Biometrics: New Solutions for Privacy and Security

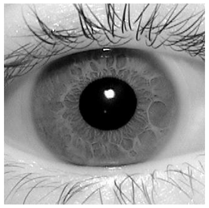
Walter Scheirer

Dir. of R&D at Securics, Inc.

Assistant Prof. Adjoint at the University of Colorado at Colorado Springs

Ethics & Science

- Motivation
  - Biometrics, those methods that can be used to recognize a person based upon physiological features, have become commonplace in recent years.
  - Pros of Biometrics: efficiency, convenience, improved access, improved security
  - Cons of Biometrics: unique identifiers, support unwarranted surveillance, difficulty with storage, questionable security



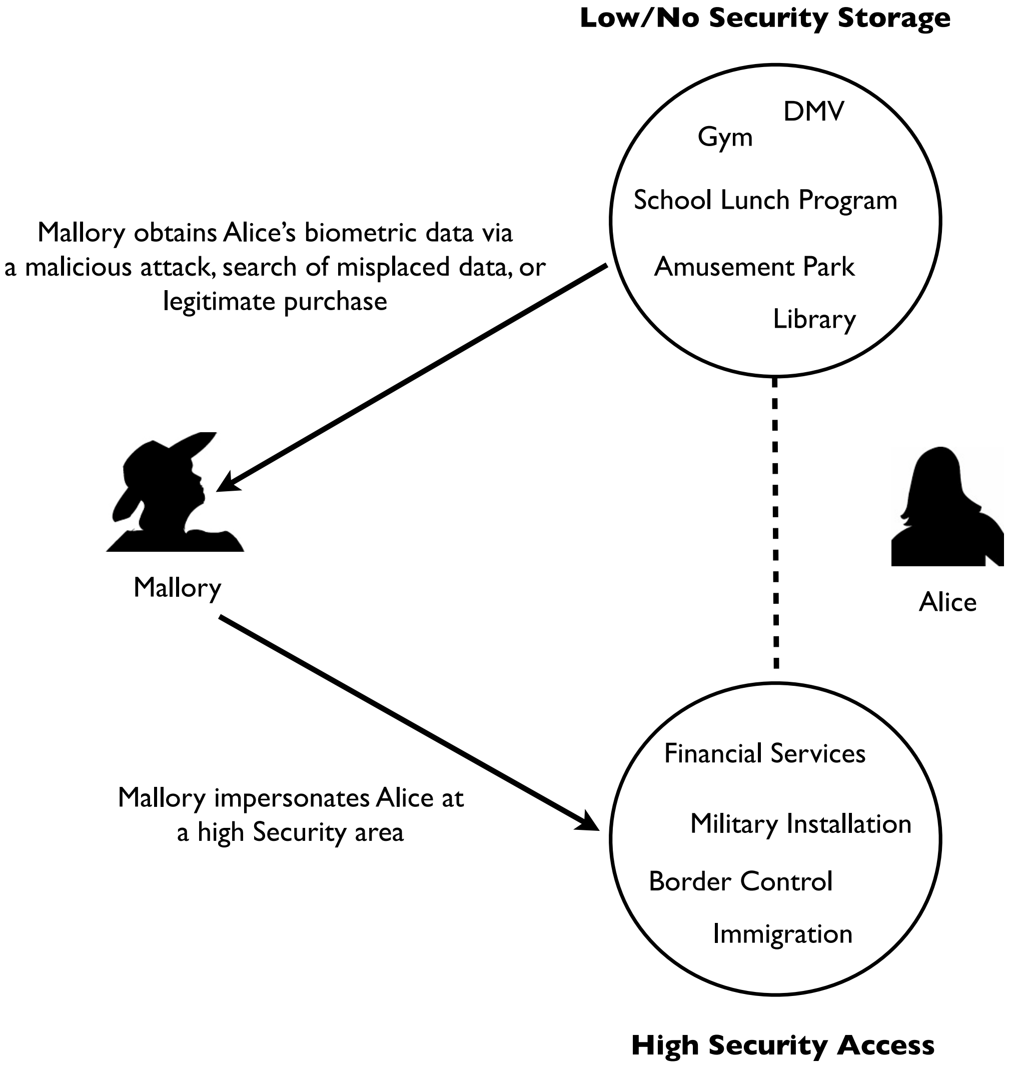
What must we be aware of?

Function Creep

"The expansion of a process or system, where data collected for one specific purpose are subsequently used for another unintended or unauthorized purpose"

- Most familiar example in the US: SSN
- Function Creep and Biometrics: in 2001, Colorado tried to sell face & fingerprint data collected by its DMV

The Biometric Dilemma



Biometrics, Body, and Identity*

- The same biometrics can be used in different ways
  - Identification, genetics research, medical monitoring, ethnic categorization
- Serious risk for discrimination based on what is measured from the human body

*E. Mordini, "Ethics and Policy of Biometrics," in M. Tistarelli et al. (eds.), Handbook of Remote Biometrics, 2009.

Informatization of the Body

- Baudrillard* describes a process of *dematerialization*:
  - Thing → Commodity → Sign → Information

What does this say about the potential for biometrics to dehumanize the body and offend human dignity?

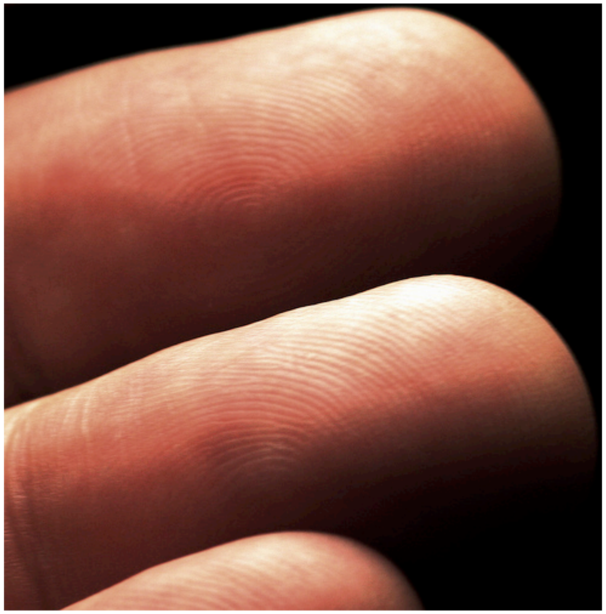
*J. Baudrillard, “Fatal Strategies: Revenge of the Crystal,” 1990.

Security is a Two-way Street

- Biometrics can be incorporated into large security frameworks
  - Identity Assurance
    - Tokens risk a disassociation of the owner from the object
- Biometrics suffer from the same flaws as traditional software security systems (and more!)
  - Limitations of Pattern Recognition

The Doppelganger Threat

- If the FAR is 1 in *X*, then an attacker can try more than *X* different prints
- Lots of public data available!
  - Fingerprint: NIST DB 14, NIST DB 29, FVC 2002, FVC 2004 …
  - Face: MBGC, FRGC, FVT, FERET …
  - Think of this as a biometric dictionary attack



Biometrics as “Liberation”

- Most developing countries have weak and unreliable identification documents
- In 2003, UNICEF* calculated that 36% of all births worldwide were not registered in any way
  - Pakistan, Bangladesh and Nepal have not yet made child registration at birth mandatory

How does this impact food distribution, education, and disaster relief?

*http://www.unicef.org/protection/files/Birth_Registration.pdf

Case Study: India*

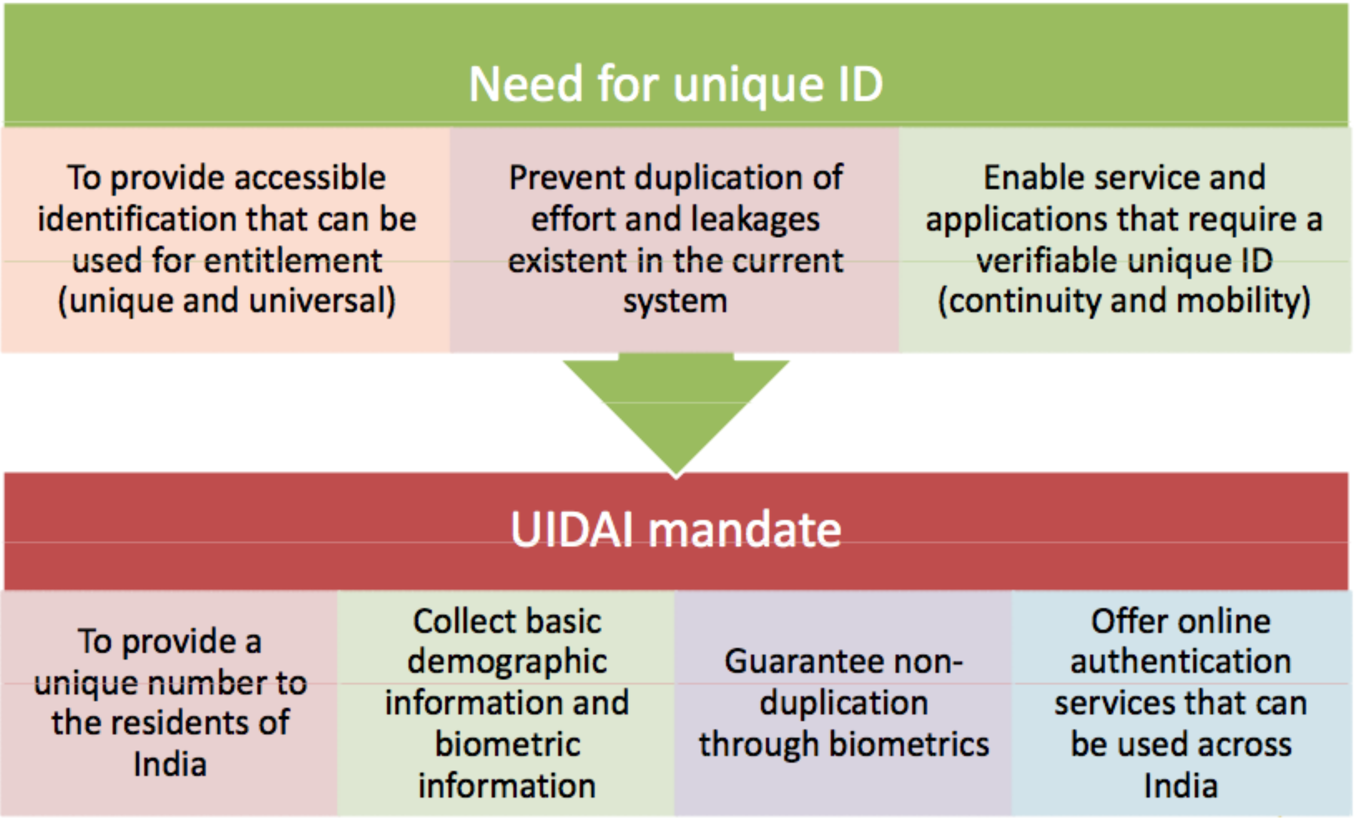
- World's 4th Largest Economy
- World's Largest Social Service Programs
  - Touches 150M Families at $30B per year
  - 20 – 40% "leakage"
- Middle Class Growth at 40M persons per year
- World's largest democracy
  - 714M Voters, 364 Political Parties
- And yet… *Over 600 Million People have no definitive identity*

