Storage Networking Industry Association
Technical White Paper

Towards a CDMI Health Care Profile

March 2015

Abstract: *This whitepaper examines the data protection needs of sharing health data across different cloud services, explores the capabilities of the Cloud Data Management Interface (CDMI) in addressing the requirements, and provides suggestions for possible extensions that are appropriate for a health care profile. This paper presents a use case for implementing shared data in the cloud, including requirements, architecture, a roadmap, and implementation challenges.*

USAGE

The SNIA hereby grants permission for individuals to use this document for personal use only, and for corporations and other business entities to use this document for internal use only (including internal copying, distribution, and display) provided that:

1. Any text, diagram, chart, table or definition reproduced shall be reproduced in its entirety with no alteration, and,

2. Any document, printed or electronic, in which material from this document (or any portion hereof) is reproduced shall acknowledge the SNIA copyright on that material, and shall credit the SNIA for granting permission for its reuse.

Other than as explicitly provided above, you may not make any commercial use of this document, sell any or this entire document, or distribute this document to third parties. All rights not explicitly granted are expressly reserved to SNIA.

Permission to use this document for purposes other than those enumerated above may be requested by e-mailing tcmd@snia.org. Please include the identity of the requesting individual and/or company and a brief description of the purpose, nature, and scope of the requested use.

All code fragments, scripts, data tables, and sample code in this SNIA document are made available under the following license:

DISCLAIMER

The information contained in this publication is subject to change without notice. The SNIA makes no warranty of any kind with regard to this specification, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The SNIA shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this specification.

Suggestions for revisions should be directed to http://www.snia.org/feedback/.

Contents

Figures

1. Introduction

Cloud computing services have received a great deal of attention and interest for addressing data storage and management. This is mainly due to the flexibility of cloud services that offer payment structures for data management and computation services to cloud customers according to the consumed resources. In addition, cloud services minimize the effort for cloud customers to create and maintain any computation and storage resources, which is a great advantage for the customers.

Rapid growth in deploying cloud computing requires advancing cloud technologies to improve cloud services. The advancement solutions provide a wider range of functionalities for customers, which enable them to have efficient and secure interactions with cloud services. SNIA is one of the standardization organizations that is active in developing new technologies in this domain. One of the main efforts of this organization is to provide appropriate interfaces that allow communication with cloud services. More specifically, SNIA provides solutions to store, manage, and retrieve data to and from cloud storage services. Cloud Data Management Interface (CDMI) is one of SNIA's standards that has been developed for cloud data management solutions.

CDMI has been designed to address API requirements for any type of cloud storage services. However, next to the generic requirements, each cloud service has specific needs that are specific to the use cases and deployment scenarios. One important class of such scenarios is focused on electronic health care services. In these services, health data is stored and shared among several clients and cloud services to streamline access to the health data. Sharing health data among a large number of cloud clients, such as doctors and health care organizations, can lead to a more accurate and efficient diagnosis of each patient. However, these use cases raise concerns over the security and privacy of the health data. As such, the data management standard must be equipped with countermeasures that protect the privacy and security of health data.

The purpose of this whitepaper is first to take a deeper look into the data protection needs of sharing health data across different cloud services. Then, this paper explores the capabilities of CDMI in addressing the requirements and provides suggestions for possible extensions that are appropriate for a health care profile.

The rest of this whitepaper is organized as follows:

- Section 2 explains the motivations for protecting health data.
- Section 3 describes health data protection requirements.
- Section 4 presents a use case that promotes the deployment of health data protection.
- Section 5 analyzes the requirements and implementation aspects of the use case.
- Section 6 presents the architecture of the use case and gives a survey of security health care standards along with the extension prospect of CDMI.
- Section 7 describes the roadmap, including a future use case and the challenges of implementation.
- Section 8 presents the conclusions.

2. Motivation

To improve the quality of health care services, there has been a huge effort and tendency in replacing paper-based health care systems with electronic data. While electronically storing and sharing health data substantially improves the efficiency and reliability of accessing the data, it enhances the risk of compromising patient privacy. Health data gives information about the disease history and medical records of patients, and thus should be treated as highly sensitive. In addition, in many applications, the electronic health data is required to be exchanged across various storage systems and jurisdictions, which are located in different countries. This underlines the importance of the compliance of the health data services with both national and global privacy and security laws and regulations. These regulations oblige the health care system to protect the data from unauthorized access and provide guidelines and rules for the data protection.

The data protection laws and regulations, which are briefly described below, give an insight for the legal issues of protecting health data.

- The General Data Protection Regulation (GDPR), which has been approved by the European Union, specifies how to protect personal data globally. This regulation provides strong privacy requirements on the health data. Under this regulation, the health data should be stored in encrypted form, and it must not be possible to link the data to individuals without additional information. The patient should be able to control how much of his or her data is revealed to data requestors according to the purpose of access. GDPR also defines the responsibilities of personal data protection, retention time, enforcement of data owner consent, security features of the database that stores data, and deletion of data. Additionally, GDPR specifies the fines for violating the regulations.

- The Health Insurance Portability and Accountability Act (HIPAA) regulations, which have been approved by the government of the United States, defines the requirements for the security and privacy of patient's data from privacy violations, abuse, and fraud. These regulations specify both physical and electronic safeguards to protect medical records. From a privacy point of view, HIPAA allows disclosure of the data only if it is de-identified and permission from the data owner has been collected. HIPAA specifies how the access policies for the health data should be created.

