IIAI International Journal of Service and Knowledge Management
International Institute of Applied Informatics
2019, Vol. 3, No. 2, 35 – 47

Secure Architecture of Visible Light Communication System for Market Expansion

Shigeaki Tanimoto [*], Chise Nakamura [*], Motoi Iwashita [*], Shinsuke Matsui [*], Takashi Hatashima [†], Hitoshi Fuji [†], Kazuhiko Ohkubo [†], Junichi Egawa [‡], Yohsuke Kinouchi [§]

Abstract

Progress in visible light technology has provided increased opportunities for new mobile communication infrastructures and business creation using visible light communication (VLC). This paper proposes a secure business architecture for VLC market expansion through a combination of VLC technologies, public key cryptography, power line communication, and ID management technology. The proposed architecture provides the light source of an LED with an optical location authentication ID characterized by a strict location authentication that enciphers data using public key cryptography. The network between the server for distributing the optical location authentication ID and the LED light source enables high security using power line communication. In addition, scalability can be achieved securely by means of the ID management technology. The results of an evaluation clarified the suitability of this architecture for utilization in concrete business services. Used in combination with VLC, it will contribute to the market expansion of new business related to optical electronic value trading platforms, optical digital signage, and optical Fintech.

Keywords: Location Authentication, Optical Location Authentication ID, Visible Light Communication, Public Key Cryptography, ID Management

1 Introduction

The global trend towards environmental protection aimed at a low carbon society is prompting changes and advancements in the field of optical lighting. The systematic replacement of old incandescent lamps with light emitting diode (LED) electric light has enabled substantial

[*] Chiba Institute of Technology, Chiba, Japan
[†] NTT Secure Platform Laboratories, Tokyo, Japan
[‡] EXGEN NETWORKS Co., Ltd., Tokyo, Japan
[§] Tokushima University, Tokushima, Japan

power savings along with lower CO2 emissions. The utilization of LEDs in visible light communication (VLC) has also attracted attention, and new telecom infrastructures brought about thanks to cooperation with power line communication has emerged [1] – [4].

Mobile communication traffic generated by cellular and smartphone usage is increasing, so VLC has generated high interest. The amount of traffic related to mobile communications in 2016 was 18 times than that in 2011 and 2.6 times than that in 2014, and the demand for mobile communication is only expected to increase [5] – [6]. These trends have led to an increased interest in optical space communication using visible light for implementation in mobile communication. Moreover, the communication path can be seen as light, in contrast to radio waves, which is advantageous because the secure side of the information disclosure range can be limited to VLC.

The Visible Light Communication Consortium (VLCC) in Japan is now focused on standardization activities. A standard method for VLC was enacted by the Japan Electronics and Information Technology Industries Association (JEITA) in 2006 [7] A business architecture utilizing this method has been proposed, and communication infrastructure as a new source of VLC has been developed. For example, many broadcast services linked to locations, such as on-the-spot explanations of art museums and information distribution linked with digital signage, have been appearing [8] – [10]. However, these models do not have satisfactory security.

In light of this background, in this paper, we propose an architecture of secure VLC by attaching "optical location authentication ID" information to the light source (LED) of VLC in combination with public key encryption and ID management technology [11] – [13]. We provide the details of this architecture and evaluate its effectiveness through an examination of several concrete service cases.

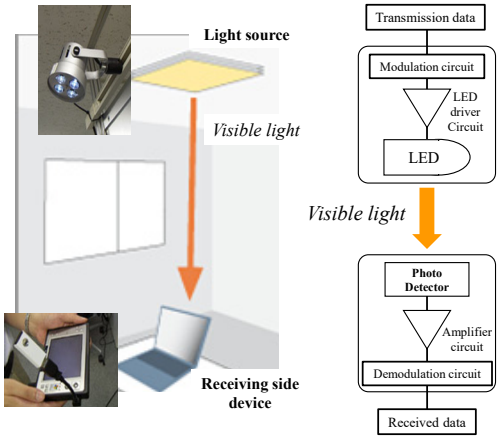
In the following, Section 2 of this paper goes over the problems facing the current VLC systems and business architectures and clarifies the necessity of a more secure design. We propose a secure business architecture using a VLC system in Section 3 and evaluate its effectiveness through an examination of concrete service cases in Section 4. We conclude in Section 5 with a brief summary and mention of future work.

