SNIA CSTI | CLOUD STORAGE TECHNOLOGIES

Cloud Data Management & Interoperability: Why a CDMI Standard Matters

Live Webcast

December 9, 2020

10:00 am PT

Today's Presenters

Alex McDonald
Moderator
Independent Consultant
Chair SNIA CSTI

Mark Carlson
Co-chair SNIA Technical Council
Principal Engineer, Industry Standards
Kioxia

Eric Hibbard
CISSP-ISSAP, ISSMP, ISSEP, CIPT, CISA, CCSK
Chair, SNIA Security Technical Working Group

SNIA Legal Notice

- 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.

SNIA-At-A-Glance

185
industry leading organizations

2,000
active contributing members

50,000
IT end users & storage pros worldwide

SNIA CSTI | CLOUD STORAGE TECHNOLOGIES

What We Do

Educate vendors and users on cloud storage, data services and orchestration

Support & promote business models and architectures: OpenStack, Software Defined Storage, Kubernetes, Object Storage

Understand Hyperscaler requirements Incorporate them into standards and programs

Collaborate with other industry associations

Agenda

- Announcing CDMI™ 2.0
- New features of the latest release
- Advantage of an Open Source specification
- New Security Features

Cloud Data Management Interface

- Cloud object storage protocol, ISO/IEC 17826:2016
- Maintained by the Storage Networking Industry Association (SNIA)
- Part of Cloud Storage Technologies 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.

A Brief Overview of CDMI

- CDMI (Cloud Data Management Interface) is a RESTful API for accessing and managing cloud storage.
- The major cloud storage object APIs are:
  - Amazon AWS: **S3 API**
  - SNIA: **CDMI API**
  - Microsoft Azure: **Storage Blob API**
  - OpenStack: **Swift API**
  - Google Cloud: **Cloud Storage API**
- CDMI is widely implemented
  - >30 server implementations
  - CDMI gateways, OpenStack support

A Brief Overview of CDMI

- **2009:** SNIA Cloud Storage Technical Working Group founded to explore API standardization
- **2011:** CDMI 1.0 ratified as a US Technical Architecture
  - CDMI 1.0.1 errata released in late 2011
  - CDMI 1.0.2 errata released in mid 2012
- **2012:** CDMI 1.0.2 becomes ISO/IEC 17826:2012
- **2013:** CDMI 1.1 under active development
  - 18 Extensions submitted
- **2016:** CDMI 1.1.1 Becomes ISO/IEC 17826:2016
    - 13 Extensions submitted, 5 incorporated
- **2017:** CDMI 2.0 under active development
- **2020:** CDMI 2.0 ratified by SNIA
    - 1 Extension submitted, 9 incorporated, 5 updated

A Brief Overview of CDMI

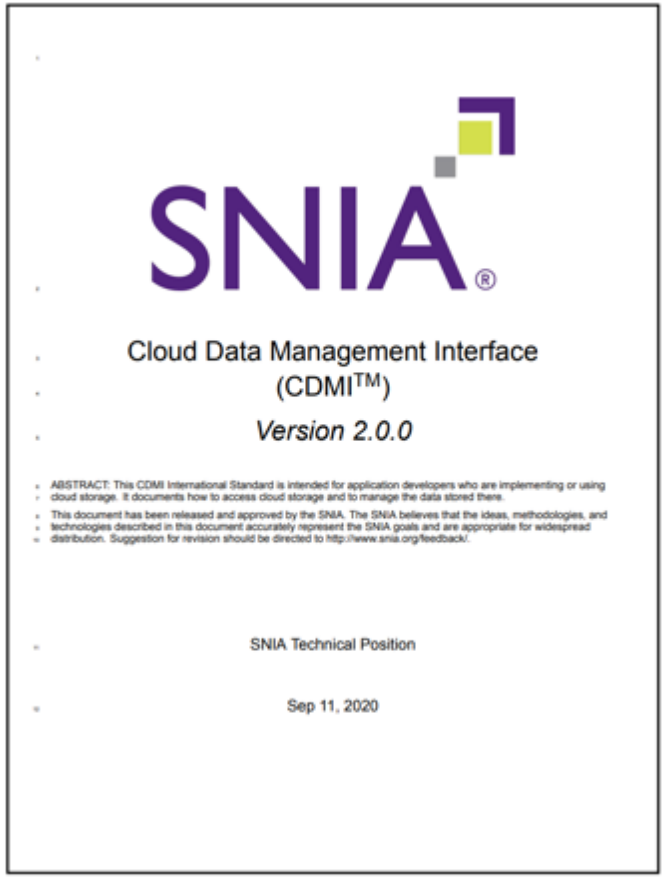
- Why Does CDMI Matter?
  - Simple and easy to implement
    - Start with HTTP and add functionality, few mandatory parts
  - Advanced functionality not found in other APIs
    - Provides a foundation for next generation cloud services, such as federation
  - Open industry standard
    - Not controlled by any one vendor, protection against patents
  - Well defined formal standard
    - Enables interoperability, testing, and cross-vendor support
  - Widespread government support and adoption

