SNIA CSI | CLOUD STORAGE

The State of Cloud Security

Mark Carlson, Toshiba
Eric Hibbard, Hitachi Data Systems

July 20, 2017

SNIA Legal Notice

SNIA CSI | CLOUD STORAGE

- 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

Mark Carlson
Toshiba

Eric Hibbard
Hitachi Data Systems

About the Presenters

SNIA CSI | CLOUD STORAGE

- Mark Carlson
  - Principal Engineer, Industry Standards at Toshiba
  - Chairman, SNIA Technical Council
  - Co-Chairman, SNA Cloud Storage TWG
  - Co-Chairman, SNIA Object Drive TWG
  - Co-Author, SNIA CDMI Specification
  - ISO Co-Editor, ISO/IEC 17826
- Eric Hibbard, CISSP, CISA, CCSP
  - HDS CTO Security & Privacy
  - Co-Chairman, SNA Security TWG
  - Co-Chairman, Cloud Security Alliance International Standardization Council
  - Vice Chairman, American Bar Association Cloud Committee
  - ISO Editor, ISO/IEC 17788:2014, ISO/IEC 27040:2015, ISO/IEC 20648:2016, ISO/IEC 22123
  - Chairman Elect, INCITS TC CS1 Cyber Security
  - Chairman, IEEE Cybersecurity & Privacy Standards Committee

SNIA CSI | CLOUD STORAGE

SNIA-at-a-Glance

160
unique member companies

2,500
active contributing members

50,000
IT end users & storage pros worldwide

Agenda

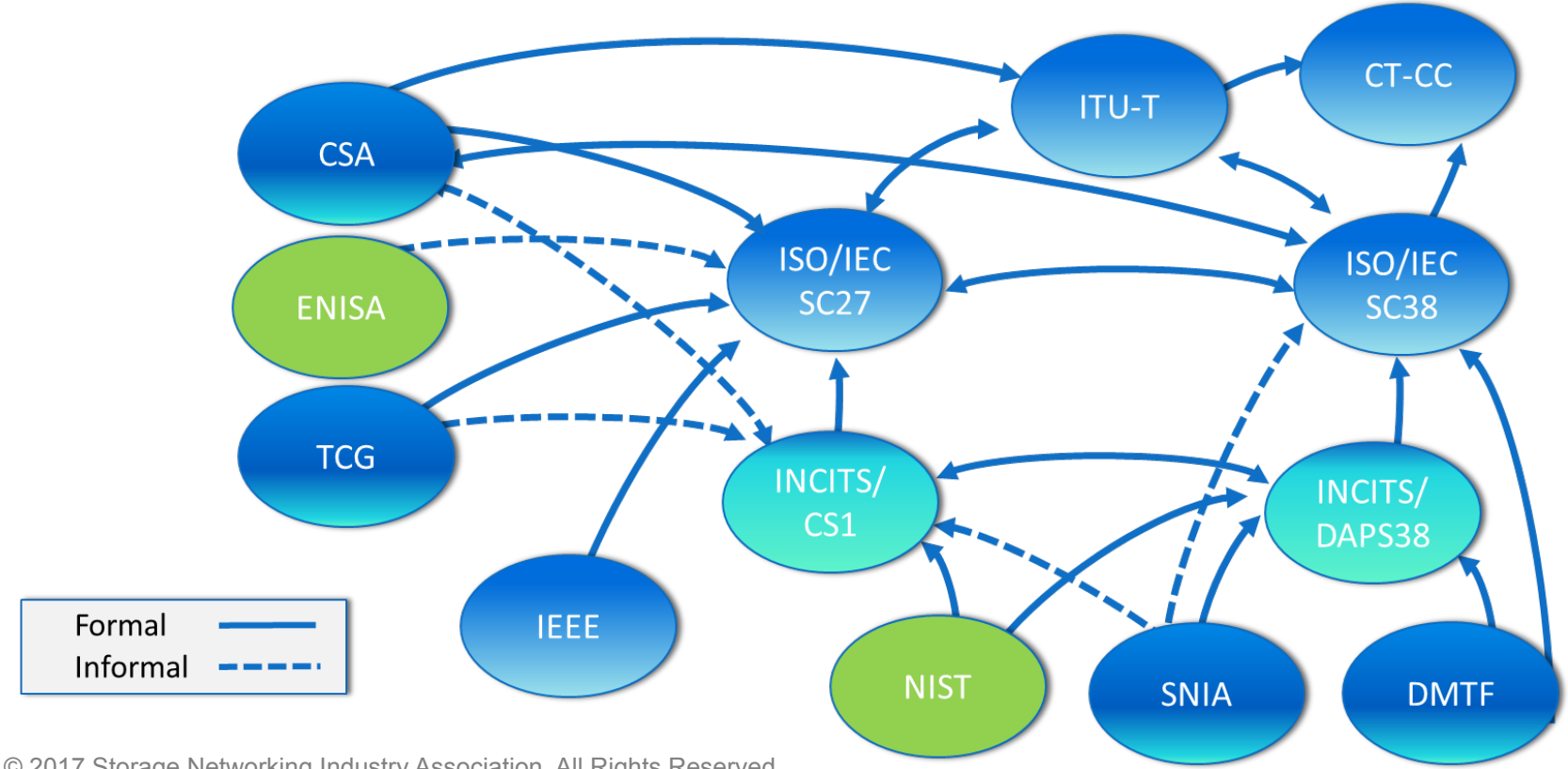
SNIA CSI | CLOUD STORAGE

Topics covered will include:

