Developing Interoperable Cloud Encryption and Access Control

December 20, 2016
The material contained in this presentation is copyrighted by the SNIA unless otherwise noted.

Member companies and individual members may use this material in presentations and literature under the following conditions:

- Any slide or slides used must be reproduced in their entirety without modification
- The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.

This presentation is a project of the SNIA.

Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.

The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.
Today’s Presenters

Peter van Liesdonk
Philips

David Slik
Co-Chair, SNIA
Cloud TWG
NetApp

Mark Carlson
Chair SNIA
Technical Council
Toshiba
Today’s Presentation Slides Available at: www.snia.org/interoperable_cloud
CDMI: Interoperable Cloud Encryption and Access Control to Secure Healthcare Records

Peter van Liesdonk
Philips Research
November 1, 2016
About Philips Research...

1918 Medical X-ray tube
1919 ‘Ideezet’ radio tube
1926 Pentode
1932 Sodium street lamps
1939 Rotary heads
1963 Compact Cassette
1971 World’s first home VCR
1966 Local oxidation
1976 NiMH battery
1981 Compact Disc

1992 Flat detector for cathlabs
1995 UHP & low Mercury TL/CFL
1996 High resolution MR
2002 Blu-ray
2003 Multi-slice CT
2004 Ambilight TV
2006 3D displays
2008 Lumiramic
2010 Lumea
2010 Fall Detector

2010 LumiMotion
2011 Digital Pathology
2011 iCT Scan
2011 Airfloss
2011 FreeStreet
2012 Hue
2012 BlueTouch Pain Relief
2013 AlluraClarity
Continuum of Care

Healthy living → Prevention → Diagnosis → Treatment → Home care

- hospital PACS systems
- multiple hospital EMR systems
- multiple ambulatory EHR systems
- clinics & doctor offices
- uncaptured vital sign information
- personal device data
HealthSuite Digital Platform

- 3rd party applications
  - Philips applications
  - Open APIs supporting Philips and 3rd party application development
    - Integrated patient and consumer data

Cloud-based HealthSuite Digital Platform

Multiple Philips & 3rd party devices & applications contributing to a rich data set

- Hundreds of thousands of consumers on ActiveLink®
- 15PB+ imaging studies in our imaging informatics solutions across 1200+ hospitals
- 2+ million ICU stays in our eICU solutions
- 190+ million patients a year monitored though our patient monitors
- 6+ million patients supported at home

Illustrative
Problem Statement

Moving medical records to other countries and hospitals using cloud technologies

- Keep access control with owner of data
- Privacy / consent regulations
- Store data in cloud environments
- Sharing of records over administrative borders
Basic Idea

1. Move encrypted record to foreign hospital
2. Call back to data owner for permission, and to obtain decryption keys

*(comparison: Digital Rights Management)*
Goals

- Storage of data in semi-trusted cloud storage
- Interoperability of medical records; backwards compatibility
- Encryption where possible
- Centralized key management / id management
- Support for consent policies
- Auditing and access control performed by data owner
- Possibility for Break-the-glass procedures
Cloud Data Management Interface (CDMI)

Maintained by the Storage Networking Industry Association (SNIA)
Part of Cloud Storage Initiative

CDMI defines RESTful HTTP operations for assessing the capabilities of the cloud storage system, allocating and accessing containers and objects, managing users and groups, implementing access control, attaching metadata, making arbitrary queries, using persistent queues, specifying retention intervals and holds for compliance purposes, using a logging facility, billing, moving data between cloud systems, and exporting data via other protocols such as iSCSI and NFS. Transport security is obtained via TLS.

