



# ***Biometric Encryption: Emerging Privacy-Enhancing Technologies***

**Alex Stoianov, Ph.D.**

**Biometrics Specialist**

**Office of the Information and Privacy**

**Commissioner of Ontario**

**Ontario Government Access & Privacy Workshop**

*October 7, 2008*



# Biometrics

Automatic systems that use measurable, physical or physiological characteristics or behavioural traits to identify or verify an individual.

Fingerprints, iris, face, hand/finger geometry, palm/finger veins, retina, voice, dynamic signature, keystroke dynamics, gait, DNA (in the future)



# IPC – Biometrics work

- Biometrics Program, Toronto (1994)
- *Ontario Works Act* (1997)
- Discussion & guidance papers (1999)
- Presentations, Speeches, etc. (2000-)
- Statement to House of Commons Standing Committee on Citizenship & Immigration (2003)
- Resolution of International Data Protection Commissioners (2005)
- Member of EBF IBAC (2005-)
- Biometric Encryption paper (2007)



# *Privacy and Biometrics*



# Privacy and Biometrics: *Concerns*

- Creation of large centralized databases
- Far-reaching consequences of errors in large-scale networked systems;
- Interoperability invites unintended additional “secondary” uses
- Security risks

**Biometric characteristics are unique and irrevocable!**



# Privacy and Biometrics

## *Risks*

- Function creep
- Linkage of the databases
- Expanded surveillance, discrimination
- Negative impacts of errors, false matches, etc.
- Diminished oversight
- Absence of individual knowledge or consent
- Loss of personal control
- Misuse of data (data breach, ID fraud, theft)
- Loss of user confidence, acceptance, trust, & use

