DSAP

DKIM Signature Authorization Protocol

Hector Santos

Santronics Software, Inc.

DSAP Summary

- Security Problem:
  - DKIM-BASE is an unprotected mail authentication and identification protocol.
- DSAP Solution:
  - Provide simple to implement DNS-based robust security wrapper to secure the unprotected DKIM-BASE protocol.
  - Provide consistent protocol support software designs.

DSAP Goal and Objective

- Protects Domain DKIM message signing Practice.
- Protects Domain Reputations.
- Reduces DKIM Verification Overhead.
- Simplifies DKIM Implementation Design considerations.
- Increases DKIM acceptability and lowers Adoptions Barriers

Unprotected DKIM Protocol

- Intentional vague semantics.
- No protection against domain name exploitations.
- No foundation for consistent DKIM verification.
- Increases verification overhead.
- Places high burden on verification receivers.
- Little payoff (low efficiency).
- Hedges future on unknown, yet to be delivered, trusted-layers protocols (Reputation Services).

How Did We Get Here?

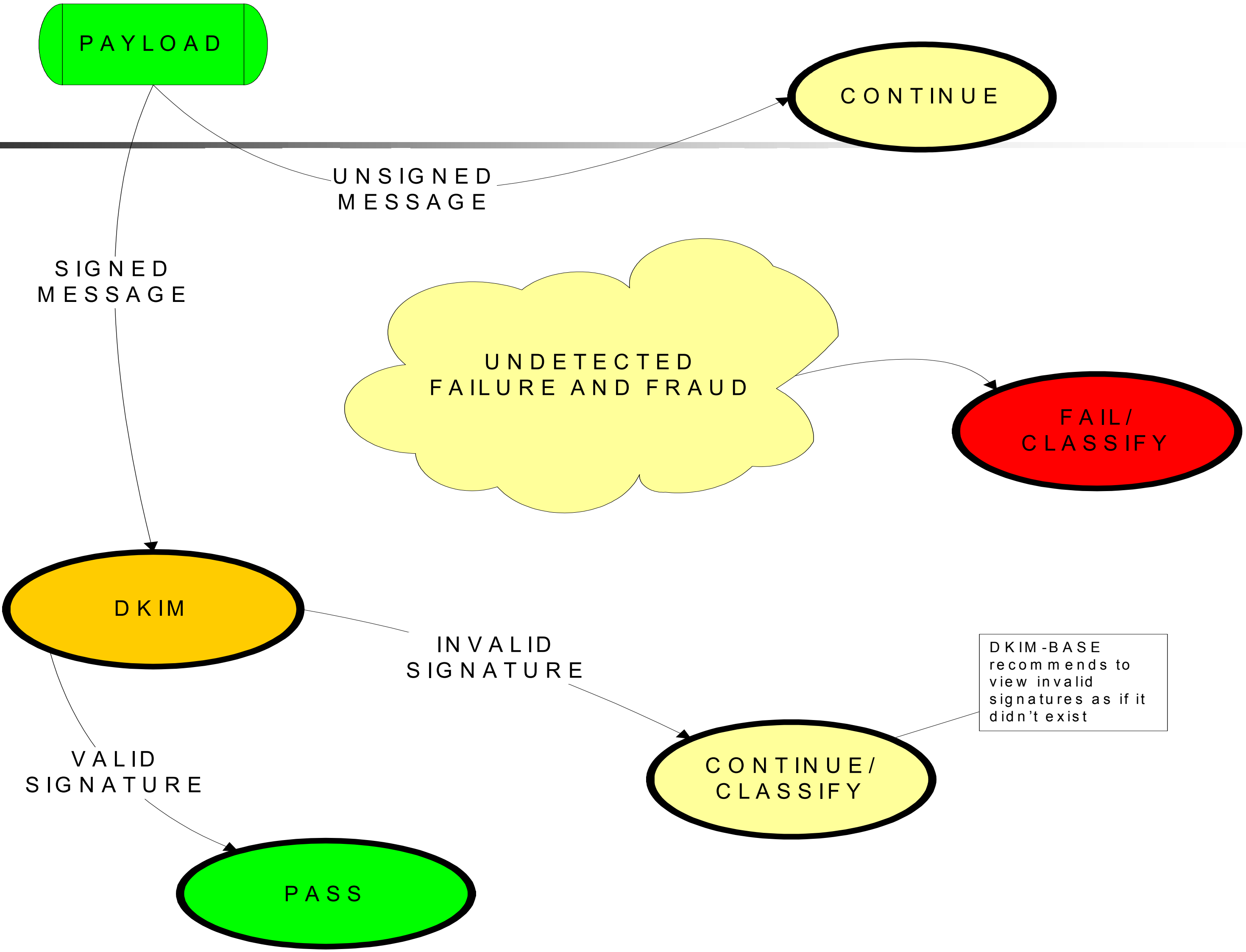
- Original DKIM proof of concept included SSP (Sender Signing Policies).
- Separation of DKIM and SSP protocol.
- Poor SSP functional specifications.
- SSP de-emphasized in lieu of future trusted-layers business ventures.
- Making DKIM-BASE a standalone and unprotected protocol.

