Public Biometrics Infrastructure (PBI)

–Authentication Technology for Digital Identity –

Kenta Takahashi

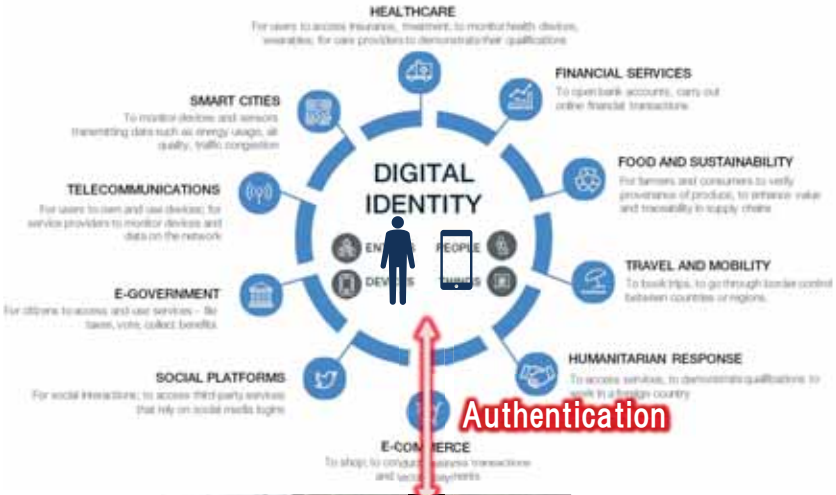
Ph.D. (Computer Science)
Senior Researcher, Research & Development Group, Hitachi, Ltd.

Contents

New Era of Digital Identity

HITACHI
Inspire the Next

"Authentication" is the trust anchor of Digital Identity



Digital World

Digital Identity

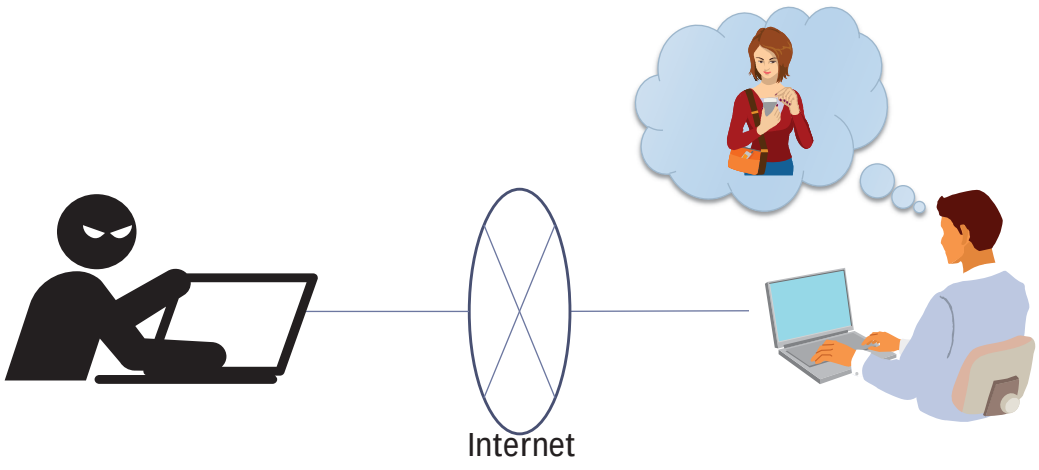
Entity
(Humans, Things,
Organizations, etc.)

Real World

Difficulties of Online Authentication

HITACHI
Inspire the Next

On what basis can we know the subject online is genuine?
All you can receive is just digital data that may be forged or falsified.

