6th ICCC 2005 in Tokyo

Introduction of Security Profile for staff verification by token based biometric authentication

NTT DATA Corporation
&
New Media Development Association

September 29, 2005

Abstract

Background:

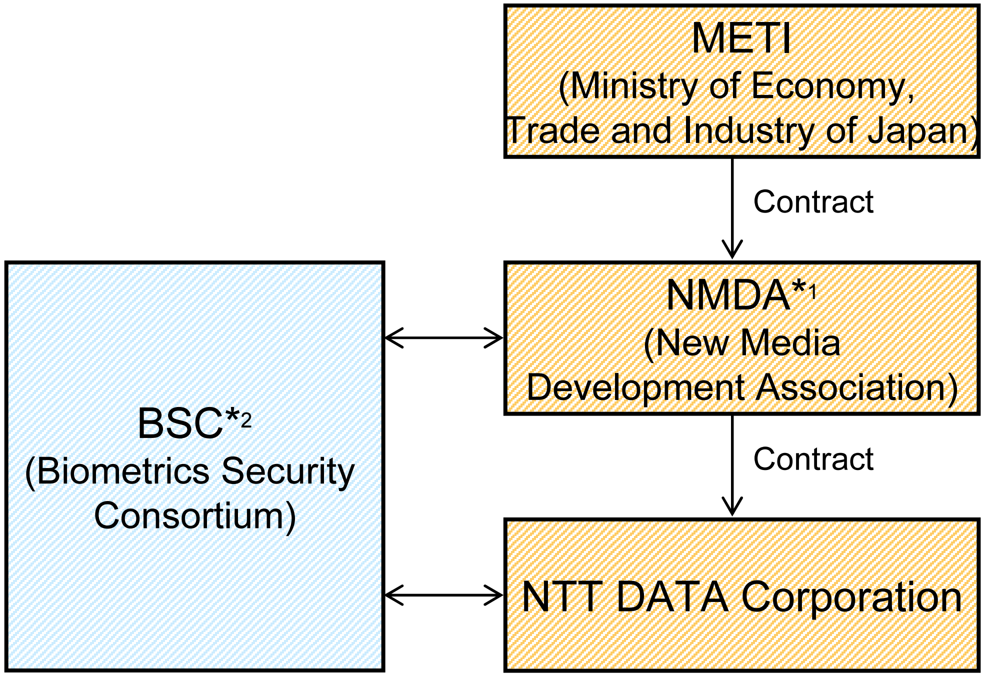
To prevent the terrorists' attack, almost security agencies actively intend to adopt biometric-based authentication in border control systems. Those purpose of using biometrics is to secure authentication systems, however, the consideration of security for biometrics is not mature and rarely discussed.

This presentation shows you the security specification called “Security Profile” regarding staff authentication system with biometrics to have following features.

Issues:	Solutions:
Existing Biometrics PP is in the abstract and unclear for their scopes and targets.	Specified the target as staff authentication system and its assets as physical units to protect from non-authorized access, we developed its protection profile based ISO/IEC 15408.
The consideration of vulnerability analysis for biometrics tends to be lack.	We analyzed the vulnerability for biometric systems exhaustively and disposed into three characteristic vulnerabilities: particular biometrics one, generic one for authentication systems and generic one for IT systems.
The functional and operational requirements are considered separately and they have no relationship with each other. Especially operational one is not sufficient to be drawn up.	To harmonize both functional (ISO/IEC 15408) and operational (ISO/IEC 17799) security requirements, we considered the method of their harmonization and proposed new style of security specification called “Security Profile”.

Project Framework

- This project is promoted and sponsored by the METI (Ministry of Economy, Trade and Industry). And the formation of this project is figured below:



METI
(Ministry of Economy, Trade and Industry of Japan)

Contract

NMDA*1
(New Media Development Association)

Contract

NTT DATA Corporation

BSC*2
(Biometrics Security Consortium)

To work out a policy of standardization of biometric authentication.

To manage the Project and its Specification.