2 Issues of Current Business Architecture with VLC

2.1 Current VLC Systems

As shown in Fig. 1(a), a typical VLC system performs data communication by means of rapidly blinking LEDs at a speed so fast that it cannot be perceived by the human eye [1] – [2]. VLC includes the transmission and reception of the characteristic data (ID) of a location and other relevant details.

As shown in Fig. 1(b), a digital modulation signal is placed on the spot where the area fixed by the light source is irradiated. Accordingly, IDs can be transmitted from a light source [8], [14].



(a) Image of VLC (b) Principle of VLC

Figure 1: Principle of data communications using VLC.

2.2 Issues of Current VLC Business Architecture

As shown in Fig. 2, the business architecture using VLC is a broadcast service linked to a location and is used for tasks such as on-the-spot explanations at a museum and information distribution linked with digital signage [8] – [10]. Security measures are largely unnecessary because the usage is small scale.

However, the use of location information for car navigation systems and GPS pedestrian navigation using mobile phones is rapidly spreading, and location information is becoming increasingly important [15]. This means that, even in VLC, examining security measures is crucial in terms of promoting business applications in the future. Incidentally, an international standard (ISO 15408, Common Criteria) is now used for computer security in software development [16] – [17]. Moreover, the concept of security-by-design, which considers the importance of how security is ensured right from the initial processes of the planning and design phases, has been proposed [18]. The aims of these proposals include reducing the cost of total security countermeasures and efficiently developing good software by investigating security countermeasures during the early stages of development.

From the above, the importance of considering security measures from the viewpoint of business architecture is clear. However, in the current VLC business architecture, this is not yet being done at a sufficient level.

(a) Spot explanation of the museum (b) Information distribution with signage

Figure 2: Typical business architecture using VLC.

3 Proposal of Secure Business Architecture using VLC

3.1 Requirement Specifications

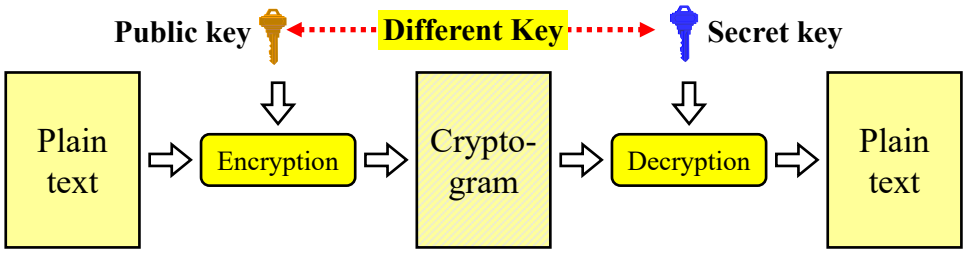
Here, we clarify the requirement specifications for implementing a VLC system into business. Obviously, the authentication function, the encryption function, and network security are indispensable here. Next, existing functions are used to reduce costs when introducing these functions. Table 1 lists the required specifications, which we briefly describe below.

Table 1: Requirement specifications and existing functions for VLC.

Requirement specifications	Corresponding existing function
Authentication function	・Public Key Cryptography ・Identity Management Technology
Encryption function	・Public Key Cryptography
Network security	・Public Key Cryptography ・Power Line Communication (PLC)

3.1.1 Public Key Cryptography

Public key infrastructure means the security infrastructure for a public key cryptosystem. As shown in Fig. 3, this technology enables various security countermeasures, such as encryption, digital signatures, and certification.



An enciphering key and a decryption key are different keys.

Figure 3: Public Key Cryptosystem.

3.1.2 Power Line Communication (PLC)

This type of communication refers to the technique of using a power line as a conduit for communication. Low-speed PLC uses frequencies of 450 kHz or less, and high-speed PLC uses frequencies of 2 to 30 MHz. In Japan, the Ministry of Internal Affairs and Communications revised a ministerial ordinance in October 2006 by adding an item that restricts indoor usage and that will accept 2–30-MHz frequency usage. Products corresponding to high-speed power line communication have been in distribution from December 2006 onward in response to this ministerial ordinance revision [19] – [20]. An example of PLC connected to a normal outlet is shown in Fig. 4 [20].

