# Hierarchical Privacy CAs for Cross-Border Transfer of Personal Data

Seira Hidano[1], Abdur Rahim Biswas[2], and Shinsaku Kiyomoto[1]
[1]KDDI R&D Laboratories
2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502 Japan
se-hidano@kddilabs.jp
[2]CREATE-NET, Trento, Italy

**Abstract**

The iKaaS (intelligent Knowledge-as-a-Service) platform integrates the data on multiple local cloud systems organically and provides the data to various types of applications as knowledge while taking security and privacy fully into account. However, access control on the iKaaS platform is not without complications because the application may access personal data in different countries from the one where the application exists. Hidano et al. thus designed a security gateway that is set at the entrance of each local cloud and controls access to the cross-border applications while interpreting regulations related to personal data for both countries. In order to help the security gateway confirm the validity of the application, they introduced the concept of the privacy certificate authority (CA), which is built for each country as an executive agency responsible for the national regulations governing the handling of personal data. In this paper, we design a hierarchical model of multiple privacy CAs responsible for regulations where the effective areas are different. The security gateway can thereby control the transfer of data not only to different countries, but also to different unions or cities.

**Keywords**: Data Transfer, Data Protection, Personal Data, Access Control, Security Policy

## 1 Introduction

The Internet of Things (IoT) paradigm is rapidly gaining momentum in modern wireless telecommunications. IoT devices, such as smart sensors designed to monitor temperature, pressure, and other environmental conditions, and wearable devices to measure an individual's state of health, generate vast amounts of time sequence data. These data are stored in the cloud and analyzed for useful information like personal preferences and to predict the environmental conditions surrounding people and the next action that people may take. The impact will increase if the heterogeneous data stored in multiple cloud systems can be organically integrated. However, vast quantities of potentially correlated data have not yet been analyzed in correlated contexts for a number of reasons. As the data obtained from IoT devices are mostly sensitive information related to an individual, namely, personal data, anxiety over security and privacy is an obstacle for the participation of users. A universal data model is also required for the analysis of the heterogeneous big data obtained from various types of sensors. Furthermore, there are legal considerations that further complicate matters. The compatibility of regulations related to personal data should be clearly addressed and handled. It is expected that with increasing trust, decentralized multi-cloud environments are about to unlock great potential for future data analysis [4, 5, 10, 11, 12].

The iKaaS (intelligent Knowledge-as-a-Service) platforms have been proposed as a way to resolve these problems [7]. On this platform, a global cloud is hierarchically built atop multiple local cloud systems that are set up in different countries. The global cloud organically integrates the data stored in the local clouds, and the integrated data are provided for various types of applications as knowledge. Security and privacy are controlled by a security gateway at the entrance to each local cloud. When using

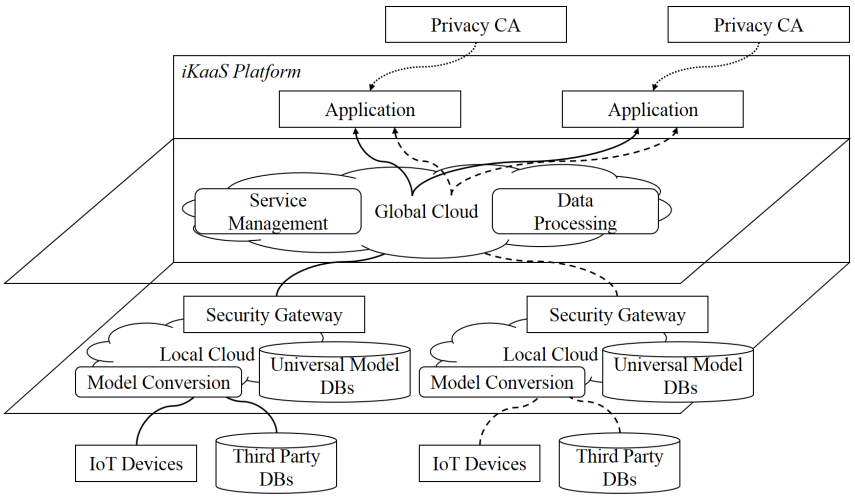


Figure 1: iKaaS platform.