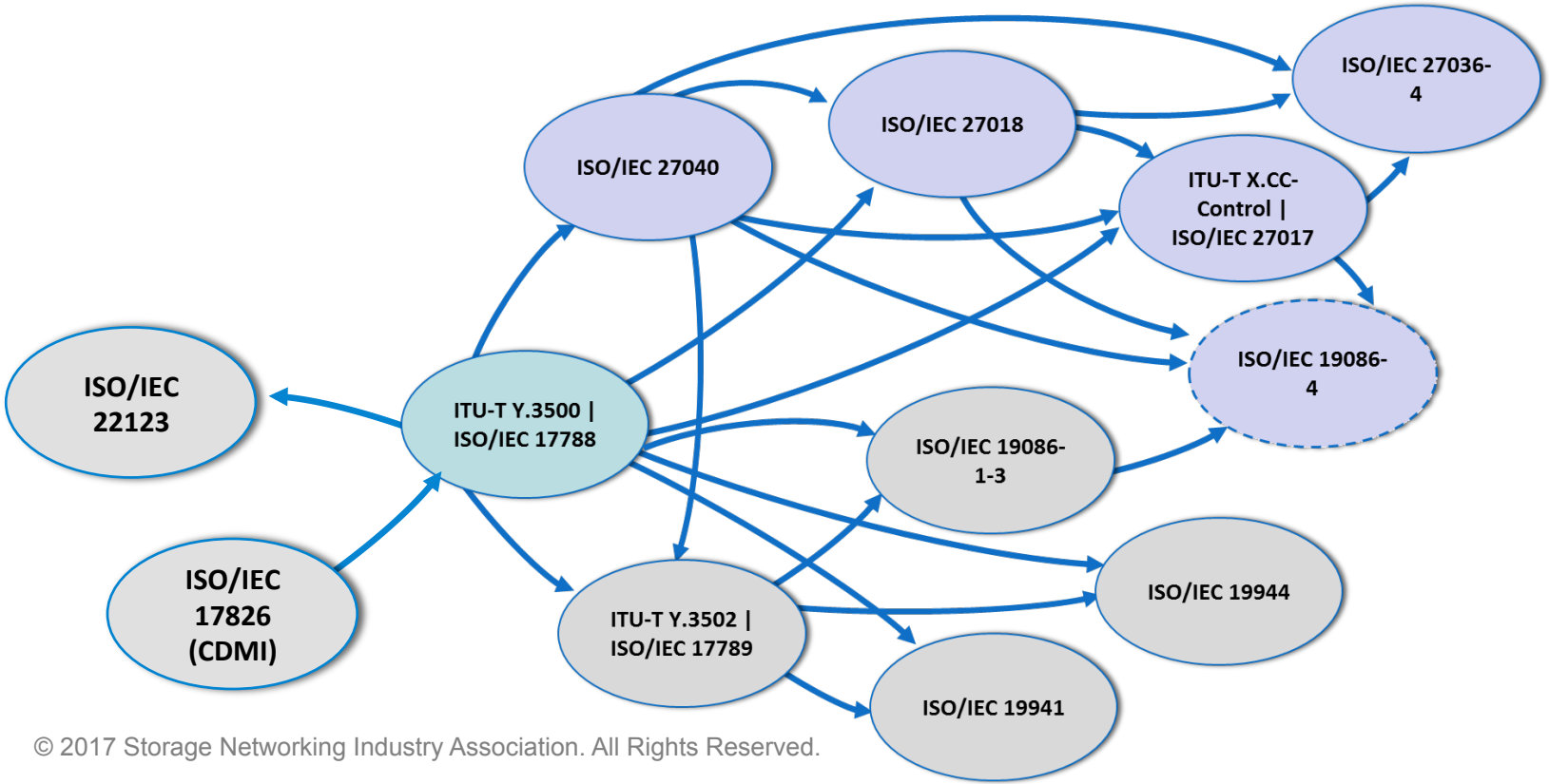
- Summary of the standards developing organization (SDO) activities;
  - Work on cloud concepts, CDMI, an SLA framework, and cloud security & privacy
- Securing the Cloud Supply Chain;
  - Outsourcing and cloud security; Cloud Certifications (FedRAMP, CSA STAR)
- Emerging & Related Technologies;
  - Virtualization/Containers, Federation, Big Data/Analytics in the Cloud, IoT and the Cloud

Summary of the standards developing organization (SDO) activities

Sample Cloud SDOs



Key ISO Cloud Standards



Other Players

SNIA CSI | CLOUD STORAGE

- Internet Engineering Task Force (IETF)
- NIST
- Storage Networking Industry Association (SNIA)
- OASIS
- Trusted Computing Group (TCG)
- Cloud Security Alliance (CSA)
- The Open Group
- Distributed Management Task Force (DMTF)

SNIA CSI | CLOUD STORAGE

SNIA CDMI as a Use Case to Explore Cloud Security

Cloud Data Management Interface

Cloud object storage protocol, ISO/IEC 17826:2016

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)

Interoperable Data Security Goals

SNIA CSI | CLOUD STORAGE

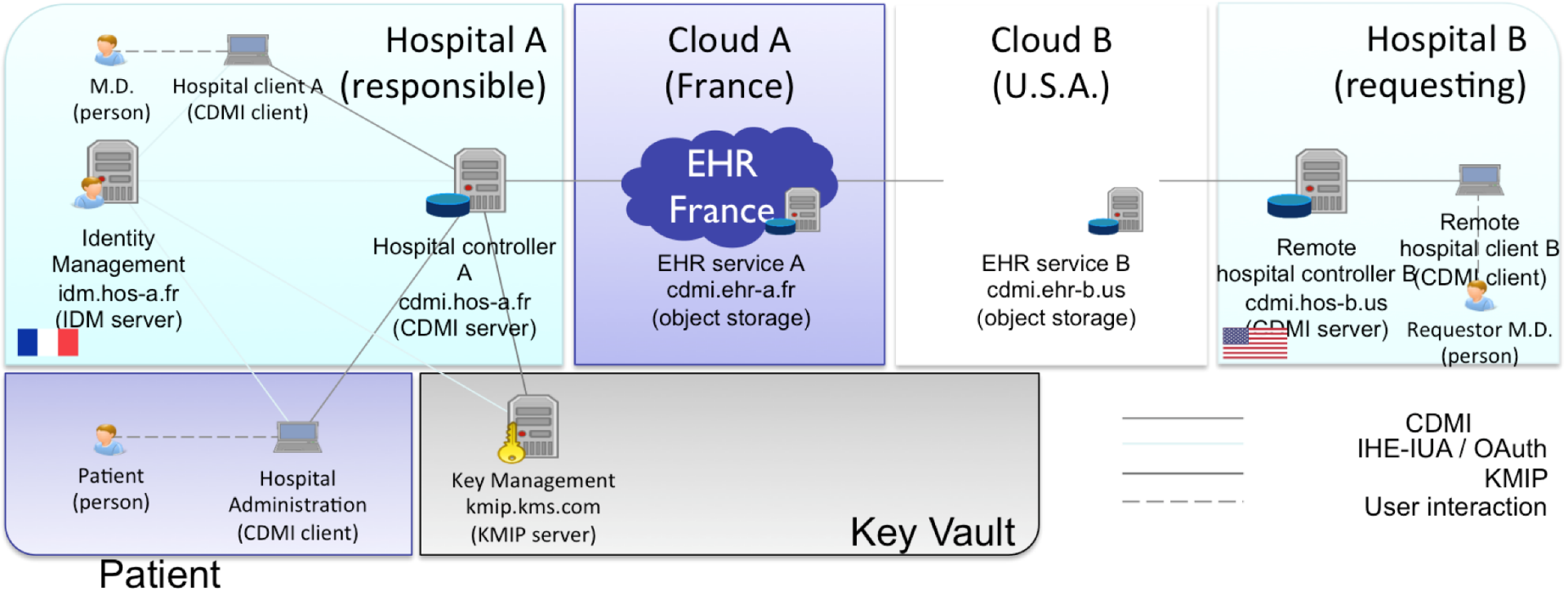
- Storage of data in semi-trusted cloud storage
- Interoperability of medical records; backwards compatibility
- Encryption where possible
- Centralized key management / id management
- Support for consent policies
- Auditing and access control performed by data owner
- Possibility for Break-the-glass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