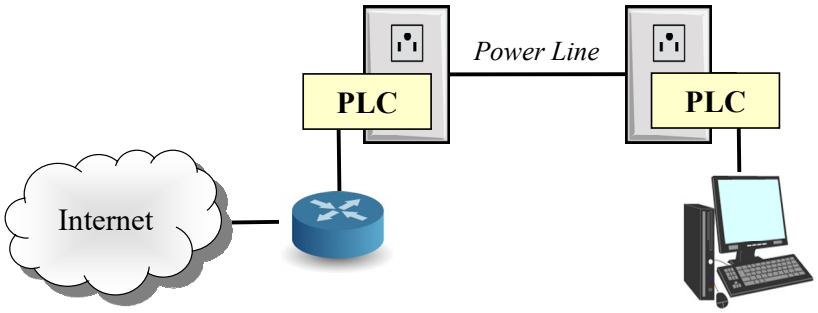
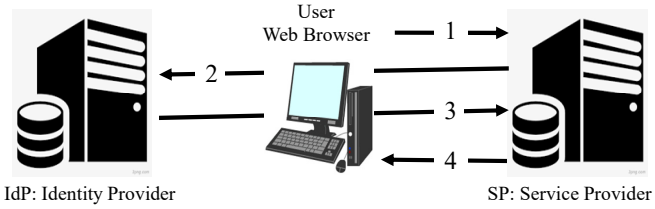


Figure 4: Usage pattern of PLC.

3.1.3 ID Management Technology

ID management guarantees the validity of the ID and provides a mechanism of access control (i.e., only people with the appropriate authority can gain access to need-to-know information). Combining the ID management infrastructure with the optical location authentication ID guarantees the validity of the optical location authentication ID and enables thorough control access by the administrator. As shown in Fig. 5, an ID management infrastructure using Shibboleth provides the system with a user ID and enables unified management of authority [21].

Using an ID management base among multiple organizations requires creating a policy for the operation management of the optical location authentication IDs. In addition, the structure of the operation (called a trust framework) has to be taken into account, including the audits for making this policy observed.



1. The SP detects the user attempting to access restricted content within the resource.
2. The SP generates an authentication request, then sends the request, and the user, to the user's IdP.
3. The IdP authenticates the user, then sends the authentication response, and the user, back to the SP.
4. The SP verifies the IdP's response and sends the request through to the resource which returns the originally requested content.

Figure 5: Example of ID management by Shibboleth [21].

3.2 Proposal of Secure Business Architecture of VLC

Here, we present a secure business architecture plan with functions that satisfy the requirement specifications shown in Table 1 for a VLC system [11]–[13].

3.2.1 Basic Architecture of Secure VLC

(1) Service flow from distribution of optical location authentication ID to user reception

Figure 6 shows how security is guaranteed by combining the new VLC system with 1) public key cryptography and 2) power line communication. Respective procedures for the service provision side and the user side are performed as follows.

(Location authentication Service Provider side (Fig. 6))

① Enter the optical location authentication ID corresponding to the location of the light source
② Create public key and secret key of the optical location authentication ID
③ Distribute the public key of the optical location authentication ID corresponding to the light source on the Web page
④ Encrypt the optical location authentication ID with the secret key corresponding to the light source (LED)
-> enc (optical location authentication ID, secret key)

(User side (Fig. 6))

⑤ Obtain the public key of the optical location authentication ID from the Web page
⑥ Decrypt the encrypted data received from the VLC system with the public key of the optical location authentication ID
-> dec (enc (optical location authentication ID, secret key), public key)

In this way, the user receives the optical location authentication ID and can access the service associated with it.