Compare proprietary protocols:

• S3 (Amazon)
• SWIFT (Openstack)
Work within SNIA Cloud TWG

1. CDMI Encrypted Object Extension

   Makes a cloud object storage server “encryption-aware”

   - Server can do in-place encryption and decryption
   - Alternatively, client can do encryption and/or decryption
   - Key management provided by external Key Management Service
   - Completely transparent and compatible with regular CDMI

2. CDMI Delegated Access Control extension

   Gives control of access decisions back to data owner

   - Can be implemented by either client or server
   - Can be used to deliver cryptographic keys
   - Generic: can be used with any HTTP-based storage protocol
Responsibilities

- **Creation of medical record on hospital computer**
  - Hospital A (responsible)
  - M.D. (person)
  - Hospital client A (CDMI client)

- **Responsible for cloud storage of encrypted records**
  - Cloud A (France)
  - EHR France
  - EHR service A cdmi.ehr-a.fr (object storage)
  - Remote hospital client B (CDMI client)
  - Requestor M.D. (person)
  - Hospital controller A cdmi.hos-a.fr (CDMI server)

- **Responsible for local replication of encrypted records (optional)**
  - Cloud B (U.S.A.)
  - EHR U.S.
  - EHR service B cdmi.ehr-b.us (object storage)
  - Remote hospital controller B cdmi.hos-b.us (CDMI server)
  - Requestor M.D. (person)

- **Responsible for policy enforcement and auditing**
  - Hospital B (requesting)
  - Remote hospital client B (CDMI client)
  - Remote hospital controller B cdmi.hos-b.us (CDMI server)
  - Requestor M.D. (person)

- **Stateless gateway responsible for encryption/decryption**
  - Cloud A (France)
  - EHR France
  - Stateless gateway
  - Cloud B (U.S.A.)
  - EHR U.S.
  - Stateless gateway

- **Sign a consent**
  - Hospital B (requesting)
  - Remote hospital client B (CDMI client)
  - Remote hospital controller B cdmi.hos-b.us (CDMI server)
  - Requestor M.D. (person)

- **Digitalization of patient consent**
  - Hospital B (requesting)
  - Remote hospital client B (CDMI client)

- **Secure place to store cryptographic keys (optional)**
  - Key Vault
  - Key Management kmip.kms.com (KMIP server)

- **Secure place to store cryptographic keys (optional)**
  - Key Vault
  - Key Management kmip.kms.com (KMIP server)
**Creation/storage of consent profile**

1. **Sign a consent**
   - Patient (person)
   - Digitalize consent profile in XACML policy
   - Hospital controller cdm.hos-a.fr (CDMI server)

2. **Upload consent profile (HTTP PUT)**
   - Hospital client A (CDMI client)
   - EHR service A cdmi.ehr-a.fr (object storage)

3. **Upload consent profile (HTTP PUT)**
   - Key Management kmip.kms.com (KMIP server)
   - Key storage

4. **In-place encryption**
   - EHR France
   - Hospital controller cdm.hos-a.fr (CDMI server)

5. **Key storage**
   - EHR service A cdmi.ehr-a.fr (object storage)

6. **Storage of encrypted consent profile**
   - Cloud A
   - Cloud B (U.S.A.)

7. **Forget consent profile & keys**
   - Hospital controller A cdm.hos-a.fr (CDMI server)
   - Identity Management idm.hos-a.fr (IDM server)

**Hospital A (responsible)**
- M.D. (person)
- Hospital client A (CDMI client)
- Remote hospital client B (CDMI client)

**Hospital B (requesting)**
- Requestor M.D. (person)
- Remote hospital controller B (CDMI client)
- Key Vault
- CDMI
- IHE-IUA / OAuth
- KMIP
- User interaction
Creation/storage of medical record

(can be asynchronous to consent profile)

1. Create a medical record on hospital PC
2. Upload medical record (HTTP PUT)
3. In-place encryption
4. Key storage
5. Storage of encrypted medical record
6. Forget medical record & keys
Local request of medical record

1. Request a medical record on hospital PC
2. Attempt to download medical record (HTTP GET)
3. Download encrypted consent profile & encrypted medical record
4. Decrypt consent profile
5. Submit consent profile to IDM
6. Make access control decision + audit trail
7. Obtain record decryption key from key vault
8. In-place decryption of medical record
9. Response with medical record
10. Clear caches
Remote access of medical record

1. Federate encrypted medical record
2. Request a medical record on hospital PC
3. Attempt to download medical record (HTTP GET)
4. Download encrypted medical record From EHR
5. Parse DAC information, Incl. certificate for Hospital A
6. Send DAC request incl. authorization claims (in secure tunnel)
7. Download and decryption of consent profile
8. Submit claims + consent profile to IDM
9. Make access control decision (auto/manual), decide license, + audit
10. Obtain record decryption key from key vault
11. Send DAC response incl. access control decision, object decryption key and usage license (in secure tunnel)
12. In-place decryption
13. Response with medical record
14. Forget all

Hospital A (responsible)
Hospital B (requesting)
Cloud A (France)
Cloud B (U.S.A.)