Work within SNIA Cloud TWG

SNIA CSI | CLOUD STORAGE

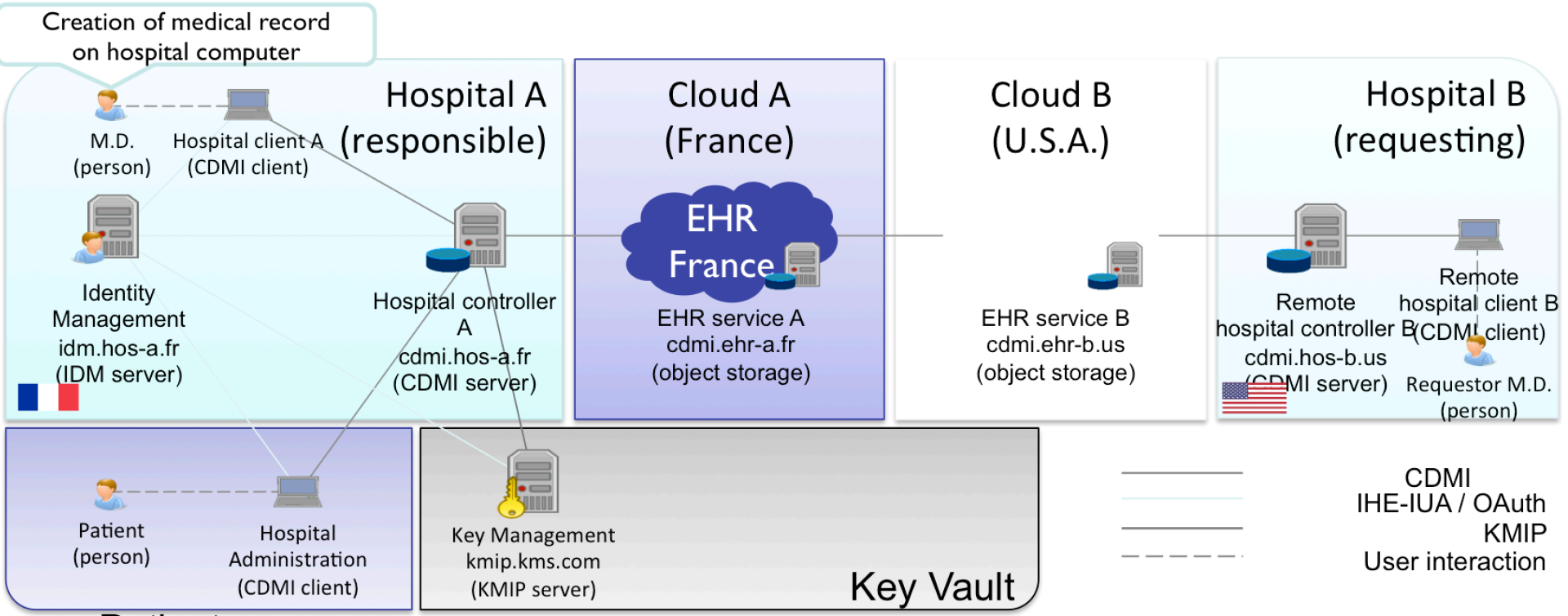
1. **CDMI Encrypted Object Extension**
   Makes a cloud object storage server "*encryption-aware*"
   - Server can do in-place encryption and decryption
   - Alternatively, client can do encryption and/or decryption
   - Key management provided by external Key Management Service
   - Completely transparent 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