the iKaaS platform, the application can access the data for different countries, conduct multiple-scale analyses, and compare different countries. On the other hand, if the application accesses personal data in different countries, the iKaaS platform must handle the data in accordance with the regulations governing personal data in both the country where the application exists and the country where the local cloud is set up. These regulations are complicated, and there are differences between countries. For instance, a Japanese act [9] permits the transfer of personal data to the EU while an EU directive [1, 3] does not permit the transfer of the data to Japan. Although there have been few technical studies on security and privacy for decentralized multi-cloud environments, these studies have not focused on privacy issues in relation to the cross-border transfer of personal data [6, 10]. In order to resolve this problem, Hidano et al. designed a security gateway to interpret the regulations in both countries that is capable of flexibly controlling the access permissions of the application while taking privacy into consideration [8]. In this model, the privacy certificate authority (CA) is built for each country as an executive agency responsible for the national regulations governing the handling of personal data. The security gateway refers the privacy certificate issued by the privacy CA in the country where the application exists and the security policy configured by the privacy CA in the country where the local cloud is set up, in order to interpret the regulations in both countries. However, Hidano et al. did not provide a way to configure access permissions for the applications of each union, city, or area. Since regulations for a union already exist, such as the EU directive stated above, and it is quite possible that, in the future, the regulations established for a city or another area for active utilization of personal data reflecting public attention in recent years, access control might become less flexible and thus less applicable to real cases.

The main contribution of this paper is to design a hierarchical model of multiple privacy CAs, which allows the iKaaS platform to be applied to cases involving multiple regulations related to personal data in the same region. The rest of the paper is organized as follows: Section 2 overviews the functional capabilities of the iKaaS platform and our contributions. Section 3 provides an architecture of hierarchical privacy CAs on the iKaaS platform and explains the cooperating functions. Section 4 describes the protocol whereby the application accesses personal data using the privacy certificate created by the hierarchical privacy CAs. Section 5 concludes this paper.

# 2 iKaaS Platform

Intelligent Knowledge-as-a-Service (iKaaS) is a concept model where the data accumulated on multiple local cloud systems are organically integrated into a global cloud, and the data are provided as knowledge while taking security and privacy into consideration. In this section, we present an overview of the iKaaS platform and the access control for cross-border applications on the iKaaS platform, followed by the contribution of our work.

## 2.1 Overview

Figure 1 shows the architecture of the iKaaS platform. The iKaaS platform encompasses a global cloud, multiple local cloud systems, IoT devices, and third party databases, which are hierarchically arranged. The multiple local cloud systems are established in different countries, such as in the UK and Japan, and each local cloud has databases for various types of data. The data are obtained not only from the newly available IoT devices, but also from existing databases designed for other purposes. The various data models converge into a universal data model before the data are stored in the databases in the local cloud. This resolves the issue where the models and formats of the data differ between local cloud systems. The global cloud has two functions: service management and data processing. When the application makes a request for information, the global cloud helps the application generate queries consistent with the objective. In order to realize this function, the global cloud has a catalog on the correspondence relationship between available services and the addresses of databases linked to the services. The global cloud not only deals with the raw data obtained from the local clouds but also processes the data statistically depending on the request. Massive-scale big data and heterogeneous data are combined and analyzed, and more useful knowledge is produced as a result [2]. However, the data that IoT devices extract are mostly sensitive information related to an individual, namely, personal data. There is also the case when the transfer of personal data to third parties is not permitted under the relevant regulations. The security gateway is thus arranged at the entrance to the local cloud and controls access by the application to the data with privacy and security considerations taken into account.

## 2.2 Access control for the cross-border application

Hidano et al. proposed a privacy privacy-conscious architecture centered on the security gateway for the iKaaS platform (see [8] for details). In this model, a security gateway is set at the touch point with the global cloud for each local cloud. The queries from the application and the data in the local cloud are all exchanged through the security gateway. The main function of the security gateway is to control access by the cross-border application under the regulations related to personal data both for the country where application exists and the country where the local cloud is set up. In order to realize this function in the model of Hidano et al., the privacy CA is built for each country as an executive agency responsible for the national regulations governing the handling of personal data. The privacy CA of the application side issues the privacy certificate to the application, and the privacy CA of the local cloud side formulates the security policy in the local cloud. When requesting access to the local cloud in a different country, the application presents the privacy certificate to the security gateway. The security gateway uses the privacy certificate to confirm that the application is capable of handling personal data in accordance with the national regulations in the country where the application exists, and refers to the security policy to determine whether to provide the data stored in its local cloud to the application on the basis of the national regulations in the country where the local cloud is set up. Additionally, access control involves the use of a token, which allows the process of the above verification to be omitted for the same application. This is because the verification process takes time, and the application may

