# Authentication Support Solution for Realizing Safe and Secure Society: Trust Eye

● Hideaki Sakatou ● Kouji Toyoshima ● Satoshi Yoshida ● Toshiaki Utsugi

**The recent development and diffusion of information and communications technology (ICT) has led to a dramatic increase in opportunities for acquiring, delivering, and utilizing information, regardless of whether those activities are done by individuals or organizations. Meanwhile, ICT is also used as "infrastructure" for large-scale and organized crimes such as cyber crimes and international terrorism, posing a significant threat to public security. In this situation, at an early stage Fujitsu started offering security products and services by gathering cutting-edge solutions from around the world to comprehensively provide the optimum combination and operation for each customer. Trust Eye, an authentication support solution, is a service that makes it possible to detect suspicious individuals using falsified official identification (ID) documents and prevent unauthorized use of official ID documents by authenticating such IDs. This paper outlines the Trust Eye products, services, and their authentication technologies. In addition, it describes activities and a future outlook for creating new businesses by making advanced use of official IDs and biometric authentication.**

## 1. Introduction

Information and communications technology (ICT) has advanced and diffused widely in recent years. It has created a new style of information flow, which the Internet exemplifies. This has made it significantly easier for individuals and organizations alike to acquire, deliver, and utilize information. Meanwhile, ICT is also used to develop "infrastructure" for large-scale and organized crimes (a platform to facilitate crimes) by cyber attack offenders and international terrorists, posing a considerable threat to public safety and security.

Against these backgrounds, the Cabinet decided in December 2013 to implement a strategy to make "Japan the Safest Country in the World."[1] Keeping the Tokyo 2020 Olympic and Paralympic Games in mind, the strategy proclaims to develop the nation into "the safest country in the world" through precise anti-crime measures, and ensure public safety through government-public cooperation, thereby fostering, nurturing and strengthening community bonds while advancing measures against new threats to public safety. Also, the 2013 amendments to the Act on Prevention of Transfer of Criminal Proceeds[2),3)] also reinforce the provisions on countermeasures for money laundering crimes, stipulating that financial institutions are obliged to ensure identify verification, retain transaction records, and report any suspicious transactions.

However, identity verification is mainly conducted visually at bank counters, by means of original or photocopied driving licenses, passports, and other official identification (ID) documents. In reality, the authenticity of such documents is not strictly checked. Meanwhile, the Prosecuted Crimes Committed by Visiting Non-Japanese Citizens 2014[4)] reports that forged passports, residence cards, and other ID fraud cases are on the increase.

Identity verification is also poorly executed with e-commerce, crowdsourcing and crowdfunding. Accounts can be easily created without strict identity verification in many cases, and the vulnerability of these service accounts is also becoming a social problem. All these suggest that the present identity verification practices are not enough to mitigate crimes (**Figure 1**).

Fujitsu's authentication support solution, Trust Eye, was developed in response to this situation. This