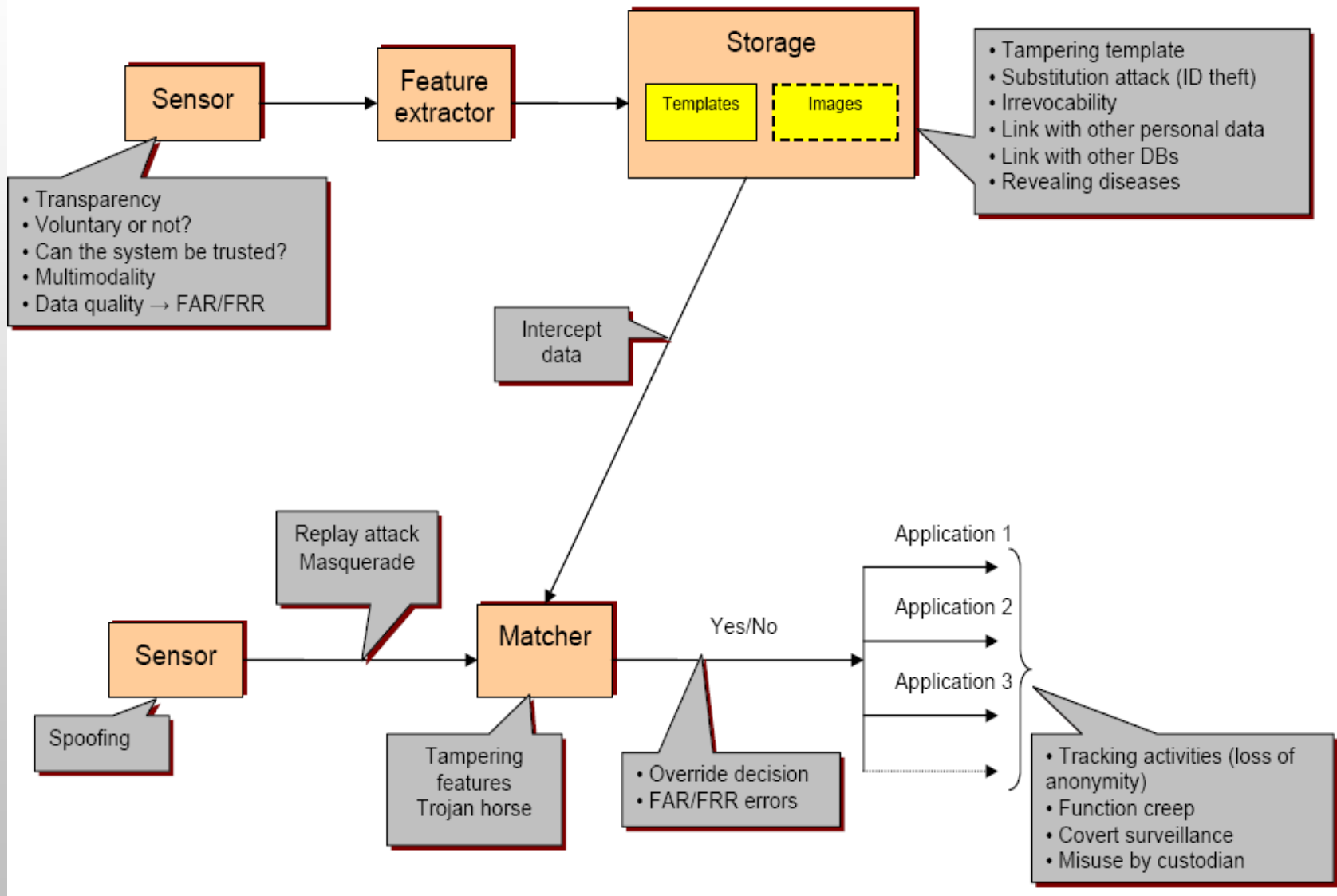


# Biometrics & Security

## *The Risks*

- Spoofing
- Replay attacks
- Substitution attack
- Tampering
- Masquerade attack
- Trojan horse attacks
- Overriding Yes/No response
- Insufficient accuracy

# Vulnerabilities of a biometric system





# Untraceable Biometrics

Class of emerging technologies that seek to irreversibly transform the biometric data provided by the user.



# *Untraceable Biometrics*

- no storage of biometric image or conventional biometric template;
- the original biometric image/template cannot be recreated from the stored information, i.e. it is untraceable;
- a large number of untraceable templates for the same biometric can be created for different applications;
- the untraceable templates from different applications cannot be linked;
- the untraceable template can be revoked or cancelled.



# *Untraceable Biometrics: Biometric Encryption*



# Biometric Encryption (BE)

- BE technologies securely bind a digital key to a biometric, or extract a key from the biometric;
- neither the key nor the biometric can be retrieved from the stored BE template, also called “helper data” ;
- the key is re-created only if a correct biometric sample is presented on verification;
- the output of BE verification is either a key (correct or incorrect) or a failure message.