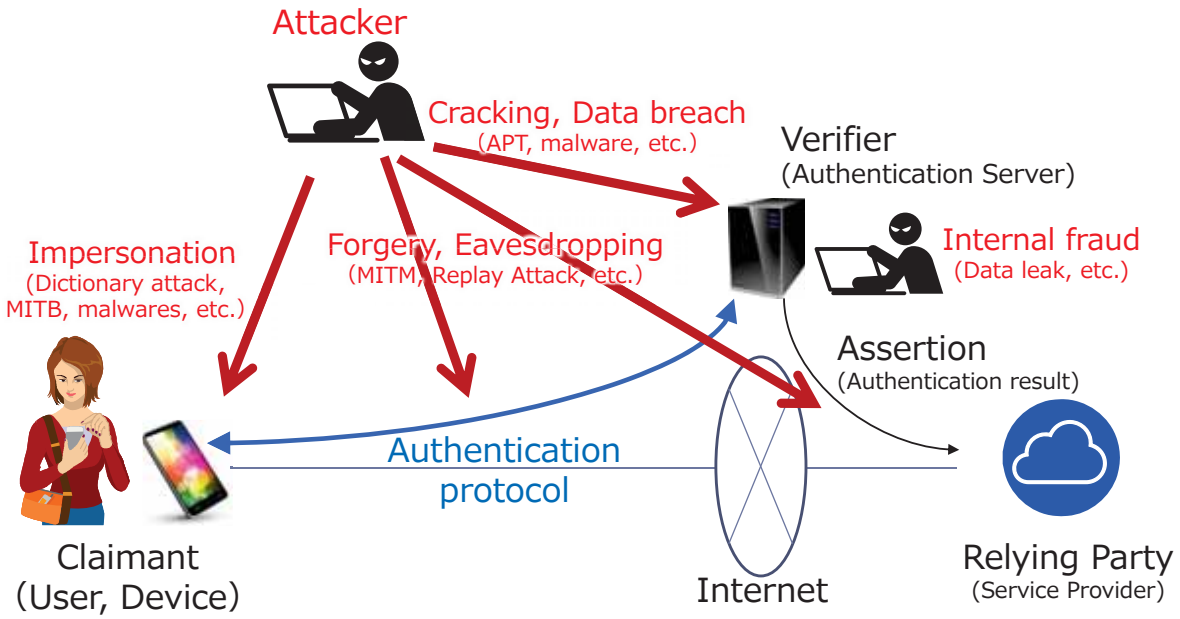


(c)New Yorker, 1993.

Difficulties of Online Authentication

HITACHI
Inspire the Next

Need security measures against every attack.

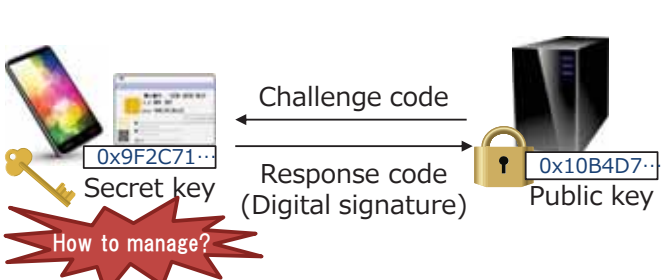


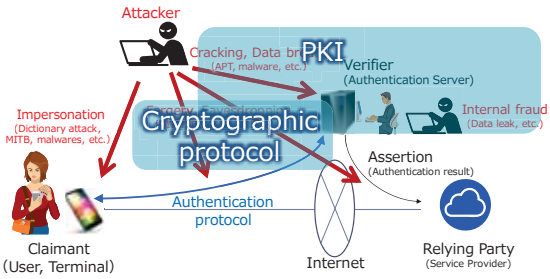
Authentication of Things

HITACHI
Inspire the Next

**Cryptographic protocols are secure against most online attacks.
The challenge is *key management*.**

- Typically based on Public Key Cryptography (PKC)
  - A thing holds a secret key. A verifier checks it's knowledge with a public key.
  - Examples: PKI, SSL, FIDO, My Number Card (in Japan)
- Pros ☺
  - Secure against most online attacks.
  - By publishing the public key, the entity can be authenticated by any verifier.
- Cons ☹
  - The security depends largely on the secret key management.
  - TPMs or TEEs are required to protect the secret keys.





PKI: Public Key Infrastructure, SSL: Secure Socket Layer, FIDO: Fast IDentity Online,
TPM: Tamper Proof Module, TEE: Trusted Execution Environment

Authentication of Humans

HITACHI
Inspire the Next

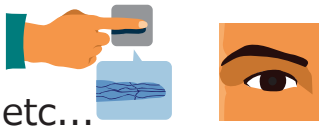
■What you know:

- Password, PIN
- ☺ Low initial cost. Suitable for confirmation of intent.
- ☹ Easy to be forgotten or guessed.

■What you have :

- Authentication of Things possessed by the user.
- Smart card, Hardware token, Smartphone
- ☺ Secure against many online attacks if appropriate cryptographic protocols is used.
- ☹ Easy to be lost or stolen.