A Brief Overview of CDMI

- CDMI 2.0 Standardizes:
  - Representations of Namespaces
  - CRUD operations (Create/Read/Update/Delete)
  - Data, Container, Queue and Domain objects
  - Security, Identity and access control model
  - Metadata (including client and vendor extensibility)
  - Data and metadata portability
  - Serialization and Notifications
  - Query and Notifications
  - Versioning
  - Management of file, block and object protocols

A Brief Overview of CDMI

- The CDMI standard can be downloaded from SNIA's web site:
  - http://www.snia.org/cdmi
- Extensions are defined to extend CDMI
  - http://www.snia.org/tech_activities/publicreview/cdmi
- We will be referring to the CDMI specification for the remainder of this session
- Download CDMI 2.0 Standard here:
  - https://www.snia.org/sites/default/files/technical_work/CDMI/CDMI_v2.0.0.pdf


SNIA

Cloud Data Management Interface
(CDMI™)

Version 2.0.0

ABSTRACT: This CDMI International Standard is intended for application developers who are implementing or using cloud storage. It documents how to access cloud storage and to manage the data stored there.

This document has been released and approved by the SNIA. The SNIA believes that the ideas, methodologies, and technologies described in this document accurately represent the SNIA goals and are appropriate for widespread distribution. Suggestion for revision should be directed to http://www.snia.org/feedback/.

SNIA Technical Position

Sep 11, 2020

Extensions in CDMI 2.0

- Incorporated into main text
  - Delegated Access Control
  - Encrypted Objects
  - Versioning
  - JSON Transfer Encoding
- Added to Annex A:
  - Summary Metadata for Bandwidth
  - Expiring Access Control Entries
  - Group Storage System Metadata
  - Header Based Metadata Extension
  - Immediate Query Extension