*UID material courtesy of Salil Prabhakar, UIDAI, and the World Bank

The Need in India

- Poor do not have access to benefits and services due to inability to prove identity
- No universality of identity means reproving again and again
- No continuity of and mobility of identity
- Financial Exclusion
  - Only 18% of people have bank accounts and only 35% have savings
  - No Access to Credit
  - Savings "under the mattress"

The Unique ID Initiative



Need for unique ID

To provide accessible identification that can be used for entitlement (unique and universal)

Prevent duplication of effort and leakages existent in the current system

Enable service and applications that require a verifiable unique ID (continuity and mobility)

UIDAI mandate

To provide a unique number to the residents of India

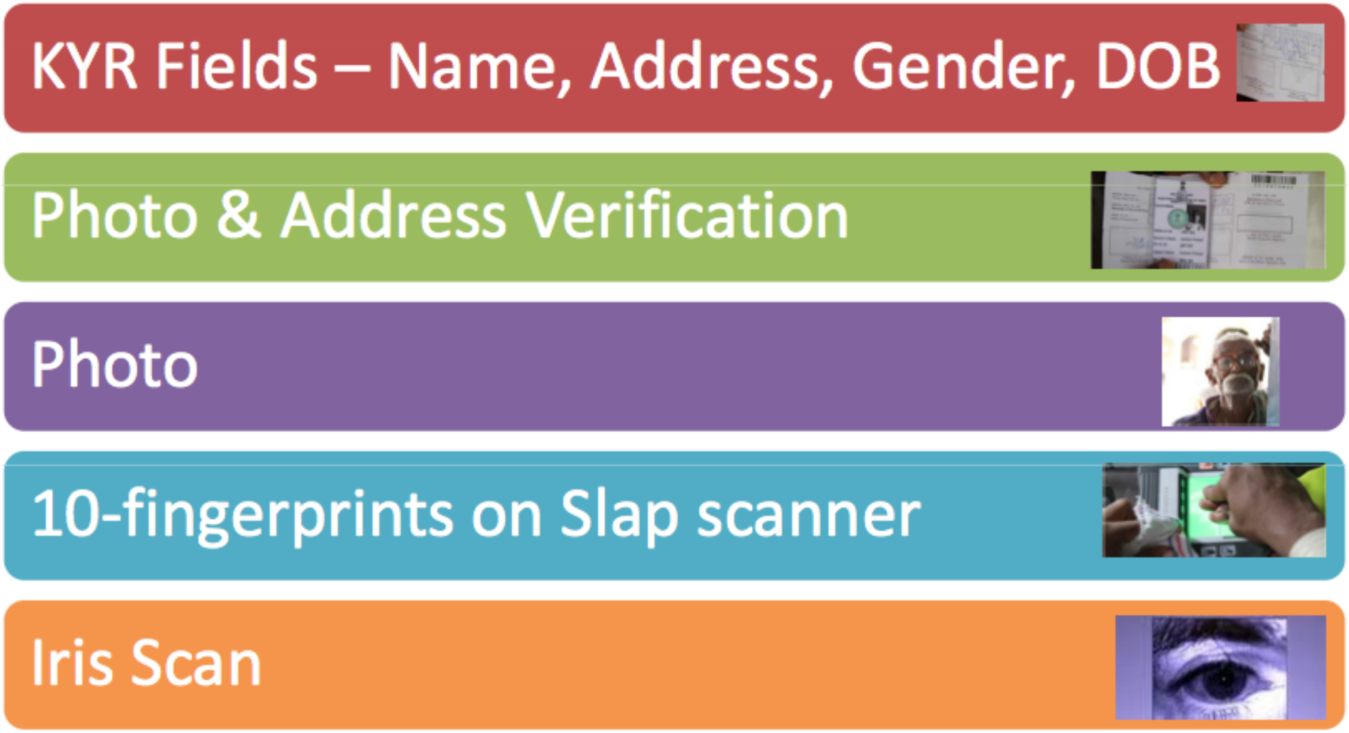
Collect basic demographic information and biometric information

Guarantee non-duplication through biometrics

Offer online authentication services that can be used across India

आधार

Information Collected for UID



KYR Fields – Name, Address, Gender, DOB

Photo & Address Verification

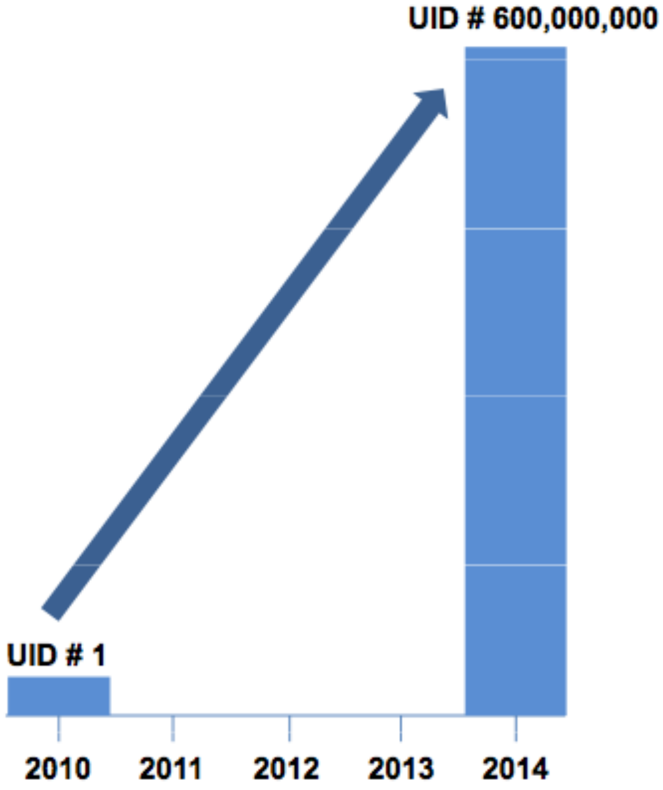
Photo

10-fingerprints on Slap scanner

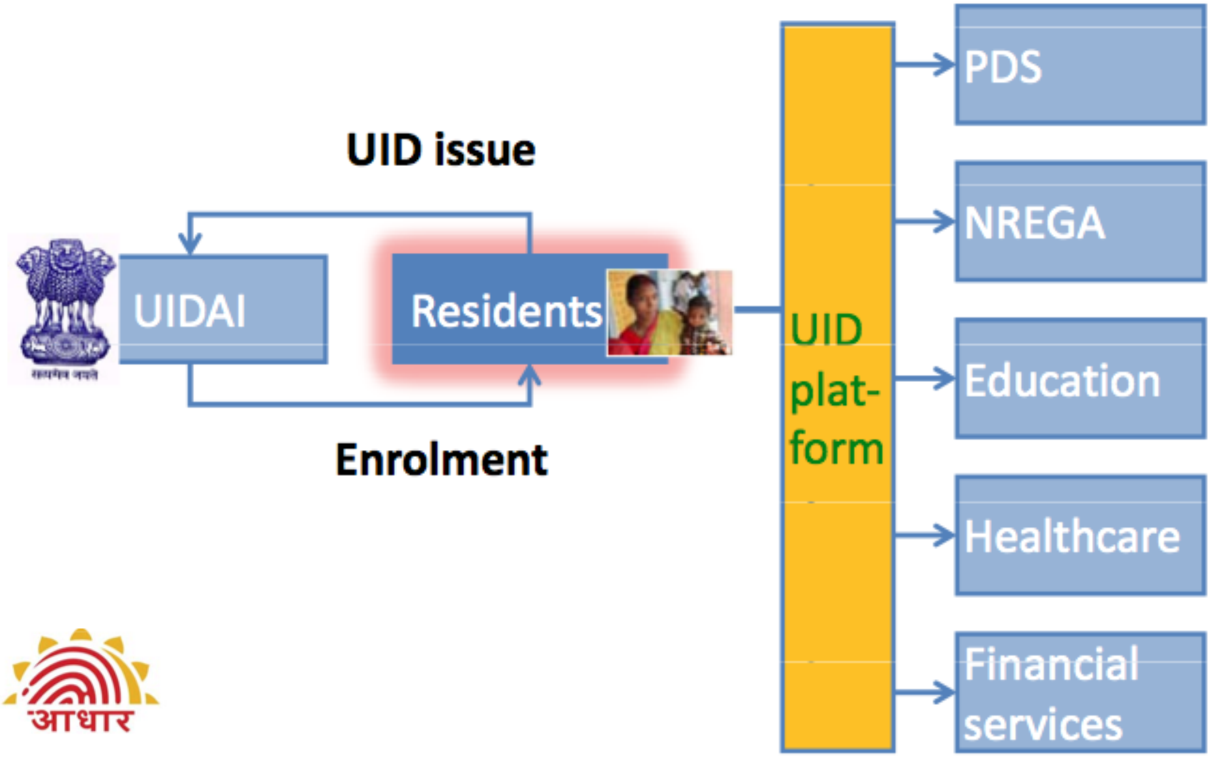
Iris Scan

UID Enrollment Goal

Ambitious Targets



UID From the User’s Perspective



Application ecosystem:

