SDC

STORAGE DEVELOPER CONFERENCE

SNIA ■ SANTA CLARA, 2015

# Mobile and Secure: Cloud Encrypted Objects using CDMI

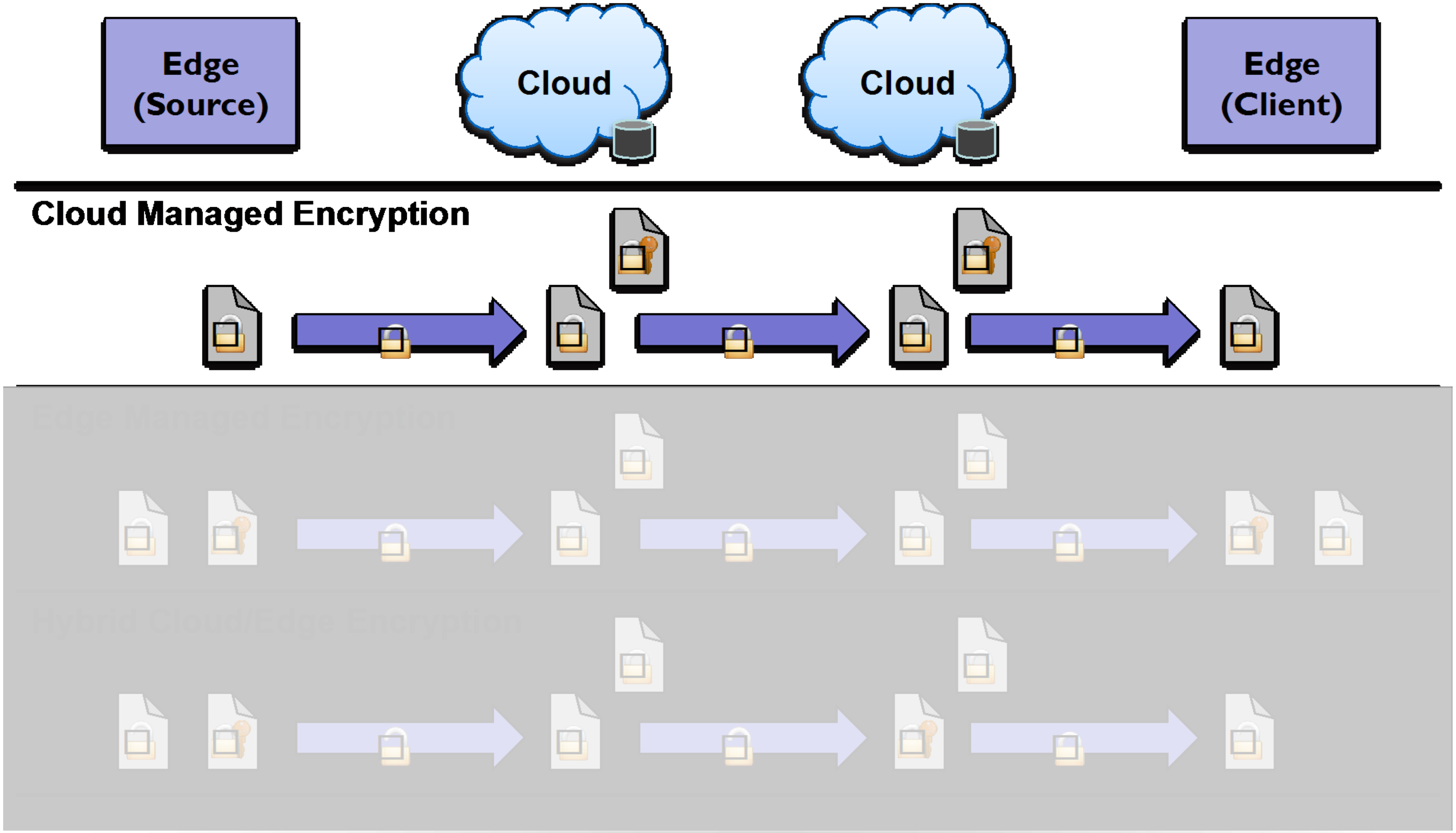
David Slik
NetApp, Inc.