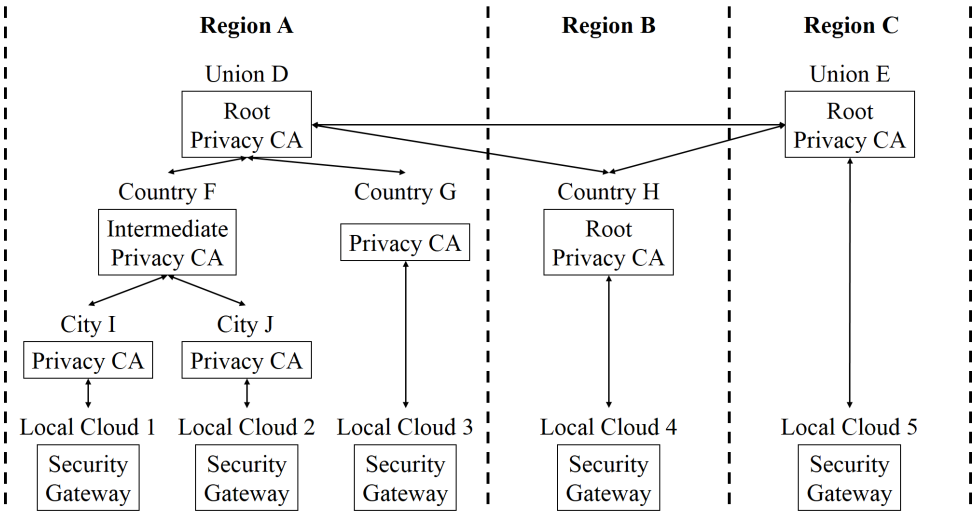


Figure 2: Architecture of hierarchical privacy CAs.

frequently request data at short intervals since the data are continuously transmitted from IoT devices.

### 2.3 Our contributions

The contributions of our work are the following:

- We designed a hierarchical model consisting of multiple privacy CAs. In this model, the privacy CA is built not only for each country but also for each regulation related to personal data. The privacy certificate is created by multiple privacy CAs in the same region where the application exists. In the case where there are multiple regulations hierarchically in a region, the security gateway can configure the access permissions for cross-border applications in the effective area of each regulation, such as a union like the EU, country, or city, simply by referencing a privacy certificate. Additionally, we introduce a way to add multiple signatures from privacy CAs to the application side of the privacy certificate, which are used by the security gateway to confirm the validity of the privacy certificate.
- We provide a way to distribute the public key of the privacy CA, which is used to verify the signature, to the security gateway. In the model by Hidano et al., the public key is sent directly from the privacy CA of the application side to the security gateway. This is not efficient because the privacy CA manages all security gateways in the different regions. In our model, the privacy certificate is passed from the application to the privacy CA of the local cloud side after the privacy CA of the application side adds the signature. That is, the public key of the privacy CA not of the application side but of the local cloud side is distributed to the security gateway. This method allows the privacy CA to avoid managing security gateways in other regions and reduces the number of security gateways that a privacy CA manages.

## 3 Hierarchical Privacy CAs

We propose a hierarchical model of multiple privacy CAs responsible for the different regulations governing the handling of personal data. In this section, we present the architecture of the hierarchical model, and then describe the cooperation among the privacy CAs.

### 3.1 Architecture of hierarchical model

Figure 2 shows the architecture for the hierarchical privacy CAs. The privacy CA is built for each area where regulations governing the handling of personal data are effective, such as a union like the EU, country, or city. Our hierarchical model is segmented into regions, and each region consists of three types of privacy CAs: the root privacy CA, intermediate privacy CA, and bottom privacy CA. The root privacy CA is responsible for regulations where the effective area is the largest in the region. If a union establishes regulations that are effective across the entire union, the privacy CA responsible for the regulations is the root privacy CA, like region A or region C in Figure 2. Each region has a root privacy CA. If there is no union in the region, or the union has no regulations related to personal data, and if the country has regulations, the privacy CA responsible for the national regulation is the root privacy CA, such as region B in Figure 2. The intermediate privacy CA is responsible for regulations where the effective area is smaller than for which the root privacy CA is responsible and larger than that for which the bottom privacy CA is responsible. There may be cases when multiple intermediate privacy CAs are built into different layers of the path continued from a root privacy CA to a bottom privacy CA. The bottom privacy CA is the privacy CA where the effective area is the smallest in the path. Each path has a bottom privacy CA. If there is no privacy CA in the lower layers from the root privacy CA, such as regions B and C in Figure 2, the root privacy CA also plays the role of the bottom privacy CA. The root privacy CA communicates with all root privacy CAs in the other regions and the privacy CAs in the one-level lower layer in the same region. The intermediate privacy CA communicates with the privacy CAs in the one-level upper layer and the one-level lower layer on the same path. The bottom privacy CA communicates with the privacy CA in the one-level upper layer on the same path and the security gateways in the area where its regulations are in effect.

