DOSETA for Application Security

draft-crocker-doseta-base / -mimeauth

D. Crocker
Brandenburg InternetWorking
bbiw.net
28 March 2011
An Amateur’s View of Security

- Ambiguous terminology (!)

- High barriers to entry

- Admin, ops, HCI usability
  - For example: certificates...

- Variety of functions, e.g., validation of...
  - Actor – author vs. recipient vs. handler
  - Content validity means content is truthful vs. accurate vs. ...?

- Compare language:
  - “XML Signatures provide integrity, message authentication, and/or signer authentication”
  - “DKIM... permit[s] verification of the source and contents of messages”
  - “DKIM permits a person, role, or organization to claim some responsibility for a message”
Perhaps...

- **Re-use core mechanisms**
  - Make a library for common algorithms and packaging, as well as simple key management
  - Easily produce purpose-built security services with related-but-different semantics

- **Permit signatures with nuance, such as**
  - Authorship (Produced message, certifies contents, …)
  - Handling
  - Receipt

- **Minimal development and deployment hassle**
  - The hard work is formulating the semantics
Domain Security Tagging (DOSETA)

- Domainkeys* → DKIM** → DOSETA
  - DNS-based identifiers ⇒ Organizational scope, not individual
- Object-oriented crypto wrapper
  - (SSL is channel-based)
  - Header/content data model
  - Meta-tag (header field) holds key retrieval information
  - Can be invisible to end-user & non-supporting app
- Modicum of transit and handling ~robustness
  - Transform-tolerant canonicalizations
  - Explicitly selective header field coverage
- Self-certifying key service
  - <selector>._domainkey.<domain name> holds public key
  - Selector permits multiple keys per domain name, for admin convenience

* Mark Delany (then of Yahoo!)
** RFC 4871
DOSETA Specification*

- Candidates for data coverage
  - JSON structure, XMPP message, XML object, vCard, vCal, Web page signing, Web ad authentication

- DOSETA authentication template

  **D-Signature association:** how is signature data linked to content and attribute data

  Semantics signaling: how is consumer application to know that semantics apply

  Semantics: the meaning of a signature

  Header/Content mapping: mappings between generic template and a particular service

  * Base (library + authentication template)

  draft-crocker-doseta-base
Exemplar: MIME Authentication*

- Template
  
  D-Signature association: Content-Authentication: field
  
  Semantics signaling: Content-Authentication: signals use
  
  Semantics: [owner of signature domain takes direct responsibility for content]?
  
  Header/content mapping: DOSETA Content to MIME Body; Header to Content-Type: + cited fields

* MIMEAUTH
draft-crocker-doseta-mimeauth (preliminary)
DOSETA/DNSSEC

- DNS “safety” foundation
  - Integration $\Rightarrow$ very strong end-to-end assurance

- Complementary application security and infrastructure protection
  - Separate net service ops from apps ops

- Requires compelling market “pull”
  - Who wants strong data assurance (yesterday)?
  - Financial services, legal, ops reporting, ops data sharing...?

D. Crocker