- State
- Financial institutions
- Education, healthcare sector

Potential Holes in UID

- Function Creep
  - One program and many target applications: Government, Healthcare, Finance, Education
  - Levels of security? Does the biometrics dilemma apply?
- Security of Biometric Data
  - Stolen identities mean food and money
  - 600,000,000 enrollments: Doppelganger Danger
- More disturbing concerns…
  - Ethnic discrimination and violence

Secure Templates as a Solution

- Protect the Privacy and Security of the Biometric Features
- Revoke and re-issue biometric templates like a password or credit card #
- Match in an encoded space
- Prevent linking across databases (solve the biometric dilemma)
- Prevent the doppelganger attack (multi-factors)

"Getting this right has been much more challenging than we first thought." – Fabian Monrose

Standard Cryptography as a Weak Solution

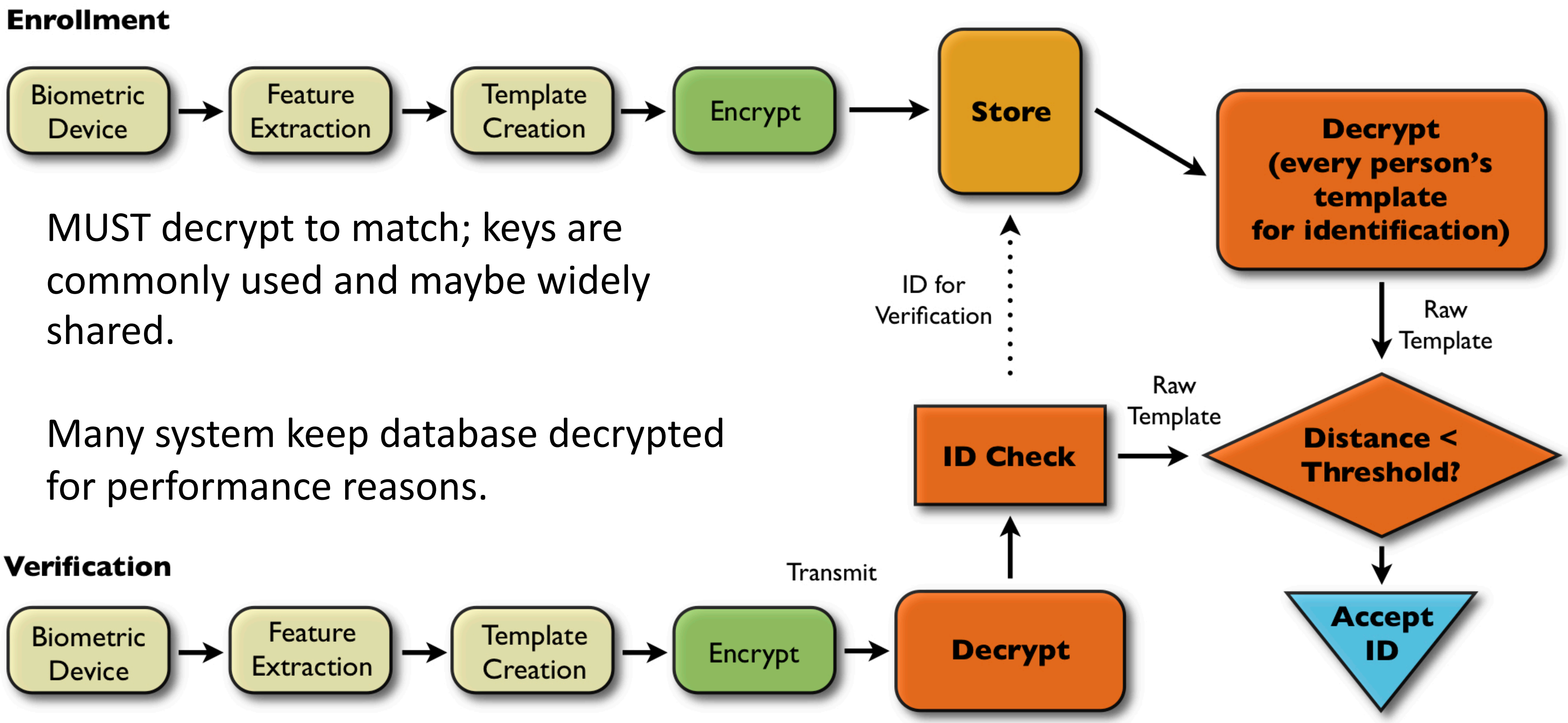
- Hashing/Crypto great for passwords.

Hire Only IEEE Members	1fc486d4b30dd490e044e40a35b6535c
Fire Only IEEE Members	53cc18345f93c390c7469e38c126a13f
Hire Only IEE Members	dfa9d634376d51d311ee55d40722950c

- Minor change results in radically different string (no match)

What does this suggest about potential for Biometrics?

Standard Cryptography as a Weak Solution



MUST decrypt to match; keys are commonly used and maybe widely shared.

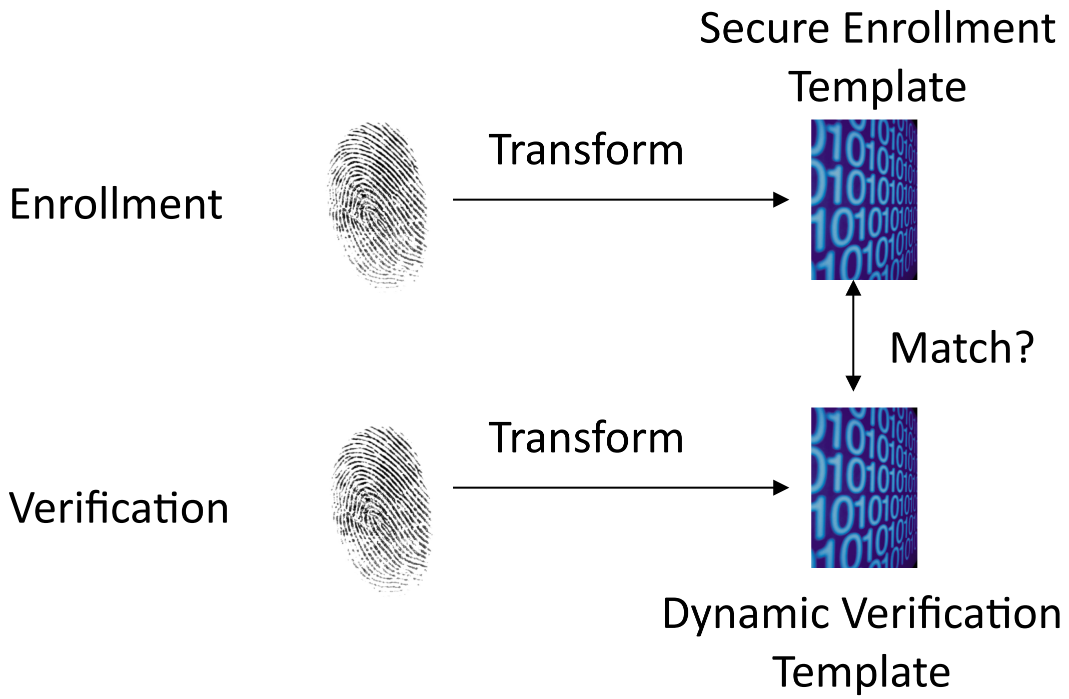
Many system keep database decrypted for performance reasons.

Secure Template Technology

- Transformation of features that can be revoked and re-issued like a password or PIN
- Additional factors (PINs, passwords) used in transformation improve security
- Two interesting classes for crypto protocols
  - Key-generating biometric cryptosystems
    - Derive key data from biometric data; Ex. Fuzzy Extractors
  - Key-binding biometric cryptosystems
    - Bind any key data with biometric data; Ex. Fuzzy Commitment, Fuzzy Vault, Revocable Biotokens