# Data Security in the Cloud

- Organizations (and individuals) are increasingly concerned about storing unencrypted data in the cloud
  - What happens if the cloud provider is compromised?
  - What happens if the cloud account is compromised?
  - What happens if a system that can access the cloud account is compromised?
  - What happens if the cloud provider goes out of business?
- All of these scenarios can result in massive data breaches, which are often undetected due to lack of audit

# Visual Taxonomy

Unencrypted Encrypted Encrypted (have key)

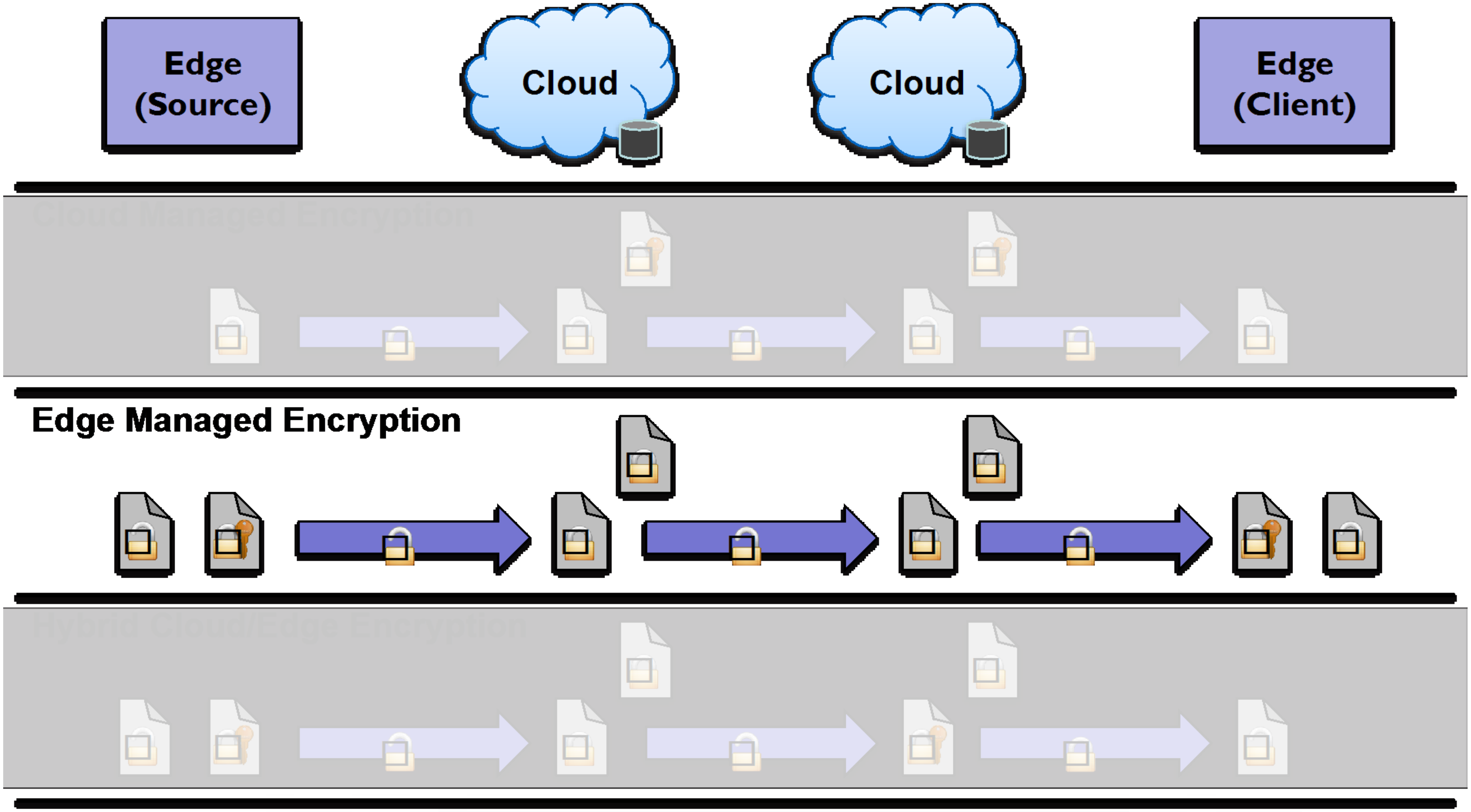


# Cloud-Managed Encryption

- Advantages:
  - Simplest approach
  - Unmodified clients, don’t have to know about keys
- Disadvantages:
  - Cloud provider knows the keys
  - Cloud compromise allows bypass of access controls
  - Cloud compromise allows bypass of audit
  - Inefficient multiple encryption/decryption operations for both in-flight and at-rest