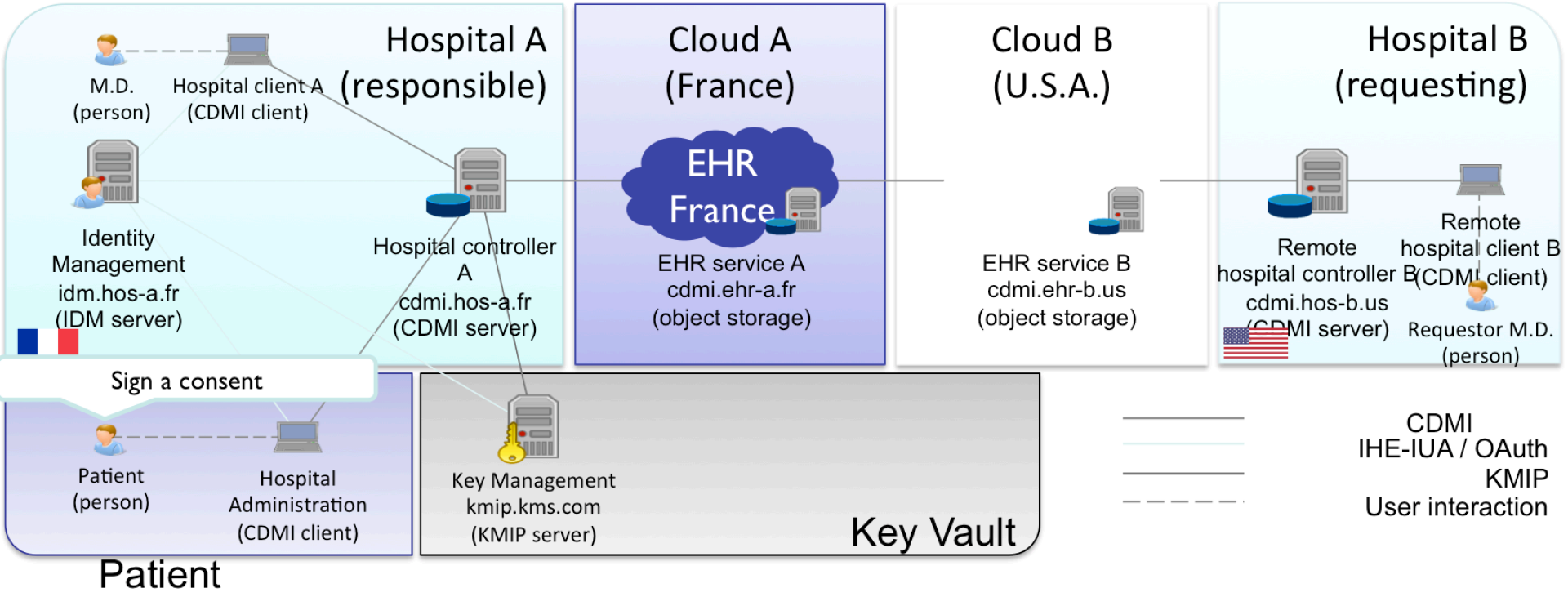


Patient

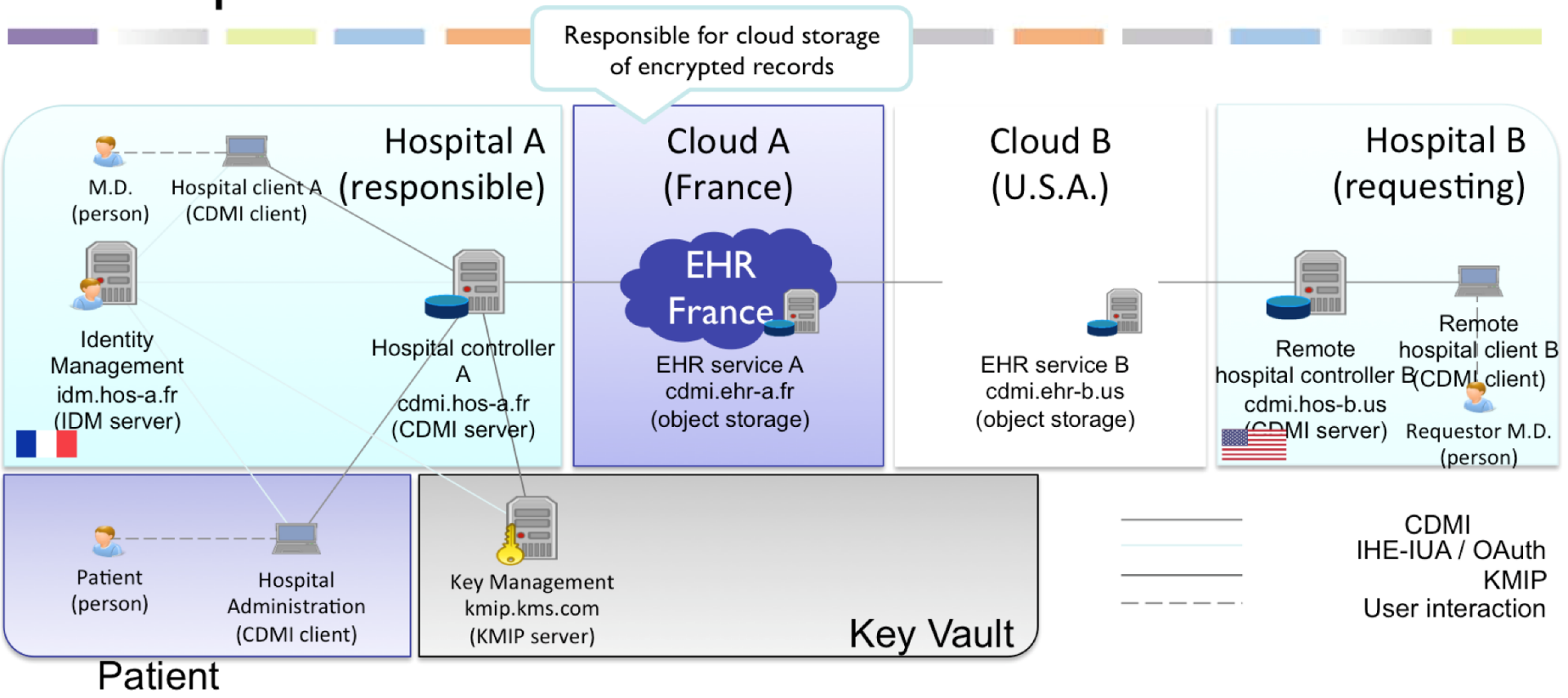
Responsibilities



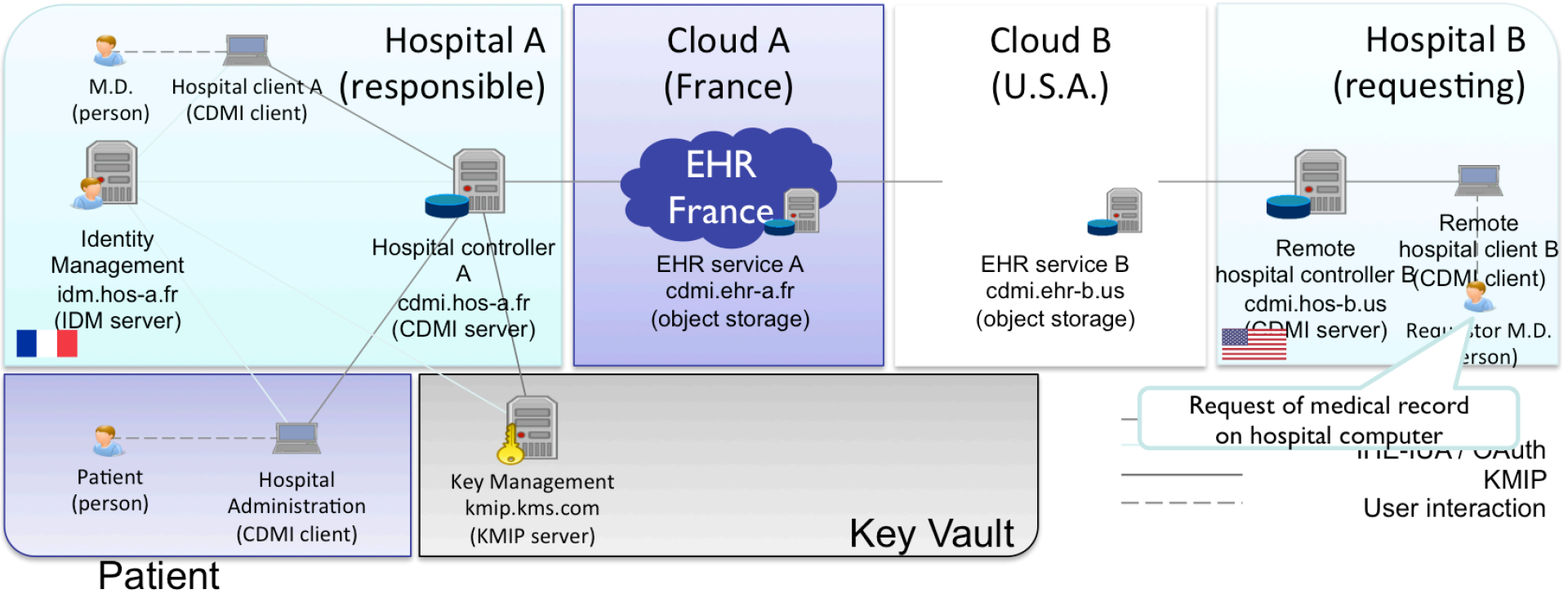
Responsibilities



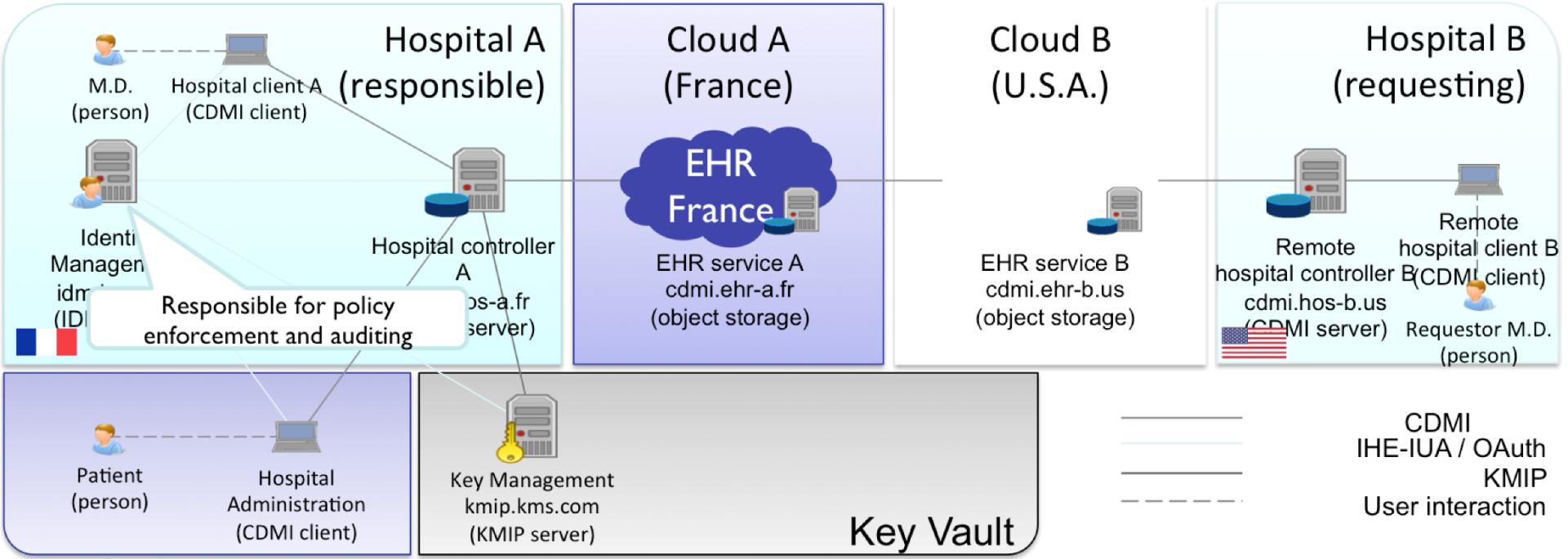
Responsibilities



Responsibilities

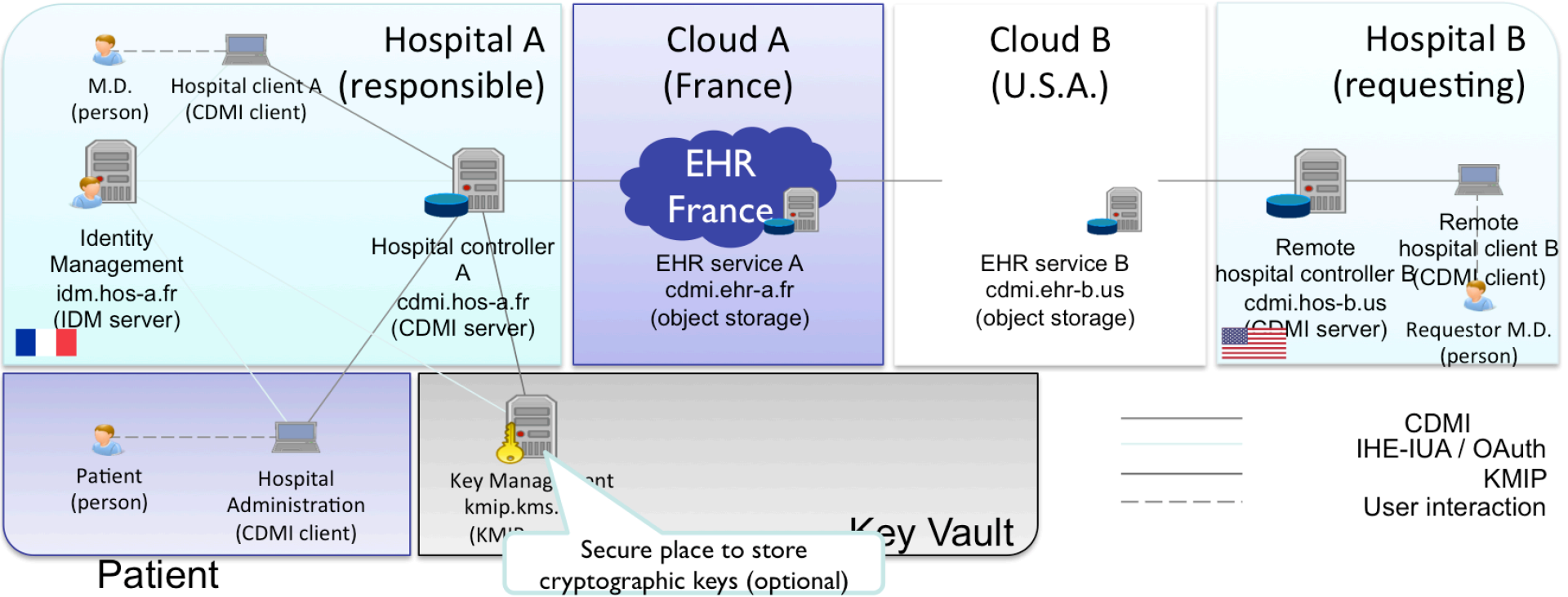


Responsibilities

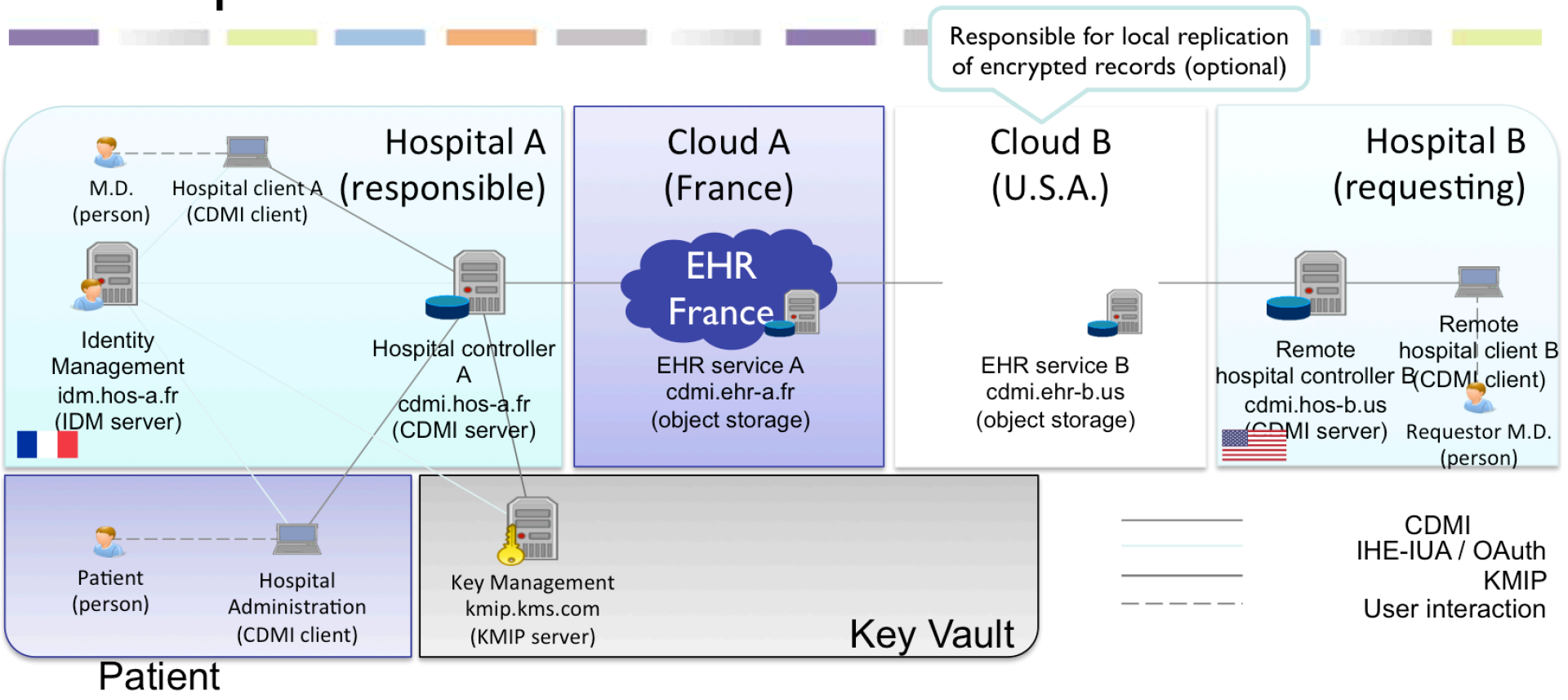


Patient

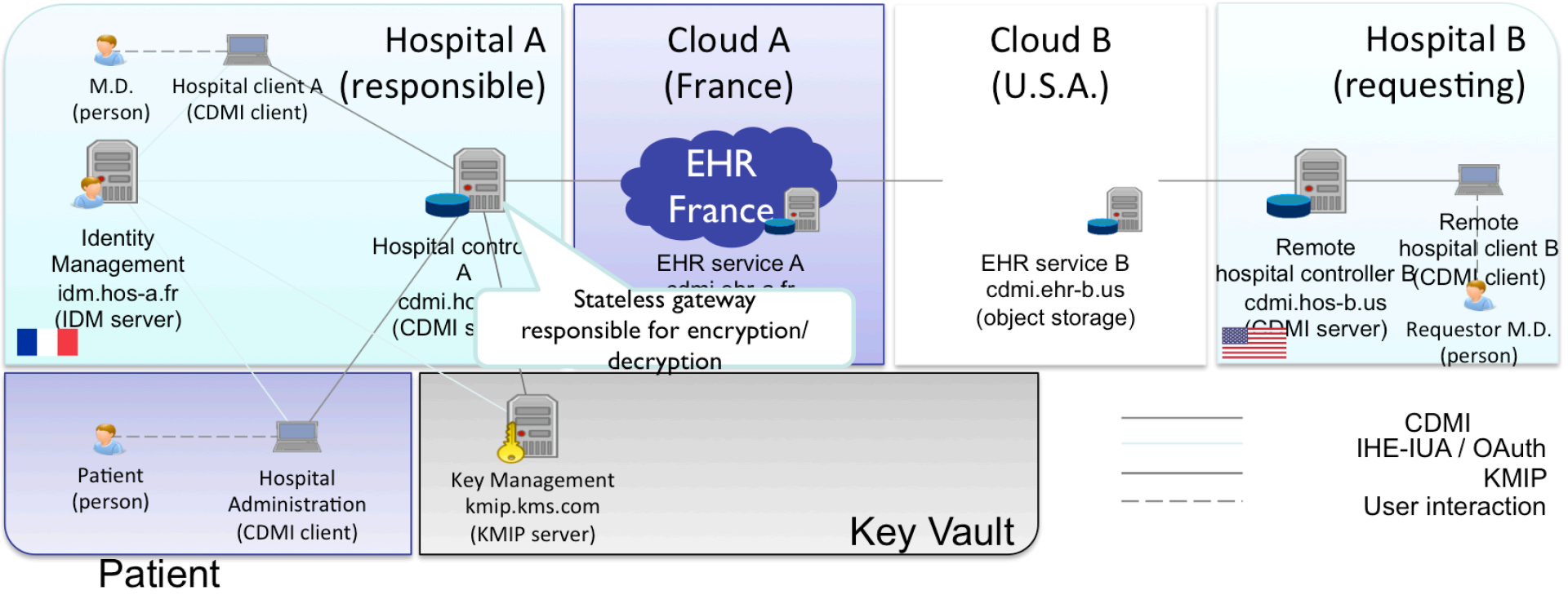
Responsibilities



Responsibilities

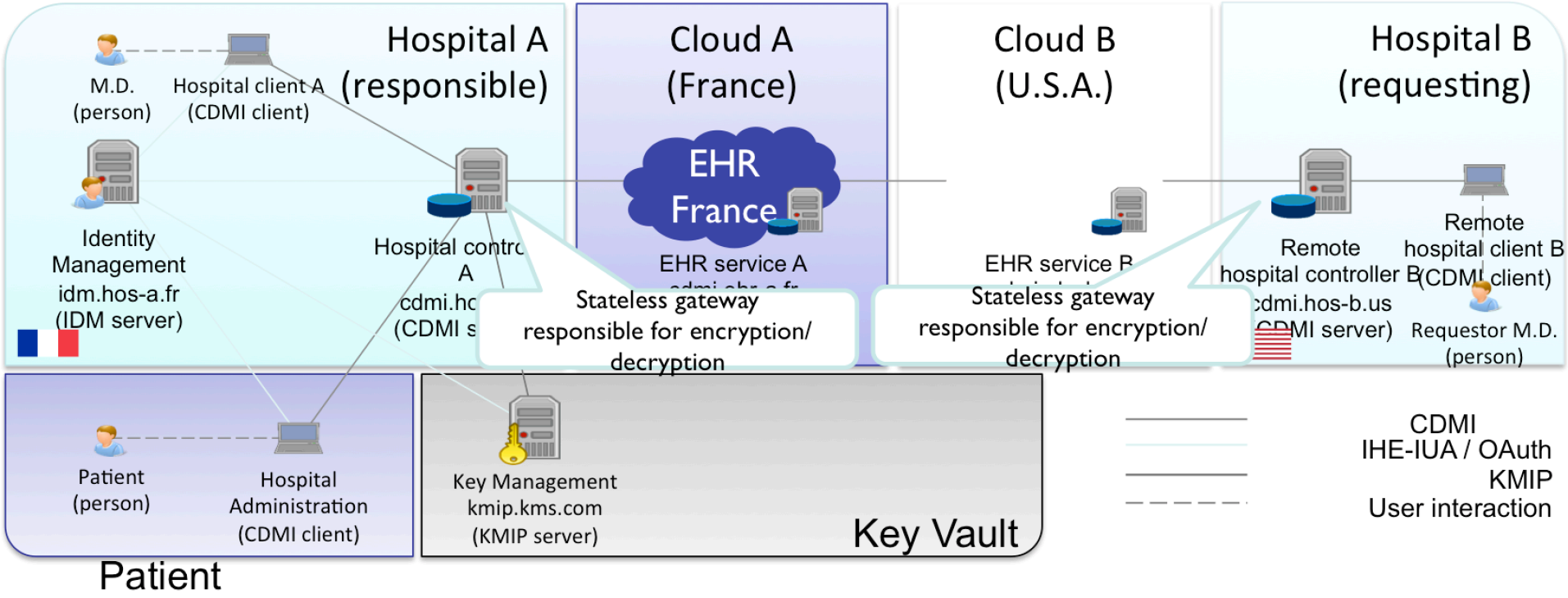


Responsibilities

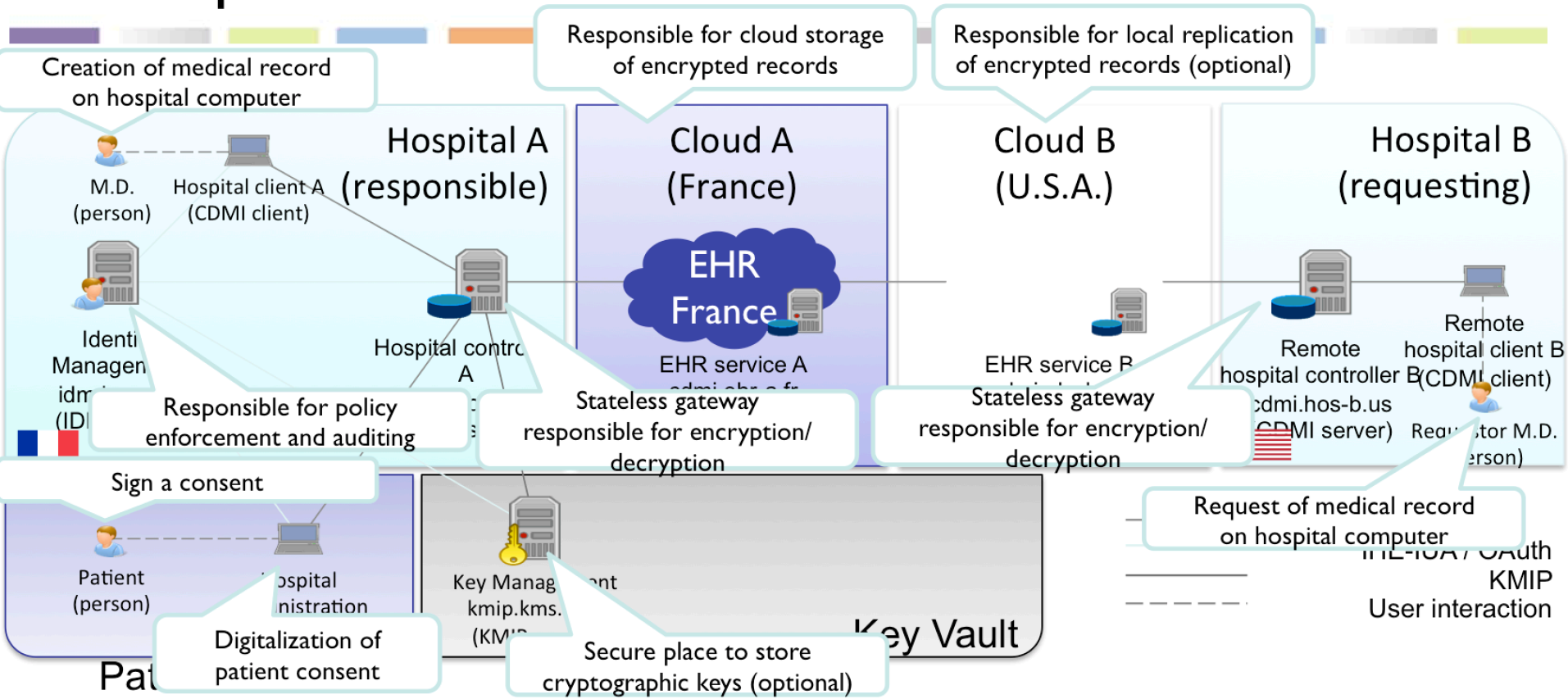


Patient

Responsibilities



Responsibilities



Key Security 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