■What you are:

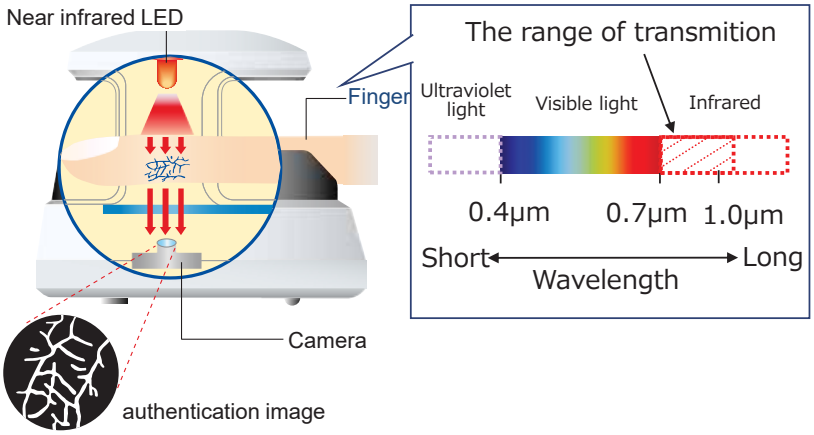


- Biometrics such as fingerprint, face, iris, vein, etc...
- ☺ Never be lost or forgotten.

Hitachi Finger Vein Biometrics Technology

HITACHI
Inspire the Next

An authentication technology developed by Hitachi, which identifies individuals by images of vein patterns obtained by transmitting light (near infrared) through fingers



Balanced precision *
- False Rejection Rate(FRR) 0.01%
- False Acceptance Rate(FAR) 0.0001%
- Failure To Enroll Rate(FTER) <0.03%

Feature

◆ Difficult to forge or tamper
(due to making images from the blood flow pattern of the living body)

◆ Quick authentication/Easy registration/Excellent operability

* 1 : 1 Measured value at certification. Accuracy calculated using the measurement method based on the international standard ISO / IEC 19795-1 for accuracy evaluation of biometrics。
FRR=False Rejection Rate、FAR=False Acceptance Rate、FTER=Failure to Enrol Rate

Challenges in Biometric Authentication

HITACHI
Inspire the Next

Biometric information is an unchangeable key.
The challenge is *biometric data management*.

(1) **Security & Privacy Issues**
- Biometric characteristics such as fingerprints can't be updated like passwords.
- Biometric data breaches cause serious problems of security and privacy.
- Server-side storage requires careful management of risks including internal fraud.

(2) Scalability & Cost Issues
- Server-side biometric authentication systems require operational cost to manage biometric data strictly.
- Client-side authentication systems (e.g., smartphones) require TPM or TEE to protect biometric data.

(3) Interoperability Issues
- Standard authentication protocols (*) such as of PKI is necessary to apply biometric authentication to existing online services, that require secret key management.

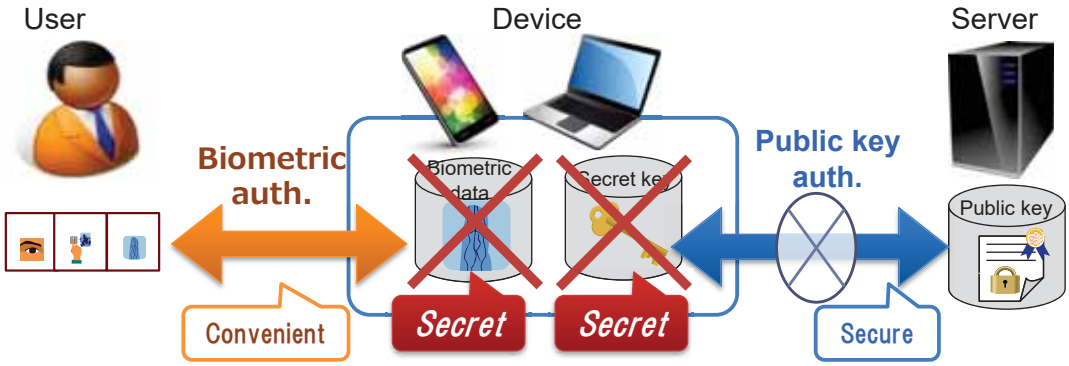
(*): SAML, OpenID, SSL/TSL, FIDO, etc.