EHR France
EHR service A
cdmi.ehr-a.fr (object storage)

EHR U.S.
EHR service B
cdmi.ehr-b.us (object storage)

Remote hospital client B
(CDMI client)
Remote hospital controller B
(CDMI server)

Hospital controller A
cdmi.hos-a.fr (CDMI server)

Key Management
kmip.kms.com (KMIP server)

Identity Management
idm.hos-a.fr

Hospital Administration
(CDMI client)

M.D. (person)
Patient (person)

CDMI-IHE-IUA / OAuth
KMIP
User interaction

102x72
Encryption technology

Encryption is built on top of state-of-the-art JSON Object Signing and Encryption

• **Object Encryption**
  – Authenticated content encryption via AES-GCM
  – Either symmetric or asymmetric key-wrapping
    (AESKW, RSA-OAEP, or ECDH-ES)

• **Object Authentication**
  – Message Authentication code (HMAC), or
  – Digital signatures (RSA or ECDSA)

• **Delegated Access Control**
  – Provides negotiated encrypted tunnel using the above primitives
  – Mutual authentication via X.509 certificates

Alternative mode: compatibility with e.g. CMS or IHE-DEN
References

- Cloud Data Management Interface website
- CDMI Specification v1.1.1
- Whitepaper: towards a CDMI healthcare profile
- Draft CDMI Extensions
  - Delegated Access Control Extension v1.1f
  - Encrypted Object Extension v1.1f

- JSON Object Signing and Encryption (JOSE)
  - JSON Web Signature (RFC 7515)
  - JSON Web Encryption (RFC 7516)
  - JSON Web Algorithms (RFC 7518)
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDMI</td>
<td>Cloud Data Management Interface (specification)</td>
</tr>
<tr>
<td>CMS</td>
<td>Cryptographic Message Syntax (specification)</td>
</tr>
<tr>
<td>DAC</td>
<td>Delegated Access Control</td>
</tr>
<tr>
<td>EHR</td>
<td>Electronic Health Record</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol (specification)</td>
</tr>
<tr>
<td>IDM</td>
<td>Identity Management</td>
</tr>
<tr>
<td>IHE</td>
<td>IHE – Integrating the Healthcare Enterprise (organization)</td>
</tr>
<tr>
<td>IHE-DEN</td>
<td>IHE Data Encryption (specification)</td>
</tr>
<tr>
<td>IHE-IUA</td>
<td>IHE User Internet Authentication (specification)</td>
</tr>
<tr>
<td>JOSE</td>
<td>JSON Object Signing and Encryption (specification)</td>
</tr>
<tr>
<td>JSON</td>
<td>JavaScript Object Notation (specification)</td>
</tr>
<tr>
<td>KMIP</td>
<td>Key Management Interoperability Protocol (specification)</td>
</tr>
<tr>
<td>OAuth</td>
<td>Open standard for authorization (specification)</td>
</tr>
<tr>
<td>SNIA</td>
<td>Storage Networking Industry Association (organization)</td>
</tr>
<tr>
<td>XACML</td>
<td>Extensible Access Control Mark-up Language (specification)</td>
</tr>
</tbody>
</table>
Using Cloud Encryption, Signing and Delegated Access Control

David Slik, Technical Director
Capacity Storage

NetApp, Inc.
Encryption and Delegated Access Control

- What if you want to use the cloud, but don’t trust the cloud?
  - Here’s what needs to be standardized in order to enable security and interoperability:

  - **Encryption - Protection against unauthorized disclosure**
    - Format: CMS (Cryptographic Message Syntax) & JWE (JSON Web Encryption)
    - Key Management (KMIP)

  - **Signatures - Protection against unauthorized alteration**
    - Format: CMS (Cryptographic Message Syntax) & JWS (JSON Web Signatures)