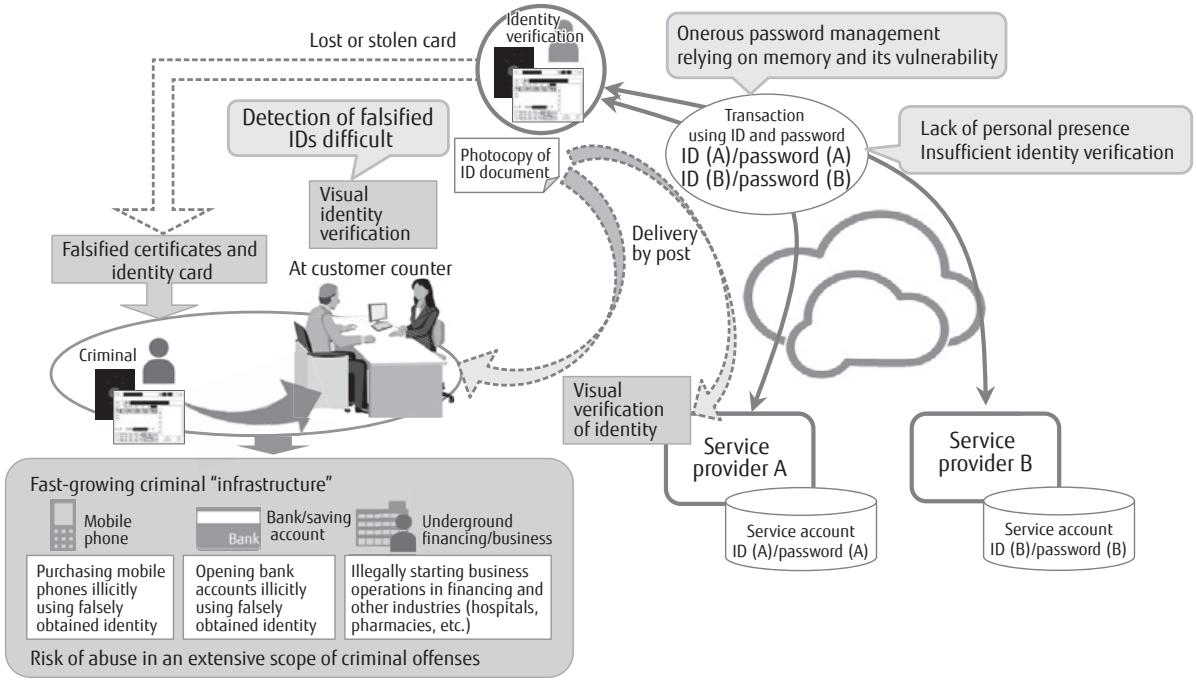


**Figure 1**
**Current status of identity verification.**

is a packaged solution designed to deliver various ICT-based services including official ID verification. It aims to enhance security at the point of customer contact, allow for secure ID card issuance, and facilitate safe and secure management of personal information that is required for identity authentication.

This paper explains Trust Eye in terms of its configuration and core technology. It also describes a project to leverage the solution to create new business opportunities.

## 2. Trust Eye configuration

Trust Eye comprises the following products and services offered in a package (**Figure 2**).

### 2.1 Trust Eye for BASE

This is a core package of Trust Eye designed to verify the authenticity of official IDs presented at the point of customer contact, in contexts like administrative applications, opening a bank account, and purchasing a new mobile phone contract. It employs public key infrastructure (PKI) to verify the official IDs against any forgery or illegal alterations.

Trust Eye can handle the following official IDs:

- IC-embedded passports (e-passport),
- IC-embedded driving licenses,
- IC-embedded residence card, and
- Individual number (referred to as "My Number" in Japan) cards (planned to be supported).

The package also includes biometric IC authentication features, using biometric information for activating IC-stored authentication data (the details can be found in the following section "3.2 Robust IC authentication leveraging biometrics").

### 2.2 Trust Eye for ID

This is an optional package designed to issue secure entering/exiting cards for access control after verifying the authenticity of the official IDs with Trust Eye.

The entering/exiting card has an embedded IC chip containing ID data coupled with biometrics, which prevents anyone other than the true owner of the card from using it. It also has an option for two-dimensional barcodes instead of IC chips for more cost-effective deployment.