# Visual Taxonomy

Unencrypted Encrypted Encrypted (have key)

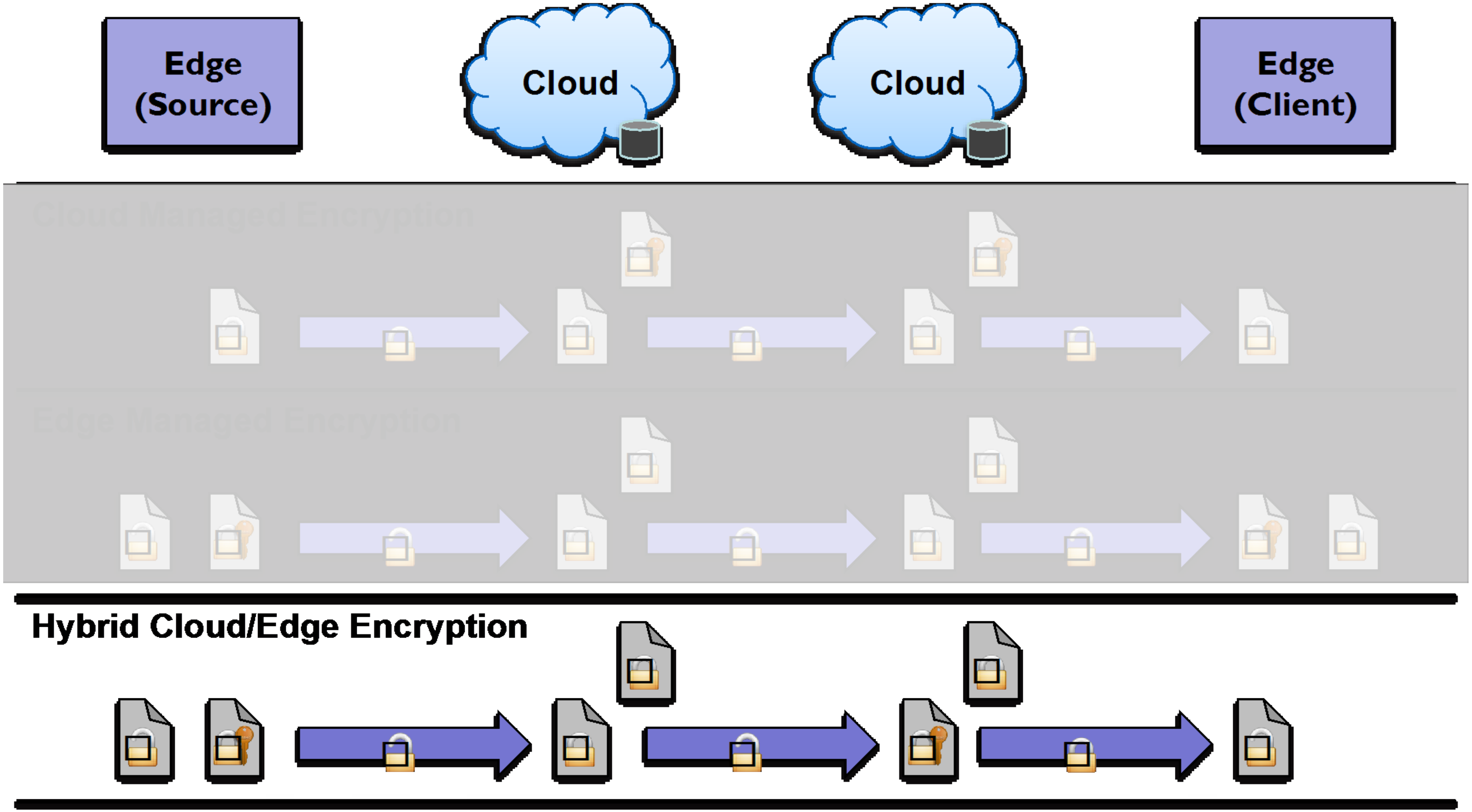


# Edge-Managed Encryption

- Advantages:
  - Keys remain private, cloud provider never sees keys
  - Cloud compromise does not compromise security.
  - Can assume all cloud data is public
  - Most efficient, only encrypt once
  - Audit for all accesses
- Disadvantages:
  - Most complex approach
  - All edge systems accessing the data must be aware of and participate in key management.