To complete the text of security profile reflected the expert's comments.

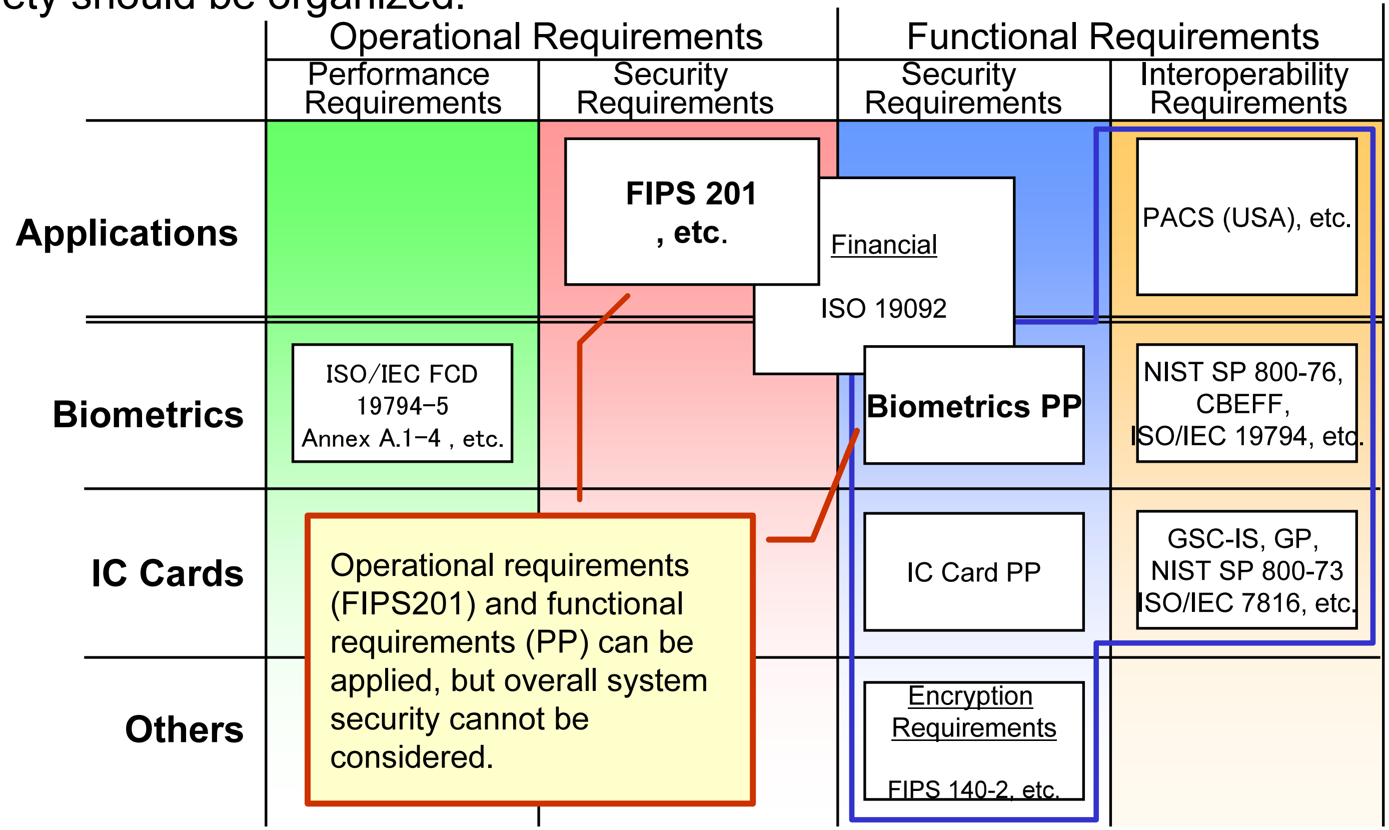
Reviewed by experts in BSC.

