Data At Rest Encryption
DARE Container / DARE Message

Phillip Hallam-Baker
Comodo Security Solutions
Encrypting log files with OpenPGP*

- Each entry is a separate message
- Big overhead, no return

*S/MIME = OpenPGP + ASN.1
DARE Container

• Designed to support **incremental encryption** & authentication
  • Append only log

• Authentication
  • Digest Chain* or Merkle Tree.
  • Signature on individual records, chain or tree

• Encryption
  • Key exchange can be used for one record or multiple records.
  • Supports encrypted payloads and attributes.

* For my ICO see www.dunningkrugerrand.com
Efficiency

• All write operations are log(n) or better
  • Open container
  • Append record

• Read efficiency depends on container type*
  • First, Last, Previous, Next are O(1).
  • Seek is O(n) for simple container Log(n) for Tree

• Choose JSON or JSON-B (Binary) encoding.
  • Can keep log entry size within O/S atomic write limit.

* If you encrypt a container and lose the key, performance will suffer
Technology

• Based on JSON Web Encryption and JSON Web Signature
  • Some reorganization of tags
  • Same semantics

• Uses binary encoding for frame headers
  • Frames are bidirectional

```
F5  01  2C  <300 Bytes>  2C  01  F5
```
Standard Key Exchange

Public Key Information

Encryption Key

Plaintext

IV

Key Exchange

Recipient Information

Ciphertext

Public Key Identifier

IV
DARE Key Exchange #1

- Public Key Information
- Key Exchange
- Master Key
- Public Key Identifier
- Recipient Information
DARE Key Derivation

Sequence Input

Sequence Output

Master Key

HKDF

Salt

Encryption Key

IV

Plaintext

Ciphertext

http://mathmesh.com/
Applications

• Format for
  • Archiving Web Sites offline
  • Lightweight persistence store
    • Messages / Bookmarks / Credentials / Calendar
  • Encrypting server logs
  • If you are told to ‘do it in blockchain’

• Applied to
  • Protecting PII in server logs to meet GDPR requirements*

* The ‘put a bird on it’ school of GDPR compliance
Next Steps...

• AD Sponsored
  • It is basically a content format

• Form Working Group
  • It has security concerns

• Wait and do with key management
  • But it is logically separate