# Visual Taxonomy

Unencrypted Encrypted Encrypted (have key)

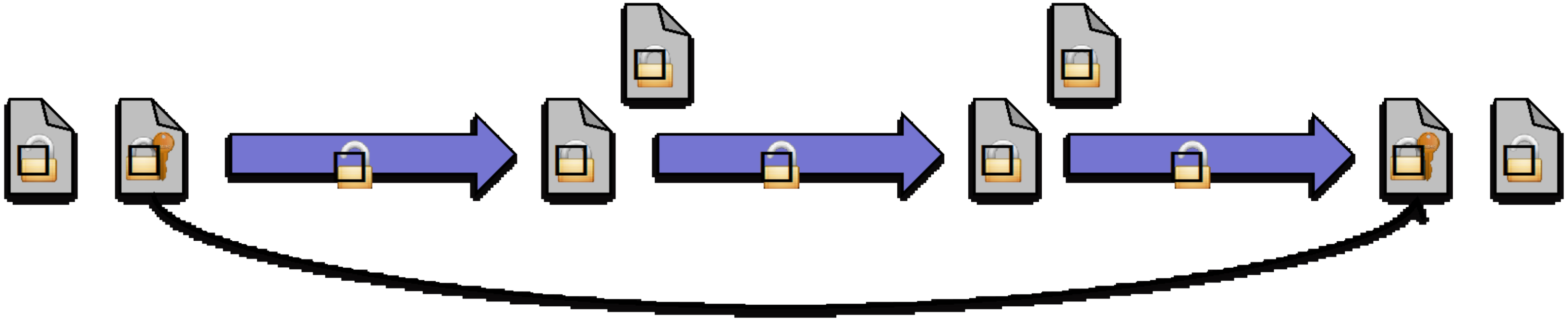


# Hybrid Cloud/Edge Encryption

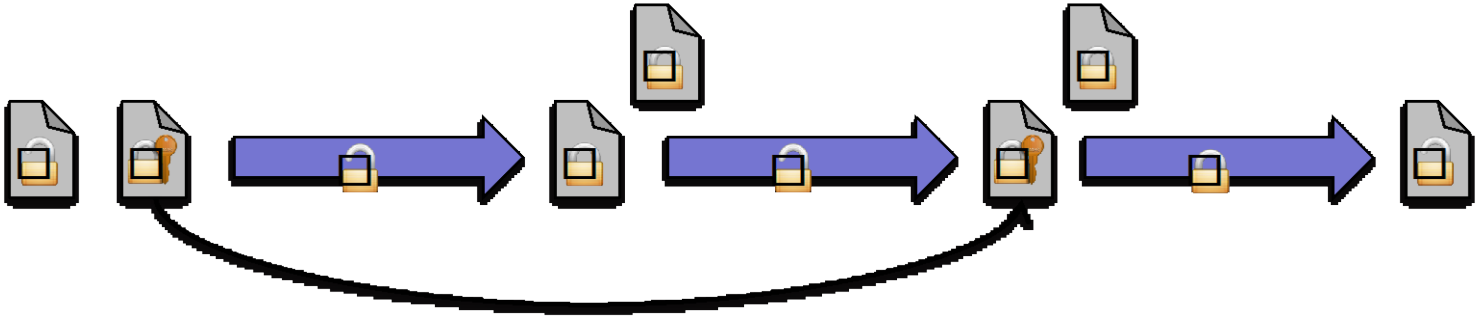
- Advantages:
  - Edge (cloud client) owns and manages the keys
  - Cloud can get access to keys if/when needed
  - Edge can make access control decisions
  - Clients can access plaintext or ciphertext
  - Edge can revoke access
  - Edge can audit all accesses
- Disadvantages:
  - Requires that the cloud software be trusted
  - Needs protocol for cloud/edge key exchange

# Current Gaps in Standards

- How to securely send keys from the Source to the Client



- How to securely send keys from the Source to the Cloud



# What do we need to standardize?

- Actors
  - Data source, including key generation & management
  - Data client, including plaintext, ciphertext and key access
  - Blind cloud (no access to plaintext or keys)
  - Trusted cloud (access to keys and thus, plaintext)
- Threats
  - Network-resident attacker
  - Compromised clouds
  - Compromised data client
  - Compromised data source

# What do we need to standardize?

- For the Data Source
  - How is data encrypted and stored to the cloud in an interoperable way?
    - CMS? JOSE?
    - Goal is to have objects be portable across clouds
    - While this standardization work focuses on CDMI, standard should fit into Azure, S3, Swift and other object protocols
  - How are requests to access keys provided?
  - How is audit requested and reported?