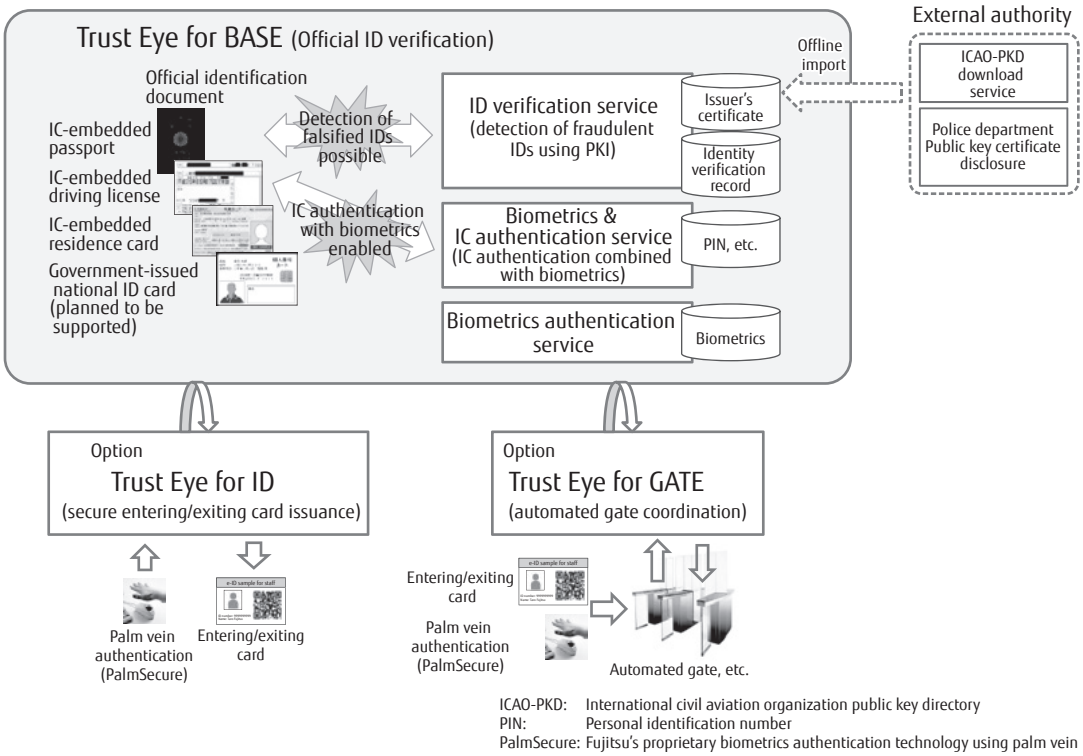


**Figure 2**
**Configuration of Trust Eye package products and services.**

## 2.3 Trust Eye for GATE

This is an optional package that allows the user to coordinate between secure entering/exiting cards and automated gates.

The secure entering/exiting card, verified with an official ID and combined with the card owner's biometrics, realizes very strict authentication and prevents illegal use by identity theft.

# 3. Trust Eye core technologies

We will describe two core technologies that represent Trust Eye's unique authentication features.

## 3.1 Detection of forged or modified official IDs leveraging PKI

With this technology, the digital signature stored in the IC chip embedded in an official ID can be loaded and verified for authenticity. This is done leveraging PKI, and it ensures that the personal identity information is not modified, and that the issuer is genuine.

We will explain this verification process below with an example of a passport (**Figure 3**).

1) Read the data stored in the official ID's IC chip.
2) Decrypt the digital certificate of the data with a public key, and obtain the hash value of this identity information. If the decryption fails, the digital signature may have been tampered with.
3) Recalculate the hash value of the obtained identity information.
4) Compare the hash values obtained in 2) and 3) above. If the hash values do not match, the identity information may have been tampered with.
5) Decrypt the public key with the root certificate acquired from the issuing authority, and obtain the hash value of the public key. If the decryption fails, the public key's certificate may have been tampered with.
6) Recalculate the hash value of the public key.
7) Compare the hash values obtained in 5) and 6) above. If the hash values do not match, the public key certificate may have been tampered with.

This method draws on the attribute of public key encryption that information encrypted with a secret key can only be decrypted using the public key that is

