



Biometric Template Protection & Usage

Colin Soutar, CTO
Bioscrypt Inc.

Biometric Consortium Conference
(BC2002)

September 23, 2002



Presentation Outline

- **Company Overview**
- **Definition of Terms**
- **User Identifier**
- **Template Protection**
- **Conclusions**

Bioscrypt Inc.



- Mytec Technologies Inc. and Biometric Identification, Inc.
- Based in Toronto and Los Angeles
- Fingerprint verification for physical and logical access
 - 40,000 devices for physical access
 - 100,000 licenses of algorithm for logical access
- TSX:BYT

BC Working Group

- Biometric Template Protection and Usage

■ Biometric Templates

- Ownership
- Protection
- (Re-)Usage
 - Legitimate
 - Rogue

■ Associated Data or “Identifier”

- Ownership
- Protection

■ Guidance specification for Application Developers/Systems Integrators

Multi-Application Use of Biometrics

- **Common Access Card – Department of Defense**
 - JAVA Card
 - Physical and Logical Access
- **Multi-Use Employee Cards**
- **Template Universality**
 - PIN/passwords assumed to be different for each system

Questions

- **Can/should a second application be able to use the same Biometric Template?**
- **If so, how is trust established between the applications?**
- **How do we restrict access to a third (non-trusted or rogue) application?**
- **How can the application data for the different applications be segregated?**
- **Can this be achieved in accordance with Privacy Principles?**

CSA Model Code

for the Protection of Personal Information

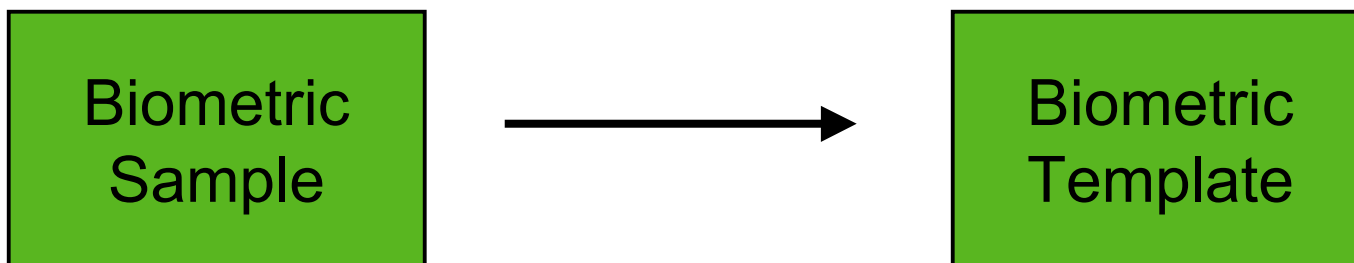
■ 10 Privacy Principles

- **Accountability**
- **Identifying Purposes*** – verification or identification
- **Consent*** – express or implied
- **Limiting Collection*** - only required information
- **Limiting Use*, Disclosure and Retention** – only for stated purpose
- **Accuracy**
- **Safeguards*** - confidentiality
- **Openness**
- **Individual Access**
- **Challenging Compliance**