### 3.2 Cooperation among privacy CAs

The privacy CA has two functions: the issuance of the privacy certificate to applications and the configuration of security policies referenced by security gateways:

**Issuance of privacy certificate.** The privacy certificate is used by the security gateway to confirm that the application is capable of handling personal data in accordance with regulations governing personal data. When receiving a request to access personal data in a different region from the application, privacy CAs of the region where the application exists determine whether the application can handle the personal data on the basis of their regulations, and then issues the privacy certificate to the application. In our model, the requirement is that the application is issued a privacy certificate by privacy CAs before requesting data in local clouds in a different region.

The privacy certificate is created in cooperation with the privacy CAs on the path from the bottom privacy CA that the application requests to the root privacy CA in the same region. After receiving the request from the application, the bottom privacy CA first checks whether the application satisfies the requirements to handle the desired personal data. If the application has no problem, an initial privacy certificate is created and passed to the root privacy CA via intermediate privacy CAs. In this process, the intermediate privacy CAs and the root privacy CA check the privacy certificate on the basis of their regulations. The security gateway can then confirm that the application is capable of handling the personal data in terms of all relevant regulations of the application side by using a privacy certificate.

The privacy certificate is composed of information in the application and the data and local clouds to which the application wants access. We present an example of parameters listed on the privacy certificate:

- *CA Names:* The names of the privacy CA that checked this privacy certificate.

- *Application ID:* The identifier of the application. On the security policy to which the security gateway refers, the access permissions are set for each application ID.
- *Application IP:* The IP address of the application. It may be used by the security gateway to authenticate the application.
- *App. Data Categories:* The types of data that the application deals with, such as location information, environmental information, health information, etc. Multiple values can be specified.
- *Expiry Date:* The expiry date of the privacy certificate.
- *Application PK:* The public key of the application. The key is used to verify the authenticity of the application when the security gateway issues a token to the application.

However, with just the above parameters, the security gateway cannot confirm that the privacy certificate is created by the correct privacy CAs. In order to resolve this problem, Hidano et al. introduced a method based on the signature of the privacy CA [8]. In this way, before issuing the privacy certificate to the application, the privacy CA generates the signature using its private key and adds it to the privacy certificate. Then, the security gateway verifies the signature using the public key of the privacy CA, which is distributed to the application in advance. We extend the method for our hierarchical model. In our model, all the privacy CAs that verify the privacy certificate adds their signatures to the privacy certificate. When passing the privacy certificate to the next privacy CA, the privacy CA send its public key as well. The next privacy CA generates the signature by encrypting the public key of the previous privacy CA using its private key. This process is repeated until the privacy certificate is passed to the root privacy CA of the application side, and then the privacy certificate is returned to the application. The security gateway can thereby verify the validity of the privacy certificate by using a public key of the root privacy CA. Additionally, we introduce the process when the privacy certificate is passed from the application to the root privacy CA in the region of the local cloud where the application wants access, although in the model of Hidano et al., the privacy CA of the application side did not cooperate with the one for the local cloud when creating the privacy certificate. The signature of the root privacy CA of the local cloud side is also added to the privacy certificate. This is because the method of distributing the public key to the security gateway directly by the privacy CA of the application side is not efficient as mentioned in Section 2.3. In our method, the privacy CAs of the local cloud side distribute the public key to the security gateway. This key distribution process is performed at the same time as the configuration of the security policy (see the next paragraph for details). The public key of the root privacy CA is also distributed to the other root privacy CAs in advance. On the privacy certificate, in addition to the above parameters, the following parameters are listed:

- *Signatures:* The signatures of the bottom privacy CA, intermediate privacy CAs, and root privacy CA of the application side, and the signature of the root privacy CA of the local cloud side.
- *CA PKs*: The public keys of the bottom privacy CA, intermediate privacy CAs, and root privacy CA of the application side.

