

# Data At Rest Encryption

DARE Container / DARE Message

Phillip Hallam-Baker

Comodo Security Solutions

# Encrypting log files with OpenPGP\*

RSA / ECDH	<b>Ciphertext</b>
RSA / ECDH	<b>Ciphertext</b>
RSA / ECDH	<b>Ciphertext</b>
RSA / ECDH	<b>Ciphertext</b>
RSA / ECDH	<b>Ciphertext</b>

- 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](http://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

# Applications

- Designed for
  - Persistence stores
    - Messages
    - Bookmarks
    - Contacts
    - Offline Internet distribution to defeat state censorship
- Applied to
  - Protecting PII in server logs to meet GDPR requirements\*

\* The 'put a bird on it' school of GDPR compliance