- The Standard Contractual Clauses for the Transfer of Personal Data to Third Countries regulations were developed under the Directive 95/46/EC of the European Parliament and of the Council. These regulations provide contractual clauses on using appropriate authorization, and they outline safeguards for transferring data to third countries that do not meet adequate data protection requirements. An amendment was defined in 2004 that introduces an alternative set of standard contractual clauses for transferring personal data to third countries.

In addition to the international data protection legislations, national regulations have been defined that provide better legislations according to the local laws, systems, and culture. For example, in the Netherlands, the Law Protection of Personal Details defines rules and procedures for processing personal data. This legislation defines who can access personal data, such as health data of patients, and for what purposes. In another example, Norway has the Personal Health Data Filing System Act. The purpose of this act is to contribute towards providing public health services and the public health administration with information and knowledge without violating the right to privacy to ensure that medical assistance may be provided in an adequate, effective manner.

3. Data Protection Requirements

Before describing the data protection requirements, the definition of data protection from the view of health data should be given. Data protection is referred to as "preserving the confidentiality, integrity, and availability of the health data." Data protection should also preserve the privacy of the patients in such a way that revealing the data to other data requestors is performed only with patient consent. To achieve health data protection, the following requirements should be satisfied.

- The platform and infrastructure used for storing, retrieving, and processing data should be well protected from cyber-attacks (cyber security).
- Data content 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 by enforcing the patient consent profile (privacy preserving).
- All of the transactions to request the data should be securely logged so that they can be audited if necessary (accountability).

In addition to the above-mentioned requirements, in health domains, the health data must be divided into several parts in such a way that each part of the data is encrypted using a different encryption key. In addition, different access policy rules should be created for each part of the data. Health data must be divided because health data are usually accessed by a wide variety of medical staff members with different backgrounds, positions, and responsibilities. For example, administrative members are allowed to read administrative data like costs, patient address, and billing information of treatments, but should not be allowed to read the content of the medical records. Therefore, division of the data simplifies protecting the data and limits the leakage of information about the data.

4. Use Case

First, we present a use case that promotes deploying appropriate security mechanisms to protect health data of patients (see Figure 1). Next, we focus on how data protection can be achieved for this use case.

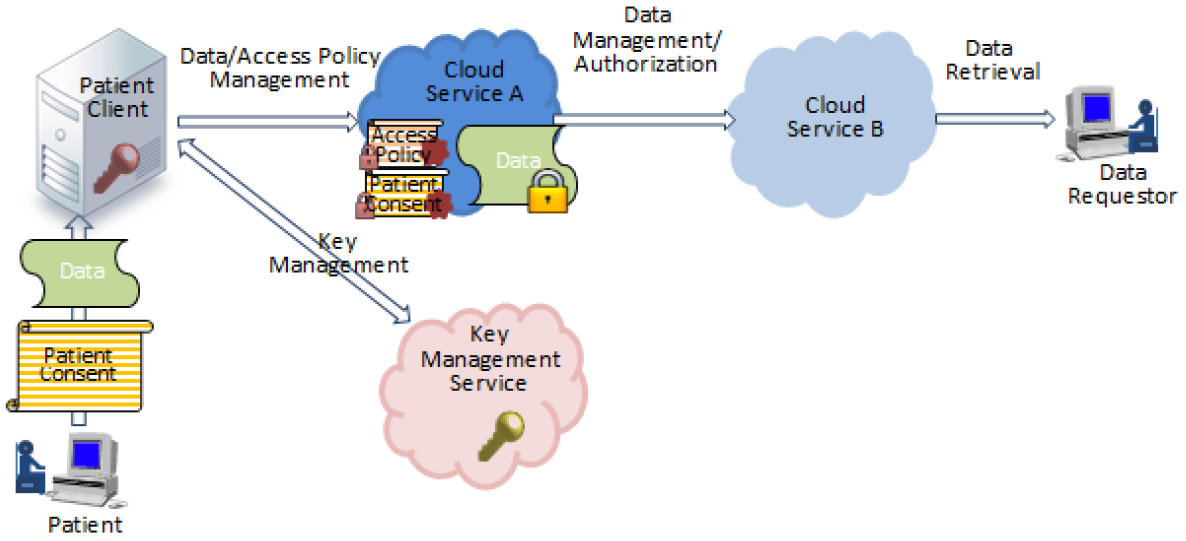

Figure 1. Use case showing health data sharing across different cloud services

This use case consists of the following actors:

- A patient who, together with some medical staff, stores and manages health data using a cloud service (for example, an Electronic Health Records (EHR) system)
- A patient client, which is a server that is responsible for protecting patient data by performing the required data protection computations on behalf of the patient
- Two cloud services (Cloud Service A and Cloud Service B) that provide storage facilities and share data with each other
- A data requester, who is a client of Cloud Service B and requests access to the data (for example, a doctor)
- A key management service, which stores and manages decryption keys to use for data encryption. The key management service has an administration that is distinct from the cloud services.

In this use case, a patient stores data in encrypted form in Cloud Service A. A data requestor from Cloud Service B requests access to the data. The encrypted data is provided to Cloud Service B once requested. If the data requestor is authorized according to the patient consent and access policies, the patient client sends to Cloud Service B the decryption key of the data. Cloud Service B decrypts and sends the data to the data requestor. A practical example and more detailed description of the use case are given below.

Example of the Use Case

Assume that the EHR services of France and the United States agree to share medical records of patients with each other. The advantage of this sharing would be to help health care centers of either country to access the medical records of the patients coming from the other country for a more accurate and reliable treatment. In the initial step, the EHR services of France and the United States create a contractual pre-agreement on how to proceed and treat the requested medical records. The contractual pre-agreement includes the type of the credentials and attributes required for authorization and a list of the hospitals that are trusted by the EHR services. The pre-agreement also includes the usage policies, which specify the period of time that the records can be used and how they should be protected after sharing the medical records. The pre-agreement also specifies how the hospital that is hosting the medical records enforces the access policies.

