

Applying the Biometric Fusion Approach to Trusted Identity Programs

Stephen Price-Francis and Robert Barnes

Biometrics Consortium Conference

Alexandria, VA, 23-25 September 2002

Part – 1

Defining the Issues

“... the [biometric] industry is fragmented, doesn't have a standard, and doesn't work well together ... I'm afraid there will be only a piecemeal adoption of biometrics technology.”

Senator Diane Feinstein (D-CA)

U.S. Senate Judiciary Subcommittee on
Technology, Terrorism, and Government
Information

14 November 2001

“A lot needs to get done. The industry is ready to step up to the challenge. Let us get to it.”

Dr. Joseph J. Atick

Keynote Speech to the Biometric
Consortium Conference

13 February 2002

Some Key Questions ...

- *Which biometric technology is best?*
- *How do we decide?*
- *Do we really need to decide?*

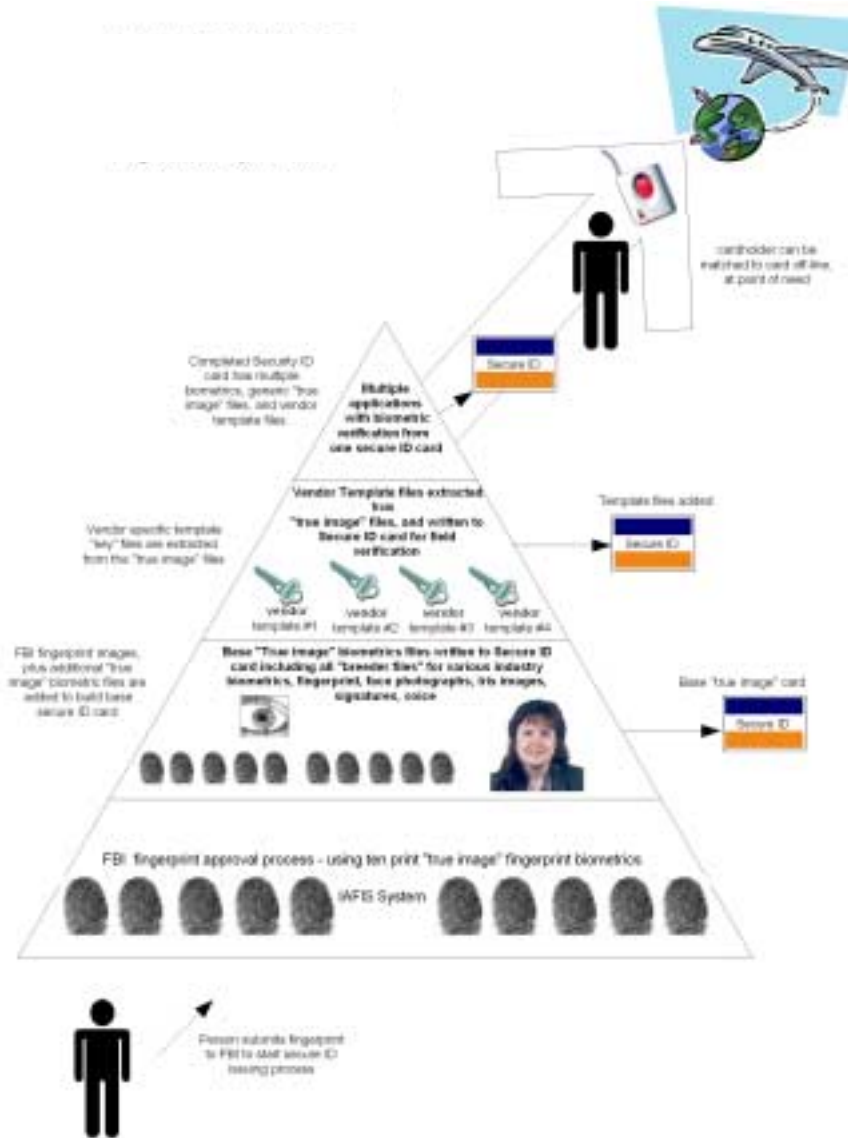
“Trusted Identity”