User Enrollment

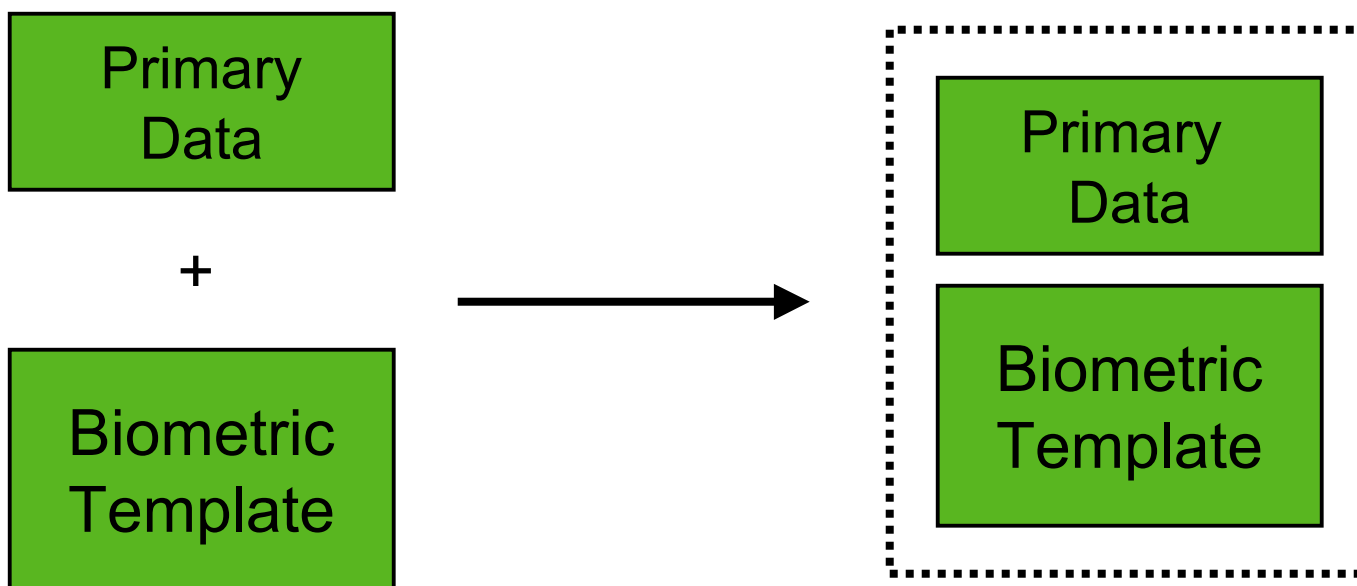
■ Enrollment Procedure

- Collection of biometric (express consent)
- Creation of Biometric Template (identify purpose)



User Registration

- **Addition of Primary Data (Limiting Collection)**
 - **Binding of Primary Data to Biometric Template**



Identity versus Identifier

- **User establishes unique identity to system via “breeder documents” such as passport, birth certificate, etc.**
 - **This step may include background check with AFIS system**

- **System “Identifier” is bound to user’s Biometric Template as Primary Data**

- **User verification is then used to verify that user is valid holder of Identifier**

Data Privacy

Confidentiality of
Associated Data

User
Record

Application specific data

↑ Primary Data

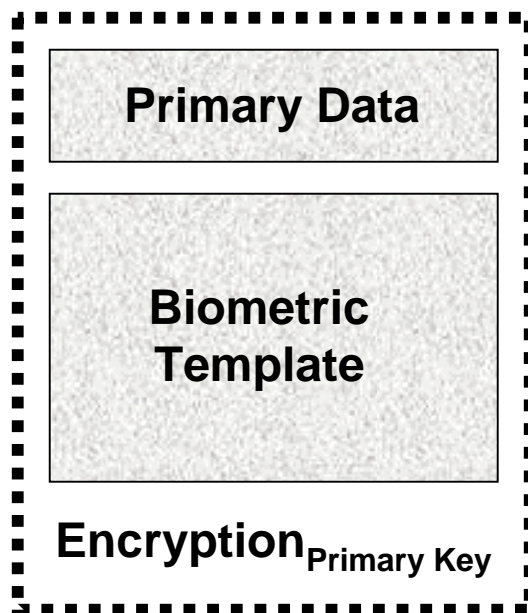
Biometric
Template

Confidentiality of
Biometric Data

↑ Transformation (proprietary or unique)

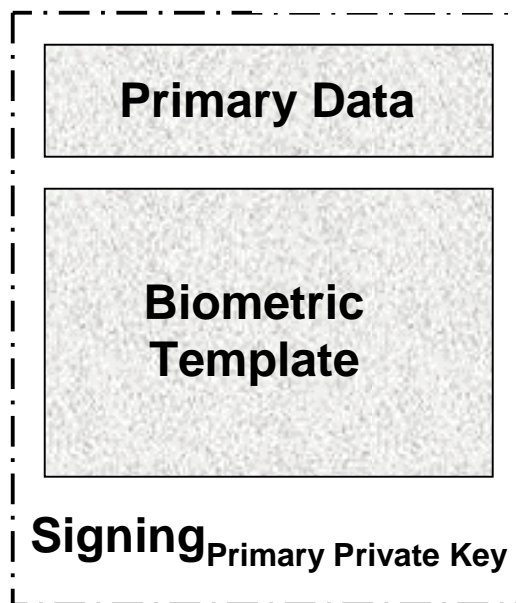
Biometric
Sample

Storage - User Record (1)