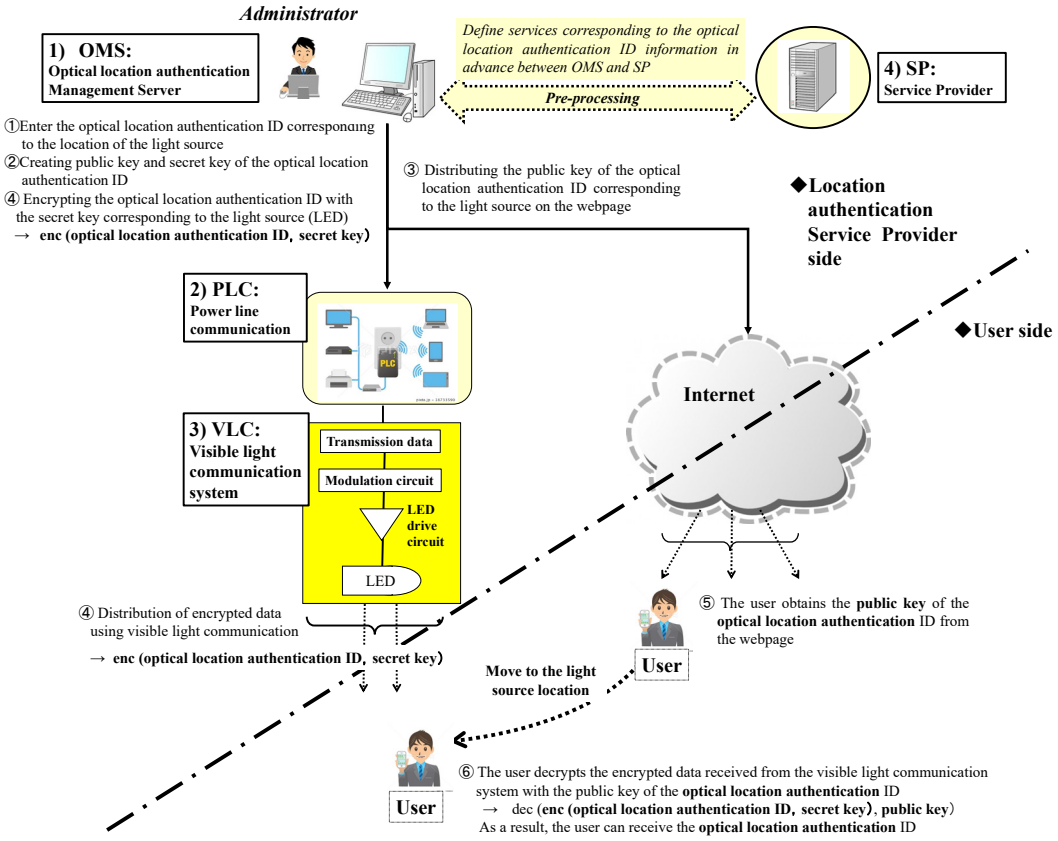


Figure 6: Basic architecture of secure VLC.

(2) Service utilization flow using optical location authentication ID

After receiving the optical location authentication ID, the user can use the service associated with it, as shown in Fig. 7. Hereinafter, we refer to the optical location authentication base as the optical location authentication service provider (OLASP).

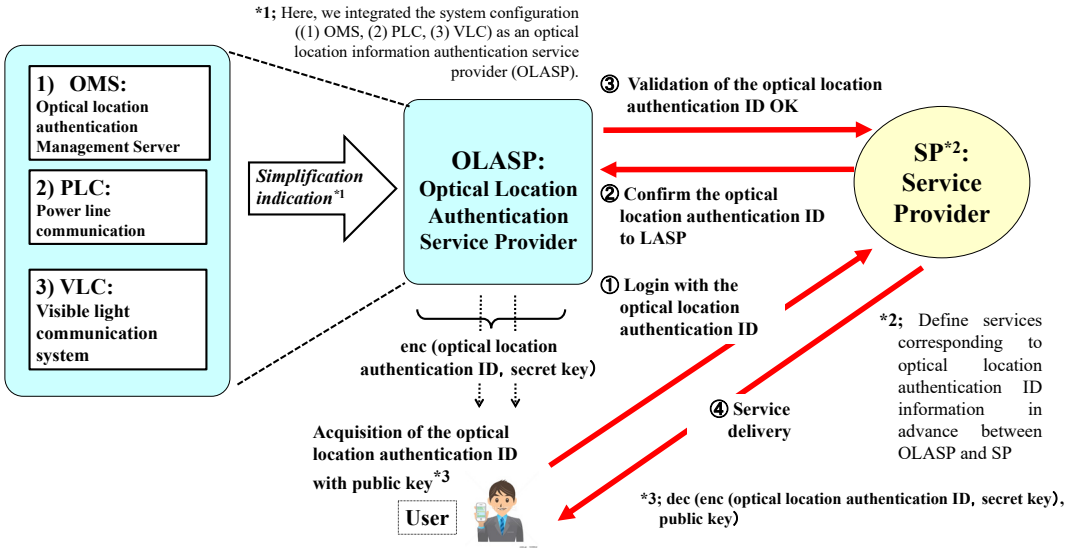


Figure 7: Service usage flow of basic architecture using optical location authentication ID.