# Biometric Encryption (BE)

**There is always a biometric dependent helper data stored in the system.**

**In essence, the key is “encrypted” with the biometric.**

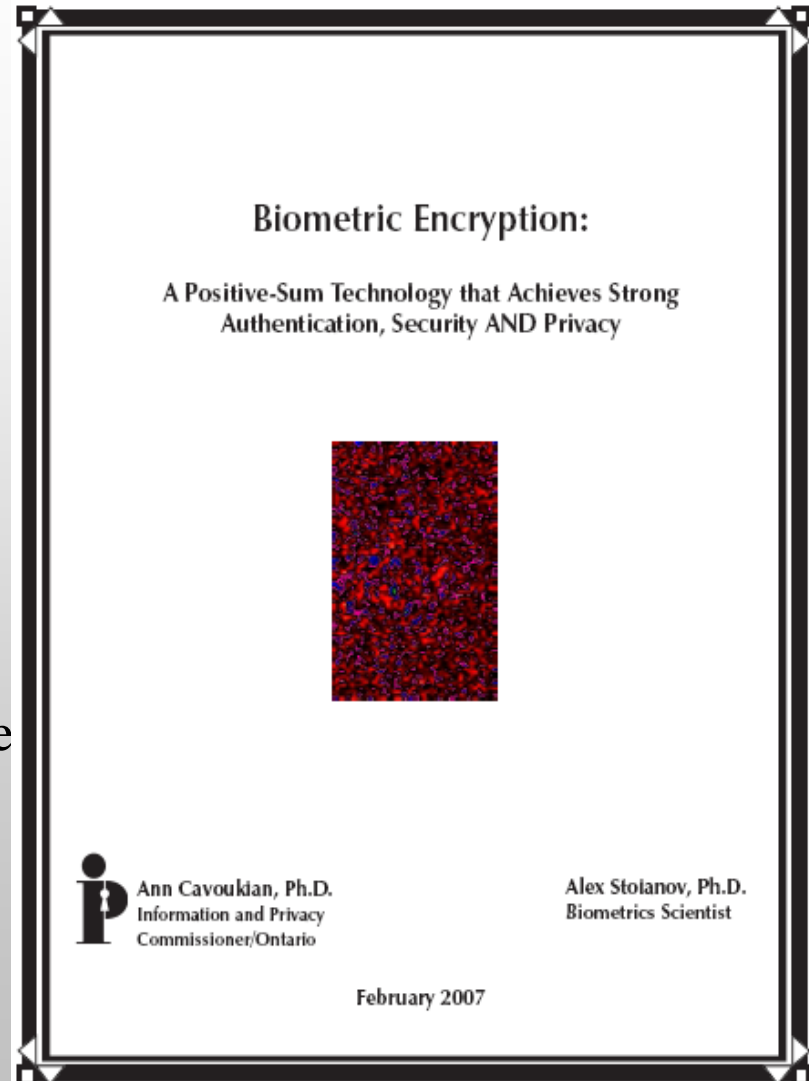
**This “encryption/decryption” process is fuzzy because of the natural variability of biometric samples.**

**Synonyms: Biometric Cryptosystem; Fuzzy Extractor; Secure sketch; Helper Data Systems; Biometric Locking; Biometric Key Generation; etc.**



# IPC Biometrics White Paper

- This paper discusses privacy-enhanced uses of biometrics, with a particular focus on the privacy and security advantages of Biometric Encryption (BE) – while engaging a broad audience to consider the merits of the BE approach to verifying identity, protecting privacy, and ensuring security;
- The central message is that BE technologies can help to overcome the prevailing “zero-sum” mentality by adding privacy to identification and information systems resulting in a “positive-sum,” win/win scenario for all stakeholders involved.





# Publications

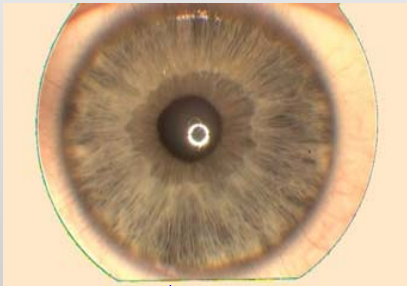
- Ann Cavoukian and Alex Stoianov, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy* (March 2007) at [www.ipc.on.ca/images/Resources/up-1bio\\_encryp.pdf](http://www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf)
- Ann Cavoukian, Alex Stoianov, and Fred Carter, *Biometric Encryption: Technology for Strong Authentication, Security AND Privacy*. In IFIP, *Policies and Research in Identity Management*; Eds. E. de Leeuw, Fischer-Hübner, S., Tseng, J., Borking, J.; (Boston: Springer), v. 261, pp. 57–77, 2008.
- A. Cavoukian and A. Stoianov, *Biometric Encryption: The New Breed of Untraceable Biometrics*. Chapter in Boulgouris, N. V., Plataniotis, K. N., Micheli-Tzanakou, E., eds.: *Biometrics: fundamentals, theory, and systems*. Wiley, London (2008).
- Ann Cavoukian and Alex Stoianov. *Biometric Encryption*. In *Encyclopedia of Biometrics*. Springer, 2008.



