Extensible Personal Authentication Framework using Biometrics and PKI

K. Okada T. Ikeda H. Takamizawa T. Saisho

IWAP2004
October 4, 2004
Contexts

• Background
• Model & Definitions
• Our Proposal
  – Concept & Proposal Framework
  – Biometric Authentication Context (BAC)
  – Personal Authentication Flow & Protocols
• Future Work
• Conclusion
Contexts

• Background
• Model & Definitions
• Our Proposal
  – Concept & Proposal Framework
  – Biometric Authentication Context (BAC)
  – Personal Authentication Flow & Protocols
• Future Work
• Conclusion
PKI-based Personal Authentication

- PKI-based Personal (Entity) Authentication
  - Done by verifying possession of the key stored in a smart card.
  - The access control to the key in the smart card relies only on PIN.

- Using biometrics instead of PIN
  - But the verifier only verifies the possession of the key, not the biometric verification result.
Biometric Personal Authentication

Applied to several applications such as border-crossing controls and financial ATMs.

However,
- these systems are specified,
- users are enforced to use specific products.
Example on On-Line Banking

The biometric verification result is really correct?

Forged
finger print

OK/NG

Template/Capture Data

BANK

Copyright © 2004 TOSHIBA SOLUTIONS CORPORATION All Rights Reserved
Purpose of Our Work

• Goal
  - To realize strict remote personal authentication on open networks using various biometric devices which are on hand of the user.

• Problems to solve
  - The verifier has to be able to confirm whether biometric processes have been performed correctly or not.
  - It must be applicable to various biometric environments of users.
Contexts

• Background

• Model & Definitions

• Our Proposal
  – Concept & Proposal Framework
  – Biometric Authentication Context (BAC)
  – Personal Authentication Flow & Protocols

• Future Work

• Conclusion
Model

Client

Personal Device (PD)
(e.g. smart card)

Biometric Device (BD)

Open Network

Server (Verifier)

TAROU TOSHIBA IC Card
Biometric Verification Process

- Acquisition (Capture)
- Raw data → Signal Processing
- Reference data → Matching
- Score → Decision
- Yes/No

- Storage
- Template
Biometric Environment on Clients

Environment differs by what entity (PD, BD, etc.) executes sub-processes of the biometric verification process.
Contexts

• Background
• Model & Definitions

• Our Proposal
  – Concept & Proposal Framework
  – Biometric Authentication Context (BAC)
  – Personal Authentication Flow & Protocols

• Future Work
• Conclusion
Our concept to solve problems

• Each entity (PD/BD) in the biometric environment of the client assures the personal verification results of each process executed by themselves.

• To inform client’s biometric environments and the verification results to servers in a way that they can check the validity of the information.
Our Proposal Framework

We propose a remote personal authentication framework using biometrics assured by PKI.

We assume that each entity
- is assured by other infrastructures (e.g. PKI),
- has private/secret keys to make assurance.

• Description format
• Authentication Protocol
Our Scope

- We propose a description format of biometric personal verification results
  - Biometric Authentication Context (BAC)
- We propose a biometric personal authentication flow using the BAC
  - Protocols for personal authentication
  - Profiles of biometric environments
Contexts

• Background
• Model & Definitions

• Our Proposal
  – Concept & Proposal Framework
  – Biometric Authentication Context (BAC)
  – Personal Authentication Flow & Protocols

• Future Work
• Conclusion
Biometric Authentication Context (BAC)

Generic Biometric Context (GBC)
- The entity which sends BAC to a server describes GBC.
- Only one GBC exists in one BAC.
- GBC consists of a header which describes the composition of the BAC and an authenticator which assures validity of the BAC.