3.2.2 Extended Architecture of Secure VLC

Sub section 3.2.1 clarified the basic architecture of the location authentication infrastructure using the optical location authentication ID for the light source. Here, we propose cooperation with ID management from the viewpoint of scalability of the optical location authentication infrastructure. From the viewpoint of the service extensibility, the optical location authentication infrastructure needs to be installed in many places (locations). In this case, multiple optical location authentication service providers (OLASP) in the basic architecture shown in sub section 3.2.1 are also generated in the optical location authentication infrastructure. Furthermore, in consideration of the scalability of the optical location authentication utilization service, management of these services is facilitated by using an intermediary between the OLASP and various service providers (SP).

In general, two ideas have been suggested for this intermediary: Idea 1) use of a certificate authority (issue digital certificate to optical location authentication ID) and Idea 2) use of ID management infrastructure [13]. In light of the strictness of the optical location authentication, using a certificate authority (Idea 1) is a superior idea. On the other hand, when users need to provide certificates, economic difficulties are incurred due to the cost of issuing certificates at the optical location authentication service provider side. Using the ID management infrastructure (Idea 2) centrally manages the optical location authentication ID by setting up the ID management infrastructure (described in sub section 3.1.3), so it is significantly superior to Idea 1 in terms of economic efficiency. Therefore, from the viewpoint of business, using the ID management infrastructure (Idea 1) is desirable as an extension of the optical location authentication ID [13].

(1) Service flow from distribution of optical location authentication ID to user reception

Figure 8 shows the extended architecture of the optical location authentication infrastructure using the VLC system utilizing the ID management infrastructure. A location authentication ID management infrastructure (LA_IDP) is newly provided as an ID management. In this case, the extension is as follows.

(a) Pre-processing

In advance, the OLASP registers the optical location authentication ID in the optical location authentication ID management provider (LA _ IDP).

(b) From distribution of optical location authentication ID to user reception

The service flow from the delivery of the optical location authentication ID to the reception of the user (Fig. 8) is the same as the basic architecture outlined in sub section 3.2.1.

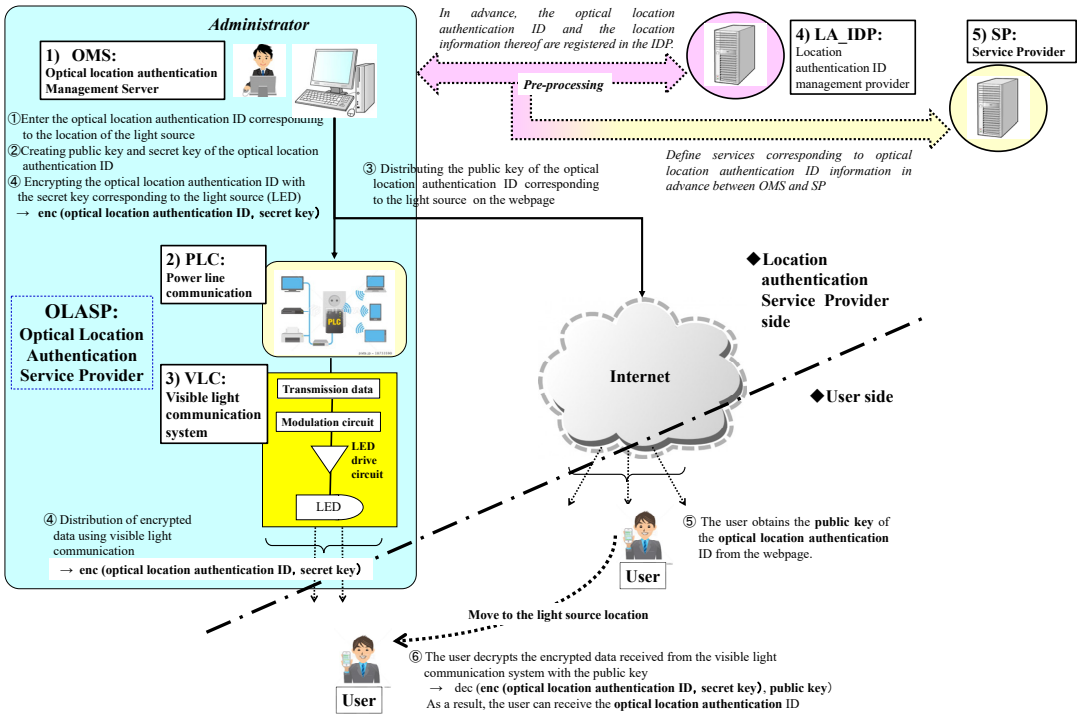


Figure 8: Extended architecture of secure VLC.