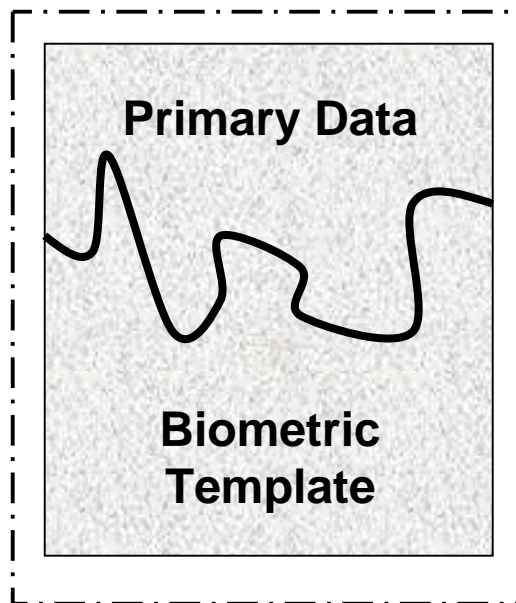
- **Addition of Primary Data such as name, etc. (Limiting Collection)**
 - Add using payload feature - BioAPI
 - Binding using encryption (Safeguard)

Storage - User Record (2)



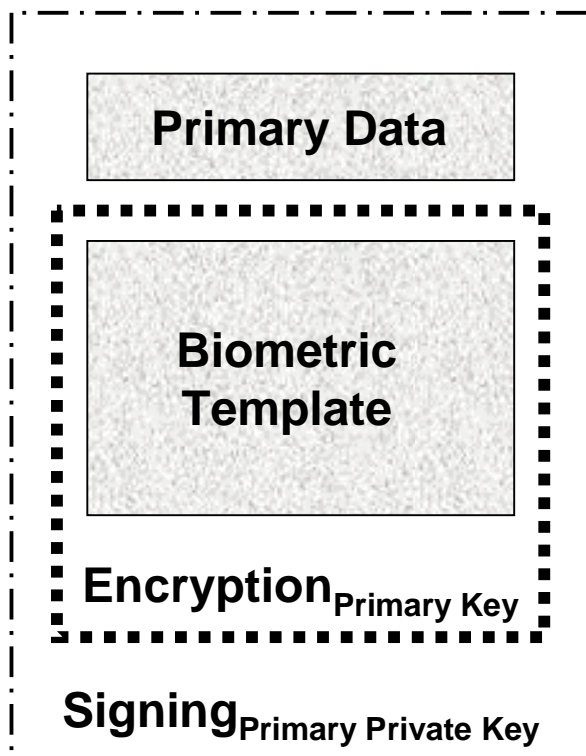
- Digital Signature Binding
 - Easier key distribution
 - No privacy of data (**Safeguard**)

Storage - User Record (3)



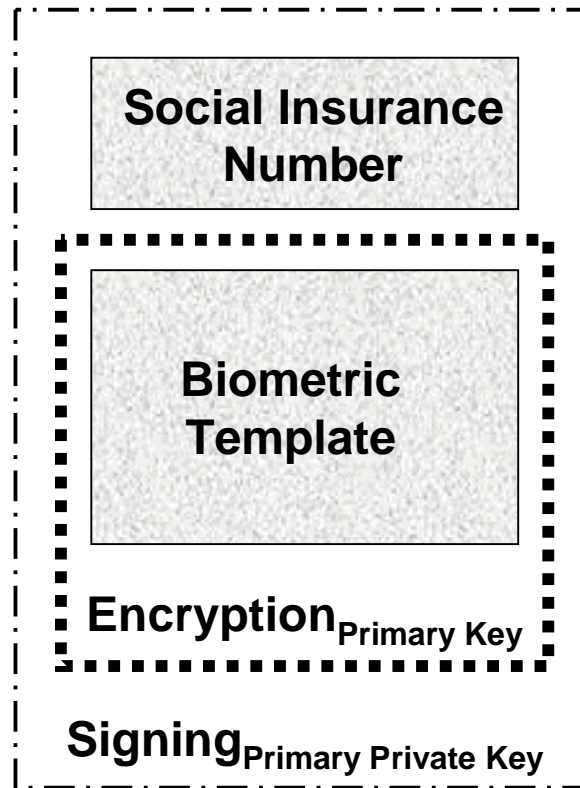
- **Proprietary techniques**
 - **U.S. patents 5,680,460 and 6,219,794**

Storage - User Record (4)