Having completed the pre-agreement phase, hospitals send the medical records of their patients in encrypted form to the EHR service. The corresponding decryption key is stored at a key management service that is managed in a distinct domain, separate from the EHR service. As such, the EHR service cannot read the content of the medical records. In addition, for each medical record item, an administrative data item is created where only the administrators are allowed access. This data item includes the financial and personal information of the patient as well as some information to track the data, but this information should not contain any information related to the health history of the patient. For the storage on the EHR service, the administrative item is encrypted using a key that is different from the medical record item. Such separate encryption ensures that the administrators cannot access the contents of medical records.

The hospitals are responsible for protecting the medical records from unauthorized access. To protect the data, the hospital creates access policies for each data item that states which hospitals and medical staff members with what roles are allowed to access the data. The hospital also allows patients to create a consent profile that states for what purposes the medical records are allowed to be revealed to the authorized requestors. For instance, the patient could create a list that excludes a number of medical staff members from accessing the medical records, even if those medical staff members meet the authorization requirements. The reason for creating the exception list could be that the patient does not want some friends or family members to access the medical records. The patient consent profile also includes all of the privacy preferences of the patient, such as specific medical staff members who are not permitted to get the data.

Now assume that a hospital from the United States wants to access the medical records of a French patient. To get the required records, the U.S. hospital sends an access request to the U.S.-based EHR service. The access request includes the credentials of the data requestor according to the pre-agreement. The U.S.-based EHR service first validates the credentials and then checks whether the requestor is permitted to access medical records from the France hospital. This access policy enforcement can be regarded as the first layer of controlling access to the data, where only the eligibility of the requestor to request access to the France-based EHR is checked. If the data requestor is eligible, the U.S.-based EHR service queries and retrieves the attributes of the data requestor from a local U.S.-based identity provider. The EHR service then sends an access request to the France-based EHR system. The access request includes the attributes of the requesting hospital and the requesting medical staff member. Before sending the access request, proper translations, linguistically and semantically, are performed.

Having received the access request, the France-based EHR service sends the requested encrypted data to the U.S.-based EHR service. To provide the data decryption key, the France-based EHR service forwards the access request along with the access policies and patient consent profile, which are stored

in encrypted form, to the France-based hospital. This hospital is responsible for protecting the French patient.

The hospital decrypts and checks the integrity of the access policies and the patient consent. In this case, the U.S.-based hospital and the medical staff who requested access to the data are authorized, and the French hospital retrieves the data decryption key from the key management service. The authorization process is performed by evaluating the access policies and the patient consent against the attributes of the requesting hospital, the requesting medical staff, and the purpose of access. In addition, the hospital decides whether the data decryption key of the medical records or the administrative data is retrieved. To limit the leakage of information about the requested data, the data decryption key is encrypted using the public key of the U.S.-based EHR service.

After the U.S.-based EHR service receives the data decryption key that is wrapped by the public key, the data decryption key is decrypted. Then the requested data is decrypted and sent back to the requesting hospital. The U.S.-based EHR service then erases the data decryption key according to the time to live (TTL) value to ensure that the data will not be accessible by any other parties. The TTL value is the time duration that is allowed by either service to keep the received data decryption key and is defined in the contract (see Assumption 1). After elapsing TTL, the decryption key should be deleted. To confirm that the data decryption key has been deleted, the U.S.-based EHR service sends a message to the France-based EHR service, which stores the message in the audit logs.

Detailed Description of the Use Case

A patient sends his or her health data with the names of medical staff to the patient client. The patient also sends his or her consent profile to the patient client specifying the privacy preferences to access the health data. The patient client associates access control policies to the health data, which specifies which data requestors are permitted to access the data. The access policies are created according to the content of the data, applicable laws and regulations, and system policies. The patient client generates a unique encryption key and encrypts the health data. The patient client encrypts and signs the access policies and the patient consent profile using its secret key and sends them, together with the encrypted data, to Cloud Service A. The patient client stores the decryption key of the data to the key management service.

A data requestor sends an access request to Cloud Service B. The data requestor is authenticated by Cloud Service B. If the data requestor and the requested health center are authorized to request data from Cloud Service A, the access request and all of the authentication information of the data requestor are sent to Cloud Service A. Given the access request, Cloud Service A sends the encrypted data to Cloud Service B. Cloud Service A sends the access request and information of the data requestor, along with the encrypted access policies, patient consent, and their signatures to the patient client. The patient client decrypts and verifies the integrity of the access policies and the patient consent profile. The patient client enforces the patient consent and access policies. If the data requestor is authorized, the patient client retrieves the decryption key from the key management service. The patient client encrypts the decryption key using the public key of Cloud Service B and forwards the encrypted decryption key to Cloud Storage B via Cloud Service A. Cloud Service B decrypts the decryption key using its private key and decrypts the data. Cloud Service B sends the data to the data requestor using a secure channel. Cloud Service B erases the data and sends a deletion confirmation to Cloud Service A. Cloud Service A securely logs the deletion signal.

Assumptions

The use case that we presented above is based on a number of assumptions, which are described below.

- **Assumption 1.** A contractual agreement between the EHR services of the U.S. and France is made to specify what health centers are eligible to access the data, what attributes should be transmitted for the access request, and what the usage policy is for using data after granting access. As part of the data usage policy, a TTL value is agreed to that specifies how long a data decryption key can be stored after receiving it from the other EHR service. After passing the TTL time, the data decryption key should be properly deleted.