(2) Service utilization flow using optical location authentication ID

After receiving the optical location authentication ID, the user can access the associated service. An example of service utilization using the ID management infrastructure (LA_IDP) is shown in Fig. 9.

① The user logs in to the SP (in this case, SP *no.1*) by using the optical location authentication ID *no. i* in order to use the service.

② SP *no. 1* confirms the validity of the optical location authentication ID *no. i* with the optical location authentication ID management provider (LA_IDP).

③ From the optical location authentication ID management provider, the verification result ("OK" in this case) of the optical location authentication ID *no. i* is received.

④ SP *no. 1* provides the service to the user.

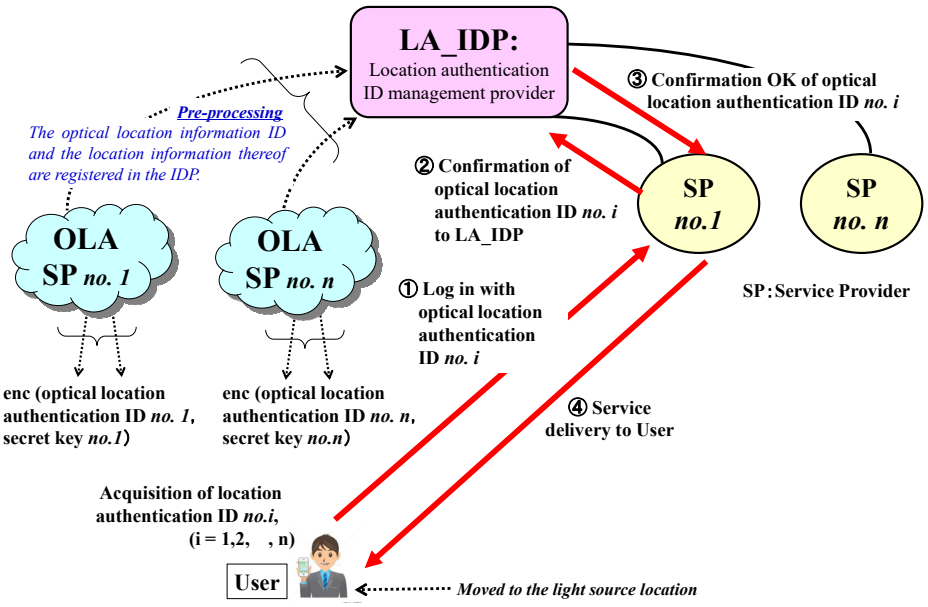


Figure 9: Service usage flow of extended architecture using optical location authentication ID.

3.3 Features of proposed business architecture

Sub section 3.2.1 clarified the basic architecture of the location authentication infrastructure using the optical location authentication ID for the light source. In sub section 3.2.2, we proposed cooperation with ID management from the viewpoint of scalability of the optical location authentication infrastructure.

As described above, the key feature of the proposed model is that the existing VLC system is linked with multiple existing secure technologies such as public key encryption, power line communication, and ID management. Specifically, as shown in Table 2, we added security functions to the conventional visible light communication system through cooperation with existing technologies. Furthermore, by distributing part of the authentication information (public key of the optical authentication ID) on the Internet, the expandability of the business of the visible light communication system is guaranteed.

Table 2: Features of the proposed model.

Viewpoint of modeling	Technical features	Application technology
Security guarantee	Strict identification of users by introducing ID management	Public key cryptography ID management infrastructure technology
	Limited information distribution of visible light communication recipients	Visible light communication technology
	Information circulation limited to power line communication network	Power line communication technology
Expansibility of conducting business	ID distribution by the Internet	Internet security technology

4 Use Case of Secure Business Architecture Using VLC

This section presents an evaluation of real operability with an application to actual business using the secure business architecture proposed in Section 3.

4.1 Use Case as a Business Architecture

As shown in Figs. 6 and 8, the proposed architecture improves on the conventional VLC system by enabling public key cryptography, power line communication, ID management infrastructure, and existing systems to cooperate. The key advantage here is that a strict location authentication infrastructure can be provided by means of the optical location authentication IDs. This is expected to promote various kinds of business creation and applications. In the following, we evaluate the proposed model on the basis of concrete business.