Other Non-SSP Considerations:

- Trusted-Layers - Reputation Services
  - No Standard
  - 3rd party Trust Required
  - “Batteries Required” Dilemma
  - Highly isolated solution.
- LMAP Solutions
  - SMTP based
  - Probably will be augmented as part of solution.

Problem?
None offer direct protection for DKIM Signature

DKIM without DSAP



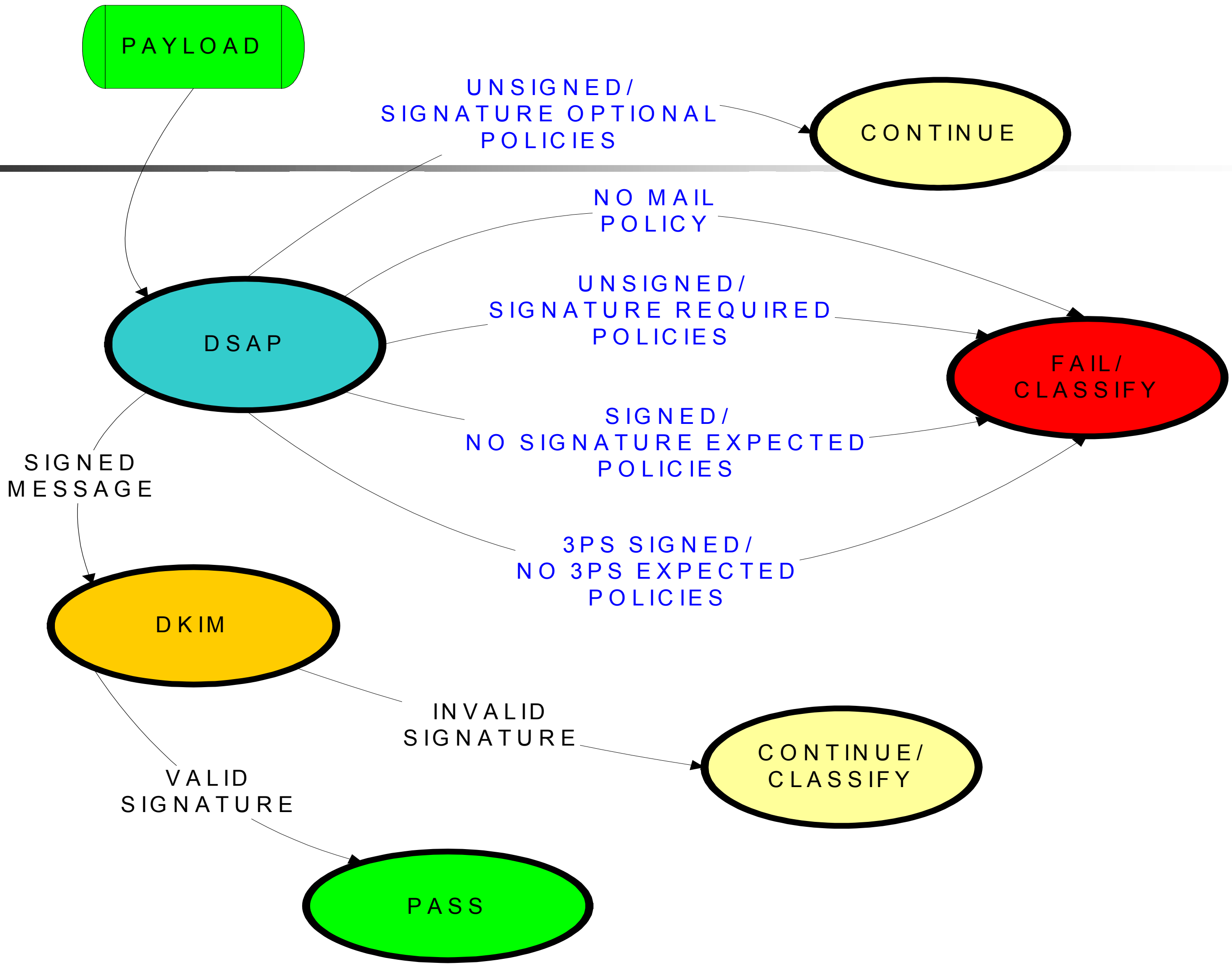
DKIM-BASE recommends to view invalid signatures as if it didn't exist

2006-04-10 (c) copyright 2006 Hector Santos

Fundamental Flaws

- Accept (Pass) Valid DKIM signatures
- Ignore Invalid DKIM signatures
- Void of Highly Detectable Failures