Online Authentication To-Be

HITACHI
Inspire the Next

Balancing security and convenience at a high level

- Biometrics are good for convenience and PKC is good for security
- Neither Devices nor servers should not store any user-specific secret
  - to solve the problems of biometric authentication and cryptographic authentication.
  - to enable the user to access his/her online assets, no matter which Device he/her uses.

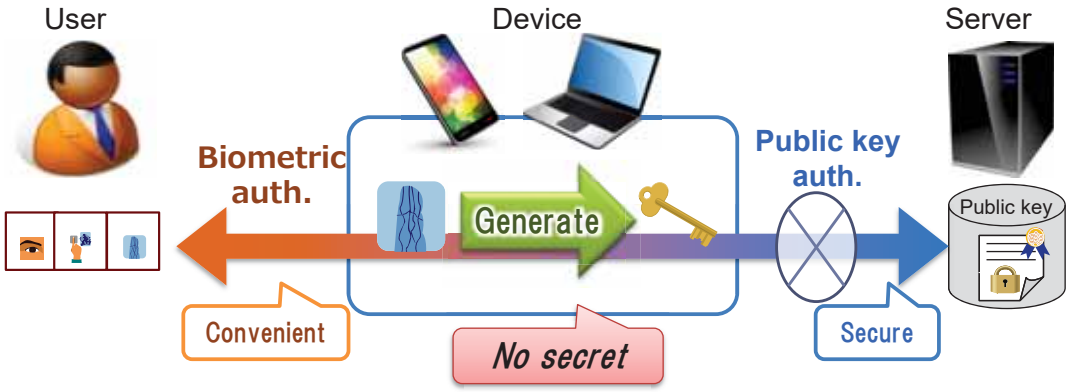


Online Authentication To-Be

HITACHI
Inspire the Next

Balancing security and convenience at a high level

- Biometrics are good for convenience and PKC is good for security
- Neither Devices nor servers should not store any user-specific secret
  - to solve the problems of biometric authentication and cryptographic authentication.
  - to enable the user to access his/her online assets, no matter which Device he/her uses.
- Is it really possible?
  - Yes, if it is possible to generate the secret key dynamically from presented biometric info.
    ⇒ PBI



Contents

HITACHI
Inspire the Next

PBI: Public Biometrics Infrastructure

HITACHI
Inspire the Next

PKC and Digital Signature using biometrics as a secret key

PBI Feature

- ◆ Enable PKC-based auth. without managing any secret key.
  - Minimize the risk of secret key leakage.
- ◆ Enable biometric auth. without managing any biometric feature data.
  - Minimize the risk of biometric data leakage.