*1 http://www.nmda.or.jp/index-en.html
*2 http://www.bsc-japan.com/en/index.html

Background and Current Challenges

Background: There have been growing demand in recent years to store biometric information in tokens such as IC cards and to perform personal verifications with them. However, companies and government agencies are defining required specifications independently from one another.

Challenges: Overall security requirements as a security system, and the basis for ensuring safety should be organized.



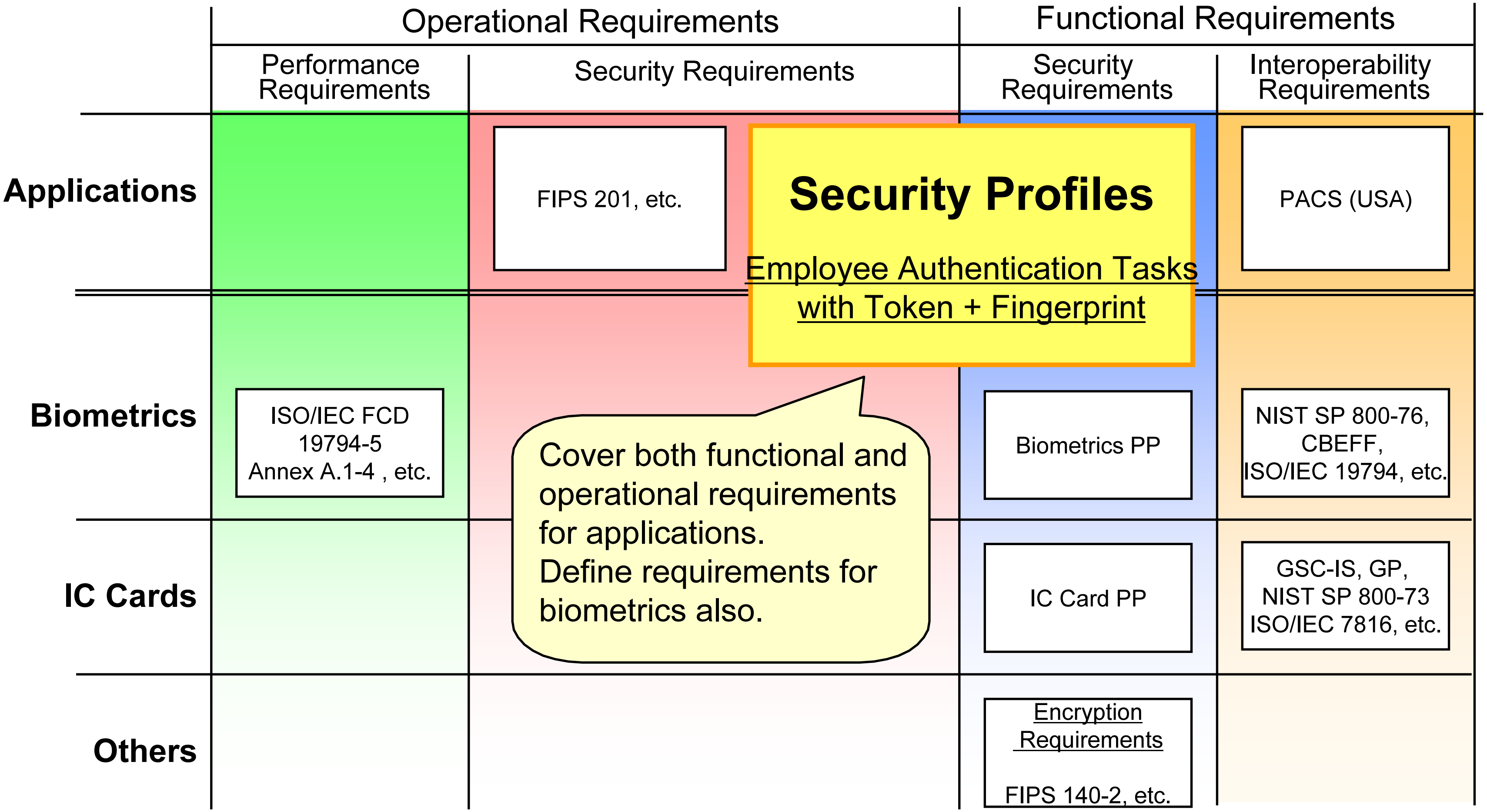
	Operational Requirements		Functional Requirements	
	Performance Requirements	Security Requirements	Security Requirements	Interoperability Requirements
Applications		FIPS 201 , etc.	Financial ISO 19092	PACS (USA), etc.
Biometrics	ISO/IEC FCD 19794−5 Annex A.1−4 , etc.		Biometrics PP	NIST SP 800-76, CBEFF, ISO/IEC 19794, etc.
IC Cards			IC Card PP	GSC-IS, GP, NIST SP 800-73 ISO/IEC 7816, etc.
Others			Encryption Requirements FIPS 140-2, etc.	