- 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 v1.1.1
- Whitepaper: towards a CDMI healthcare profile
- Draft CDMI Extensions
  - Delegated Access Control Extension v1.1f
  - Encrypted Object Extension v1.1i
- JSON Object Signing and Encryption
  - JSON Web Signature (RFC 7515)
  - JSON Web Encryption (RFC 7516)
  - JSON Web Algorithms (RFC 7518)

Securing the Cloud Supply Chain

Cloud Supply Chain

SNIA CSI | CLOUD STORAGE

- Hyperscalers are very large customers
  - One estimate notes that ½ of all bytes shipped now are to Hyperscalers
  - Total (Server + Storage) Market to grow to $71.2 Billion by 2022 with 20.7% CAGR*
  - They can and do request specific features from storage devices via the RFP acquisition process
- Drive vendors will add these features in order to sell to these customers
  - Each vendor differs in how these features are implemented and in how they extend standard interfaces to accommodate them
- Software Defined Storage (SDS) products will also benefit from these features as they are added
  - Many Enterprises are taking advantage of the Hyperscalers techniques by using SDS

* Allied Market Research

Hyperscale Infrastructure for drives

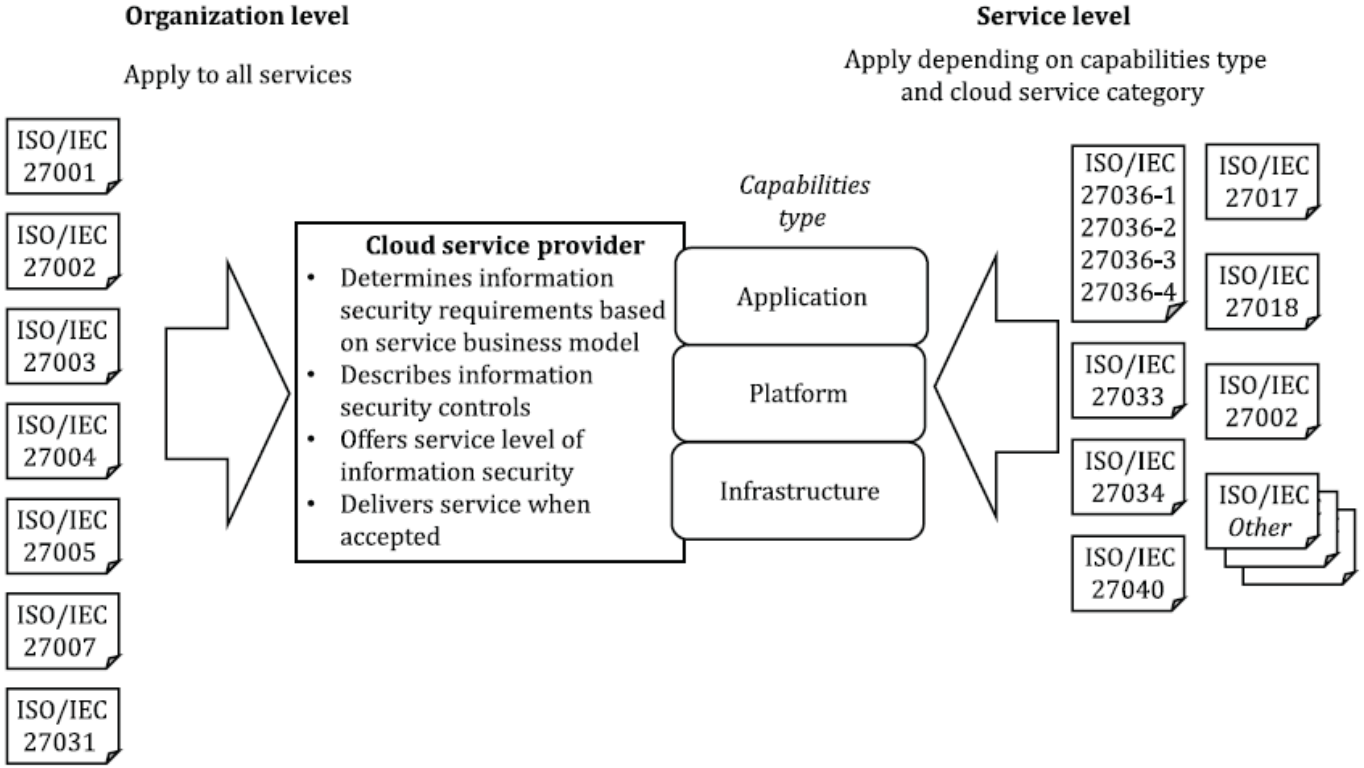
- Higher layer software handles data availability and is resilient to component failure.
  - Thus no need for expensive (No Single Point of Failure) storage systems
- Primary model has been Direct Attached Storage (DAS) with CPU (memory, I/O) sized to the servicing needs of however many drives of what type can fit in a rack's tray (or two).
  - See the OCP Honey Badger
- With the advent of higher speed interfaces (PCI NVMe) SSDs are moving off of the motherboard onto an extended PCIe bus shared with multiple hosts and JBOF enclosure trays.
  - See the OCP Lightning proposal
- Custom Data Center monitoring (telemetry), and management (configuration) software monitors the hardware and software health of the storage infrastructure.