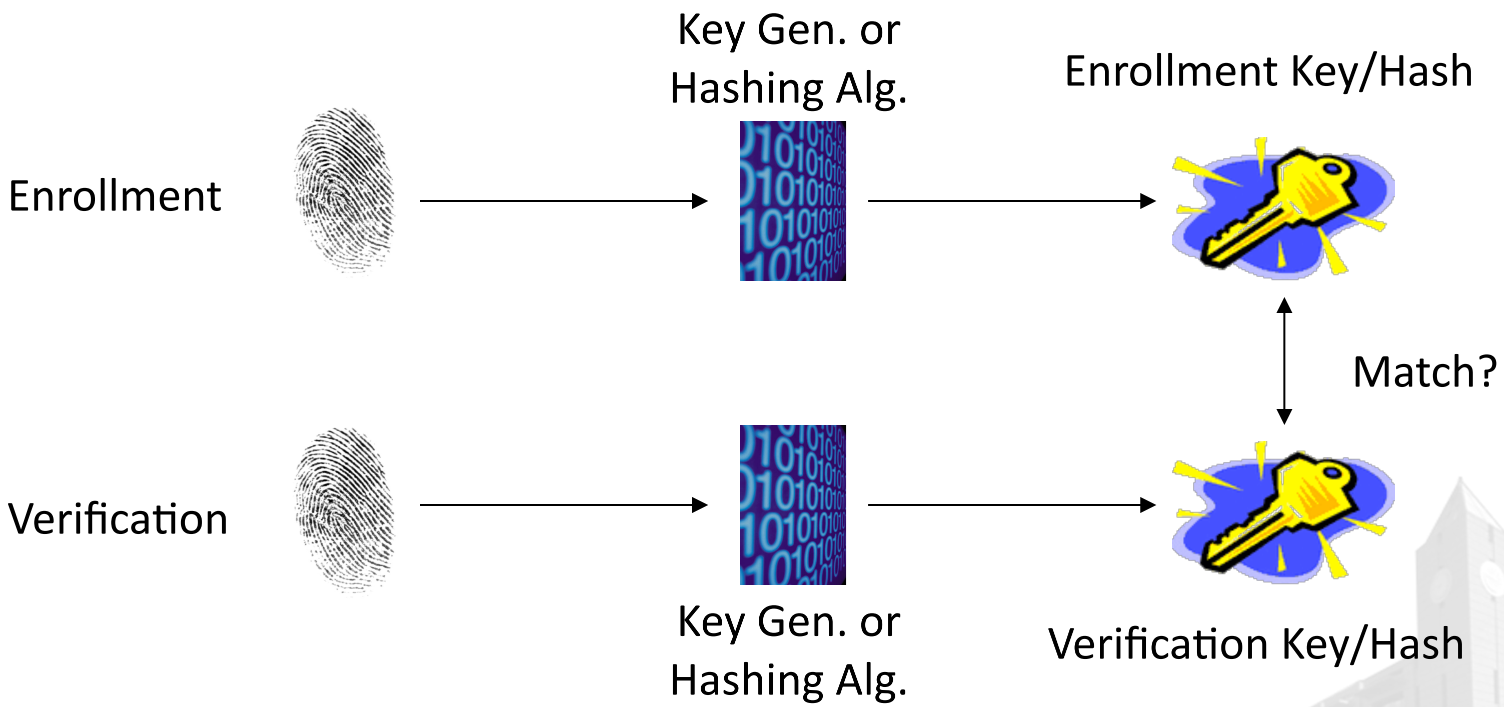
Secure Template Architectures

- Simply protect the original biometric features using some transformation that allows matching in encoded space



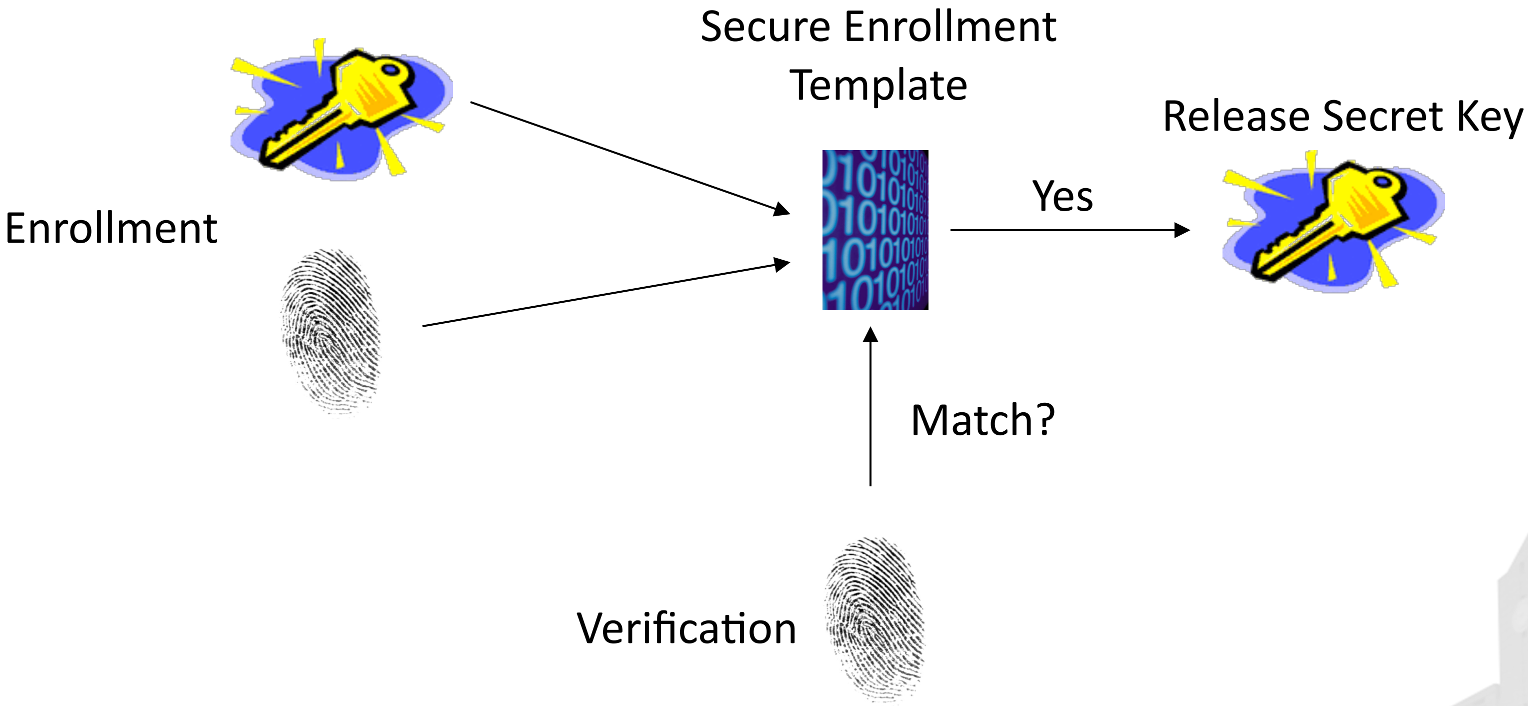
Secure Template Architectures

- Key-generating: Biometric cryptosystem that derives a key from the biometric data

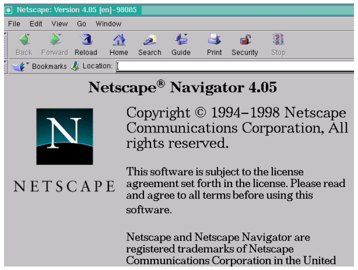


Secure Template Architectures

- Key-binding: Biometric cryptosystem that binds key data with the biometric data



Remember the 90s?

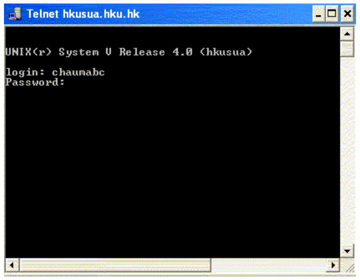


Netscape® Navigator 4.05

Copyright © 1994–1998 Netscape Communications Corporation, All rights reserved.

This software is subject to the license agreement set forth in the license. Please read and agree to all terms before using this software.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United



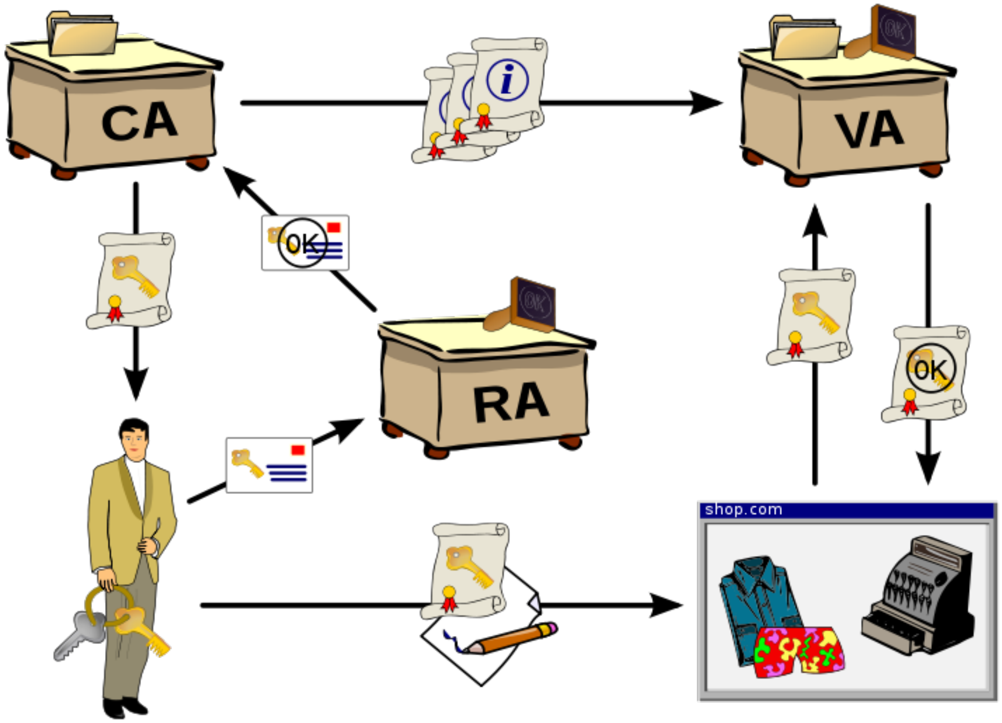
```
UNIX(r) System V Release 4.0 (hkusua)

login: chaumabc
Password:
```

- Huge explosion in new network protocols for e-commerce, electronic record keeping, access control, etc.
- Security of these protocols was an afterthought!
  - We need cryptography to protect insecure channels
  - How can Alice verify a public key?

Solution: Public Key Infrastructure

Public Key Infrastructure

- PKI is the infrastructure for handling the complete management of digital certificates (x.509 compliant)
  - Certificates contain trusted information: a public key



Problems with PKI

- Ellison and Schneier (2000)*
  - “Risk #1: Who do we trust, and for what?”
  - “Risk #2: Who is using my key?”
  - “Risk #4: Which John Robinson is he?”
  - “Risk #6: Is the user part of the security design?”
  - “Risk #8: How did the CA identify the certificate holder”?