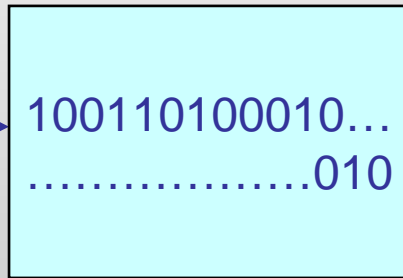
# Use Biometric as the Encryption Key

**Enrollment**

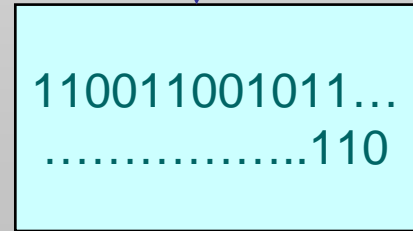
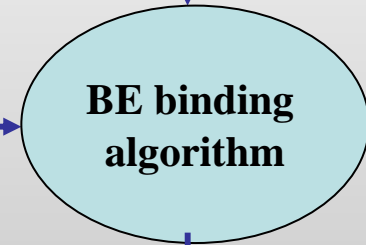
**Biometric Image**



**Biometric Template**



**Randomly generated key**



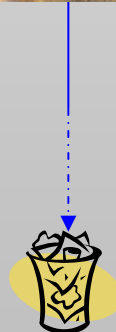
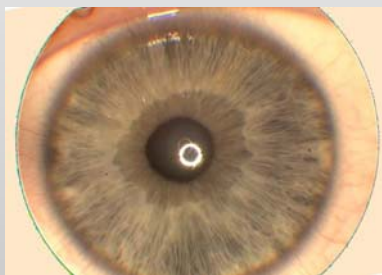
**Biometrically-encrypted key is stored**



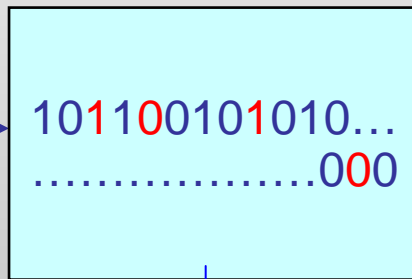
# Decrypt with Same Biometric

Verification

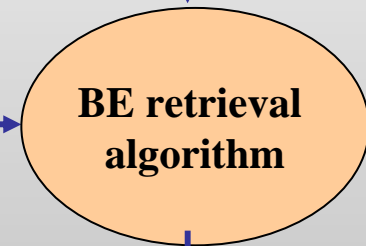
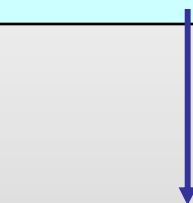
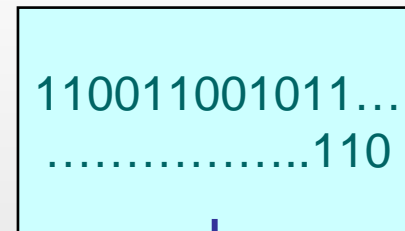
Fresh Biometric Image



Fresh Biometric Template



Biometrically-encrypted key



Key retrieved



# Advantages of Biometric Encryption

BE technologies can enhance both privacy and security:

1. NO retention of biometric image or template
2. Multiple / cancellable / revocable identifiers
3. Improved security of personal data and communications
4. Greater public confidence, acceptance, and use; greater compliance with privacy & data protection laws
5. Suitable for large-scale applications



# Advantages of Biometric Encryption

6. Improved authentication security
  - longer, more complex identifiers
  - no need for user memorization
  - less susceptible to security attacks:
    - No substitution attack: nobody knows the key and cannot create a fake template;
    - No tampering: biometric features aren't stored;
    - No Trojan horse attacks: no score is used;
    - No overriding Yes/No response;
    - More resilient to a masquerade attack.