- *“... it should be a mandated designation if your job is within the critical infrastructure of the nation.”*
 - Transportation Workers Identification Card
 - Nuclear Facility Workers Identification Card
- *“... we should make available the notion of ‘trusted identity’ to other programs ...”*
 - Drivers licenses
 - Trusted traveler

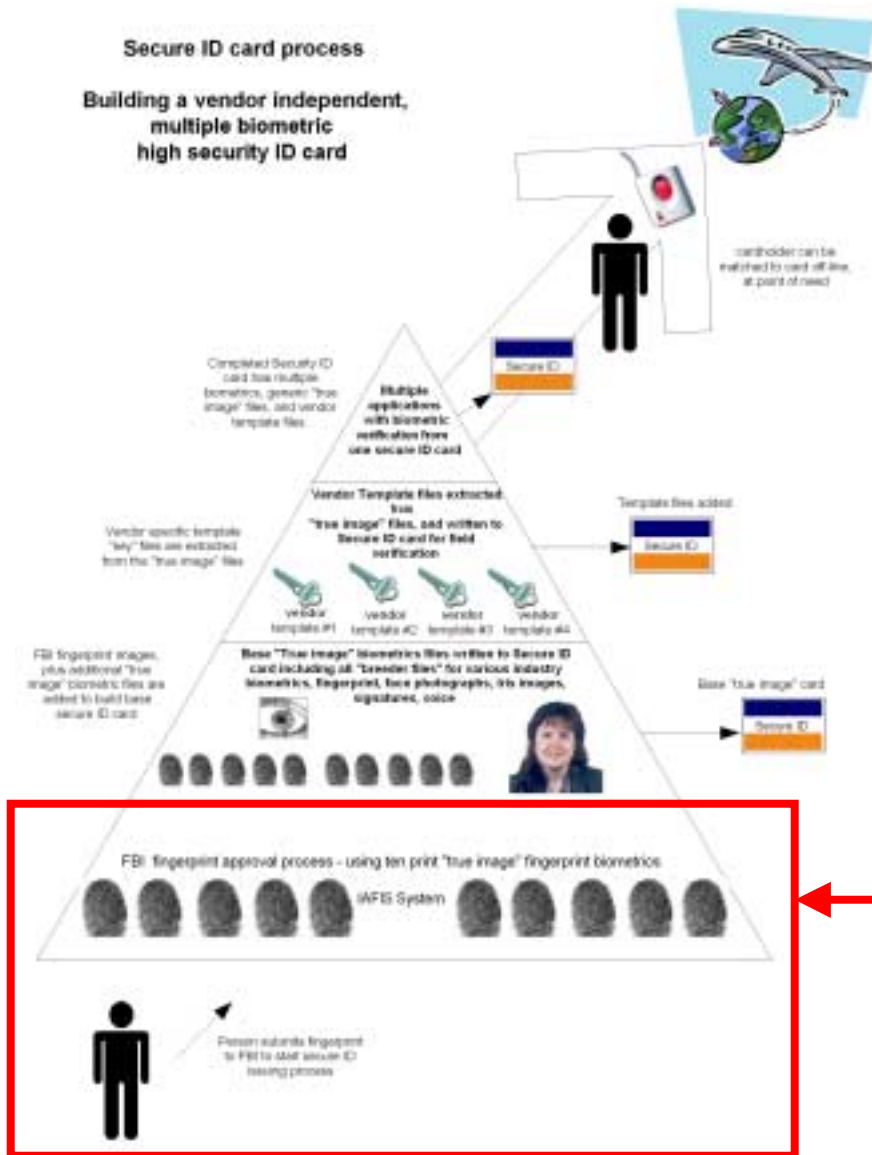
Using Biometrics Effectively

- Biometric identification systems are not perfect ... each system has a margin of error.
- Biometric Fusion ...
 - Uses a multiple biometric decision-making process
 - Reduces probability of false rejection
 - Enhances security of the biometric system
- Store “true images” rather than proprietary templates to ensure a vendor-independent biometric system