# What do we need to standardize?

- For the Data Client
  - How does a data client retrieve encrypted data from the cloud?
  - How does a data client request and receive a key for encrypted data?
  - How is data client audit requested and managed?

# What do we need to standardize?

- For the Trusted Cloud
  - How does a trusted cloud request and receive a key for encrypted data?
  - How does a trusted cloud provide access to both ciphertext and plaintext?
  - How is trusted cloud audit requested and managed?

# What do we need to standardize?

- Common themes
  - Need an “over the wire” self-describing encrypted object format
  - Need a way to distinguish plaintext vs. ciphertext requests
  - Need a way to securely request a key
  - Need a way to securely receive a key
  - Need a way to securely specify auditable events
  - Need a way to securely report back audit events

# How is this being standardized?

- Encrypted Object CDMI Extension
  - Defines capabilities for server-side encryption and decryption
  - Defines standardized format for encrypted objects
    - Mime-type (or transfer encoding)
    - CMS or JOSE under consideration
    - Encryption of metadata

# How is this being standardized?

- Delegated Access Control CDMI Extension
  - Defines capabilities for Delegated Access Control
  - Metadata to specify Delegated Access Control
    - Originator URL & Certificate
    - Metadata for Key Lookup
  - Plaintext and key access methods
    - Credentials, request message, response message
  - Optional redirection to key-per-request object
  - Key expiry and caching controls
  - Audit requirements

# Example (1/5)

- Client requests ciphertext of encrypted object from cloud
  1. Cloud receives access request for ciphertext
  2. Cloud validates client credentials and ACLs
  3. Cloud sends ciphertext to client

# Example (2/5)

- Client requests ciphertext and key for encrypted object
  1. Cloud receives access request for ciphertext & key
  2. Cloud determines that remote access control required
  3. Cloud creates request, embeds client details
  4. Remote access control provider validates request and client credentials, approves request
  5. Remote access control provider checks out key from KMS
  6. Remote access control provider encrypts key for client
  7. Remote access control provider returns response to cloud
  8. Cloud sends ciphertext and encrypted key to client
  9. Client decrypts client
  10. Client decrypts encrypted object

# Example (3/5)

- Client requests plaintext of an encrypted object from cloud
  1. Cloud receives access request plaintext
  2. Cloud determines that remote access control required
  3. Cloud creates request, embeds client details
  4. Remote access control provider validates request and client credentials, approves request
  5. Remote access control provider checks out key from KMS
  6. Remote access control provider returns response to cloud
  7. Cloud uses key to decrypt content, sends plaintext to client
  8. Cloud purges key
  9. Cloud generates audit message indicating access and key purge

# Example (4/5)

- Client requests ciphertext and key for encrypted object (Key-per-request, with redirect)
  1. Cloud receives access request for ciphertext & key
  2. Cloud determines that remote access control required
  3. Cloud creates request, embeds client details
  4. Remote access control provider validates request and client credentials, approves request
  5. Remote access control provider checks out key from KMS
  6. Remote access control provider creates new encrypted object encrypted with a new request-specific access key
  7. Same process as in example 2, with redirect to newly created object and request-specific access key returned

# Example (5/5)

- ❐ Client requests plaintext of an encrypted object from cloud (Key-per-request, with redirect)
  1. Cloud receives access request for plaintext
  2. Cloud determines that remote access control required
  3. Cloud creates request, embeds client details
  4. Remote access control provider validates request and client credentials, approves request
  5. Remote access control provider checks out key from KMS
  6. Remote access control provider creates new encrypted object encrypted with a new request-specific access key
  7. Same process as in example 3, with redirect to newly created object and request-specific access key returned

# Summing up: Why is this important?

- Allows edge systems to use clouds as untrusted repositories
- Allows trusted edge clouds to federate with untrusted clouds
- Allows clients and clouds be able be abstracted from the remote access control provider
- Allows access control decisions for distributed cloud operations to be locally controlled
- Allows audit for distributed cloud operations to be locally collected

# How to get involved

- Encrypted object and delegated access control CDMI extensions are currently in draft:
  - http://www.snia.org/tech_activities/publicreview/cdmi

- Join the Cloud Storage Technical Work Group
  - Attend weekly TWG call
  - Attend bi-monthly face-to-face work meetings

- Attend plugfests for system and interoperability testing
  - Bi-monthly, and at SDC in room TBA

Thank you!

Questions

dslik@netapp.com