- **Assumption 2**. The patient client is the entity that is responsible for protecting the patient data and thus can be fully trusted by the patient. The patient client is also assumed to be equipped with sufficient computational resources to handle all of the required computations. In EHR systems, the patient client is a software service running on the servers of the hospital. For Personal Health Record (PHR) systems, the patient client is a data protection program running on the machines of the patient.

- **Assumption 3**. The health data of the patient is created at the location of the patient client, and therefore, no protocol is required to send the data to the patient client.

- **Assumption 4**. The patient consent profile can be created and managed using mail or any paper-based forms. Therefore, no electronic protocol is needed to handle consent management.

- **Assumption 5.** The health data is divided into two parts. The first part consists of the medical records, and the second part consists of the administrative information about the patient. These pieces of data are encrypted using different keys.

5. Requirements and Gap Analysis

In this section, the use case is analyzed further from the aspects of meeting data protection requirements and implementations. Also investigated is to what extent SNIA can address the implementation.

Fulfillment of Data Protection Requirements

The data protection requirements are explained in Section 3. This section explains how these requirements can be fulfilled in the use case.

Cyber security

All of the actors of this use case should deploy appropriate countermeasures against cyber-attacks. The details of the countermeasures are out of the scope of this whitepaper.

Data confidentiality

The data is encrypted by the patient client and remains encrypted except for authorized data requestors. To provide the data decryption key to the data requestor, the data decryption key is wrapped with an encryption key that allows only Cloud Service B to decrypt. Cloud Service B also transfers the data to the data requestor via a secure channel that encrypts data at transit (such as HTTPS). Therefore, assuming that Cloud Service B erases the decryption key after the data requestor receives the data, end-to-end encryption is achieved from the patient client to the data requestor. As mentioned in the use case, each data item has a unique decryption key, which limits the loss of data in case a decryption key is leaked.

Data integrity

In this use case, the authorization information, which consists of the patient consent profile and the access policies associated with the data, are appropriately signed by the patient client. The signature ensures that any modifications by Cloud Service A can be detected. The signature can be generated using a keyed hash function that takes the data and the patient client private key as input and generates a hash value. The signature can be later verified using the private key and the authorization information and checking the hash result with the signature value. The signature can also be performed using the public key infrastructure (PKI), in such a way that the messages are signed using a private key and then verified using the corresponding public key. However, the former signature is more efficient than the PKI signature.

Separation of duties

The key management service and the cloud services are administered by distinct entities. These actors also do not have direct interfaces with each other but via the patient client. Therefore, none of these actors can access the data without permission by the patient client, because the cloud service has access to the encrypted data only and the key management system has access to the decryption key only.

Authentication

Any data requestor is appropriately authenticated via the corresponding cloud service before sending any access request to the cloud storage service.

Authorization

Any data requestor who is authenticated must be authorized by the patient client to access and use the data according to the applicable policies. The authorization process checks the eligibility of the data requestor for accessing the decryption key. Authorizing the data requestor is performed in two steps. First, Cloud Service B checks the eligibility of the data requestor in sending any access request. Then, the patient client evaluates access policies against the attributes of the data requestor. Note that next to the technical requirements of authorization, legal agreements between Cloud Service A and Cloud Service B are needed. This legal agreement should clarify what attributes are needed from the data requestor and what health institutes or members are permitted to request data.

Patient privacy preservation

Patient privacy preferences are specified in the patient consent profile. Using this profile, the patient can state that revealing his or her health data to data requestors is permitted under what purposes (for example, for emergency situations only). For each access request, the patient client should first check the patient consent profile. If the permission is given to reveal the data to other parties for the requested purpose, then the patient client evaluates access policies to decide whether the data requestor is authorized.

Accountability

All of the transactions from Cloud Service A, Cloud Service B, and the key management service are securely logged. The secure logging and auditing is out of the scope of this whitepaper.

Implementation Requirements of the Use Case

Implementing this use case requires using the appropriate protocols and deploying the technologies to exchange required messages and invoke functionalities, respectively. The protocols that are required for this use case are as follows:

- *Data management protocols* provide interfaces with cloud services to store, update, delete, and retrieve data.
- *Key management protocols* provide interfaces to the key management service to store, update, retrieve, and delete decryption keys.
- *Authentication protocols* provide interfaces with cloud services to transfer the data requestor credentials and also to exchange the attributes and other access information of the data requestor from one cloud service to another cloud service.
- *Authorization protocols* allow access policies and patient consent to be transferred from or to the patient client or cloud services.
- *Auditing protocols* allow audit logs of all transactions to be stored securely.

This whitepaper focuses on protocols that address the use case. However, to give further information about the underlying technological services and infrastructures, brief explanations are given below.

- Data center encryption and infrastructures, such as PKI, allow the data and the corresponding decryption key to be encrypted.

- Authentication and identity management infrastructures provide unique identities to the data requestors and patients and store the attributes of data requestors. The authentication infrastructure also allows data requestor credentials to be verified.

- Authorization infrastructures allow access policies for access policy enforcement to be created, stored, and interpreted. XACML is an example of authorization infrastructure.

Extent to which SNIA addresses this use case

The Cloud Data Management Interface (CDMI) international standard is a protocol that has been standardized by SNIA to address data management protocols with cloud computing services. Therefore, it is clear that CDMI fully addresses the data management requirements of the use case, including the storage, update, deletion, and retrieval of data. Additionally, CDMI provides functionalities to discover the capabilities of a cloud service—for example, what encryption functions the cloud service supports, or how large the size of the metadata should be.