# Summary of Advantages of Biometric Encryption

## **BE embodies core privacy practices:**

1. Data minimization: no retention of biometric images or templates, minimizing potential for unauthorized secondary uses, loss, or misuse;
2. Maximum individual control: Individuals may restrict the use of their biometric data to the purpose intended, thereby avoiding the possibility of secondary uses (function creep);
3. Improved security: authentication, communication and data security are all enhanced.



# Challenges to BE Adoption

- Technological challenges
- Claim of overriding public interests or (secondary) purposes
- Unwillingness of system designers and operators to relinquish control over biometrics
- Anti-fraud needs or requirements (e.g., background checks)
- Need to retain evidence
- Backup needs and escrow requirements
- Unavailability of suitable, reliable, and cost efficient privacy-enhanced biometric technologies and systems
- Unreliable biometric enrolment/verification procedures and practices
- Pressures from technology vendors and/or advice from independent consultants and integrators;
- Simplistic conflation of privacy and security
- Weak public demand and guidance from the privacy communities.



# Core BE technologies

- Mytec1 (Tomko et al, 1994, 1995);
- Mytec2 (Soutar et al, 1997);
- ECC check bits (Davida et al, 1998);
- Biometrically hardened passwords (Monrose et al, 1999);
- Fuzzy Commitment (Juels and Wattenberg, 1999);
- Fuzzy Vault (Juels and Sudan, 2002);
- Quantization using correction vector (Lyseggen et al, Duffy and Jones, 2001; Linnartz and Tuyls, 2003; Buhan et al, 2007);
- Several Fuzzy Extractor schemes (Dodis et al, 2004);
- BioHashing with key binding (Teoh et al, 2004);
- ECC syndrome with graph-based LDPC coding (Martinian et al, 2005)



# State of the art of BE

- Philips priv-ID: (face, 2D and 3D; fingerprints);
- Hao et al (iris);
- Sagem Securite: Bringer et al (iris);
- Nandakumar et al (Fuzzy Vault for fingerprints);
- Mitsubishi: Martinian et al (iris; fingerprints);
- Genkey solution (fingerprints) – not much information.



# Possible Applications and Uses of Biometric Encryption

- Biometric ticketing for events;
- Biometric boarding cards for air travel;
- Identification, credit and loyalty card systems;
- “Anonymous” (untraceable) labeling of sensitive records (medical, financial);
- Consumer biometric payment systems;
- Access control to personal computing devices;
- Personal encryption products;
- Local or remote authentication to access files held by government and other various organizations.



# BE pilots

- Philips (the Netherlands) priv-ID™ : Leuden hospital; the university health club.
- EU TURBINE (TrUsted Revocable Biometric IdeNtitiEs) project:
  - Sagem, Philips, Precise Biometrics, academic groups, etc.;
  - 3-year;
  - 9.6 M€funding;
  - aims at piloting a fingerprint-based BE technology at an airport in Greece.
- The Genkey BioCryptic® technology: has been deployed for a Rickshaw project in New Delhi (India).