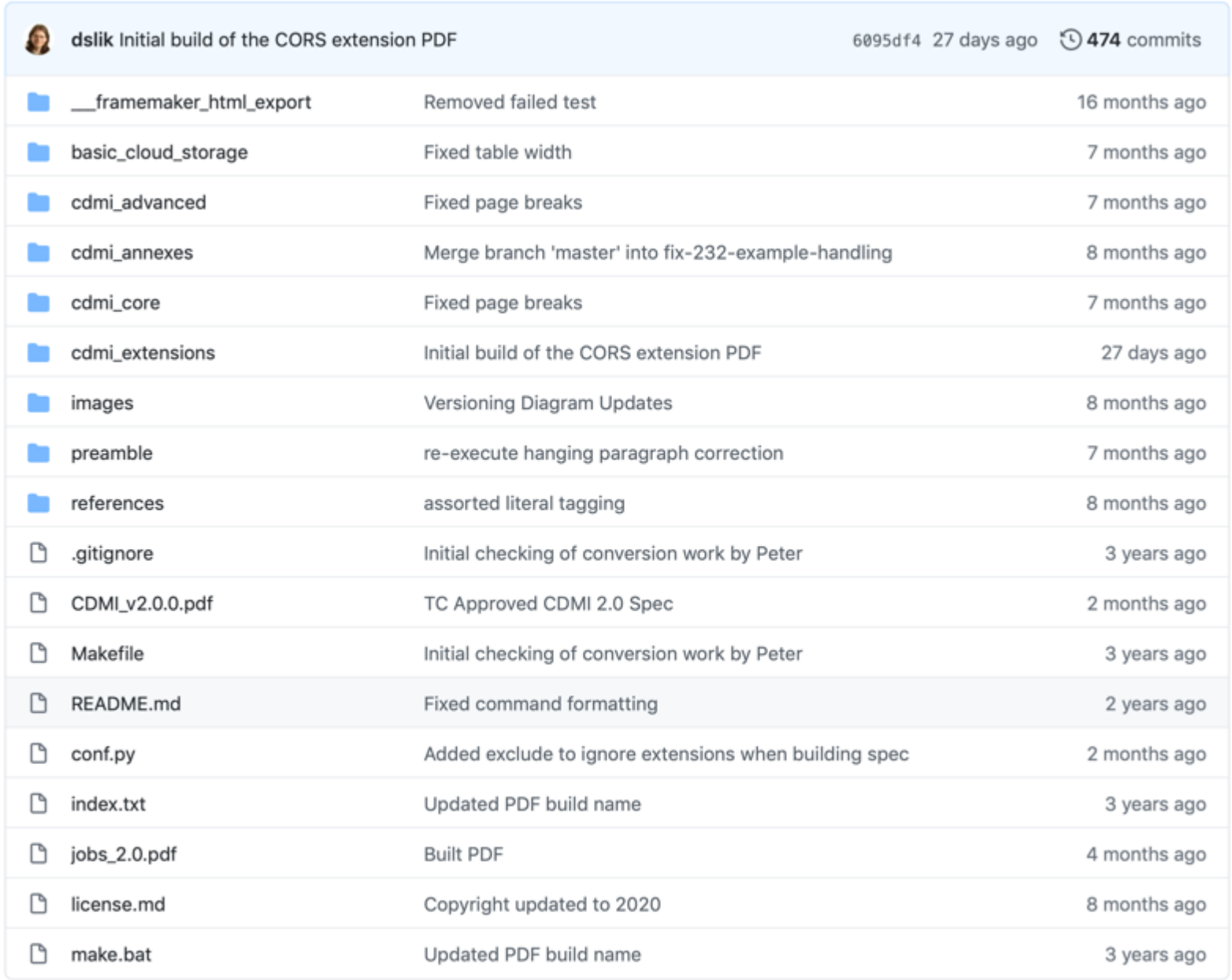
Updated Extensions

- Data Affinity Extension
- Jobs Extension
- Capabilities Selection Extension
- Cross Origin Resource Sharing Extension
- Partial Upload Extension

CDMI 2.0 Specification is Open Source

- Github repository:
  - https://github.com/SNIA/CDMI-spec
- Built on an Open Source Tool Chain
  - Sphinx based https://www.sphinx-doc.org/en/master/
- Allows multiple developers to work in parallel rather than locking a common document
  - All the power of Github!
- Contributions/Issues can easily be submitted by non-SNIA members!

- Github Repository
- Specification is a series of txt files built into a .pdf file by the tool chain
- Readme details how to install the tool chain for your system
- Pull requests can be made as a contributor and approved by the TWG



dslik Initial build of the CORS extension PDF	`6095df4` 27 days ago	**474** commits
__framemaker_html_export	Removed failed test	16 months ago
basic_cloud_storage	Fixed table width	7 months ago
cdmi_advanced	Fixed page breaks	7 months ago
cdmi_annexes	Merge branch 'master' into fix-232-example-handling	8 months ago
cdmi_core	Fixed page breaks	7 months ago
cdmi_extensions	Initial build of the CORS extension PDF	27 days ago
images	Versioning Diagram Updates	8 months ago
preamble	re-execute hanging paragraph correction	7 months ago
references	assorted literal tagging	8 months ago
.gitignore	Initial checking of conversion work by Peter	3 years ago
CDMI_v2.0.0.pdf	TC Approved CDMI 2.0 Spec	2 months ago
Makefile	Initial checking of conversion work by Peter	3 years ago
README.md	Fixed command formatting	2 years ago
conf.py	Added exclude to ignore extensions when building spec	2 months ago
index.txt	Updated PDF build name	3 years ago
jobs_2.0.pdf	Built PDF	4 months ago
license.md	Copyright updated to 2020	8 months ago
make.bat	Updated PDF build name	3 years ago