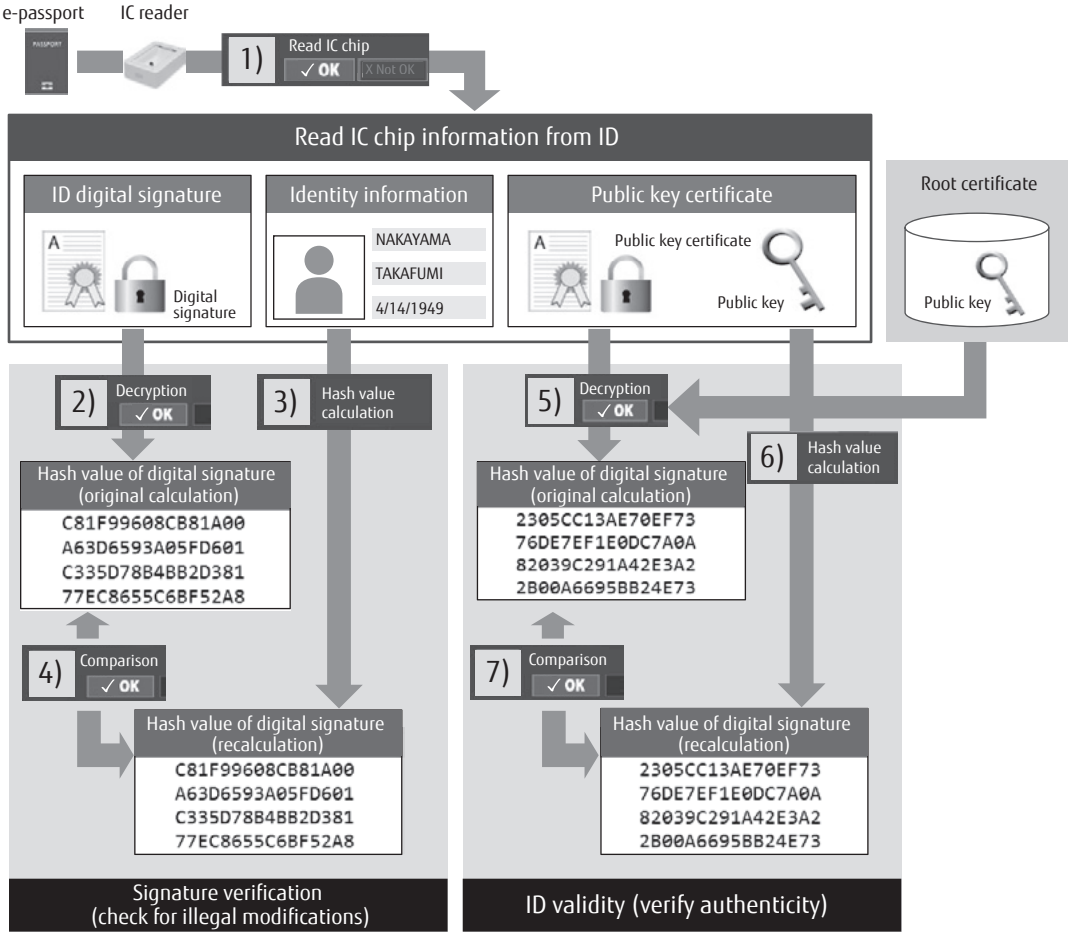


**Figure 3**
**Processes of falsified card detection.**

paired with the secret key. Therefore, successful decryption with a public key signifies that the information was encrypted with a paired secret key. Thus, PKI verification can detect falsified ID documents with 100% accuracy, provided that the official ID issuers appropriately manage their secret keys, protect them from theft and leaks, and also maintain their encryption strength at an appropriate level.

## 3.2 Robust IC authentication leveraging biometrics

Instead of entering a personal identification number (PIN) to read the data in the IC chip on official IDs, Trust Eye employs Fujitsu's proprietary biometrics authentication technology using palm vein (PalmSecure). **Figure 4** illustrates this robust IC authentication system based on biometric information.

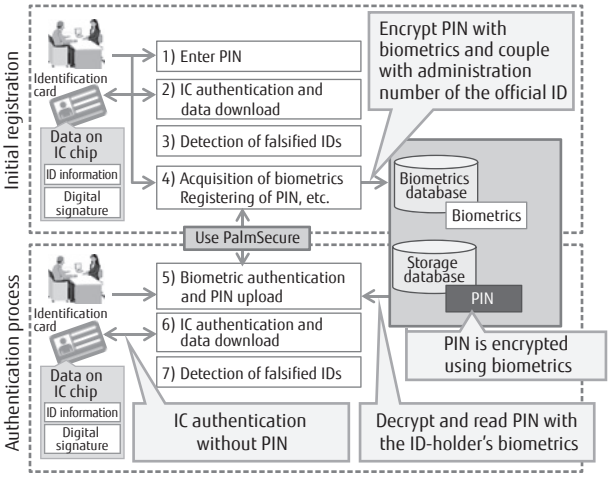


**Figure 4**
**IC authentication coupled with biometrics.**

After the initial registration of a PIN and biometrics to associate with the administration number unique to the official ID, a user does not need to enter the PIN again because the IC chip is read using the ID's administration number and the user's biometric information. The PIN is recorded and stored in a safe and secure manner; it is encrypted and decrypted using an encryption key which is generated from the biometrics of the ID holder. This will help to solve the vulnerability issue of PIN management being based on user's memory or memorandums, and improve security and utility of the authentication system.

Figure 4 illustrates the IC authentication processes.

- Initial registration

1) Register a PIN for reading the IC chip embedded in the official ID.
2) Authenticate the IC using the PIN entered, and read the information stored on the IC chip.
3) Based on the information read from the IC chip, verify the official ID's authenticity.
4) After successful verification, the ID holder's biometric information is obtained and used to generate an encryption key. The PIN is encrypted using this key, and linked to the ID's administration number before being saved in the database.

- Authentication process

5) Read the ID holder's biometrics and verify the person's identity. Then decrypt the PIN associated with the ID administration number, and obtain the PIN.
6) Authenticate the IC using the PIN obtained, and read the information stored on the IC chip.
7) Based on the information read from the IC chip, verify the official ID's authenticity.

It should be noted that biometric readings typically fluctuate, and every reading may yield a slightly different pattern. This has been the problem that makes biometrics unsuitable for generating encryption keys. Trust Eye has overcome this problem by incorporating the authentication process into a system that ensures the reading of biometrics will find an identical pattern in a set of pre-registered biometric data.

