



SPF / DomainKeys / CSV

Tom Kistner
<tom@duncanthrax.net>



The Problem

Consider this real-world analogy:

"Hi, I'm Joe from FedEx. Here's a parcel for you from ACME Inc."

In the current state of SMTP, you have no way of knowing if his name is really Joe, if he's really from FedEx and if anyone has allowed him to deliver parcels. You can't even tell securely that ACME Inc. really exists. All you see is how Joe looks like. Do you trust him?

What is missing



- **Authentication:** In the real world, you can ask Joe for his Company ID to “authenticate” him.
- **Authorization:** Joe’s company ID also confirms that he is allowed to deliver parcels on behalf of FedEx.
- **Accreditation:** You have heard of FedEx, and you know they are in the parcel business.
- **Accountability:** When there is something wrong with the parcel, you can contact someone at FedEx or the original sender.

SPF, DK and CSV



Back to our (imperfect) analogy:

- **SPF** can tell you that Joe is allowed to deliver parcels from ACME Inc. (!?)
- **DomainKeys** can tell you that the parcel really comes from ACME Inc. and that its contents are unmodified. It does not tell you anything about Joe and FedEx.
- **CSV** can tell you that Joe's name is really Joe and that he is indeed an authorized FedEx delivery agent (This is close to Joe’s company ID). It can also tell you about FedEx's reputation.

SPF



- Original Idea: As domains announce receiving servers in DNS (MX), they can do the same for sending servers.
- Uses MAIL FROM as "sender domain" source, with fallback to HELO domain for bounces.
- Domains announce failure policy along with allowed sending hosts.
- SPF offers **Authorization**.

SPF & Forwarding



- The problem: SPF breaks forwarding
 - Forwarding means rewriting envelope recipient addresses on hosts outside of the sender's domain.
 - Forwarding is very common.
- The "fix": SRS
 - Rewrite both sender and recipient.
- The stalemate: Deployment
 - Domains can't securely announce a strict failure policy until SRS is globally deployed.
 - Receivers should not adhere to a strict remote policy until SRS is globally deployed.
 - SRS will never be globally deployed.

SPF in Exim



- Available when compiled with EXPERIMENTAL_SPF (4.5x).
- Requires linking with libspf2.
- Adds “spf” ACL condition.
- Simple example:

```
warn log_message = SPF check failed.  
spf = fail
```

DomainKeys (DK)



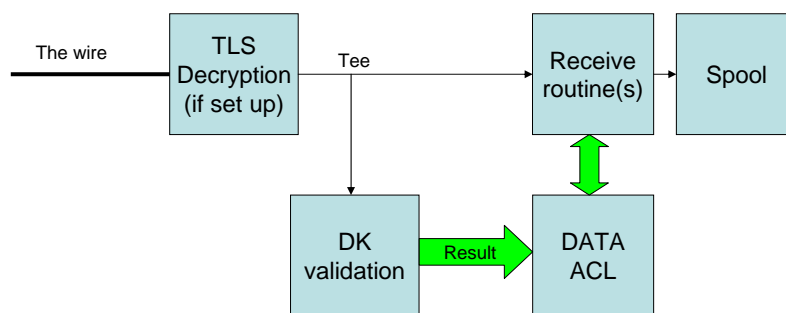
- Each domain has a private/public RSA key pair
 - Same keys can theoretically be used for a bunch of domains.
- Domains publish public key part in DNS.
- Prepends a DomainKey-Signature header to the message.
 - Contains a signed hash (SHA1 signed with RSA) of the message data.
- Uses address headers as "sender domain" source.
 - Does not use any SMTP-related metadata (but processing logic may examine message headers relating to SMTP transactions).
- DK authenticates the message sender, not the calling SMTP client.
- DK offers direct **Accountability**.

DK Problems



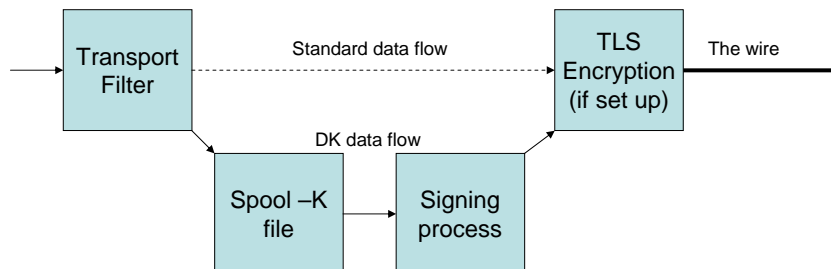
- Complex implementation.
- Resource usage: Processing overhead is large (depends on implementation).
- Message mangling is very common:
 - Adding, removing, rewriting headers ...
 - Adding stupid disclaimer footers.
 - MIME “sanitizing”

Exim DK verification



DK validation runs synchronously with Exim's message reception. The result can be evaluated in the DATA ACL.

Exim DK signing



DK signing requires the complete message to be run through a hashing algorithm. Since Exim's transport filter feature feeds data directly to the SMTP/TLS socket, we must

- Create an intermediate file containing the data that would have been sent.
- Create a signature with that data.
- Send the signature header first, followed by the data.
- If signing fails, send only the original data, or abort if dk_strict is set.

DK Examples



- Check DK validity: In the DATA ACL

```
# Forward DK result to end users
warn message = Domainkey-Status: $dk_status
# Deny bad or unsigned mail from "all-signed" domains
deny message = Bad or no signature from $dk_domain
dk = *:bad,no_signature/signsall
```

- Sign outgoing messages: Add this to your remote_smtp transport

```
dk_selector = feb2005
dk_private_key = /etc/exim/dk/$dk_domain-$dk_selector
dk_canon = nofws
dk_strict = 1
```

CSV: Many new acronyms



- **CSV**: Client Server Validation
- **CSA**: Client SMTP Authentication
 - Source of authorization/authentication
- **DNA**: Domain Name Accreditation
 - Source of accreditation (optional)
- CSV offers **Authentication**, **Authorization** and **Accreditation**. It also offers indirect **Accountability**.

CSV: How it works



- Domains publish authorized SMTP clients in DNS using SRV records [CSA]. They can also publish accreditation services they are listed in using PTR records [DNA].
- Receiving SMTP relays query this information using the domain from the HELO string presented by a caller. [CSA]
- Additionally, accreditation services can be queried to return a recommendation. [DNA]

CSV



- Pro
 - Very low overhead (1-n DNS additional DNS queries per received HELO).
 - Easy implementation.
- Contra
 - Who will run the “top” accreditation services?
 - Can good reputation be bought?
 - Must good reputation be bought?

CSV in Exim



- External implementation was made by David Woodhouse.
- No internal implementation yet. [Tony Finch has announced he'll do at least CSA].

The Final Slide before Dinner



- SPF does not look like a good idea.
- CSV and DK can nicely complement each other.
- Exim will support whatever comes along.