=*" optional tag (default none)
- the list of header fields to be signed, with reasonable defaults : From, subject, date, To, Message-Id, In-Reply-to, ...

Broadcast messages to subscribers

3 possibilities :

1. configure each robot to sign all list outgoing messages : Sympa could then be used with or without DKIM activation. This is the very minimum requirement.
2. configure each list to sign all outgoing messages or not : this could be used in order to apply signature for lists where the control of broad casted messages is strict (for example newsletter) and not for lists that are open forums. The signature parameters including private key and selector could be defined list by list. In that solution the configuration parameters will be defined for each list, with a default that can be inherited by the virtual host setup or the global setup
3. Same as solution 2 but in addition, for each message, the "authorization scenario" could be use in order to decide if DKIM signature should be apply or not before broadcasting message. The goal would be to sign messages that have been validated by the list moderator or messages that have been authenticated and not to sign others. This may not be compatible with the SSP for the LS domain.

What ever solution is chosen, the configuration will allow the same level of parameters as for service messages. The recommendation should be to use "*i=li stname-request@robot.domain*" when broadcasting message to subscribers.

Solution 3 seems pretty and should not be too deficult to introduce into Sympa code but is that choice the good one ? It may be a bit complicated for many listmasters. Choice 1 is really simple and provide a great advantage : only one policy for all outgoing message of a LS.