Securing the Suppliers

SNIA CSI | CLOUD STORAGE

- Unless drives can be confidently erased, they must be shredded (includes persistent memory)
- Data path protocols of choice: TCP/IP or PCIe preferred, SAS & SATA are widely deployed for Direct Attach
- Hyperscalers secure their own management path infrastructure
- SDS layers also implement standard, securable interfaces

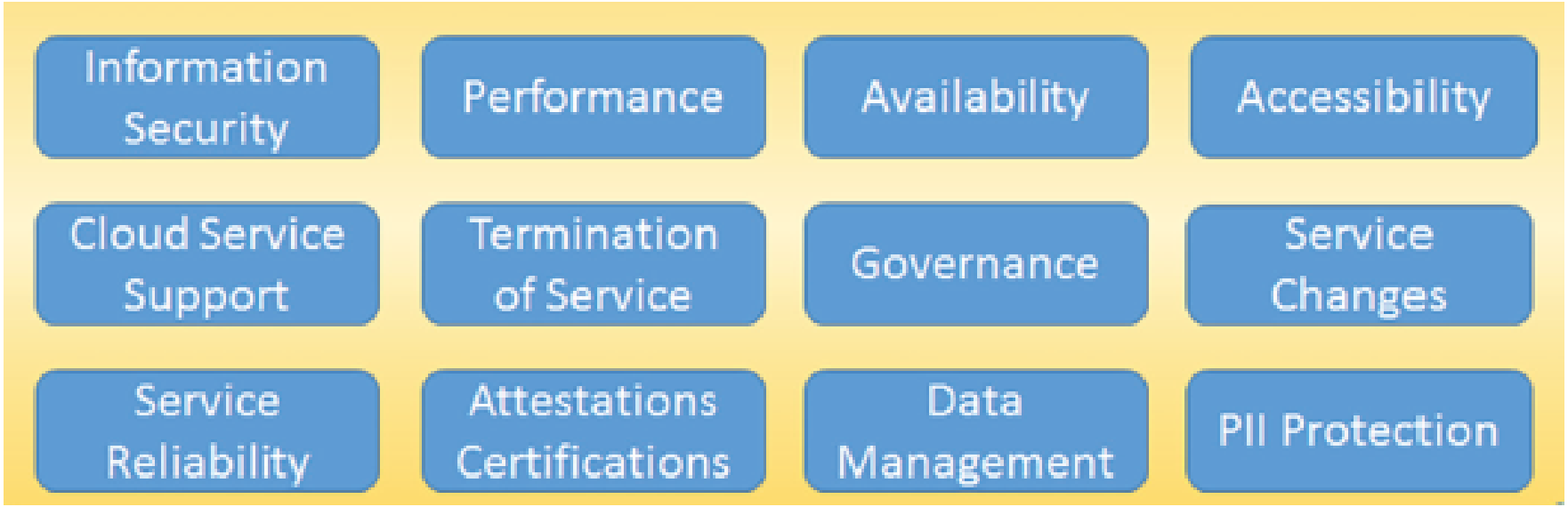
Outsourcing to the Cloud
(ISO/IEC 27036)



Cloud SLA Framework
(ISO/IEC 19086)

SNIA CSI | CLOUD STORAGE

SLA Content Areas



Cloud Security Certifications

SNIA CSI | CLOUD STORAGE

- Federal Risk and Authorization Management Program (FedRAMP)
  - U.S. Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services
  - The program's primary decision-making body is the Joint Authorization Board (JAB), comprised of the CIOs from DOD, DHS, and GSA.
  - Security criteria based on NIST SP 800-53r4

- CSA Security, Trust & Assurance Registry (STAR)
  - International certification program
  - STAR consists of three levels of assurance/certification: 1) Self-assessment, 2) 3rd-party Assessment-based, and 3) Continuous Monitoring-based
  - Security criteria based on the CSA's Cloud Controls Matrix (CCM) and the Consensus Assessments Initiative Questionnaire (CAIQ)

Cloud and Emerging Technologies

(Will Everything Play Nice)

Secure Multitenancy

SNIA CSI | CLOUD STORAGE

- Multitenancy/Secure Multitenancy
- Virtualization/Containers
- Big Data/Analytics
- IoT & Related Technologies

After This Webcast

- Please rate this webcast. We value your feedback
- This webcast will be available on-demand along with a copy of the on the SNIA Cloud Storage website http://www.snia.org/forum/csi/knowledge/webcasts
- A Q&A from this webcast, including answers to questions we couldn't get to today, will be on the SNIACloud blog
  - http://www.sniacloud.com/
- Follow us on Twitter @SNIACloud

Thank You

Standards (1)

- ISO/IEC 17788 | ITU-T Rec. Y.3500, *Information technology — Cloud computing — Overview and vocabulary*
- ISO/IEC 17998 | ITU-T Rec. Y.3502, *Information technology — Cloud computing — Reference architecture*
- ISO/IEC 17826, *Information technology — Cloud Data Management Interface (CDMI)*
- ISO/IEC 19086-1,*Information technology — Cloud computing — Service level agreement (SLA) framework — Part 1: Overview and concepts*
- ISO/IEC 19086-2,*Information technology — Cloud computing — Service level agreement (SLA) framework — Part 2: Metrics*
- ISO/IEC 19086-3,*Information technology — Cloud computing — Service level agreement (SLA) framework — Part 3: Core conformance requirements*
- ISO/IEC 19086-4,*Information technology — Cloud computing — Service level agreement (SLA) framework — Part 4: Security and privacy*
- ISO/IEC 19941, *Information technology — Cloud computing — Interoperability and portability*
- ISO/IEC 19944, *Information technology — Cloud computing — Data and their flow across devices and cloud services*

Standards (2)

- ISO/IEC 22123, *Information technology — Cloud computing — Concepts and terminology*
- ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*
- ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*
- ISO/IEC 27017 | ITU-T Rec. X.1631, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
- ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*
- ISO/IEC 27036-1, *Information technology — Security techniques — Information security in supplier relationships — Part 1: Overview and concepts*
- ISO/IEC 27036-2, *Information technology — Security techniques — Information security in supplier relationships — Part 2: Requirements*
- ISO/IEC 27036-3, *Information technology — Security techniques — Information security in supplier relationships — Part 3: Guidelines for information and communication technology supply chain security*
- ISO/IEC 27040, *Information technology — Security techniques — Storage security*