Figure 3 is the data structure of the privacy certificate. The root privacy CA of the local cloud side also checks the privacy certificate on the basis of the regulations related to the transfer of personal data in its own area when receiving the request of its signature, and determines whether to provide the data that are classified to the categories specified by the parameter *App. Data Categories* listed on the privacy certificate. The only categories that the application can access are extracted from the categories specified by the parameter *App. Data Categories*, and listed on the privacy certificate as the values of the parameter *LC Data Categories*.

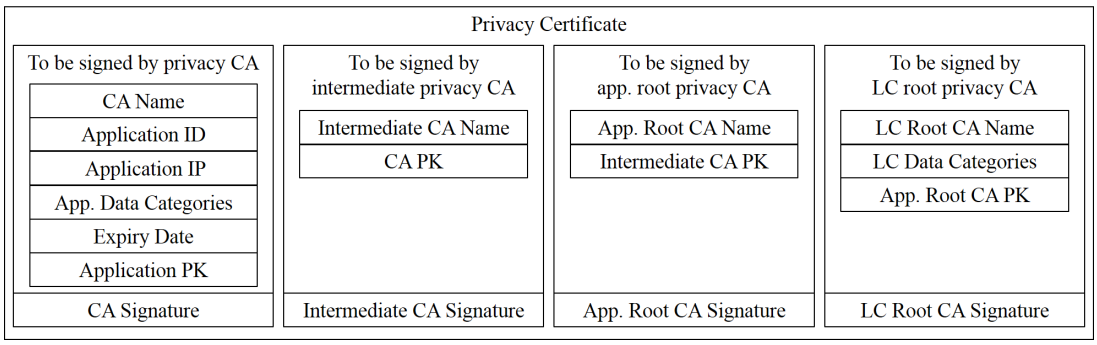


Figure 3: Data structure of privacy certificate.

Table 1: Security policy.

| Application ID | Data Category 1 | $\cdots$ | Data Category $N$ |
|---|---|---|---|
| 1 | 2 months | $\cdots$ | 0 |
| 2 | 3 weeks | $\cdots$ | 0 |
| $\vdots$ | $\vdots$ | $\ddots$ | $\vdots$ |

**Configuration of security policy.** The bottom privacy CA manages the local clouds with personal data in its own area. After adding the signature to the privacy certificate, the root privacy CA of the local cloud side informs the bottom privacy CAs of the values of parameters listed on the privacy certificate via the intermediate privacy CAs. Each bottom privacy CA configures the security policies of relevant local clouds on the basis of the information instead of the root privacy CA. Table 1 shows an example of the security policy. On the security policy, the expiry periods of the access permissions are defined. The expiry periods are set on the basis of the value of the parameter *Expiry Date* listed on the privacy certificate or from the viewpoint of security. At the same time, the public key of the root privacy CA of the local cloud side is also distributed to the security gateway via the intermediate privacy CAs and the bottom privacy CA. Cooperation among privacy CAs reduces the number of local clouds that a privacy CA manages, achieving the load distribution of the privacy CA.

# 4 Protocol for Cross-Border Data Transfer

When accessing data stored in a local cloud on the iKaaS platform, the application must present the privacy certificate to the security gateway of the local cloud. If the security gateway can confirm the validity of the application and the query by verifying the privacy certificate and the corresponding security policy, then the data are provided to the application. In this section, we describe the step sequences of two operations: the privacy certificate issuance and data access, while referring Figures 4 and 5.

## 4.1 Privacy certificate issuance

The privacy certificate is issued to the application in accordance with the following procedure:

1. An application requests the bottom privacy CA in its own area to issue a privacy certificate. The application then needs to specify the categories of data that it wants to access.