*C. Ellison and B. Schneier, “Ten Risks of PKI: What You’re Not Being Told About Public Key Infrastructure,” *Computer Security Journal*, 16(1):1-7, 2000.

A Recent Attack: Chosen Prefix Collisions

- Stevens et al. (2009)*

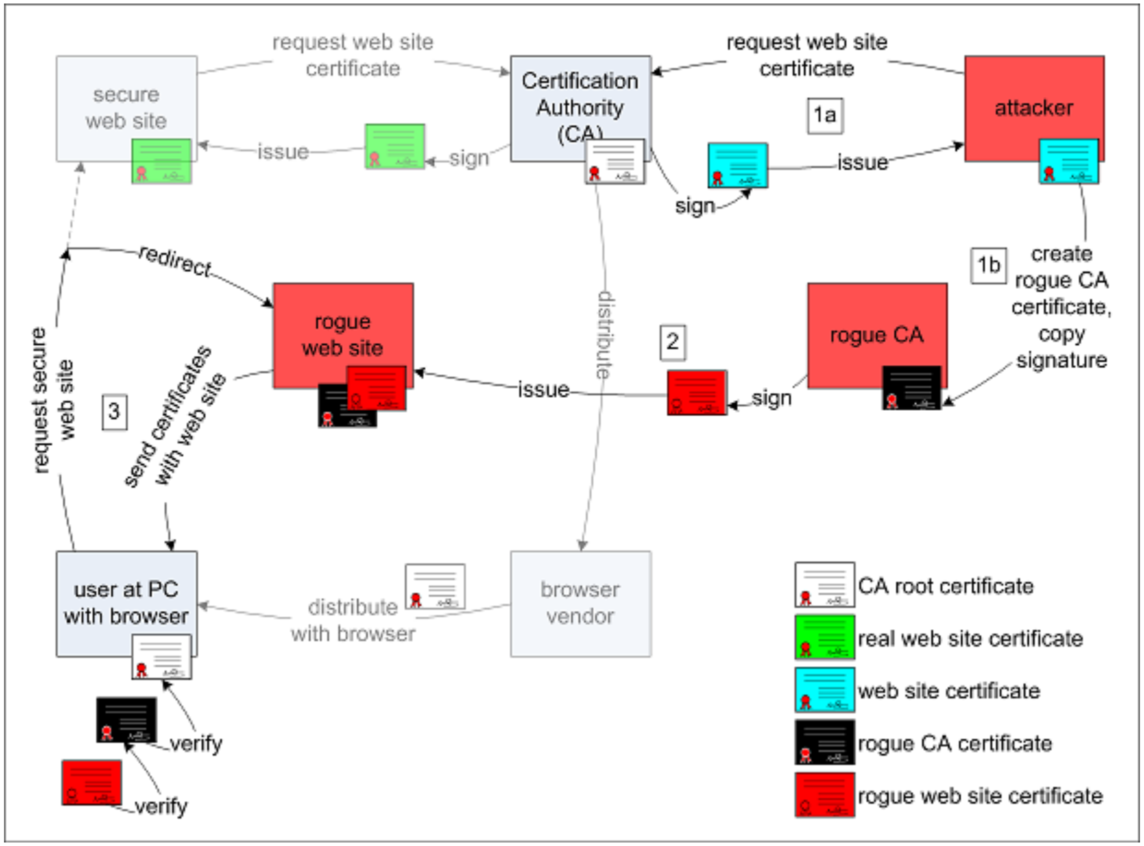


*image credit: http://www.win.tue.nl/hashclash/rogue-ca/

A Recent Attack: Chosen Prefix Collisions

- Why does this attack work?
  - MD5 hash collision against the digital signatures used for certificate validation
    - All trust is placed in expected messages derived from *legitimate* key
    - There is no way to tell the difference between a Man-in-the-Middle and a legitimate site
- The entire infrastructure is always susceptible to trust related attacks if any crypto component is flawed

Can we only trust an entity based on expected numbers?

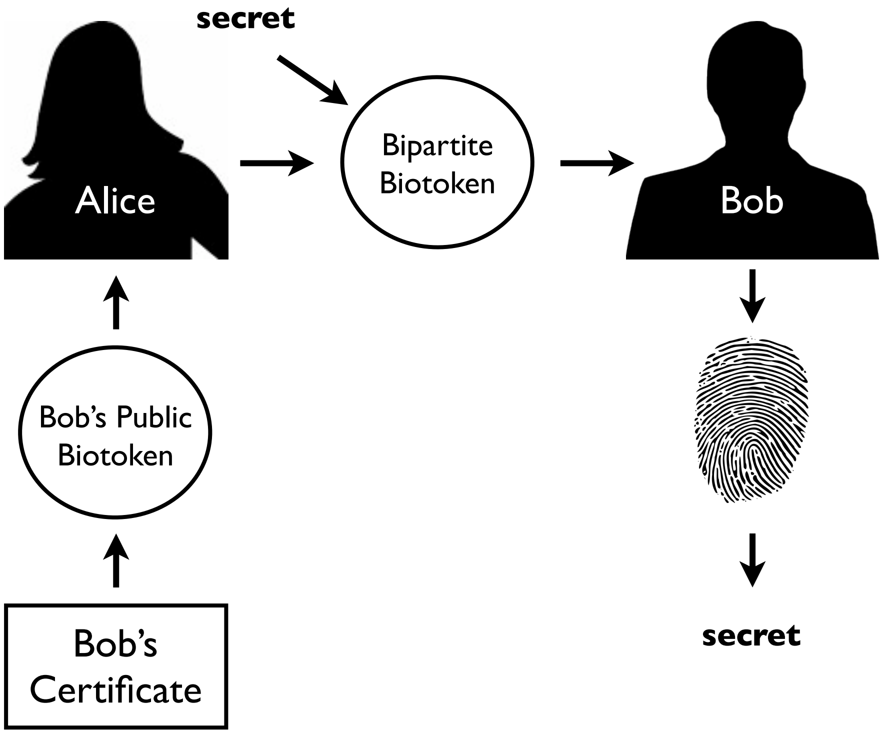
Biometric Solution?

- By adding a second factor, we can mitigate the inherent trust problems with PKI
- What about Biometrics?
  - Improved non-repudiation
  - Strong verification for actors in a transaction, certificate authority establishment, and general certificate issue

Address the trouble with Biometrics using Secure Templates

Benefit of a BKI

- Ability to store public biotokens in digital certificates
  - Any entity in the infrastructure can send secret data that only the owner of the biotoken can unlock



Requirements for a Biocryptographic Key Infrastructure

1. Cryptographically strong protection of the underlying biometric features
2. Ability to revoke and re-issue templates
3. Nested re-encoding, allowing a hierarchy of templates to be generated from a single base template
4. Support for public templates
5. Key-binding capability without the need of intervention by the person associated with the template

Case Study: Revocable Biotokens

- Boult et al. 2007*
  - Assume a biometric produces a value v that is transformed via scaling and translation
    - $v' = (v - t) * s$
  - Split v' into stable component q and residual component r
  - For user j, leave the residual un-encoded (base scheme)
    - $r_j(v')$
  - Encrypt q with public key P
    - $w_{j,1}(v', P)$

*T. Boult, W. Scheirer and R. Woodworth, "Revocable Fingerprint Biotokens: Accuracy and Security Analysis," CVPR 2007.

Nesting Property

- w_j is re-encoded using a transformation function T

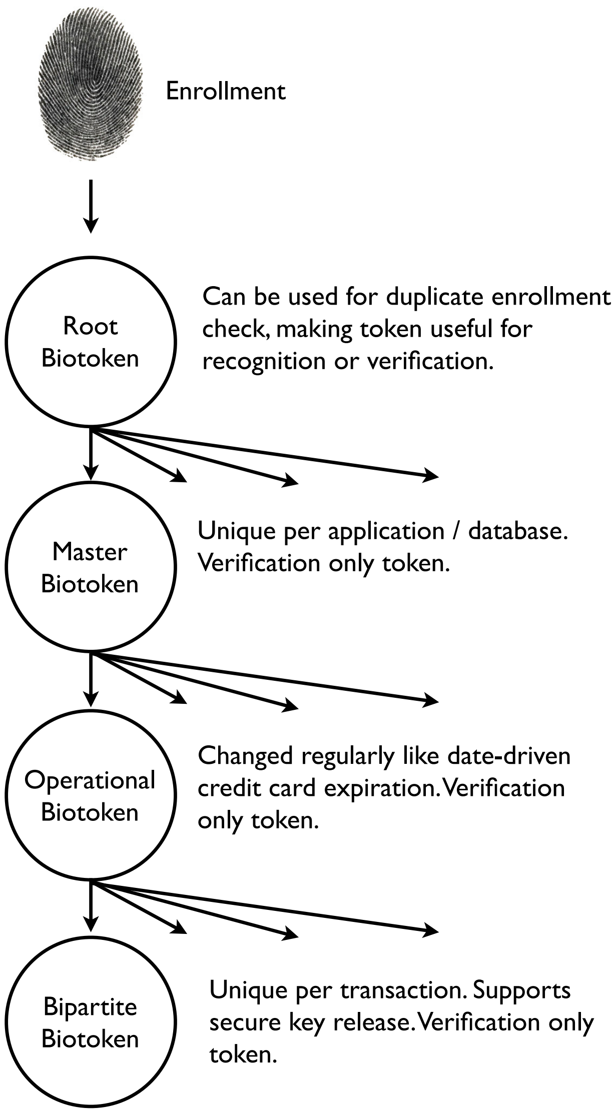
  1st encoding: $w_{j,1}(v', P)$

  2nd encoding: $w_{j,2}(w_{j,1}, T_2)$

  nth encoding: $w_{j,n}(w_{j,n\text{-}1}, T_n)$

- The nesting process is formally invertible via the keys, but cryptographically secure

Biotoken Issue/Re-Issue Tree



Enrollment

Root Biotoken

Can be used for duplicate enrollment check, making token useful for recognition or verification.