- **Delegated Access Control - Protects against unauthorized access**
  - The focus of this standardization effort
  - Provides an interoperable message exchange for access control & key disclosure
  - Works with CDMI & other cloud storage protocols
Encryption, Signing and Delegated Access Control

Scenario 1 – Completely Untrusted Cloud

Step 1
Object Encryption, Signing and Key Registration

Modified Cloud Client

Regis ter

Encrypted & Signed Object

Key Server
Encryption, Signing and Delegated Access Control

Scenario 1 – Completely Untrusted Cloud

Step 2
Store to Cloud

Modified Cloud Client

Key Server

Untrusted Cloud Provider

Encrypted & Signed Object

Standard HTTPS PUT

Administrative Boundary
Encryption, Signing and Delegated Access Control

Scenario 1 – Completely Untrusted Cloud

Step 3
Retrieve from Cloud

Modified Cloud Client

Untrusted Cloud Provider

Encrypted & Signed Object

HTTPS GET

Modified Cloud Client

Encrypted & Signed Object

Administrative Boundary

Administrative Boundary

Key Server
Encryption, Signing and Delegated Access Control

Scenario 1 – Completely Untrusted Cloud

Step 4
Request Access

Modified Cloud Client

Key Server

Access Control Provider

Untrusted Cloud Provider

Administrative Boundary

Administrative Boundary

Modified Cloud Client

Encrypted & Signed Object

Delegated Access Control Request
Client Credentials
Encryption, Signing and Delegated Access Control

Scenario 1 – Completely Untrusted Cloud

Step 5
Access Control Decision

Modified Cloud Client

Key Server

Key Retrieval

Access Control Provider

Untrusted Cloud Provider

Encrypted & Signed Object

Modified Cloud Client

Administrative Boundary

© 2015 NetApp, Inc. All rights reserved. NetApp Confidential – Limited Use
Encryption, Signing and Delegated Access Control

Scenario 1 – Completely Untrusted Cloud

Step 6
Access Granted
Encryption, Signing and Delegated Access Control

Scenario 1 – Completely Untrusted Cloud

Scenario 1 Demonstration
Encryption, Signing and Delegated Access Control

Scenario 2 – Trusted Edge Cloud for Access

Step 1
Object Encryption, Signing and Key Registration
Encryption, Signing and Delegated Access Control

Scenario 2 – Trusted Edge Cloud for Access

Step 2
Store to Cloud

Modified Cloud Client

Standard HTTPS
PUT

Untrusted Cloud Provider

Encrypted & Signed Object

Key Server

© 2015 NetApp, Inc. All rights reserved. NetApp Confidential – Limited Use
Encryption, Signing and Delegated Access Control

Scenario 2 – Trusted Edge Cloud for Access

Step 3
Federate to Edge Cloud

Modified Cloud Client

Key Server

Untrusted Cloud Provider

Encrypted & Signed Object

Trusted Edge Cloud

Encrypted & Signed Object

Administrative Boundary
Encryption, Signing and Delegated Access Control

Scenario 2 – Trusted Edge Cloud for Access

Step 4
Retrieve from Cloud

Modified Cloud Client

Key Server

Untrusted Cloud Provider

Encrypted & Signed Object

Trusted Edge Cloud

Unmodified Cloud Client

© 2015 NetApp, Inc. All rights reserved. NetApp Confidential – Limited Use
Encryption, Signing and Delegated Access Control

Scenario 2 – Trusted Edge Cloud for Access

Step 5
Request Access

1. Key Server
2. Access Control Provider
3. Untrusted Cloud Provider
4. Trusted Edge Cloud
5. Encrypted & Signed Object
6. Delegated Access Control Request
7. Client + Edge Cloud Credentials
8. Modified Cloud Client

© 2015 NetApp, Inc. All rights reserved. NetApp Confidential – Limited Use
Encryption, Signing and Delegated Access Control

Scenario 2 – Trusted Edge Cloud for Access

Step 6
Access Control Decision

- Key Server
  - Key Retrieval
- Access Control Provider
- Modified Cloud Client
  - Key Retrieval
- Untrusted Cloud Provider
  - Encrypted & Signed Object
- Trusted Edge Cloud
  - Modified Cloud Client
- Administrative Boundary
  - Unmodified Cloud Client
Encryption, Signing and Delegated Access Control