PKC: Public Key Cryptography

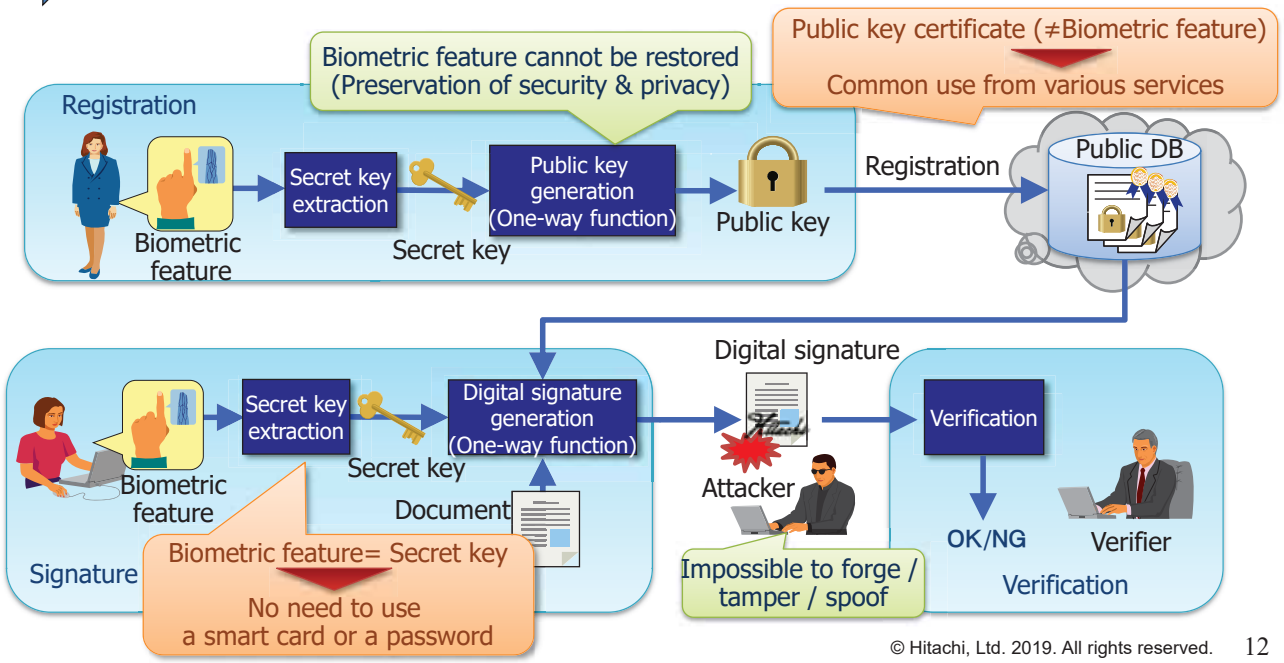
Overview of a PBI system

HITACHI
Inspire the Next

Public keys and signatures are generated based on biometrics

- ■ Registration : Public key is generated by one-way transformation of biometric feature.
- ■ Authentication : Digital sig. is generated from biometrics, and verified by public key.

➡ Neither biometric data nor a secret key is stored on the system.



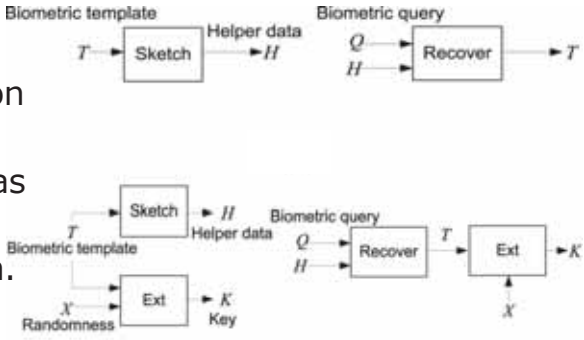
Enabling technologies of PBI (1)

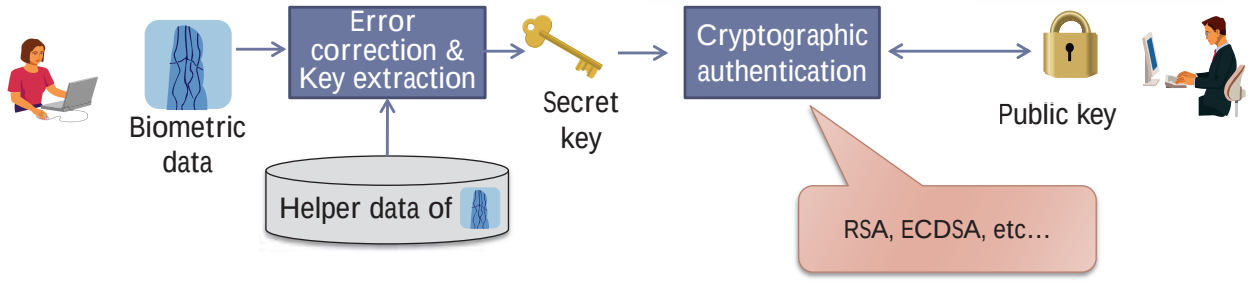
HITACHI
Inspire the Next

(1) Key Extraction Approach:

- Extract a stable key from fuzzy biometric data using error correction code.
- Any cryptographic primitives such as RSA and ECDSA can be used.
- Use helper data for error correction.
- Ex., Fuzzy Extractor

【Fuzzy Extractor】





[1] Y. Dodis, et. al., "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," SIAM J. Comput., 38(1):97-139, 2008.