2. The bottom privacy CA creates an initial privacy certificate on the basis of the request from the application and the regulations in its own area, and then adds its name and the signature generated

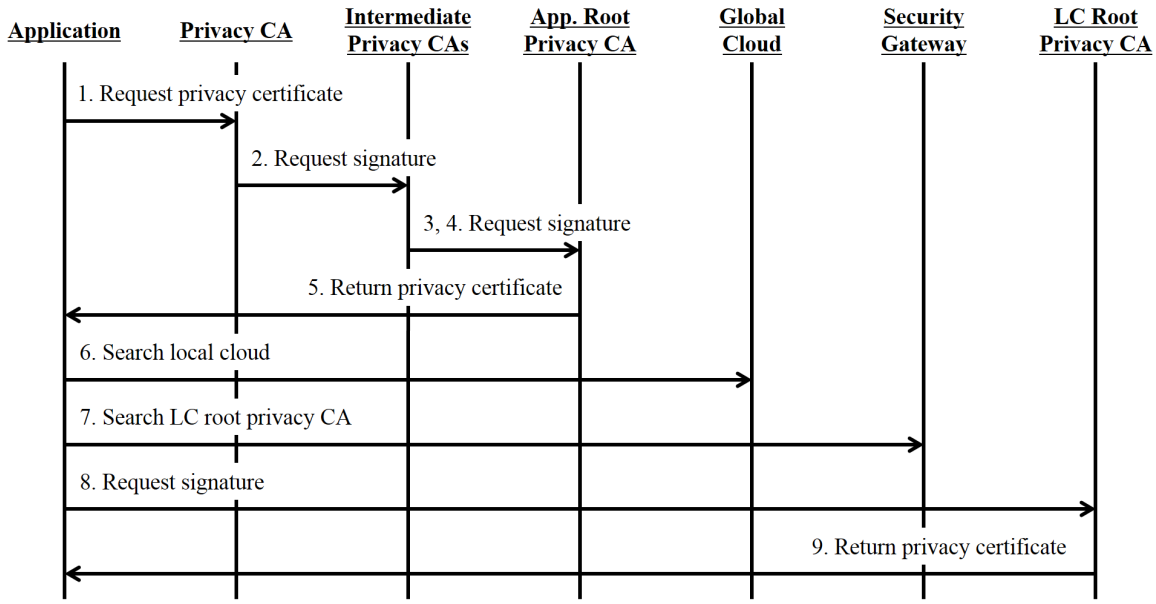


Figure 4: Step sequence of privacy certificate issuance.

with its private key to the privacy certificate. After adding its public key to the privacy certificate, the bottom privacy CA sends the privacy certificate to the intermediate privacy CA in the one-level upper layer on the path to the root privacy CA in the region.

3. The intermediate privacy CA verifies the privacy certificate on the basis of the regulations in its own area. If confirming that the privacy certificate has no problem, the intermediate privacy CA adds its name, the signature generated with its private key, and its public key to the privacy certificate. After that, the privacy certificate is passed to the intermediate privacy CA in the one-level upper layer.

4. Step 3 is repeated until the privacy certificate is passed to the root privacy CA in the region where the application exists.

5. The root privacy CA of the application side verifies the privacy certificate on the basis of the regulations in its own area, and adds its name and signature to it. It is returned to the application via the intermediate privacy CAs and the bottom privacy CA that the application requested to issue the privacy certificate.

6. The application finds the address of the security gateway of the local cloud storing data it wants to access by using the function of the global cloud on the iKaaS platform.

7. The application asks the corresponding security gateway the name of the root privacy CA in the region where the local cloud is set up.

8. The application requests the signature to the corresponding root privacy CA of the local cloud side to put its signature.

9. After selecting the categories that the application can access from the categories specified by the parameter *App. Data Categories* listed on the privacy certificate on the basis of the regulations in its own area, the root privacy CA of the local cloud side adds its name, the selected categories, the