Scenario 2 – Trusted Edge Cloud for Access

Step 7
Request Access

Modified Cloud Client

Key Server

Access Control Provider

Untrusted Cloud Provider

Trusted Edge Cloud

Unmodified Cloud Client

Delegated Access Control

Response

Decryption Key

Administrative Boundary

Administrative Boundary

Encrypted & Signed Object

Decrypted & Verified Object
Encryption, Signing and Delegated Access Control

Scenario 2 – Trusted Edge Cloud for Access

Step 8
Data Delivered

- **Modified Cloud Client**
- **Untrusted Cloud Provider**
- **Access Control Provider**
- **Key Server**
- **Trusted Edge Cloud**

Data Delivery Flow:
1. Key Server encrypts data and signs it.
2. Data is delivered to the Trusted Edge Cloud.
3. Data is decrypted and verified.
4. Unmodified Cloud Client receives the data.

Key Points:
- Data is encrypted and signed before delivery.
- Data is decrypted and verified upon receipt.
- The Trusted Edge Cloud acts as a secure gateway.

© 2015 NetApp, Inc. All rights reserved. NetApp Confidential – Limited Use
Encryption, Signing and Delegated Access Control

Scenario 2 – Trusted Edge Cloud

Scenario 2 Demonstration
Encryption, Signing and Delegated Access Control

Scenario 3 – Trusted Edge Cloud for Encryption

Step 1
Object Store

Unmodified Cloud Client

Standard HTTPS PUT

Trusted Edge Cloud

Object Unencrypted

Key Server
Step 2
Create and Register Key
Encryption, Signing and Delegated Access Control

Scenario 3 – Trusted Edge Cloud for Encryption

Step 3
Encrypt Object
Server side

Unmodified Cloud Client

Unencrypted Object

Trusted Edge Cloud

Key Server

Standard HTTPS PUT
Encryption, Signing and Delegated Access Control

Scenario 3 – Trusted Edge Cloud for Encryption

Step 4
DAC Request/Response to obtain key

Unmodified Cloud Client

Trusted Edge Cloud

Unencrypted Object

Key Server

Access Control Provider

Standard HTTPS PUT

DAC Response
Scenario 3 – Trusted Edge Cloud for Encryption

Step 5
Encrypt Object
Server side

Unmodified Cloud Client

Unencrypted Object

Encrypted & Signed Object

Access Control Provider

Key Server

Standard HTTPS PUT

Trusted Edge Cloud

🔒 Encrypted & Signed Object

🔑 Access Control Provider
Encryption, Signing and Delegated Access Control

Scenario 3 – Trusted Edge Cloud for Encryption

Step 6
Federate to Cloud

Unmodified Cloud Client

Trusted Edge Cloud

Access Control Provider

Key Server

Encrypted & Signed Object

Untrusted Cloud Provider

Administrative Boundary

Standard HTTPS PUT
Encryption, Signing and Delegated Access Control

Scenario 3 – Trusted Edge Cloud for Encryption

Access

Same as Scenario 1
(Modified client)
Steps 3 through 6

or

Same as Scenario 2
(Unmodified client)
Steps 3 through 8
Encryption, Signing and Delegated Access Control

Scenario 3 – Trusted Edge Cloud for Encryption

Scenario 3 Demonstration
Encryption and Delegated Access Control

- Questions and Discussion

- Links to resources
  - CDMI Encrypted Object Extension
  - CDMI Delegated Access Control Extension

http://www.snia.org/tech_activities/publicreview/cdmi

- CDMI Reference Implementation

https://github.com/SNIA/CDMI
After This Webcast

- This Webcast and a copy of the slides will be on the SNIA Cloud Storage website and available on-demand
  - [http://www.snia.org/forum/csi/knowledge/webcasts](http://www.snia.org/forum/csi/knowledge/webcasts)
- A PDF of these slides at [www.snia.org/interoperable_cloud](http://www.snia.org/interoperable_cloud)
- A Q&A from this webcast, including answers to questions we couldn't get to today, will be on the SNIACloud blog
- Follow us on Twitter @SNIACloud, @macsun