cdmi_access_control.txt	re-execute hanging paragraph correction	7 months ago
cdmi_advanced_toc.txt	Added versioning section	2 years ago
cdmi_capability_object.txt	Fixed page breaks	7 months ago
cdmi_delegated_access_control.txt	Fixed literal typeface	7 months ago
cdmi_domain_object.txt	Fixed page breaks	7 months ago
cdmi_encrypted_objects.txt	re-execute hanging paragraph correction	7 months ago
cdmi_exports.txt	Fixed word wrap	7 months ago
cdmi_metadata.txt	Fixed word wrap	7 months ago
cdmi_notifications.txt	Fixed literal typeface	7 months ago
cdmi_query_queues.txt	final chunk of table reviews	8 months ago
cdmi_queue_object.txt	Fixed page breaks	7 months ago
cdmi_results.txt	Fixed indentation	7 months ago
cdmi_retention.txt	Merge branch 'master' into fix-232-example-handling	8 months ago
cdmi_scope.txt	Example indentation	7 months ago
cdmi_serialization.txt	re-execute hanging paragraph correction	7 months ago
cdmi_snapshots.txt	re-execute hanging paragraph correction	7 months ago
cdmi_versioning.txt	Fixed literal typeface	7 months ago

SNIA CDMI & Security

CDMI Security Summary

- Required elements
  - Implementation of TLS
  - Security capability queries
- Optional elements
  - Authentication and Access Control
  - Data Integrity/Authenticity
  - Cryptographic Support
  - Deletion and Sanitization
  - Retention, Immutability, and Holds

Interoperable Data Security Goals

- Storage of data in semi-trusted cloud storage
- Storage of data with mixed security requirements in the same Namespace
- Support for needs of highly regulated data types (e.g. medical records)
- Encryption where possible
- Centralized and Federated key management / ID management
- Auditing and access control performed by data owner
- Possibility for Break-the-glass procedures

SNIA Transport Layer Security (TLS) Specification for Storage Systems (ISO/IEC 20648)

- TLS-specific requirements for CDMI, SNIA Swordfish, & SMI-S
- https://www.snia.org/tech_activities/standards/curr_standards/tls

- Version 2.0 Public Review Draft
  - Mandates TLS 1.2 and permits TLS 1.3; deprecates TLS 1.0 and 1.1
  - Mandates certain cipher suites; recommends others
  - Changes to validation
  - PSK versus self-signed certificates
  - https://www.snia.org/tech_activities/publicreview

New CDMI Security

- 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)

New CDMI Security (cont.)

- 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

Key Security Technology

Encryption is built on top of 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

SNIA CDMI as a Use Case to Explore Cloud Security

Mobile and Secure Healthcare

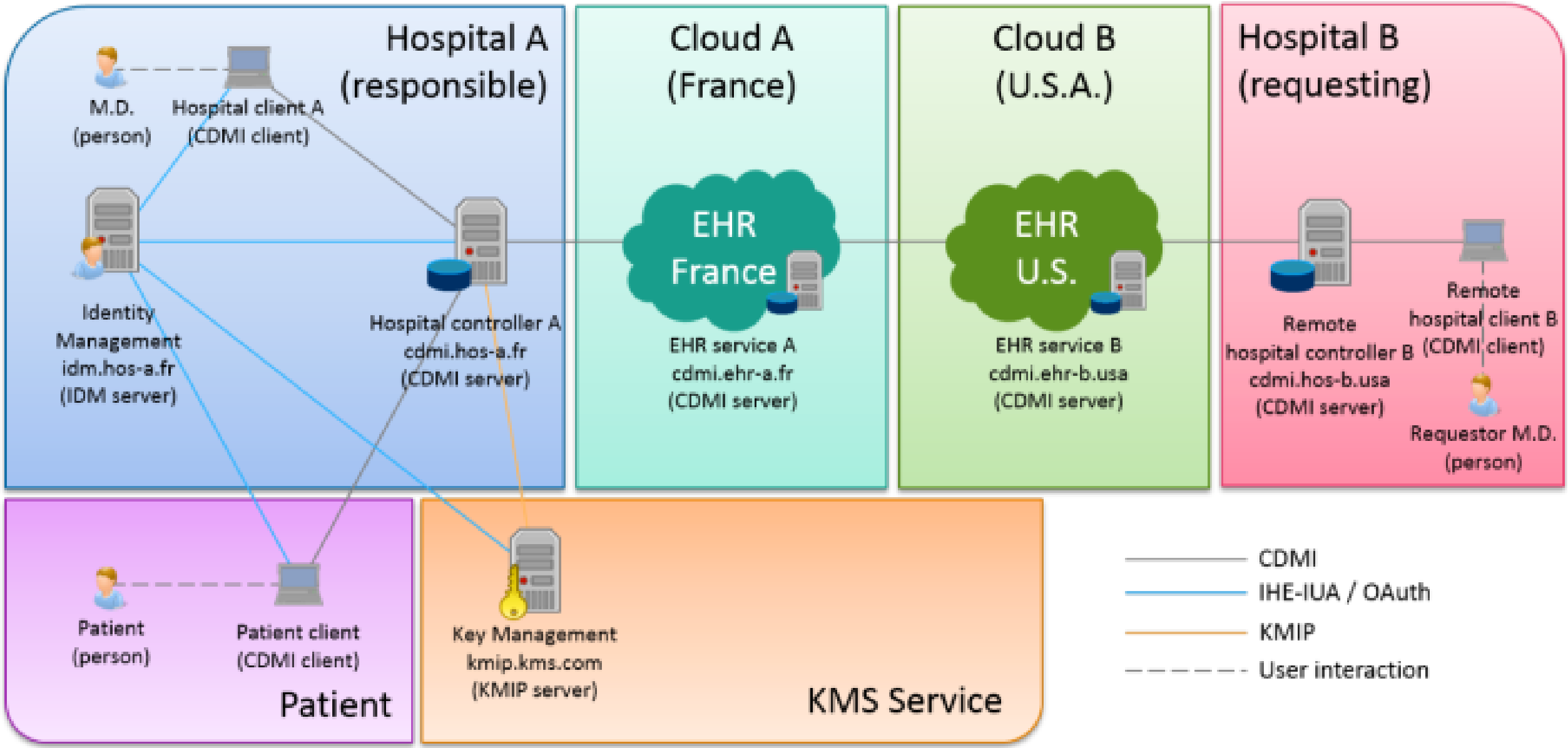
https://www.brighttalk.com/webcast/663/185821