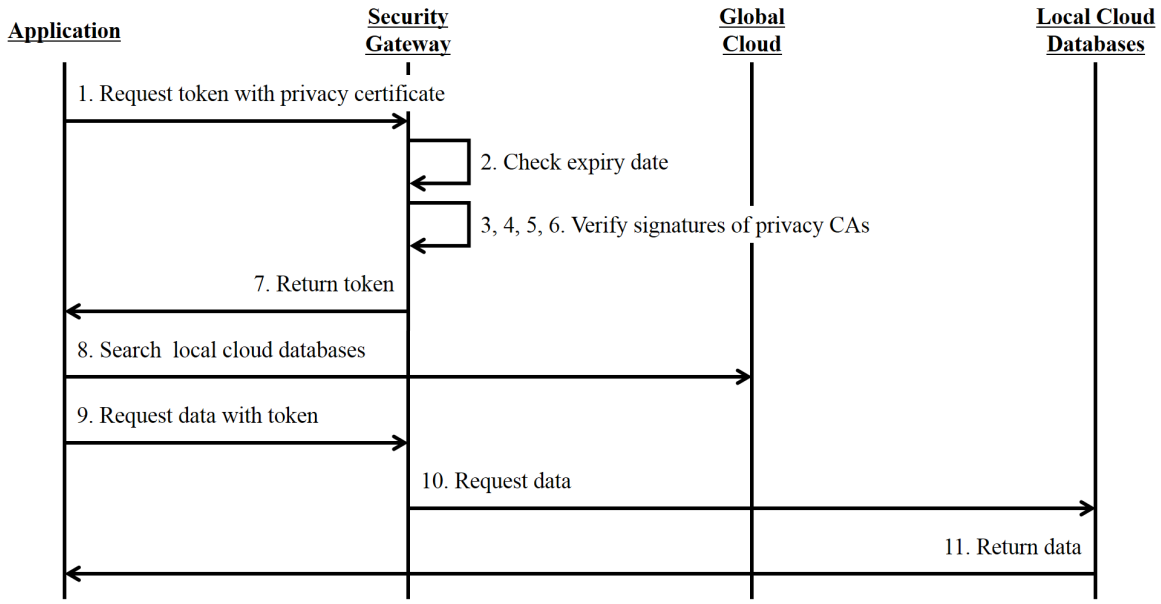


Figure 5: Step sequence of data access.

public key of the root privacy CA of the application side, and its signature to the privacy certificate. It is returned to the application. In addition, the root privacy CA of the local cloud side informs the bottom privacy CAs via intermediate privacy CAs of the parameters listed on the privacy CA, and then each bottom privacy CA sets the security policies in the relevant local cloud systems in its own area.

## 4.2 Data access

The application with the privacy certificate accesses data in the local cloud as follows:

1. The application sends the privacy certificate to the corresponding security gateway. The application then needs to specify the desired data categories.

2. After checking the value of the parameter *Expiry Date* listed on the privacy certificate, the security gateway verifies the signature of the root privacy CA of the local cloud side by using the public key of the root privacy CA distributed in advance.

3. The security gateway verifies the signature of the root privacy CA of the application side by using the public key of the root privacy CA listed on the privacy certificate.

4. The security gateway verifies the signature of the intermediate privacy CA in the one-level lower layer from the root privacy CA of the application side by using the public key of the intermediate privacy CA listed on the privacy certificate.

5. Step 5 is repeated until the security gateway verifies the signature of the bottom privacy CA of the application side.

6. The security gateway determines whether to provide the data classified into the requested data categories to the application by referencing the privacy certificate and the security policy.

7. The security gateway generates a token, encrypts it with the *Application PK* listed on the privacy certificate, and returns the encrypted token to the application.

8. The application confirms the information and the identifiers of the sensors to acquire the data that are classified into the categories specified by the parameter *LC Data Categories* by using the function of the local cloud.

9. The application decrypts the token with its private key, and sends a query including the identifiers of the desirable sensors to with the token to the security gateway.

10. After confirming the validity of the token, the security gateway sends the query to the databases in the local cloud on the basis of the sensor IDs specified in the query.

11. The security gateway acquires the requested data from the databases and returns the data to the application.

# 5 Conclusion

The iKaaS (intelligent Knowledge-as-Service) platform integrates data in multiple local cloud systems organically and provides the data as knowledge to cross-border applications. On the iKaaS platform, the security gateway set at the entrance of each local cloud controls the access of the application to personal data. We introduced a hierarchical model of multiple privacy certificate authorities (CAs) to the iKaaS platform. The privacy CA is built for each regulation related to personal data as its executive agency, and issues a privacy certificate to the application in cooperation with other privacy CAs. The privacy certificate is used by the security gateway to confirm that the application is capable of handling personal data in accordance with the regulations. Our hierarchal model allows the security gateway to configure the access permissions of the application for each union such as EU, each county, or each city. Additionally, we provided an efficient way to distribute the public key of the privacy CA, which is used to verify the privacy certificate, to the security gateway.

# Acknowledgments

The work is supported by the EUJ-1-2014 Research and Innovation action: iKaaS; EU Grant number 643262, Strategic Information and Communications R&D Promotion Programme (SCOPE), Ministry of Internal Affairs and Communications, Japan.

# References

[1] Article 29 Data Protection Working Party. Opinion 8/2014 on the on Recent Developments on the Internet of Things, 2014.