Key management is out of the scope of CDMI. However, CDMI is fully compatible with the Key Management Interoperability Protocol (KMIP). KMIP is a well-established standard to address key management requirements. CDMI allows the data item to be assigned a globally unique identifier in such a way that the same identifier can be associated with the decryption key of the data. Using the identifier, decryption keys can be linked to their corresponding data items.

One of the main features of CDMI is that this international standard allows metadata to be associated with the data. The purpose of using metadata is to transfer all essential information to protect data, and particularly, to address authorization requirements to the cloud service. The current version of CDMI allows only using Access Control Lists (ACLs) in the metadata. Using ACLs, it can be specified which groups of data requestors are allowed to access the data. In addition, the ACLs can be updated later.

To address data confidentiality requirements, end-to-end encryption is needed from the patient client, where the health data is created, to the data requestor. Achieving end-to-end encryption requires both encryption of data at rest and encryption of data at transit. CDMI provides encryption of data at transit using TLS, which is needed to transmit the decrypted data securely from Cloud Service B to the data requestor. To protect confidentiality and integrity of data at rest, CDMI provides guidelines to the storage cloud service (or client) for the encryption functions, encryption mode, and the size of the encryption key, and hash functions that should be used for encryption/signature.

Gap for health care profile

As mentioned above, apart from key management, CDMI fully addresses the data management requirements of the use case. In addition, KMIP can fulfill the key management functionalities and is compatible with CDMI. However, other requirements of the use case—especially authorization and access policy management needs—can only be partially addressed by the current version of CDMI. As such, several extensions should be considered to address the requirements completely.

From a high-level view, the extension should be performed from three aspects—compatibility with health care standards, delegation of the storage of access policies and patient consent, and the provision of decryption keys to the data requestor.

First, as the use case is in the context of health care, the extended version of CDMI should be compatible with health care standards such as HL7 and FHIR. In this case, the definitions of the metadata that are used in CDMI should be extended to include security labels of these standards. In addition, the definition

of the metadata should be extended to include the patient consent profile as well as the purpose of action of the data requestor, which is required to enforce patient consent. The current profile allows metadata to include ACLs only.

Second, because the storage of access policies and patient consent is delegated to the cloud service while the enforcement is done by the patient client, it is crucial to verify the integrity of this authorization information. The use case addresses this requirement by signing the authorization information and storing the signatures on the cloud service. However, the current version of CDMI does not specify how to include and distinguish signature messages to or from the metadata. Therefore, the extended version of CDMI needs to address this problem.

Third, for each access request, the patient client needs to provide the decryption key to Cloud Service B via Cloud Service A, in such a way that only Cloud Service B can access the decryption key. Therefore, the decryption key should be encrypted using the public key of Cloud Service B. To provide the public key to the patient client, Cloud Service A should include the certificate of Cloud Service B in the access request that is forwarded to the patient client. Hence, CDMI should have the capability of transferring public key certificates along with the access request.

6. Architecture

The architecture of the use case is illustrated in Figure 2, where all of the message exchanges and invoked functions are shown. According to Assumption 2, the data and the associated patient profile are created on the patient client side or by mail. Therefore, no electronic protocol/functionality is required between the patient and the patient client. Therefore, the actor patient is not shown on the actor lists of the architecture.

Secure Storage

As Figure 2 shows, given the health data and the patient profile, the patient client first creates the access policies according to the laws, regulations, content of the data, and the system policies. The patient client then associates the access policies and the patient consent profile and their signatures to the data item. Access policy and patient consent and their signatures are shown as authorization information in this figure. To store the data securely on Cloud Service A, the patient client generates a unique encryption key for the data and encrypts the data. The patient client then stores the encrypted data on Cloud Service A and the corresponding decryption key on the key management service. Both the encrypted data and the corresponding decryption key are associated with a unique identifier that binds the data and the decryption key.

Secure Retrieval

For a data requestor to access the health data, an access request is sent to Cloud Service B. The request includes identification information (attributes) of the data requestor, as well as the type and purpose of access to the data. Given the access request, Cloud Service B verifies the credentials and identity of the data requestor. If verified, Cloud Service B retrieves the attributes of the data requestor from the local identity provider that keeps the up-to-date attributes of the data requestors subscribed to Cloud Service B. The retrieved attributes are translated into the semantics of Cloud Service A and then sent to Cloud Service A along with the access request.

Having received the access request, Cloud Service A sends the encrypted data to Cloud Service B. Recall that the authorization of the data requestor is used for accessing the decryption key only. To provide the corresponding decryption key to the data requestor, Cloud Service A sends an access request to the patient client. The access request includes authorization information and the signature associated with the data (access policy and patient consent), translated attributes of the data requestor, and the action or purpose of the access to the patient client.

The patient client verifies the integrity of the access policy and the patient client. If the integrity is verified, the patient consent and access policies are evaluated against the purpose of action, type of action and attributes, and the data requestor. If the data requestor is authorized, the patient client retrieves the decryption key using the identifier that is associated with the encrypted data. To retrieve the key, the patient client sends the key management system the identifier of the encrypted data and the credentials that prove the identity of the patient client. If the authentication of the patient client is performed successfully, the key management system sends back the requested decryption key.