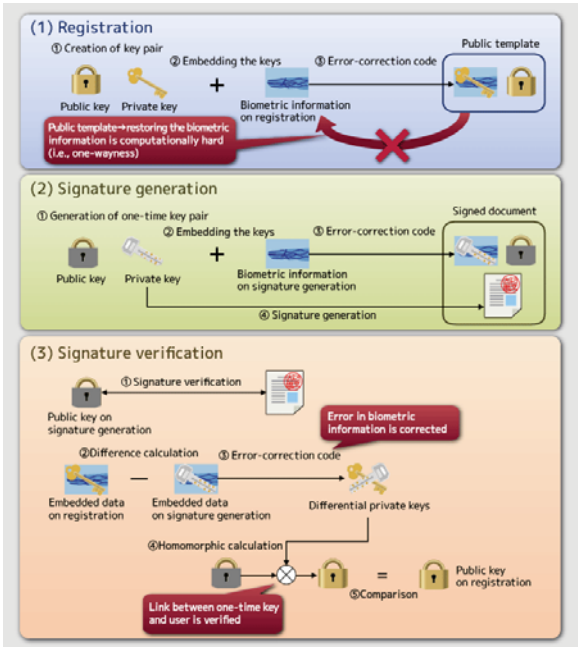
Enabling technologies of PBI (2)

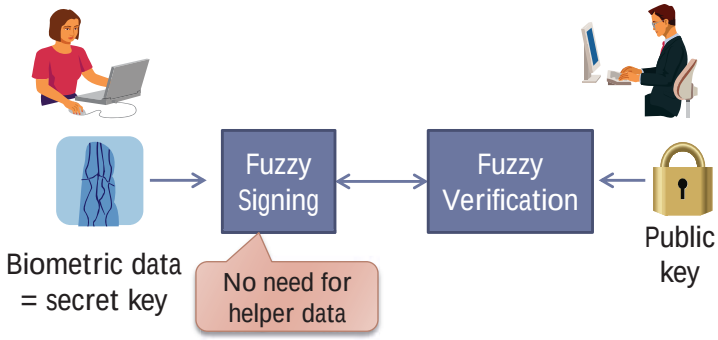
HITACHI
Inspire the Next

(2)Fuzzy Primitive Approach:

- Construct new cryptographic primitives with a fuzzy secret key.
- No need for helper data.
- Ex., Fuzzy Signature

【Fuzzy Signature】





[1] K. Takahashi, et. al., "A Signature Scheme with a Fuzzy Private Key", ACNS'15.
[2] T. Matsuda, et. al., "Fuzzy Signatures: Relaxing Requirements and a New Construction", ACNS'16.

Application Examples

HITACHI
Inspire the Next

Card-less and Sign-less Transactions and Payments

PBI solved the problem of biometric data breach risk from servers and clouds.

Card-less ATM

3 banks in Japan have launched card-less ATM services based on PBI.

Cash-less payment

A supermarket chain have started Proof of Concept of finger-vein payment with PBI.

Password-less IDaaS / SSO

Several ID management services have adopted a cloud-based PBI authentication service.

Standardization Trend

HITACHI
Inspire the Next

Standardizations have been developed about Biometric Template Protection (BTP) Technologies

Biometric Template Protection (BTP)
- Cancelable (Revocable) Biometrics
- Homomorphic Encryption
- Biometric Cryptosystem / PBI

Encryption
- Encrypt the template, (however, need to decrypt at the time of verification)

Operational measure
- Access control to servers
- Tamper Proof Modules (e.g., smart cards)

・Internal frauds
・Decryption key management
・Attacks aiming at the moment of decryption

・Intrusions
・Internal frauds
・Loosing, abusing

【Standards】
・ISO/IEC 24745:2011
"Biometric information protection"
・ISO/IEC 30136:2018
"Performance testing of biometric template protection schemes"

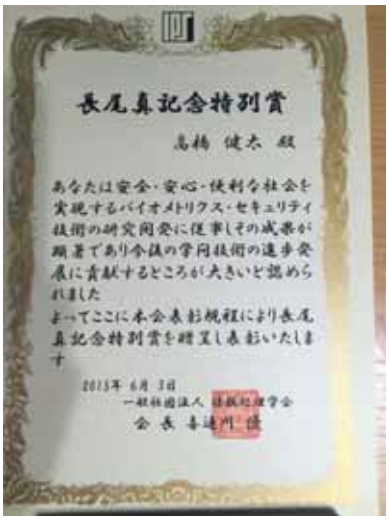
Awards

HITACHI
Inspire the Next

Received prestigious awards for establishment of PBI tech.