Operational requirements (FIPS201) and functional requirements (PP) can be applied, but overall system security cannot be considered.

Specification Map Regarding Tokens and Biometrics

Purpose of Security Profiles

- To achieve an overall system security by defining security requirements that cover both functional and operational requirements.



	Operational Requirements		Functional Requirements	
	Performance Requirements	Security Requirements	Security Requirements	Interoperability Requirements
Applications		FIPS 201, etc.		PACS (USA)
Biometrics	ISO/IEC FCD 19794-5 Annex A.1-4 , etc.		Biometrics PP	NIST SP 800-76, CBEFF, ISO/IEC 19794, etc.
IC Cards			IC Card PP	GSC-IS, GP, NIST SP 800-73 ISO/IEC 7816, etc.
Others			Encryption Requirements FIPS 140-2, etc.	

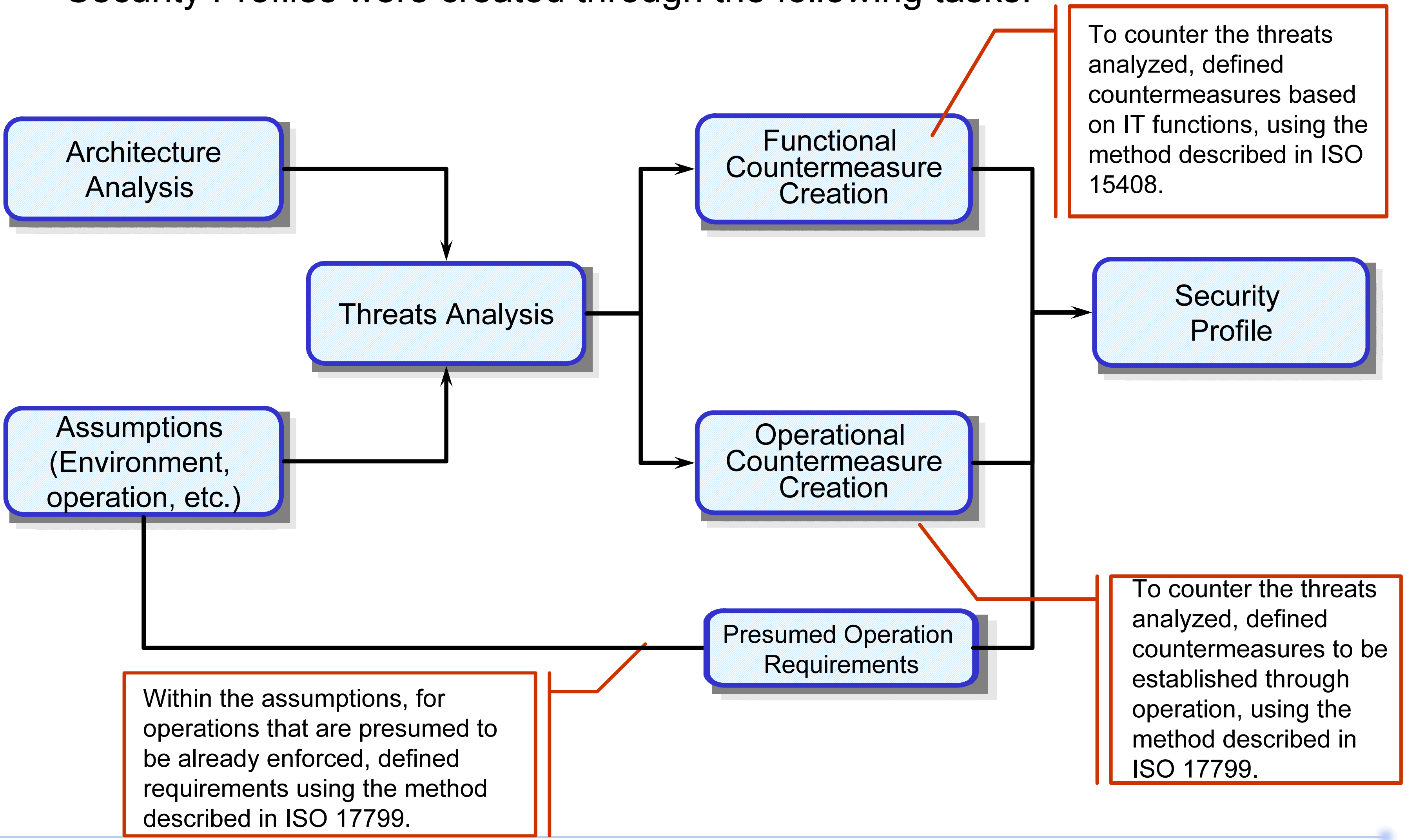
Security Profiles

Employee Authentication Tasks with Token + Fingerprint

Cover both functional and operational requirements for applications.
Define requirements for biometrics also.

Approaches

- Security Profiles were created through the following tasks.


Architecture Analysis
Assumptions (Environment, operation, etc.)
Threats Analysis
Functional Countermeasure Creation
Operational Countermeasure Creation
Presumed Operation Requirements
Security Profile

To counter the threats analyzed, defined countermeasures based on IT functions, using the method described in ISO 15408.

To counter the threats analyzed, defined countermeasures to be established through operation, using the method described in ISO 17799.

Within the assumptions, for operations that are presumed to be already enforced, defined requirements using the method described in ISO 17799.

Target Application

- In considering a Security Profile, Target Application was defined as follows.

Target Application

"All tasks that require strict personal identification of employee"

Authentication tasks by limited staff who access backbone infrastructure that may suffer significant damage by terrorist activities and/or those who access sensitive information and classified facilities.

Assumed Environment:

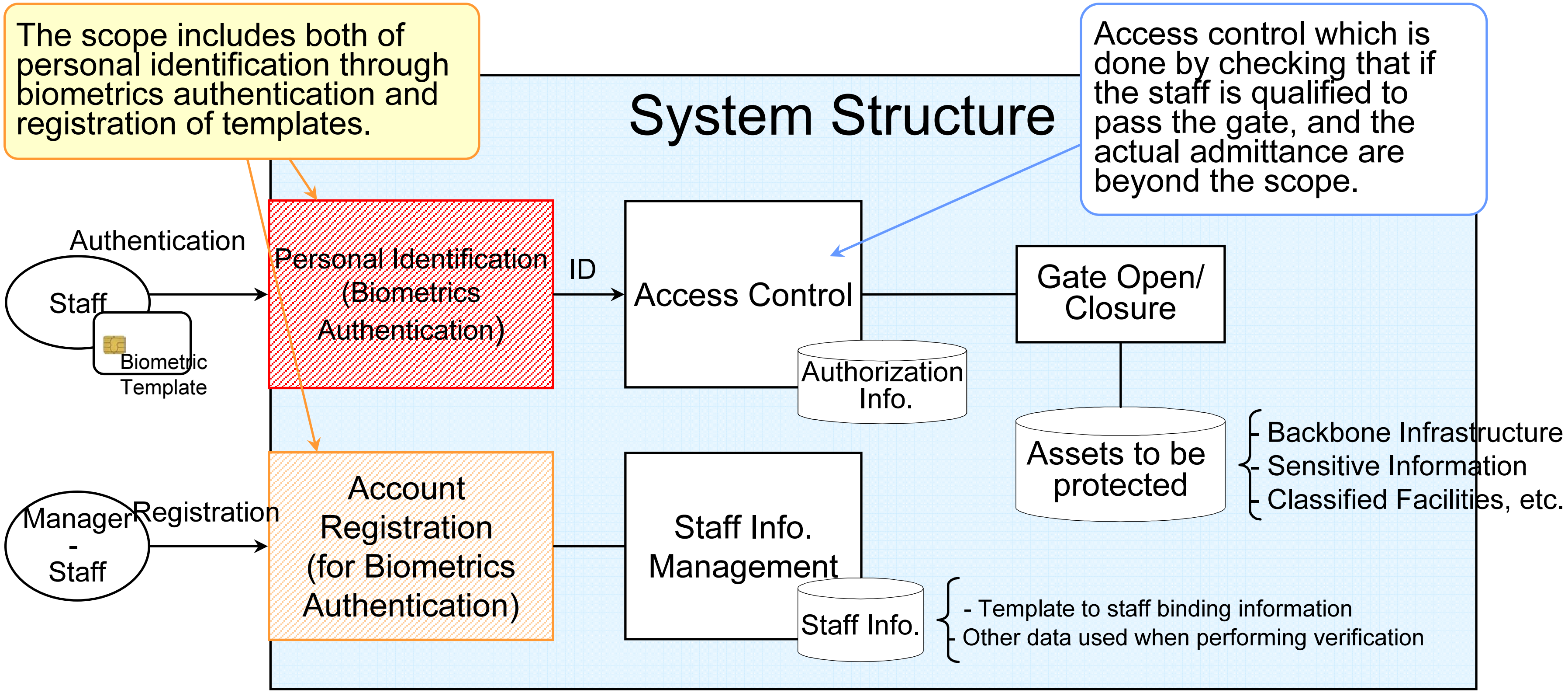
- Employee identification at gate facilities for physically control access to areas where assets to be protected exist.

Actual Examples:

- Government officials
- Airport staff, airline crew
- Staff of nuclear power plants, etc.

Scope

- The scope of the Security Profile was defined as follows, within the system structure. However, only requirements for personal identification (verification mode) are defined in this contribution.



The scope includes both of personal identification through biometrics authentication and registration of templates.