DKIM with DSAP:


PAYLOAD
UNSIGNED/ SIGNATURE OPTIONAL POLICIES
CONTINUE
NO MAIL POLICY
DSAP
UNSIGNED/ SIGNATURE REQUIRED POLICIES
FAIL/ CLASSIFY
SIGNED/ NO SIGNATURE EXPECTED POLICIES
SIGNED MESSAGE
3PS SIGNED/ NO 3PS EXPECTED POLICIES
DKIM
INVALID SIGNATURE
CONTINUE/ CLASSIFY
VALID SIGNATURE
PASS

Detectable Failures Before Hash Verification

DKIM	SIGNING PRACTICE
	NO MAIL EXPECTED
UNSIGNED	EXPECTED
SIGNED	NOT EXPECTED
3rd PARTY SIGNED	NO 3rd PARTY EXPECTED

Non-Detectable Failures

- Altered Message Body Integrity
- Reordering of RFC 2822 headers

Why not use SSP?

- Concerns about additional DNS lookups.
- Incomplete Protection.
- Incorrect DKIM integration.
- Not well understood (because of flaws)
- No consensus (because of flaws).

DNS Interface

- Two DNS records
  - DSAP Policy Record
  - Public DKIM Key Record
- Two Maximum Lookups
  - Policy: _selector._dkim.domain.com
  - Key: _dkim.domain.com
- With DSAP, Policy can short circuit Key lookup minimizing additional lookup concerns.

Current SSP Policies:

SSP Policy	Declaration
NXDOMAIN	No SSP record defaults to NEUTRAL
NOMAIL (0=.)	No Mail Expected
NONE (undefined)	No Signature Expected
WEAK (o=? proposed)	Signature Optional, No 3PS
NEUTRAL (o=~)	Signature Optional, 3PS allowed
STRONG (o=-)	Signature Expected, 3PS allowed
EXCLUSIVE (o=!)	Signature Expected, No 3PS
USER (o=^)	Signature Expected

DSAP - Verifier Viewpoint:

- Original Party Signature (OPS)
  - Not Expected (-)
  - Expected (+)
  - Optional (~)
- 3rd Party Signature (3PS)
  - No Expected (-)
  - Expected (+)
  - Optional (~)

Possible OPS and 3PS Policies

OPS	3PS	SSP (o=)	DSAP (sp=)
NO MAIL		NOMAIL	SP=;
NOT EXPECTED	NOT EXPECTED	NONE	OP-,3P-
NOT EXPECTED	EXPECTED	**UNDEFINED**	OP-,3P+
NOT EXPECTED	OPTIONAL	**UNDEFINED**	OP-,3P~
EXPECTED	NOT EXPECTED	EXCLUSIVE	OP+,3P-
EXPECTED	EXPECTED	**UNDEFINED**	OP+,3P+
EXPECTED	OPTIONAL	STRONG	OP+,3P~
OPTIONAL	NOT EXPECTED	WEAK	OP~,3P-
OPTIONAL	EXPECTED	**UNDEFINED**	OP~,3P+
OPTIONAL	OPTIONAL	NEUTRAL	OP~,3P~

Multiple Signatures:

- Policies allows 3rd Party Signatures (3PS).
  - OP+,3P+
  - OP+,3P~ (SSP, o=STRONG)
  - OP~,3P+
  - OP~,3P+
- Reasons for 3PS (or re-signers).
  - Broken Integrity
  - Vendor Relationships (ISP, EPS, Clearinghouse)
  - Middleware requirements
- Original domains need to decide if multiple signatures are acceptable. If not, declare a 3P- policy.
- Domains with signature requirements but allow middleware changes should declare a strong resigning requirement policy (OP+, 3P~).

Middle Ware & List Servers:

- Identify middle ware design change requirements.
- Problem remains with LS integrity changes.
- Regulate Subscription from Restrictive DSAP Policies.
- Use DSAP policies to determine and honor 1st party versus 3rd party signature requirements.

Recommendation

- Domains should not expose their domain reputation with a DKIM-BASE only implementation.
- Implement DSAP with DKIM-BASE.
- Analyze Domain Usage for proper DSAP policy declarations.

What’s Next?

- Obtain WG feedback,
- Assist Developers with cross platform implementation DSAP models.

Conclusion

In order for DKIM to be well accepted, it needs to offer value to all parties.

DSAP adds a simple to implement security layer around the unprotected core DKIM protocol.

DSAP should be a fundamental natural part of DKIM protocol.

If implemented, DKIM will have less of a negative impact on domain reputations and verifiers, and also makes it easier for developers to add DKIM signing support.

Hector Santos

- hsantos@santronics.com
- http://www.santronics.com
- Wildcat! Interactive Net Server
- Silver Xpress Mail System