Specific Biometric Context (SBC)
- SBC describes the result of the verification process executed by each entity.
- One or more SBCs exist in one BAC.
- SBC consists of a header which specifies a profile, a profile specific block which describes the result of the verification process and an authenticator which assures validity of the SBC.
Example: Capture on BD/Matching on Card (COBD/MOC) Model

- Validity Check (against Device)
- Matching

**Personal Device**
- Reference Template
- Personal Certificate
- Personal Private Key

**Client**
- Capturing
  - e.g. fingerprint

**Biometric Device**
- Device Certificate
- Device Private Key

**Response**

**Server**
- Validity Check (against User)
- Validity Check (against Device)

**Biometric Authentication Context**
- Request
- Response

- Biometric Sample/Data
- Capturing Information
- Hash (Biometric Sample/Data)
- Signature (Device Private Key)
Example : Specific Biometric Context (SBC) for COBD/ MOC Model

Specific Biometric Context

- Context Header
  - Profile Identifier
  - Biometric Type
  - PD Unique Identifier
  - Generation Time
  - Requestor Name
  - Challenge Value

- Verification Result
  - Verification Algorithm
  - Template Information
  - Result Information

- BD Authenticator
  - BD Authenticator Header
    - BD Unique Identifier
    - Generation Time
    - Requestor Name
    - Challenge Value
  - BD Authenticator Body
    - Sample Data Hash Value
  - BD Authenticator/Signature

- PD Authenticator/Signature

Result of matching on PD
Result of capturing on BD and an authenticator calculated by BD
Authenticator calculated by PD
Example: Multimodal Model

Multimodal Biometric Fusion Model
(e.g. Abstract level - Parallel)

- Biometric Algorithm A
- Fusion Algorithm
- Biometric Algorithm B

Biometric Authentication Context (BAC)

- GBC
- SBC of Multimodal Biometric Fusion Algorithm
- SBC of Biometric Algorithm A
- SBC of Biometric Algorithm B
Contexts

• Background
• Model & Definitions

• Our Proposal
  – Concept & Proposal Framework
  – Biometric Authentication Context (BAC)
  – Personal Authentication Flow & Protocols

• Future Work
• Conclusion
Personal Authentication Flow using BAC

Profile
A rule set which defines a biometric environment,
- Structures of entities,
- Interactions between entities,
- Functional security requirements, etc.

Specify acceptable profiles following the policy

Biometric Environment which supports some profiles

Negotiate a profile
Send a request

Perform biometric verification processes
Generate a BAC which describes the results

Send the BAC

Verify the validity of the BAC

Biometric Authentication Context

Protocols

IC Card

Copyright © 2004 TOSHIBA SOLUTIONS CORPORATION All Rights Reserved
Protocols required for the personal authentication

- **PD/BD**
  - Capability Query Protocol
    - Capability Query
    - Capability Response (supported by PD/BD)

- **Client**
  - Handshake Protocol
    - Profile List Query
    - Profile List Response (supported by Client)
    - Specified Profile

- **Server**
  - Request-Response Protocol
    - Request (nonce)
    - Response (Biometric Authentication Context)
      - (Key Establishment)
Contexts

- Background
- Model & Definitions
- Our Proposal
  - Concept & Proposal Framework
  - Biometric Authentication Context (BAC)
  - Personal Authentication Flow & Protocols
- Future Work
- Conclusion
Future Work

• Sufficiency of BAC format
  - The proposed BAC format is sufficient to describe all biometric environments?

• Guide-line to make profiles
  - How to make a rule set to restrict client’s biometric environments.
  - The balance between the restriction and the flexibility has to be estimated.

• Practicality
  - Data size of contexts may grow up?
  - To calculate authenticators or signatures is possible on low-resource BDs?
Contexts

• Background
• Model & Definitions
• Our Proposal
  – Concept & Proposal Framework
  – Biometric Authentication Context (BAC)
  – Personal Authentication Flow & Protocols
• Future Works
• Conclusion
Conclusion

• We proposed a remote personal authentication framework using biometrics assured by PKI
  – Biometric Authentication Context (BAC)
  – Biometric personal authentication flow using the BAC

• Advantages of our proposal
  – Our proposal framework realizes strict remote personal authentication on open networks using various biometric devices which are on hand of the user.
  – It is expected that the framework is widely used in web application services.

• Future Activity
  – Contribute to ISO/IEC JTC1/ SC27 Study Period