Information Processing Society of Japan, *Nagao Special Researcher Award* ('15)

"Research and development of biometric security technologies realizing secure, safe and convenient society"



https://www.ipsj.or.jp/award/2014nagao.html

DoCoMo Mobile Science Award ('16)

"Pioneer work and practical realization of next-generation infrastructure for biometric authentication with cryptographic proof of security"

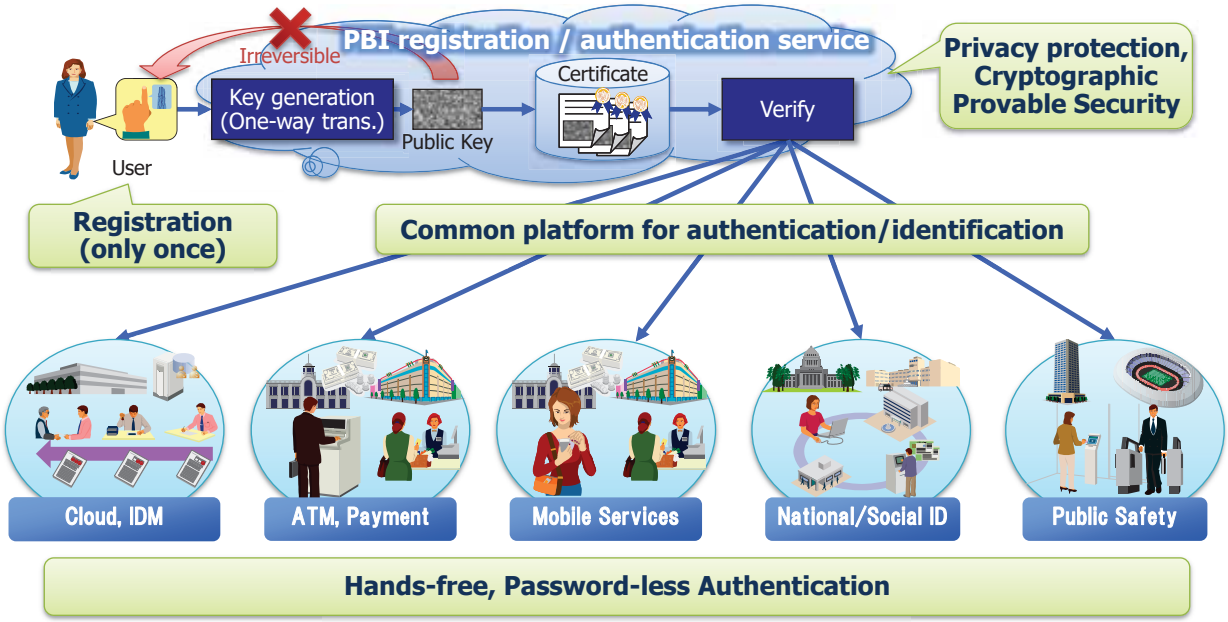
http://www.mcfund.or.jp/mobilescience/award/no15.html

PBI : Future Vision

HITACHI
Inspire the Next

Common biometric authentication platform for secure, safe and convenient society.

*PBI requires only **one-time registration** and enables **universal authentication** for every service, both cyber and physical, without any possessions or knowledge, while **protecting the privacy**.*



Summary

HITACHI
Inspire the Next

1. In the new era of Digital Identity,
   - "Authentication" is a trust anchor.
   - "Key management" is the remaining challenge of cryptographic auth.
   - "Template protection" is the remaining challenge of biometric auth.

2. PBI (Public Biometrics Infrastructure)
   - PKC and Digital Signature using biometrics as a secret key.
     - No need to store and manage secret keys and biometric information.
     - Realized by error-torelant cryptosystems such as Fuzzy Extractor and Fuzzy Signature.
   - Application examples: Banking, Payment, SSO cloud service.
   - Vision: Common biometric authentication platform for secure, safe and convenient society.

Merits of Hitachi Finger Vein PBI System

HITACHI
Inspire the Next

☺Finger Vein is Civil-Liberty Friendly Biometrics

non-Criminal Evidence Type ☹

non-Surveillance Type ☹

non-Pressive type ☹

+

☺Finger Vein is Highly Confidential Biometrics Inside Body

+

☺Privacy Friendly & Strong Cyberattack Resistance by PBI

↓

Ideal Biometrics Infrastructure for Smart City