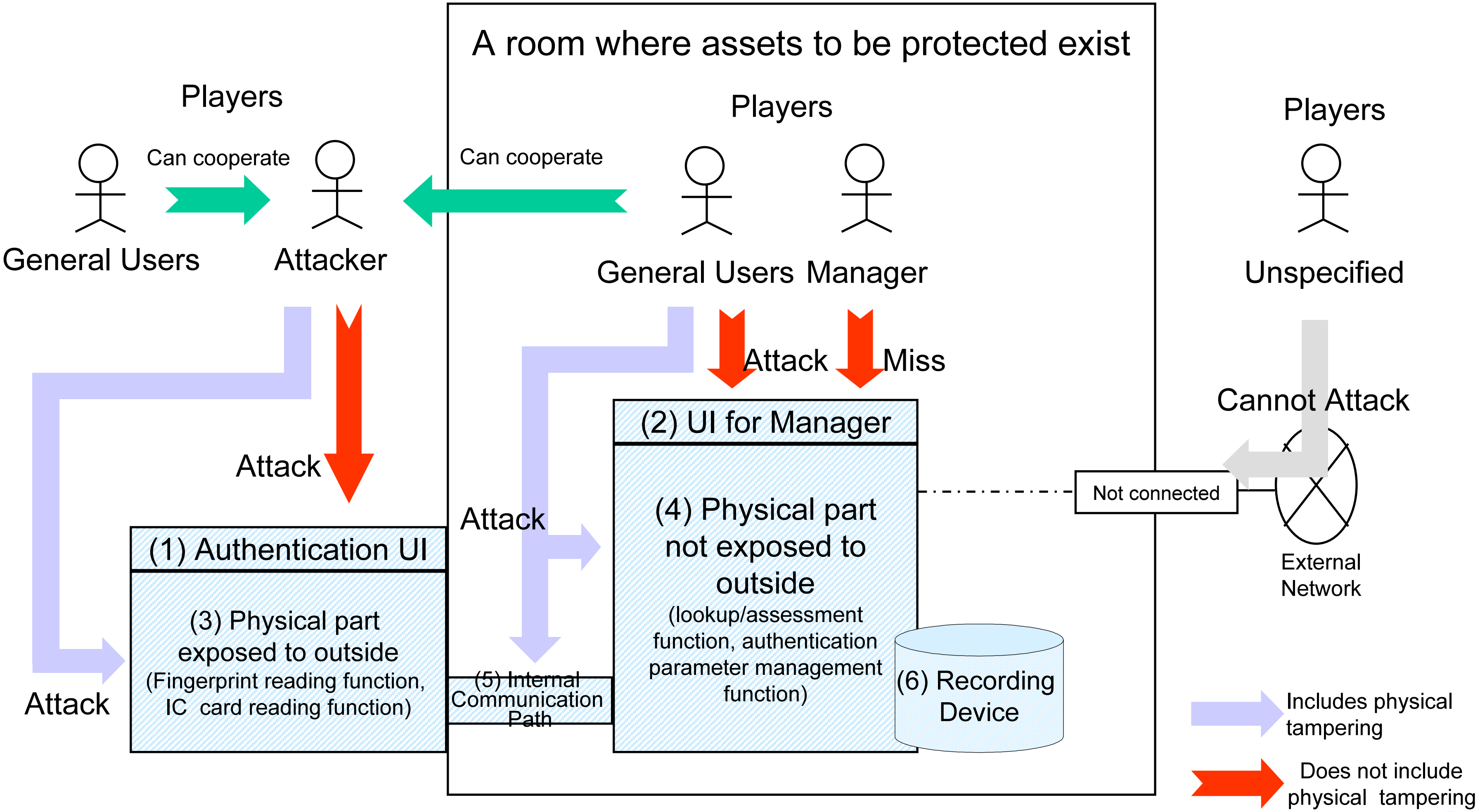
Access control which is done by checking that if the staff is qualified to pass the gate, and the actual admittance are beyond the scope.

System Structure
Authentication
Staff
Biometric Template
Personal Identification (Biometrics Authentication)
ID
Access Control
Authorization Info.
Gate Open/ Closure
Assets to be protected
- Backbone Infrastructure
- Sensitive Information
- Classified Facilities, etc.
Manager - Staff
Registration
Account Registration (for Biometrics Authentication)
Staff Info. Management
Staff Info.
- Template to staff binding information
- Other data used when performing verification

▨ Scope of this Contribution ▨ Scope to be discussed in preparation for the Kyoto Conference

Assumed Environment

- Location and player of the attack (threat) to the system was assumed as follows.


A room where assets to be protected exist
Players
Can cooperate
General Users
Attacker
Players
Can cooperate
General Users
Manager
Players
Unspecified
Attack
Attack
Miss
Cannot Attack
(2) UI for Manager
(4) Physical part not exposed to outside
(lookup/assessment function, authentication parameter management function)
Not connected
External Network
Attack
(1) Authentication UI
(3) Physical part exposed to outside
(Fingerprint reading function, IC card reading function)
Attack
(5) Internal Communication Path
(6) Recording Device
Attack
Includes physical tampering
Does not include physical tampering

Summary of the Threats

- The threats identified for the purpose of the Security Profile contribution are as follows.