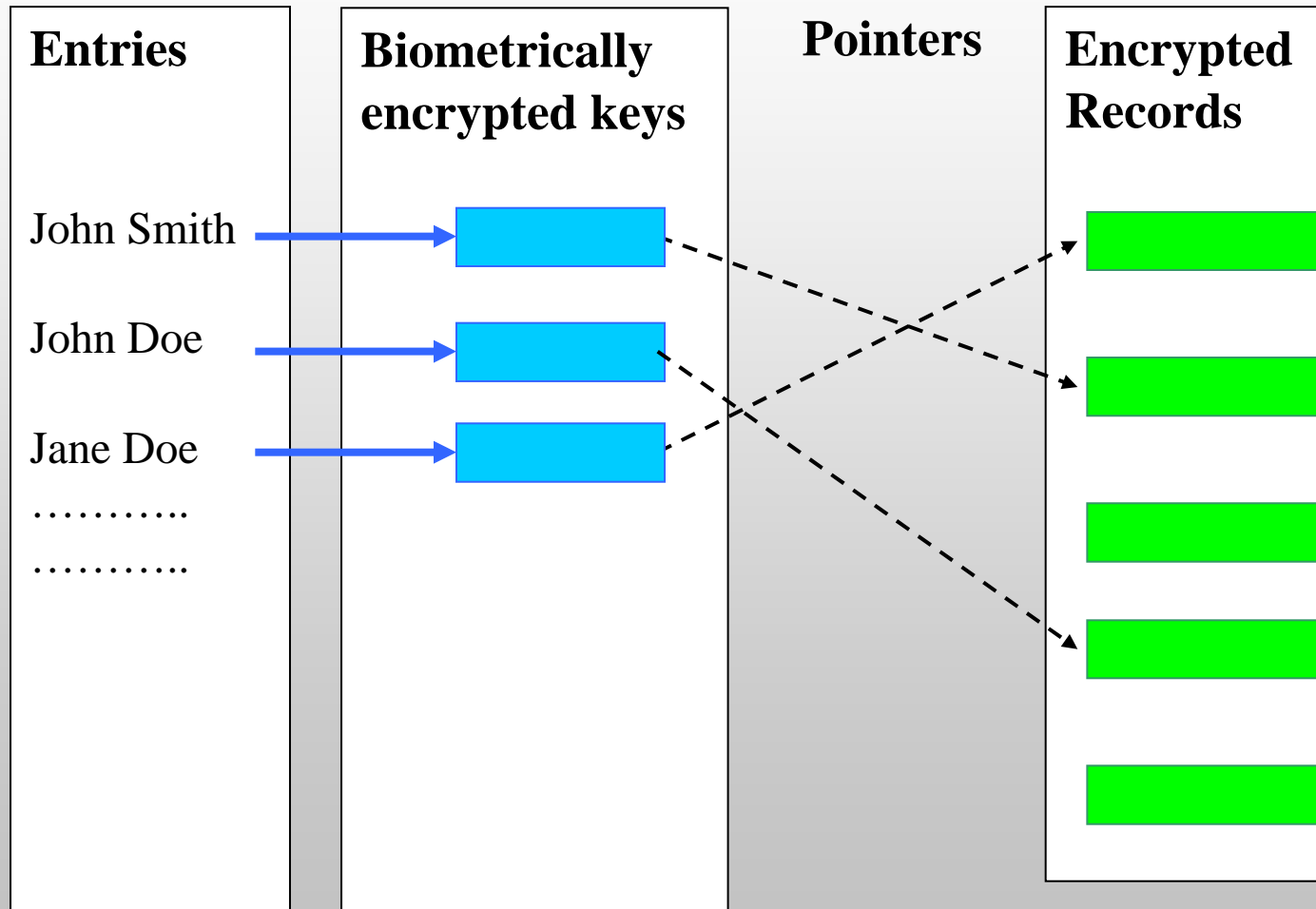


# BE Case Scenarios

1. Anonymous (untraceable) database  
(access to hospital records);
2. Travel documents  
(3-way check).

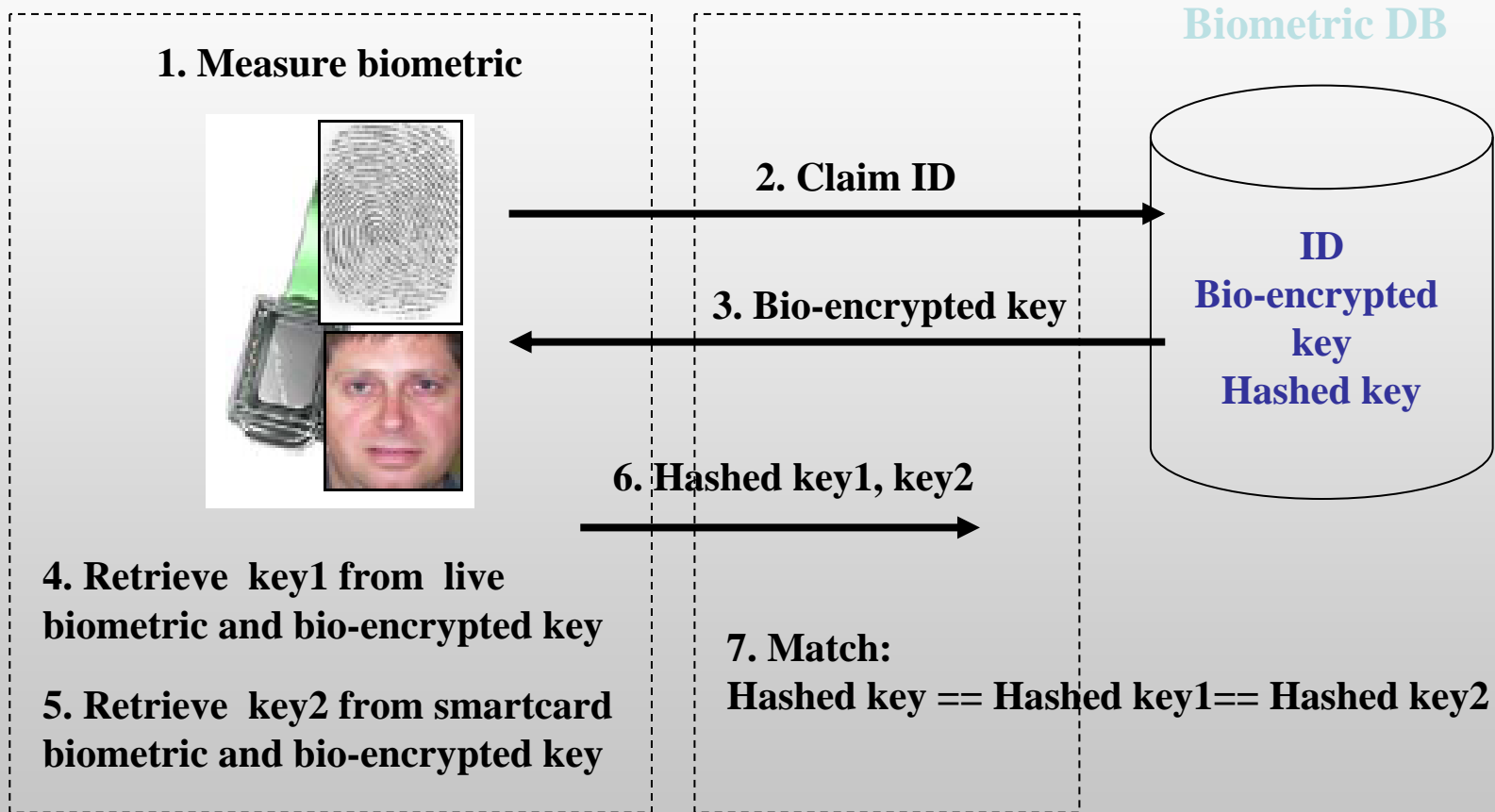


# Scenario 1: Anonymous (Untraceable) Database





# Scenario 2: Three-way-Check in the ePassport Scenario (Philips)



Kiosk

Border control



# Summary

- Privacy and biometrics
- Untraceable Biometrics
- Biometric Encryption technologies
- BE technological challenges:
  - performance;
  - resilience to offline attacks;
  - development of applications.



# How to Contact Us

**Information and Privacy Commissioner of Ontario**  
**2 Bloor Street East, Suite 1400**  
**Toronto, Ontario, Canada**  
**M4W 1A8**

**Phone:** (416) 326-3333 / 1-800-387-0073

**Web:** [www.ipc.on.ca](http://www.ipc.on.ca)

**E-mail:** [info@ipc.on.ca](mailto:info@ipc.on.ca)