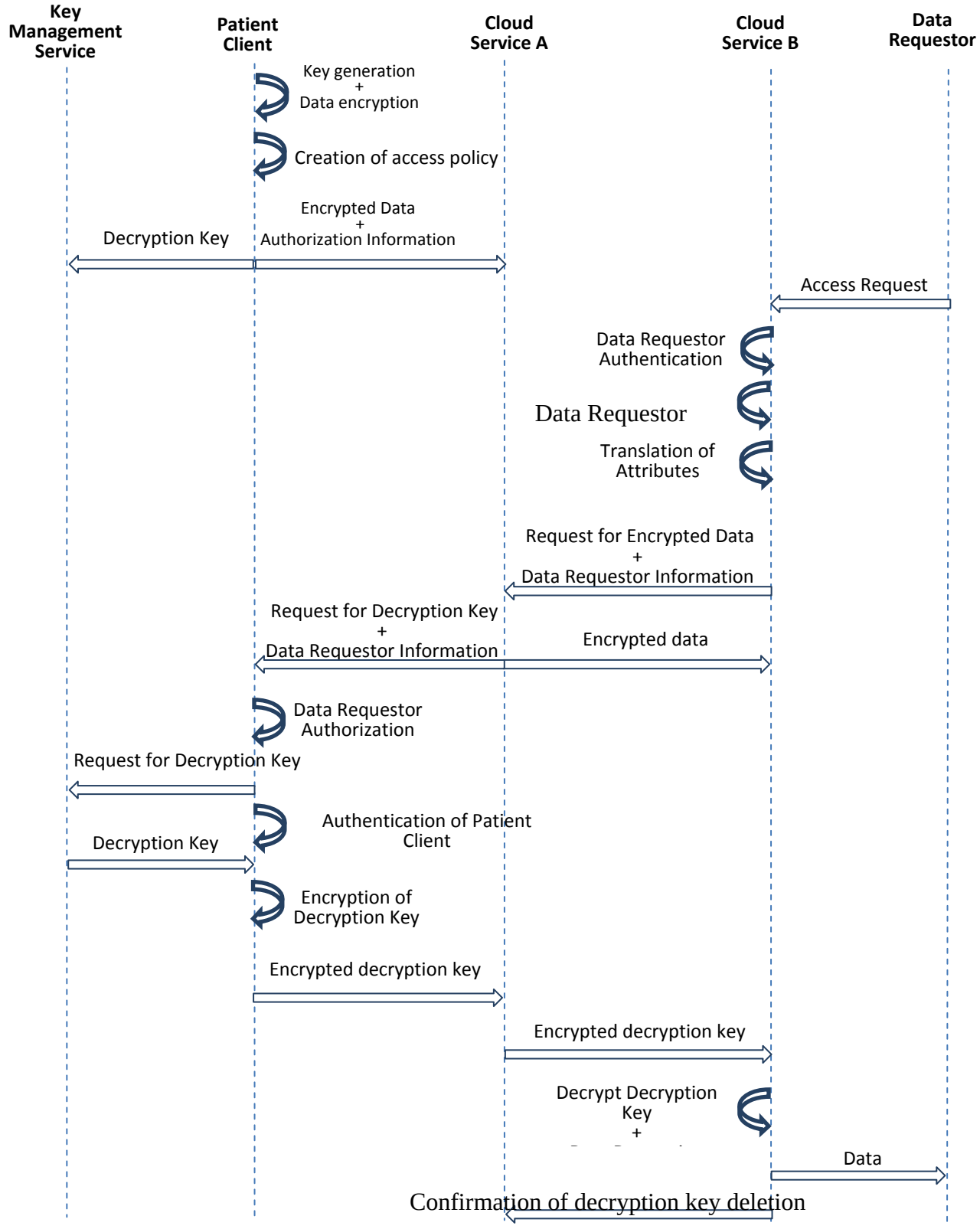

Figure 2. Architecture of the use case

Since the decryption key needs to be sent to Cloud Service B via Cloud Service A, it should be encrypted in such a way that only Cloud Service B can decrypt it. This encryption can be performed either by sharing a secret key between the patient client and Cloud Service B, or by using the public key of Cloud Service B. The patient client sends the encrypted decryption key to Cloud Service B via Cloud Service A. Given the encrypted decryption key, Cloud Service B first decrypts the decryption key and then decrypts the data. The data is then sent to the data requestor using a secure channel. Finally, Cloud Service B erases the decryption key according to the value TTL, which is mentioned in the data sharing contractual agreement, and sends a confirmation to Cloud Service A for the deletion.

Implementation of the Architecture

As mentioned above, to address the data management requirements, extension to CDMI may be necessary. This extension should be performed from three aspects—compatibility with health care standards, delegation of the storage of access policies and patient consent, and the provision of decryption keys to the data requestor. Before explaining more details about the extension considerations, related health care security standards are presented.

Survey of HIE Standards

This section provides a brief survey of the relevant security and privacy standards in health care. The purpose of this survey is to provide a better view on the extension prospect of CDMI and to show what parts of the architecture can be addressed by the extended version.

HL7/FHIR Security Labels [1]

HL7 and FHIR define a framework and standards on how to exchange, share, and integrate health data. From a security point of view, these frameworks define a set of security labels that give extra information about the health data. The security labels provide some security or privacy information about the health data to increase the granularity of access policy enforcement. Using the security labels, the patient can define the level of sensitivity of data, how the patient is known to the public and the medical staff of the institute, and what part of the information about the health data can be revealed to authorized parties. In our use case, security labels should be used with access policies for a fine-grained policy enforcement.

Basic Patient Privacy Consent (BPPC) [2]

This standard supports patient privacy. BPPC provides a semantic model on how patients can express their privacy preferences for health data. This standard is supported by HL7 and allows patient to specify what parts of their health data can be revealed to authorized data requestors for what purposes. The main elements of BPPC in expressing patient privacy are opt-in and opt-out, where opt-in is used to give permission for sharing information, and opt-out is used to refuse permission. BPPC is one of the essential components of the use case for specifying privacy preferences of the patient.