(1) B2C tourism industry
The optical location authentication ID and the public key cryptography technology can be applied to the tourism industry, where strict location authentication of users is possible. First, light sources can be installed in tourist spots. The light source is given an optical location authentication ID (Fig. 6 ①) and encrypted using a secret key (Fig. 6 ④). Next, the sightseeing spot associated with OMS distributes a public key (Fig. 6 ③) corresponding to the optical location authentication ID through its own Web page. Users (in this case, tourists) obtain the public key (Fig. 6 ⑤) from the Web page and visit the sightseeing spot. This allows them to receive their optical location authentication ID (Fig. 6 ⑥) from the light source using VLC.

In this case, linking the optical location authentication ID to tourists with discount tickets (electronic value) in the tourist spot enables the user to receive the intended benefits. In other words, added value (e.g., discount tickets) can be given exclusively to tourists who visit the tourist spots without fail, thereby improving the cost effectiveness of the tickets. In this way, the electronic value can be distributed only to specific users (in this case, tourists who obtain a public key after viewing the Web page).

In the same way, this concept can be applied to location authentication services for YouTubers by enabling rigorous location authentication. If YouTubers go to a specific sightseeing area and send locational proof, more reliable information can be sent, and the number of views can be expected to increase.

(2) The B2C advertising industry
Similarly, in the case of digital signage (where a sign is a light source), the security performance of a service provider can be improved by utilizing public key cryptography. In addition, the effectiveness of advertisements can be improved using digital signage because the system can strictly confirm that an intended user has come to the location of the digital sign.

(3) Optical Fintech
The proposed architecture can also be applied to Fintech. The new optical location authentication ID can be utilized as a base for distributing electronic value, as in the aforementioned tourist spots example.

(4) Other business applications
The following business adaptations are also possible.

- Education: A system for managing attendance. A light source for classrooms. Students are not allowed to attend unless they are actually in the class.
- Entertainment: Orienteering. The user can prove that he or she actually went to the designated spot by acquiring the optical location authentication ID of the light source set at various points.

4.2 Consideration

The key idea of the proposed model (as shown in Figs. 6 and 8) is that, by incorporating cryptographic technology into conventional VLC, it is possible to strictly specify which user visited the location of the light source. As a result, as shown in Section 4.1, it becomes possible to use B-C type business and even strict location authentication for electronic value distribution. In other words, by utilizing VLC, we can achieve a new electronic value distribution infrastructure (optical FinTech infrastructure).

Figure 10 shows the extendibility of the existing VLC business with this proposed architecture. Although qualitative, the results clearly show that business broadening by the extension of reliability based on strengthening the security function is possible.

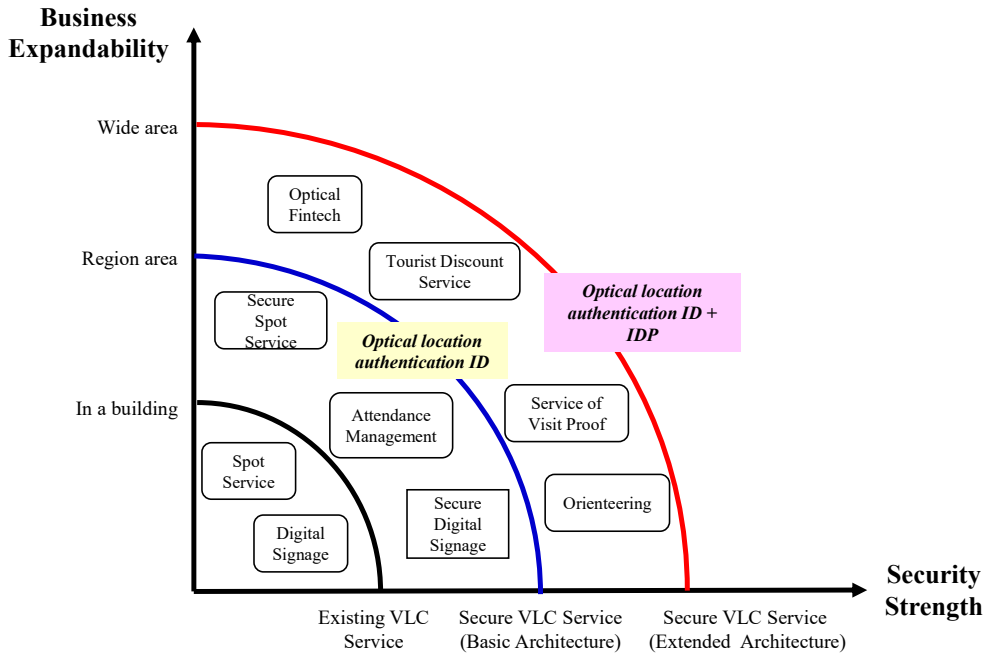


Figure 10: Scalability evaluation result of VLC business based on enhancement of security function.