Master Biotoken

Unique per application / database. Verification only token.

Operational Biotoken

Changed regularly like date-driven credit card expiration. Verification only token.

Bipartite Biotoken

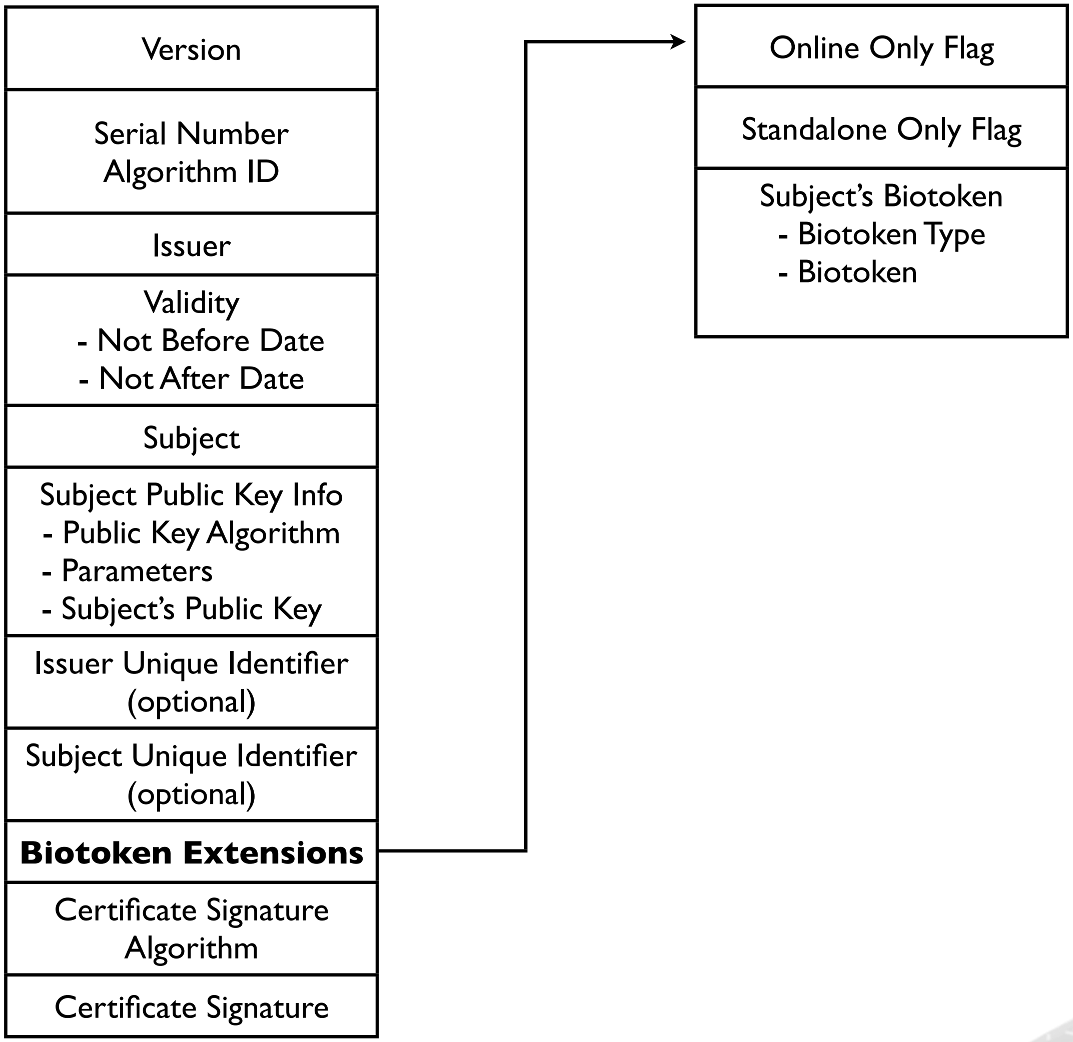
Unique per transaction. Supports secure key release. Verification only token.

Bipartite Biotokens

- Scheirer and Boult 2009*
  - Let B be a revocable biotoken. A bipartite biotoken B_p is a transformation $bb_{j,k}$ of user j's k^{th} instance of B. Any bipartite biotoken $B_{p,k}$ can match any revocable biotoken B_k for the same user.
  - $bb_{j,k}$ must allow the embedding of some data d into B_p
    - $bb_{j,k}(w_{j,k}, T_k, d)$
  - If $B_{p,k}$ and B_k match, d is released

* W. Scheirer and T. Boult, "Bipartite Biotokens: Definition, Implementation, and Analysis," ICB 2009.

Digital Cert. Supporting Biotokens



x.509 v3 digital certificate

Version

Serial Number
Algorithm ID

Issuer

Validity
- Not Before Date
- Not After Date

Subject

Subject Public Key Info
- Public Key Algorithm
- Parameters
- Subject's Public Key

Issuer Unique Identifier (optional)

Subject Unique Identifier (optional)