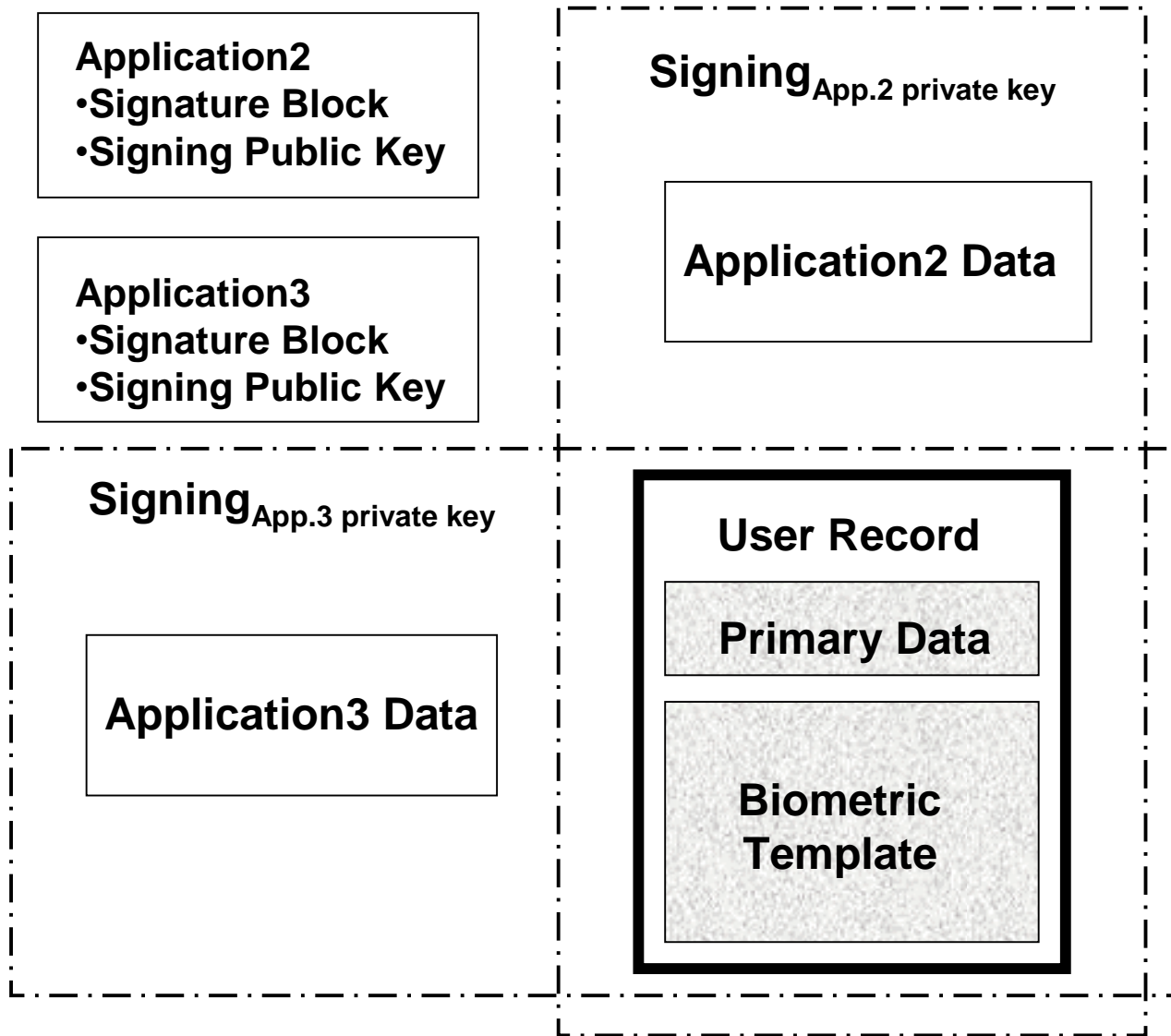


- **Combination binding**
 - **Privacy of Biometric Template (Safeguard)**
 - **Availability of Primary Data (Safeguard)**

User Record (4) - example



- Privacy of Biometric Template (Safeguard)
- Availability of Primary Data (Safeguard)



- All application data needs to be Safeguarded (Accountability)
- Privacy of Biometric Template (Safeguard)

Conclusions

- **Protection Techniques**
- **Privacy Principles**
- **Scenario should be chosen based on application**

Colin Soutar, CTO
Bioscrypt Inc.

T: (905) 624 7707

E: colin.soutar@bioscrypt.com