Use Case Summary

- A French citizen with a pre-existing condition must seek treatment at a Denver hospital while on travel in the US
- The patient's hospital (A) uses Cloud A
- The treating hospital in Denver (B) uses Cloud B
- The M.D. in Denver requests access to the patient's existing EHR
- Assumptions:
  - A contractual agreement exists between the EHR services of the US and France
  - The health data is divided into at least two parts: medical record & administrative
  - The patient consent (profile) has been handled

Data Protection Requirements

- The platform and infrastructure used for the storage, retrieval and processing of data should be well protected from cyber-attacks (Cybersecurity).
- Content of data should be kept hidden except for authorized users (Data Confidentiality).
- Data should be protected against any unauthorized modifications (Data Integrity).
- Data protection mechanisms should not be enforced by one party only (Separation of duties).
- Every party involved in data management should be uniquely identified (Authentication).
- Every party requesting access to the data should be authorized according to applicable policies (Authorization).
- The privacy of the patient should be protected using enforcement of patient consent profile (Privacy Preserving).
- All the transactions to request the data should be securely logged, so they can be audited if necessary (Accountability).



CDMI Role in Use Case

- CDMI used as a back-end for distributing health information between different locations
- End-to-end security of the health information is provided by two new extensions to the CDMI:
  - The *Encrypted Object Extension* allows exchange of encrypted health information, with options for in-place encryption and decryption; it will be used to allow storage of health information in cloud environments.
  - The *Delegated Access Control Extension* allows delegation of access decisions to other parties; it will allow us to control what health information can be requested from other hospitals.
- Note: There are dependencies on other technologies including KMIP for key management, BPPC and HL7/FHIR for defining access policies, IHE-IUA for authentication, and IHE-DEN for actual encryption of content.

Summary

- Update of ISO/IEC 17826 is underway
- Get involved with CDMI development. SNIA membership is not required.
- Consider implementing CDMI for multi-cloud
- CDMI Reference Implementation update to match CDMI 2.0

After This Webcast

- Please rate this webcast and provide us with feedback
- This webcast and a copy of the slides will be available at the SNIA Educational Library https://www.snia.org/educational-library
- A Q&A from this webcast will be posted to the SNIA Cloud blog: www.sniacloud.com/
- Follow us on Twitter @SNIACloud

References

- Mobile and Secure Healthcare: Encrypted Objects and Access Control Delegation
- Developing Interoperable Cloud Encryption and Access Control (mp4 file, slides)
- Cloud Data Management Interface website
- CDMI Specification v.20
- Whitepaper: towards a CDMI healthcare profile
- JSON Object Signing and Encryption
  - JSON Web Signature (RFC 7515)
  - JSON Web Encryption (RFC 7516)
  - JSON Web Algorithms (RFC 7518)

Thank you!

Q & A