5 Conclusion and Future Work

In this paper, in light of the ongoing spread of VLC development, we proposed a secure business architecture using our previously researched concept, “optical location authentication ID” information, by combining an ID management function with a location authentication infrastructure on the basis of multiple VLC systems. A qualitative comparative evaluation demonstrated that it is possible to construct a secure business model using this architecture.

In future work, we will evaluate the infrastructure in real-world situations using an actual system configuration. An accounting function will also be added for increased functionality.

References

[1] T. Komine, M. Nakagawa, Fundamental analysis for visible-light communication system using LED lights, IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, pp.100-107, FEBRUARY 2004

[2] L. Grobe, et al., High-Speed Visible Light Communication Systems, IEEE Communications Magazine, pp.60-66, Dec., 2013

[3] T. Komine and M. Nakagawa, Integrated System of White LED Visible-Light Communication and Power-Line Communication, IEEE Transactions on Consumer Electronics, Vol. 49, No. 1, pp.71-79, FEBRUARY 2003

[4] S. Shimada, Y. Takeda, Trends in Visible Light Communication and Application to ITS, Toshiba Review, Vol.64, No.4, pp.27-30, 2009, in Japanese

[5] H. Saini, LI-FI (LIGHT FIDELITY)-THE FUTURE TECHNOLOGY IN WIRELESS COMMUNICATION, Journal of Computer Application, Volume 7, No. 1, pp.13-15, January, 2016

[6] Psychic thought, The next "Li-Fi" coming after Wi-Fi - Relationship between Li-Fi and 5G in IoT era -, http://blog.livedoor.jp/utakknn/archives/2017-01-15.html, in Japanese, 2017

[7] Visible Light Communication Consortium, About a standard, http://vlca.jp/standard/, in Japanese, 2014

[8] Panasonic, Started business of information linkage service using "optical ID" technology, https://news.panasonic.com/jp/press/data/2015/12/jn151209-3/jn151209-3.html, in Japanese, in Japanese, 2015

[9] Nakagawa Lab., Inc., Products Information, http://www.naka-lab.jp/product/index_e.html, 2018

[10] K. Suzuki, Visible Light Communication System for Application to ITS, Toshiba Review, Vol.61, No.8, pp.20-23, 2006, in Japanese

[11] S. Tanimoto, et al., Concept Model of Electronic Value Trading Platform with Visible Light, Proceedings of LED synthesis forum 2018 in Tokushima, P-25, pp.157-158, 2018

[12] S. Tanimoto, et al., Proposal of Secure Business Architecture by Visible Light Communication System, Proceedings of 7th International Congress on Advanced Applied Informatics, pp.817-822, Yonago, July, 2018

[13] S. Tanimoto, et al., Secure Visible Light Communication Business Architecture Based on Federation of ID Management, Advances in Network-Based Information Systems, The 21st International Conference on Network-Based In-formation Systems (NBiS-2018), pp.

578–589, Springer, ISBN 978-3-319-98529-9, 2019

[14] H. Ueno, et al., Visible Light ID System, Toshiba Review, Vol.62, No.5, pp.44-47, 2007, in Japanese

[15] Y. Takahashi et al., The Study for the Position Authentication and the Security of Location Information, CSEC-38, pp.1-6, IPSJ, 2007

[16] ISO, ISO/IEC 15408-1:2009, https://www.iso.org/standard/50341.html

[17] S. Tsujii, Paradigm of Information Security as Interdisciplinary Comprehensive Science, Proceedings of the 2004 International Conference on Cyberworlds (CW'04), pp.1-12, 2004

[18] T. Kaneko, Introduction to security by design, https://www.ipa.go.jp/files/000055823.pdf, in Japanese, 2016

[19] Kobelco Systems, Internet connected to an outlet? ! -What is PLC (Power Line Communications) -, http://www.kobelcosys.co.jp/column/itwords/42/, in Japanese, 2007

[20] CNET Japan, Currently the "HD-PLC" communication standard using power lines, https://japan.cnet.com/article/35089788/, in Japanese, 2016

[21] Shibboleth, Component Interface, https://wiki.shibboleth.net/confluence/display/CONCEPT/Home, 2017