Biotoken Extensions

Certificate Signature Algorithm

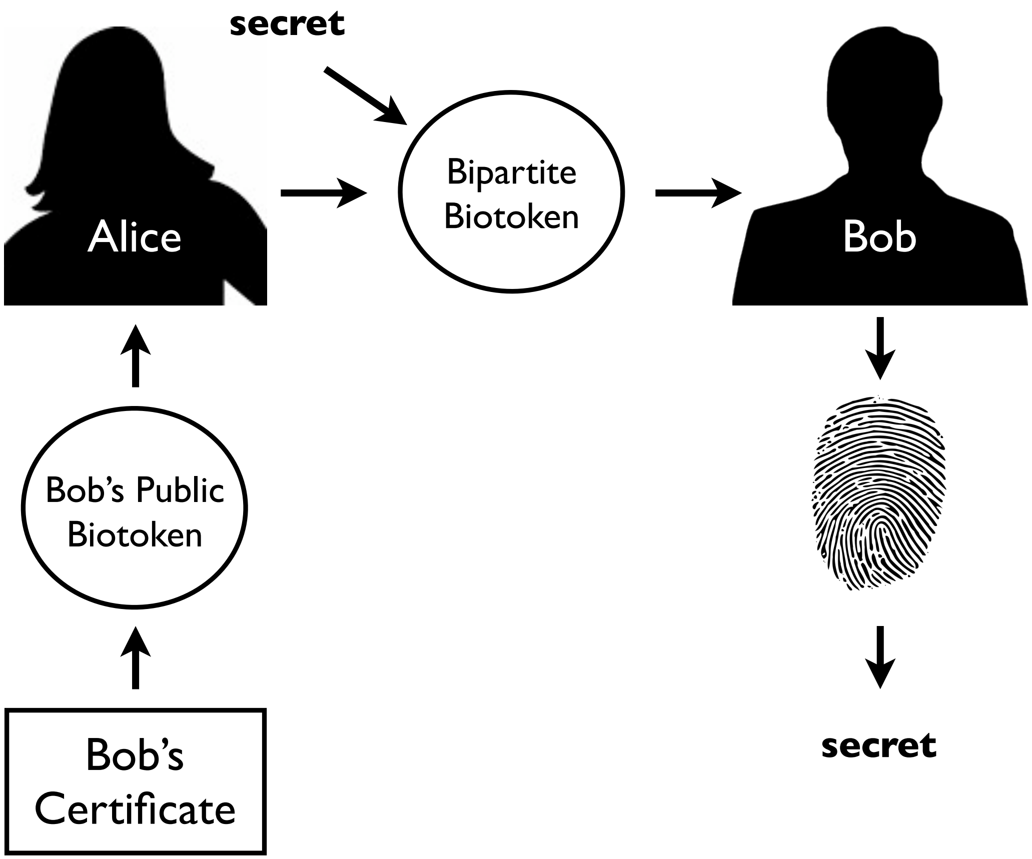
Certificate Signature

Online Only Flag

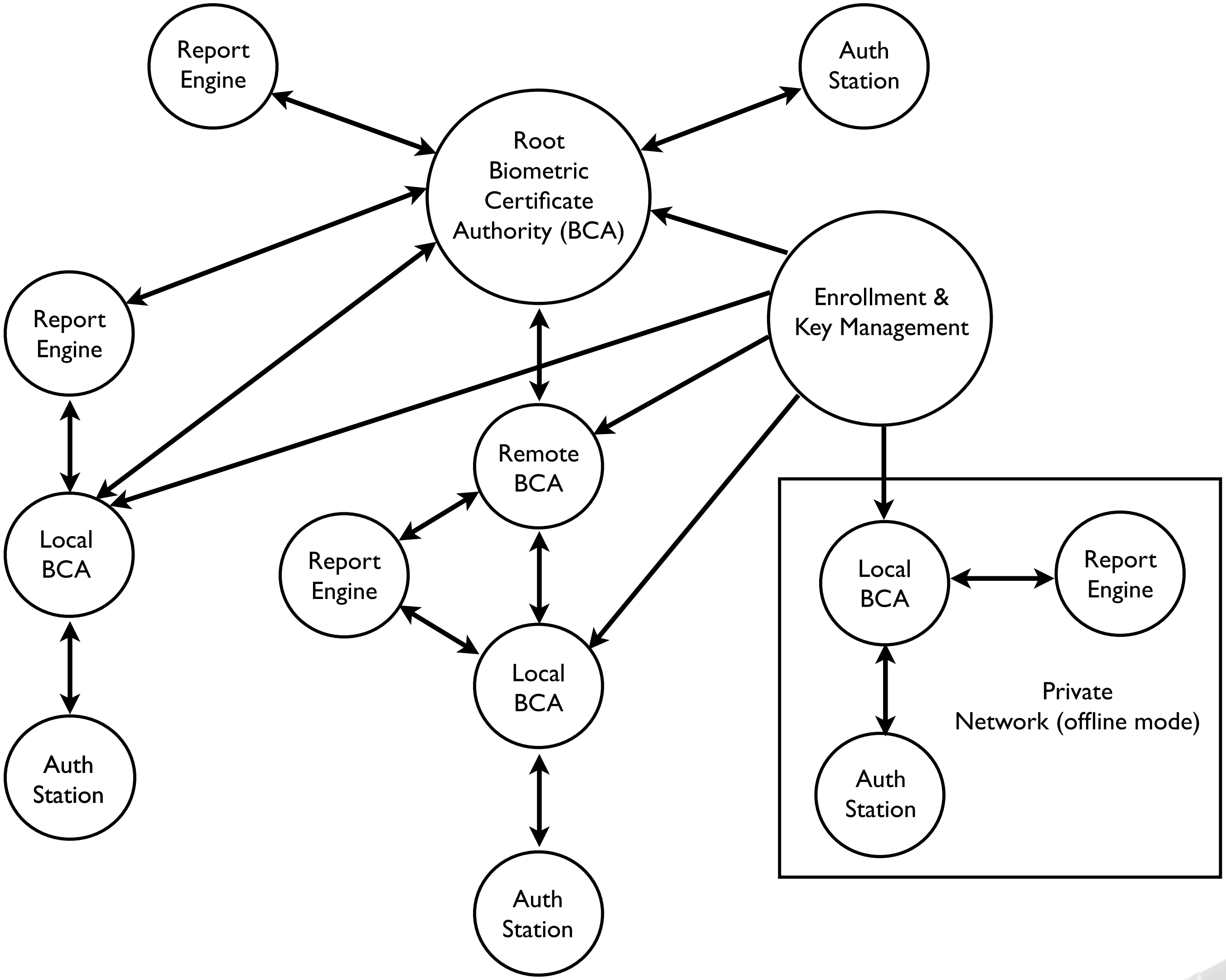
Standalone Only Flag

Subject's Biotoken
- Biotoken Type
- Biotoken

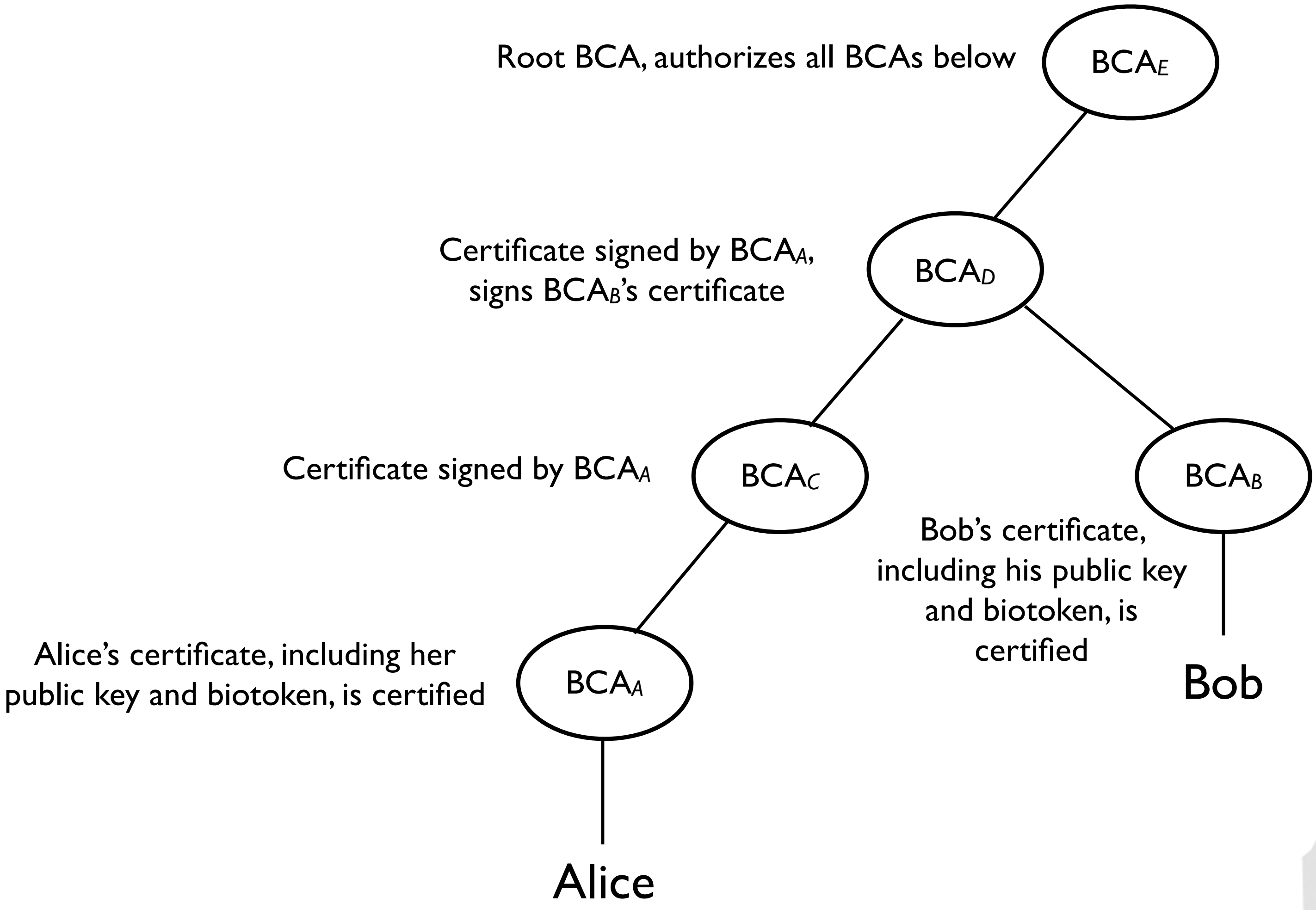
Benefit of a BKI



A Biocryptographic Key Infrastructure



Certificate Retrieval Path



Root BCA, authorizes all BCAs below

BCA$_E$

Certificate signed by BCA$_A$,
signs BCA$_B$'s certificate

BCA$_D$

Certificate signed by BCA$_A$

BCA$_C$

BCA$_B$

Bob's certificate,
including his public key
and biotoken, is
certified

Bob

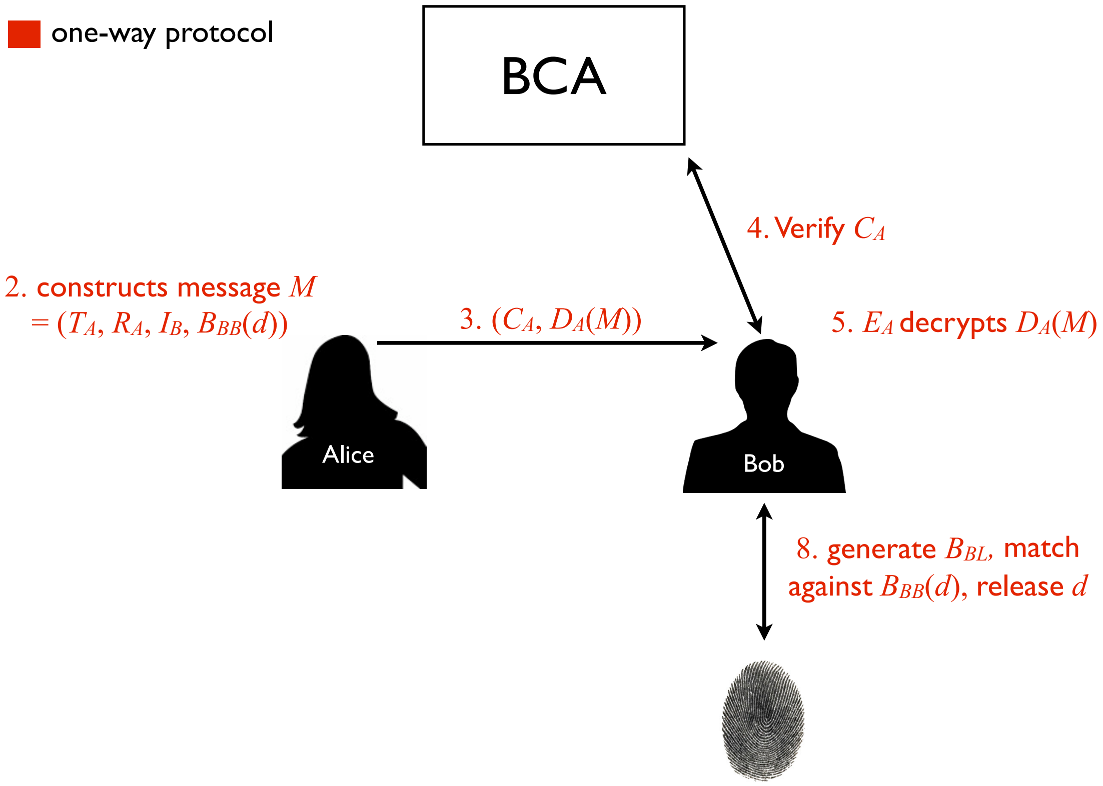
Alice's certificate, including her
public key and biotoken, is certified

BCA$_A$

Alice

One-Way Protocol

- Sender creates bipartite biotoken using Receiver’s public certificate
- Establishes identity & trust of message Receiver
- Provides secure one-way data channel