IHE-IUA [3]

This standard provides authorization services using the HTTP protocol and is a substitution of OAuth for low power and constrained resource devices such as smart phones and tablets. Like OAuth, IHE-IUA allows a data owner to delegate generation of access tokens to external authorization parties. In addition, handling single sign-on authentication between several authorization systems is supported.

This standard is not directly relevant for the use case, but it is needed if using several authorization services or delegating generating access tokens.

IHE-DEN [4]

This standard provides a way to encrypt any type of data, such as media or text documents. The patient client can use this standard to encrypt health data.

IHE-XUA [5]

This standard is a substitution of SAML for health care services. IHE-XUA allows assertion and transfer of authentication information of data requestors among several parties. This standard is required to implement the use case to transfer access request and attributes of the data requestor from Cloud Service B to Cloud Service A.

CDMI Extension

Before explaining the consideration to extend the CDMI international standard, some background information about CDMI metadata should be given. In general, CDMI allows associating four types of metadata to the data, as follows:

- HTTP metadata, which provide information about the HTTPS protocol
- User metadata, which gives information about data ownership
- System metadata, which includes information about the data
- Storage system metadata, which provides some information about the cloud storage service

The access control information, including the ACL and the patient consent profile, should be included in the system metadata. Currently, CDMI allows associating only ACL as access control information to the system metadata. However, to implement the use case, CDMI needs to be extended to support patient consent profile and security labels defined by HL7. In addition, the metadata should also contain the signature of the access control information. The extension should make it possible to distinguish the signature of the ACL from the signature of the patient consent profile.

The storage system metadata is used to contain information about the cloud service that stores the data. However, for this use case, the storage system metadata should not only contain information about Cloud Service A, but also information about Cloud Service B. The information about Cloud Service B should be the name and/or features of the cloud as well as the public key certificate of the cloud.

Therefore, in summary, the extended version of CDMI should support the following:

- Patient consent according to the BPPC standard
- HL7/FHIR security labels
- Access control information signatures
- Identity information of the cloud service that is requesting access to the data
- Purpose of access for enforcement of patient consent
- Name/features and public key certificate of the cloud service requesting access to the data

Figure 3 illustrates the architecture with the protocols that could be used for the implementation. In this figure, the extended version of the CDMI that meets the extension requirements mentioned above is denoted by CDMI+.