Attacks Specific to Biometric Authentication
1. Impersonation with artifact
2. Impersonation with fake template
3. Impersonation through replay attacks using information left in sensors
4. Impersonation through hill-climbing attacks
5. Impersonation through alternation of thresholds
6. Impersonation attributed to authentication accuracy
7. Impersonation due to use in unexpected environments
Threats to Authentication Systems in General
8. Impersonation by bypassing biometrics component devices
9. Impersonation through piggy back attacks
10. Impersonation through brute force attacks
11. Impersonation by taking advantage of fallback system
Threats to IT Systems in General
12. Illegal execution of administrative function by illegally obtaining administration privileges
Seven others (omitted here)

Summary of the Functional Requirements

-The functional requirements defined for the purpose of the Security Profile contribution are as follows. (Only requirements to counter threats listed in previous page are listed)

Threat Description	Function Requirements	
	Mandatory Requirements	Optional Requirements
1. Impersonation by having artificial finger captured	* Liveness Detection Function	* Employment of forgery-proof tokens * Authentication functions of tokens
2. Impersonation through counterfeited tokens and fingerprint of attacker	* Template authenticity check function	
3. Impersonation using token of most recent person authenticated and having fingerprints left on the sensor surface captured	* Use of sensors that do not leave fingerprints, or sensors that do not read left over fingerprints	* Liveness Detection Function
5 .Impersonation due to inappropriate authentication parameters resulting from operation errors, etc.	* Display of confirmation prompts when changing settings * Function for recording operation history	* Automatic setting value checking functions
10. Impersonation through multiple authentication with legitimate tokens and fingerprint of attacker	* Notification of consecutive failures to administrator	* Limitation to number of consecutive failures
12. Administrator privilege obtained by attack on vulnerable administrator login, etc. Or, no function for administrator login	* Administrator identification/authentication functions * Function for recording operation history	* Use of multiple authentication mechanisms for administrator login

Summary of the Operational Requirements

- Similarly, operational requirements were defined as follows. (Only requirements to counter threats listed in the page before the last are listed).

Threat Description	Operational Requirements	
	Mandatory Requirements	Optional Requirements
1. Impersonation by having artificial finger captured		* Educate cases about artificial fingers * Monitoring
2. Impersonation through counterfeited tokens and fingerprint of attacker		* Establishment of encryption usage policies
3. Impersonation using token of most recent person authenticated and fingerprints left on the sensor surface	* Maintenance of fingerprint sensors	* Monitoring
5. Impersonation due to inappropriate authentication parameters resulting from operation errors, etc.	* Educate administrators of cases regarding setting of threshold * Recording and inspection of audit trails * Backup/Restore	
9. Accompanying an authenticated legitimate user to whom the gate opens	* Educate general users * Monitoring	* Establishment of penalties when accompanied entrance is found
10. Impersonation through multiple authentication with legitimate tokens and fingerprint of attacker		* Monitoring
11. Impersonation through exploitation of a vulnerable fallback system that is used since the impersonator lacked support or could not collect fingerprints	* Define operation rules for fallback methods * Define operation rules for lost IC cards	
12. Administrator privilege obtained by attack on vulnerable administrator login, etc. Or, no function for administrator login	* Define and enforce access control policies * Regular checks of audit trails	* Vulnerability Analysis

Conclusion

- We developed a PP as following.

  ⇨ Specified the target as staff authentication system and its assets as physical units to protect from non-authorized access

  ⇨ We analyzed the vulnerability for biometric systems exhaustively and disposed into three characteristic vulnerabilities: particular biometrics one, generic one for authentication systems and generic one for IT systems.

- We developed operational requirements in the manner of ISO17799. And made its relation with PP.

  ⇨ We clarified the concrete operational requirements of "Assumptions" and "Security requirements for the TOE environment" in the PP with ISO17799.

- We are developing the next version of Security Profile (v2.0) for the registration portion of staff authentication system. We think it might be the first challenge in the biometrics trade.

Question?

SHIRAKATA Takashi
shirakatat@nttdata.co.jp
R&D Headquarters, NTT DATA Corporation

Special Thanks to:
Experts from BSC (Security Profile SWG)