🟥 one-way protocol

BCA

4. Verify C_A

2. constructs message $M = (T_A, R_A, I_B, B_{BB}(d))$

3. $(C_A, D_A(M))$

5. E_A decrypts $D_A(M)$

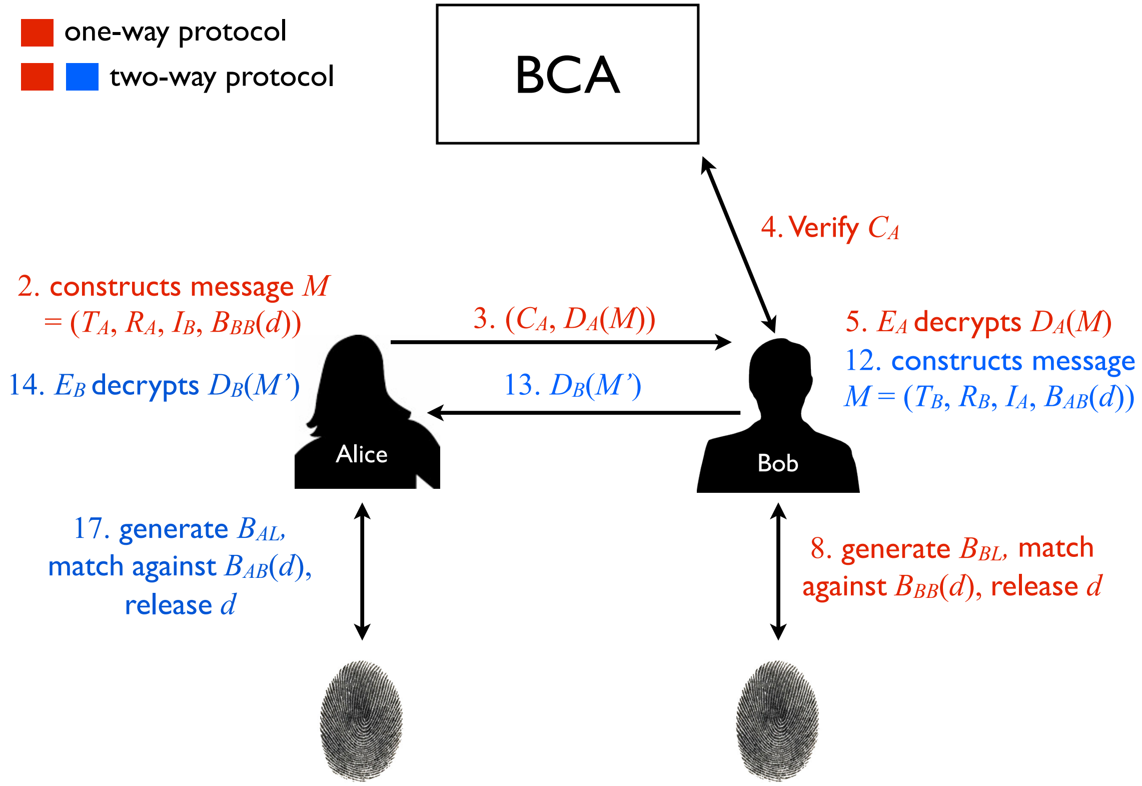
Alice

Bob

8. generate B_{BL}, match against $B_{BB}(d)$, release d

Two-Way Protocol

- Provides Sender assurance that the Receiver is not an impostor
- Validates one identity in the transaction



🟥 one-way protocol

🟥 🟦 two-way protocol

BCA

4. Verify C_A

2. constructs message $M = (T_A, R_A, I_B, B_{BB}(d))$

3. $(C_A, D_A(M))$

5. E_A decrypts $D_A(M)$

12. constructs message $M = (T_B, R_B, I_A, B_{AB}(d))$

13. $D_B(M')$

14. E_B decrypts $D_B(M')$

Alice

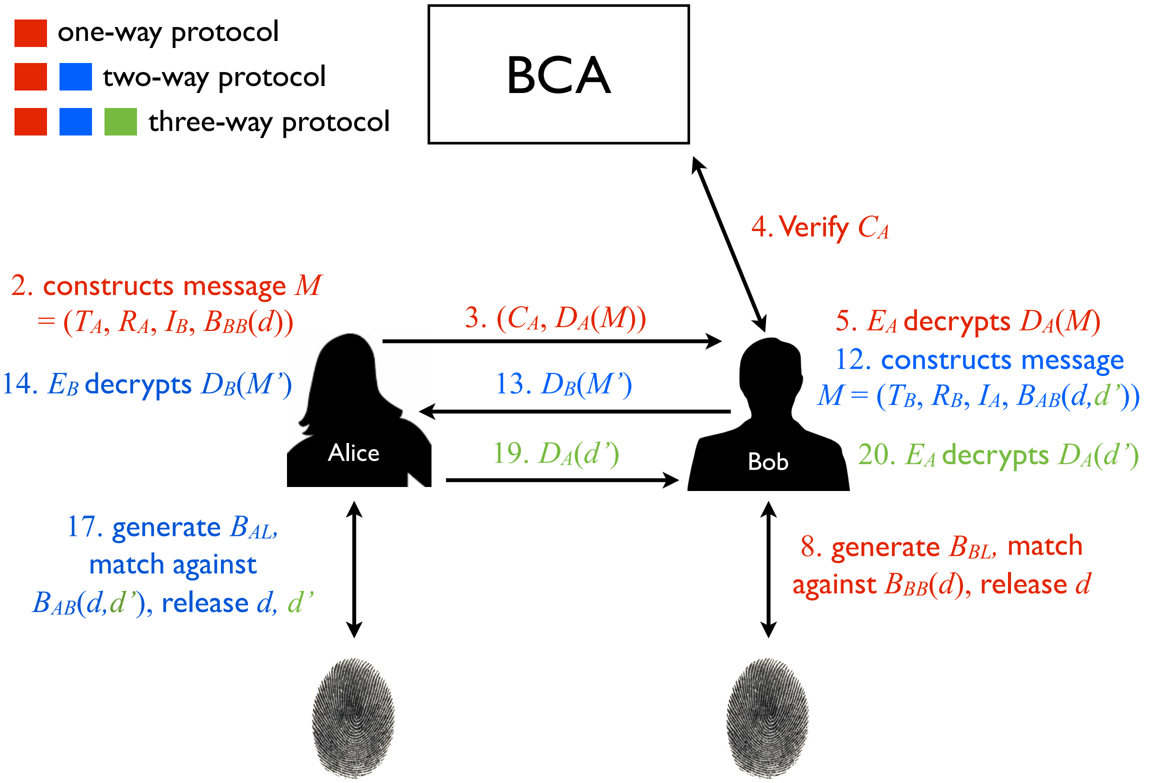
Bob

17. generate B_{AL}, match against $B_{AB}(d)$, release d

8. generate B_{BL}, match against $B_{BB}(d)$, release d

Three-Way Protocol

- Provides Receiver assurance that the Sender is not an impostor
- Validates both identities in the transaction



🟥 one-way protocol

🟥 🟦 two-way protocol

🟥 🟦 🟩 three-way protocol

BCA

4. Verify C_A

2. constructs message $M = (T_A, R_A, I_B, B_{BB}(d))$

3. $(C_A, D_A(M))$

5. E_A decrypts $D_A(M)$

12. constructs message $M = (T_B, R_B, I_A, B_{AB}(d,d'))$

14. E_B decrypts $D_B(M')$

13. $D_B(M')$

Alice

19. $D_A(d')$

Bob

20. E_A decrypts $D_A(d')$

17. generate B_{AL}, match against $B_{AB}(d,d')$, release d, d'

8. generate B_{BL}, match against $B_{BB}(d)$, release d

Certificate Revocation

- We must consider certificate *and* biometric re-issue
- Scenario 1: Manual re-issue
  - Certificate owner generates a new public-private key pair and a new biotoken
- Scenario 2: Automatic re-issue of biotoken
  - BCA retains transformation keys, reverts public biotoken to a lower level, issues new transformation keys and public biotoken
- Scenario 3: Automatic re-issue of key-pair
  - BCA issues new key-pair, transmits secret key to owner via bipartite biotoken

CRN Message

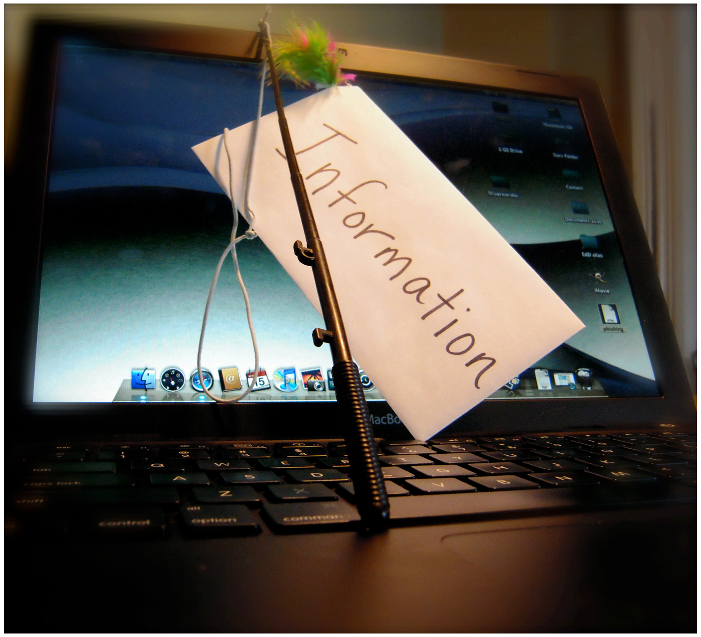
Certificate Re-issue Notification

Serial Number
New Serial Number
Biotoken Re-issued Flag
Key-pair Re-issued Flag
Biotoken and Key-pair Revoked Flag
*Keyring for Biotoken (Optional)
Biotoken Type (Optional)
Biotoken (Optional)
Signature

*Keyring is encrypted with the user's public key

New Applications

- Thwart Man-in-the-Middle and Phishing attacks!
- Bio-Kerberos
- Bio-S/Key
- BKI-enabled LDAP
- Biometric Digital Signatures



The BKI bring identity to crypto protocols!

What does this mean for a program like UID?

- Measures against Corruption
  - The user has control over their biometric data
  - Per application biotokens from a single base enrollment
  - If a biotoken is stolen, we have a process to revoke and re-issue credentials
- Secure framework for financial transactions
  - Microfinance

Thank You!

Questions?