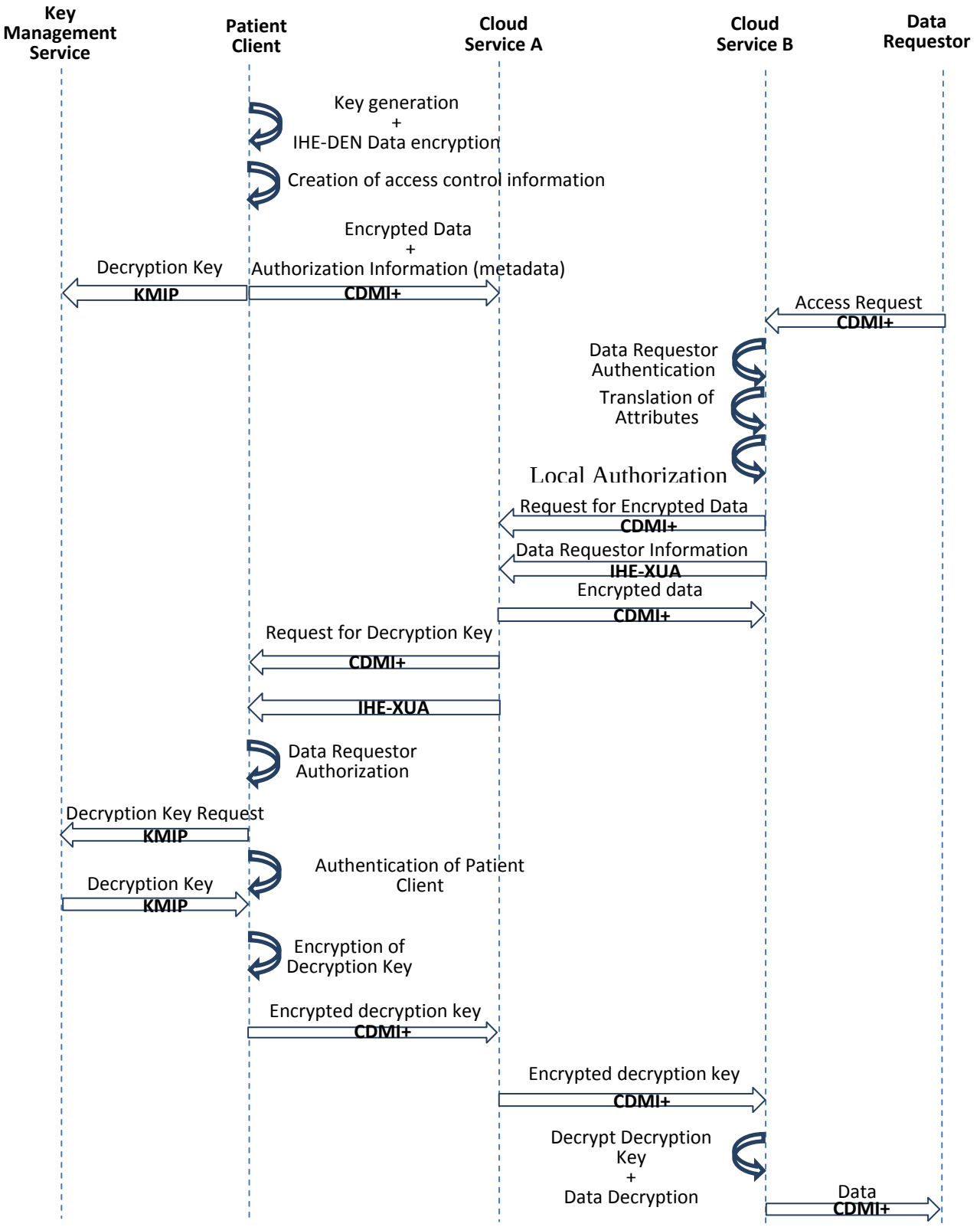

Figure 3. Protocols that implement the architecture

7. Roadmap

Future use cases can evolve from the use case sketched in this whitepaper. In the use case discussed in this document, the patient client enforces the access policies. The advantage of such a use case is that it provides a higher level of trust in honest enforcement of the access policy. However, implementing this use case requires that the patient client to be equipped with computation resources that support invoking all of the access control functionalities. If the patient client has constraints in computational resources, it would be more efficient if the cloud service that requests access to the data were delegated to enforcing the access policies.

Figure 4 shows the use case that allows the enforcement of access control information to be delegated. In this use case, Cloud Services A and B share both the encrypted data and the access control information. Therefore, with each access request from the data requestor, Cloud Service B evaluates and enforces access control information.

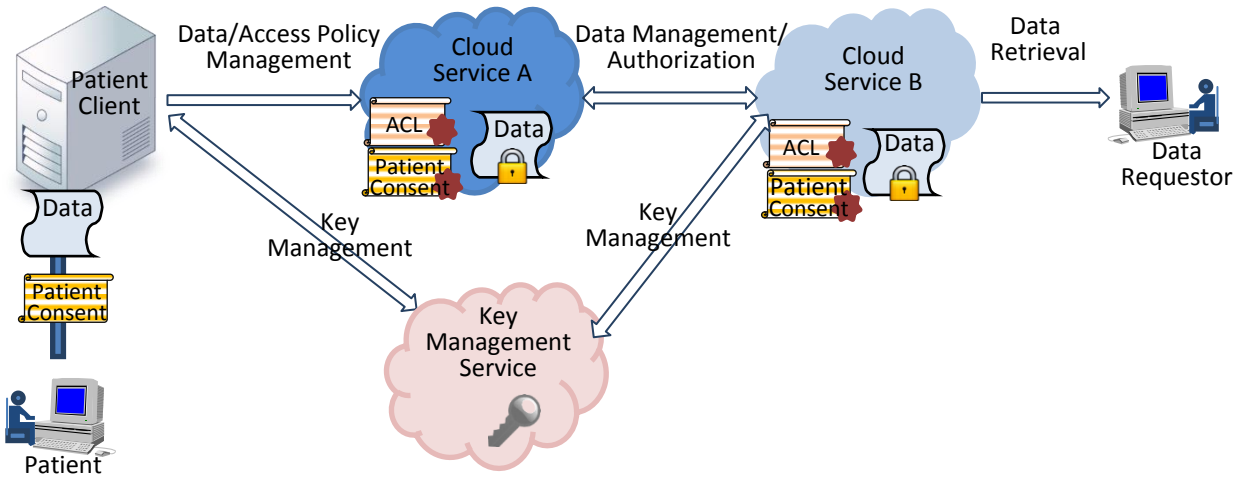

Figure 4. Health data protection use case with delegation of access control information

The main challenges of implementing this use case are establishing a trust relationship with Cloud Service B with respect to honestly enforcing policies and synchronizing access control information. More specifically, the patient client needs to be ensured that Cloud Service B completely adheres to access control information of the health data. Not adhering to the access control information can result from cyber-attacks or by deliberate actions of the cloud service. In addition, no standard protocol provides synchronization of access control information. For example, as soon as the patient updates his or her consent profile from Cloud Service A, the adjustment should be reflected in the patient consent profile that is stored on Cloud Service B.

8. Conclusions

This whitepaper presents a use case that provides functionalities to exchange health data across different cloud services. We showed how protecting health data against unauthorized access can be achieved. To implement this use case, a set of security and health care standards are considered for extending CDMI. We explained that CDMI could only partially address the data management requirements of the use case; thus, an extension should be considered to address the outlined requirements. The extension should be applied mainly on the definition of the metadata. In this way, the metadata should include the patient consent profile, signatures of access policies and patient consent profile, security labels, and the purpose of the access. In addition, the metadata should include information not only about the cloud service that stores data, but also about the cloud service that requests accessing the data.

References

[1] HL7 Website, http://www.hl7.org/implement/standards/fhir/security-labels.html , accessed 3/19/2015.

[2] M. Berry, N. Artz, "Privacy Consents and HIE," Journal of AHIMA, 2008.

[3] ITI Technical Committee, "IHE ITI Technical Framework Supplement-Internet User Authentication (IUA)," published by IHE International Inc., 2013, http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_IUA_Rev1-0_PC_2013-06-03.pdf, accessed 3/19/2015.

[4] ITI Technical Committee, "IHE ITI Technical Framework Supplement-Document Encryption (DEN)," Published by IHE International Inc., 2011, http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_IUA_Rev1-0_PC_2013-06-03.pdf, accessed 3/19/2015.

[5] ITI Technical Committee, "IHE ITI Technical Framework Supplement Cross-Enterprise User Authentication (XUA)," published by IHE International Inc., 2006, http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_White_Paper_CrossEnt_User_Authentication_PC_2006-08-30-2.pdf, accessed 3/19/2015.