## 4. Application in business contexts

This section introduces some cases of Trust Eye applied in a business context.

### 4.1 Ascertaining identity verification at point of service

This is the most basic point for Trust Eye application. The ID verification and detection of falsified ID documents helps to prevent criminal abuse by impersonators and identify suspicious individuals. It enhances the accuracy of identity verification at the point of service, where accurate verification is crucial.

Trust Eye can be employed for identity verification in the following contexts of customer services:

- Bank counters for opening a new account,
- Telecoms and telephone shops for purchasing a new contract for data access devices and/or mobile phones,
- Ticket shops for purchasing tickets that require identity verification,
- Companies for hiring foreign workers,
- Hotel receptions for checking in,
- For receiving a government-issued national ID card, and
- For collecting a parcel from a post office.

### 4.2 Building entering/exiting control coordinated with biometrics authentication

With a combination of an ID card issued upon accurate identity verification, and strict identity authentication utilizing biometrics authentication technology, Trust Eye's optional features offer support for robust, safe and secure building of an access control system that only allows persons holding an authenticated ID card to enter/exit the controlled area.

Possible application cases for access control with identity authentication are as follows:

- Sporting event venues and other facilities where entry/exit of personnel is controlled (e.g., by volunteers),
- Access to high-security venues such as international state-head conferences and governmental offices,
- Public facilities and event venues, and
- Public infrastructure premises (e.g., electricity, gas, water utilities).

## 5. Discovering new business opportunities and expected performance

In view of the above-mentioned features and contexts in which Trust Eye can be applied, we are endeavoring to create new business opportunities.

We introduce a case as an example, and describe the expected performance. This is a project to deploy Trust Eye in a venue for international sporting events. In this context, the service needs to adapt to a non-fixed and transient group of people; for example, a flux of temporary volunteer members as well as foreign visitors.

The deployment of many volunteers necessitates the personal identity verification of participating volunteers at reception, and biometric authentication during the event. These make it easier to manage a large number of people in a short period of time, and to organize the event safely and securely. This requires efficient, accurate and strict identity authentication. Trust Eye makes it possible to set up a highly reliable authentication system in a short period of time, at a reasonable expense.

Foreign visitors may be issued with visitor cards as temporary ID documents that contain immigration data or passport information combined with their biometric information. This will contribute toward the visitors' security during their stay and maintaining public safety. It can also be used with various services such as long-stay accommodation, rentals, and duty-free shops for accurate identity verification.

## 6. New possibilities with Trust Eye

As Japan's individual number system started in January 2016 and gradually expands its scope of application, not only the administrative offices, but also the private sector will need to take actions to adapt to the scheme. In adopting the individual number card, in particular, the combination of Fujitsu's integrated authentication platform (integrated IDs and biometric authentication databank) and Trust Eye together will offer administrative institutions and private corporations alike, a considerable benefit in cost-saving as well as security risk management (**Figure 5**). We will work to further diffuse Trust Eye from within the Fujitsu Group to the governmental and private sectors as well as to consumers.

In the following, we discuss prospects for new businesses to apply Trust Eye.

1) Administrative management under natural disaster and emergency situations

Trust Eye will help with the identity verification of disaster victims even if they have lost their official IDs or forget the PINs, thereby facilitating accurate and