[2] A. Bantouna, G. Poulios, K. Tsagkaris, and P. Demestichas. Network load predictions based on big data and the utilization of self-organizing maps. *Springer Journal of Network and Systems Management*, 22(2):150–173, April 2014.

[3] EU. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 1995.

[4] EU FP7/ICT project 257115. OPTIMIS: Optimized Infrastructure Services. June 2010–May 2013.

[5] EU FP7/ICT project 287708. iCore: Internet Connected Objects for Reconfigurable Eco-systems. October 2011–September 2014.

[6] EU FP7/ICT project 609094. RERUM: REliable, Resilient and secUre IoT for sMart city applications. September 2013–August 2016.

[7] EU HORIZON 2020 project 643262. iKaaS: intelligent Knowledge-as-a-Service. October 2014–September 2017.

[8] S. Hidano, S. Kiyomoto, Y. Murakami, P. Vlacheas, and K. Moessner. Design of a security gateway for ikaas platform. In *Proc. of the 6th EAI International Conference on Cloud Computing (CloudComp 2015), Daejeon, South Korea, LNCS*, volume 167, pages 323–333. Springer-Verlag, October 2015.

[9] Japan. Act on the Protection of Personal Information. Act No. 57 of May 30, 2003.

[10] H. Meer, H. C. Pohls, J. Posegga, and K. Samelin. On the relation between redactable and sanitizable signature schemes. In *Proc. of the 6th International Symposium (ESSoS 2014), Munich, Germanym, LNCS*, volume 8364, pages 113–130. Springer-Verlag, February 2014.

[11] J. Poncela, P. Vlacheas, R. Giaffreda, S. De, M. Vecchio, S. Nechifor, R. Barco, M. C. Aguayo-Torres, V. Stavroulaki, K. Moessner, and P. Demestichas. Smart cities via data aggregation. *Journal of Wireless Personal Communications*, 76(2):149–168, May 2014.

[12] P. Vlacheas, R. Giaffreda, V. Stavroulaki, D. Kelaidonis, A. Somov, V. Foteinos, G. Poulios, A. R. Biswas, K. Moessner, and P. Demestichas. Enabling smart cities through a cognitive management framework for the internet of things. *IEEE Communications Magazine*, 51(6):102–110, June 2013.

---

## Author Biography

**Seira Hidano** received the B. Eng., M. Eng. and Dr. Eng. degrees in computer science and engineering in 2007, 2009 and 2012 from Waseda University, Tokyo, Japan. In 2010, he was a JSPS research fellow. In 2011 and 2012, he was a research assistant at Waseda University. In 2013, he joined KDDI. Since 2014, he has been a research engineer of the Information Security Lab. in KDDI R&D Laboratories. His research interest includes biometric authentication, information theoretic security, and privacy preservation.

**Abdur Rahim Biswas** (Dr.-Ing) is a Technical Group Leader at Create-Net, International research center, Italy. Dr. Rahim completed his Bachelor degree in Electrical and Electronics from Bangladesh Institute of Technology, Rajshahi in 2001 and Master's in Electronics and Telecommunications degree from University of Gävle, Sweden in 2005. In 2009, he received his Doctor degree in Electrical and Electronics engineering from Technical University Dresden. Currently, he is the project co-coordinator of H2020 WAZIUP (www.waziup.eu) and technical manager of H2020 iKaaS (www.ikaaS.com). He was also project manager of EU large-scale integrated project iCore (www.iot-icore.eu) for empowering Internet of Thing through cognitive technologies. He serves as technical working group leader of several EU projects and European cluster activities. His main research interests are Internet of Thing, Big Data, Short and Long Range Wireless Communication and Networking, Personal Data Privacy and Security. Dr. Rahim has more than 50 publications in conference, journal, book chapters.

**Shinsaku Kiyomoto** received his B.E.in engineering sciences and his M.E. in Material Science from Tsukuba University, Japan, in1998 and 2000, respectively. He joined KDD (now KDDI) and has been engaged in research on stream ciphers, cryptographic protocols, and mobile security. He is currently a senior researcher at the Information Security Laboratory of KDDI R&D Laboratories Inc. He was a visiting researcher of the Information Security Group, Royal Holloway University of London from 2008 to 2009. He received his doctorate in engineering from Kyushu University in 2006. He received the IEICE Young Engineer Award in 2004 and Distinguished Contributions Awards in 2011. He is a member of IEICE and JPS.