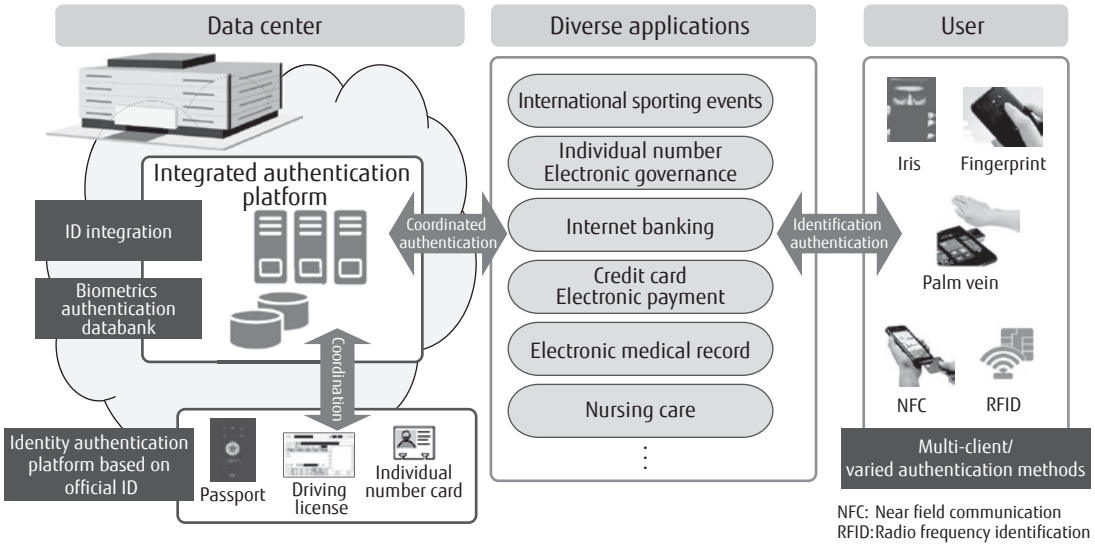


**Figure 5**
**Smart society through integrated authentication platform.**

reliable administrative work to provide emergency aid and medical support, issue damage certificates, and work on post-event administration.

2) Anti-crime measures in public institutions

Trust Eye will provide affordable and reliable access control at nurseries, schools, hospitals and offices of local governments, thereby helping them to pursue anti-crime measures and prevent possible offenses such as kidnapping and privacy invasion.

3) Application to medical and nursing care

Trust Eye can be employed to verify the identity of elderly people and address typical problems associated with them, such as aimless wandering due to senile dementia, ensuring medications, recalling medical history at times of medical emergency, locating carers at times of natural disaster, and even controlling illegal claims for pensions and social security.

4) Enhancing the protection of expatriates

With Trust Eye, information about expatriates, which has so far been managed separately from the information about residents in Japan, can be shared seamlessly between the Ministry of Foreign Affairs and Japanese local governments. Expatriates can be swiftly identified under emergency situations such as a dispute. This will help to significantly expedite administrative processes when, for example, an emergency evacuation is needed. It will also liberate travelers and expatriates from the need to carry passports and reduce the risk of losing them.

These are some examples of possible business opportunities that suggest the wide scope of applicability of Trust Eye as the service continually develops.

It is undeniable that there will be concerns regarding such highly technical services being centrally managed under government or administrative offices. The service providers need to have high standards of morals, equality and impartiality as well as to implement robust security measures. Therefore, Fujitsu believes it is important to provide technology that helps meet these requirements so that people can use the services securely and easily with peace of mind.

## 7. Conclusion

This paper outlined Trust Eye, which forms a part of Fujitsu Security Initiative[5] "Common/Business Applications (authentication, access control and ID management)," and described the initiatives for creating new business opportunities as well as future prospects regarding this service.

We will continue our endeavor to develop packaged solutions that make customer services better, securer and richer by leveraging ICT, and contribute towards a sustainable growth.

## References


1) The strategy to make "Japan the Safest Country in the World" (in Japanese).
*http://www.kantei.go.jp/jp/singi/hanzai/kettei/131210/honbun.pdf*
2) National Police Agency etc.: The Act on Prevention of Transfer of Criminal Proceeds (in Japanese).
*https://www.npa.go.jp/sosikihanzai/jafic/pdf/leaf20130401.pdf*
3) National Police Agency: The Act on Prevention of Transfer of Criminal Proceeds Outline (in Japanese).
*https://www.npa.go.jp/sosikihanzai/jafic/hourei/data/filowcls20160101.pdf*
4) National Police Agency: Prosecuted crimes committed by visiting non-Japanese citizens 2014 (in Japanese).
*https://www.npa.go.jp/sosikihanzai/kokusaisousa/kokusai/H26_rainichi.pdf*
5) Fujitsu: Fujitsu Organizes Security Products and Services under New FUJITSU Security Initiative.
*http://www.fujitsu.com/global/about/resources/news/press-releases/2014/0120-01.html*



**Hideaki Sakatou**
*Fujitsu Public Solutions Ltd.*
Mr. Sakatou is currently engaged in the development of packaged solutions in general, and of business solutions for local governments.



**Kouji Toyoshima**
*Fujitsu Public Solutions Ltd.*
Mr. Toyoshima is currently engaged in the planning and sales promotion for Trust Eye.

**Satoshi Yoshida**
*Fujitsu Public Solutions Ltd.*
Mr. Yoshida is currently seconded to Fujitsu Security Initiative Center, and engaged in the planning and sales promotion of various solutions, including Trust Eye.

**Toshiaki Utsugi**
*Fujitsu Public Solutions Ltd.*
Mr. Utsugi is currently engaged in the development of Trust Eye and other packaged solutions.