Ensuring a “Trusted Identity”



Building a Vendor-Independent Multiple-Biometric High Security Identification Card

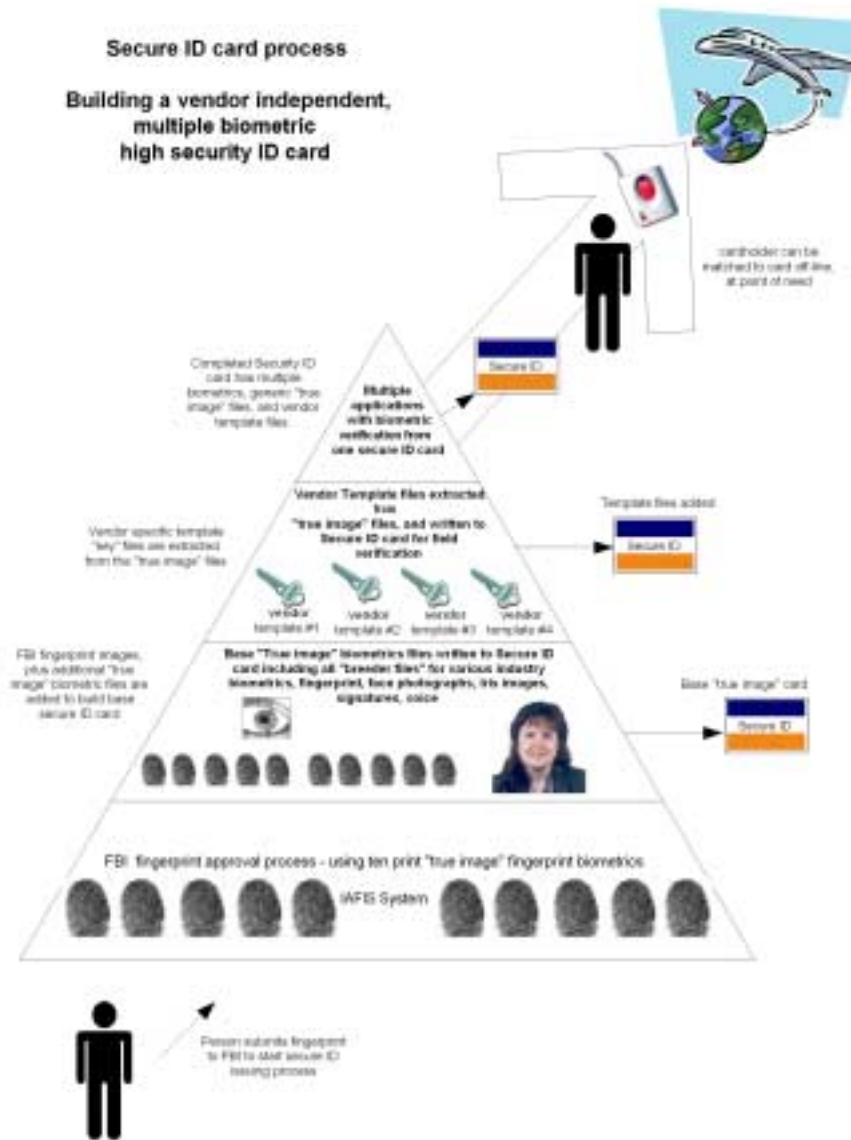


Establish True Identity

Any ID card issued on a false identity is worthless

- Authorization for a requested service or activity must be determined at application and re-validated periodically during the life of that authorization.
- To avoid privacy concerns, databases used during application should only be those determined to be relevant to the requested service or activity.
- Fingerprint-based Criminal History Records Checks (CHRC) could become a minimum requirement for establishing true identity at application.

Verifying Identity

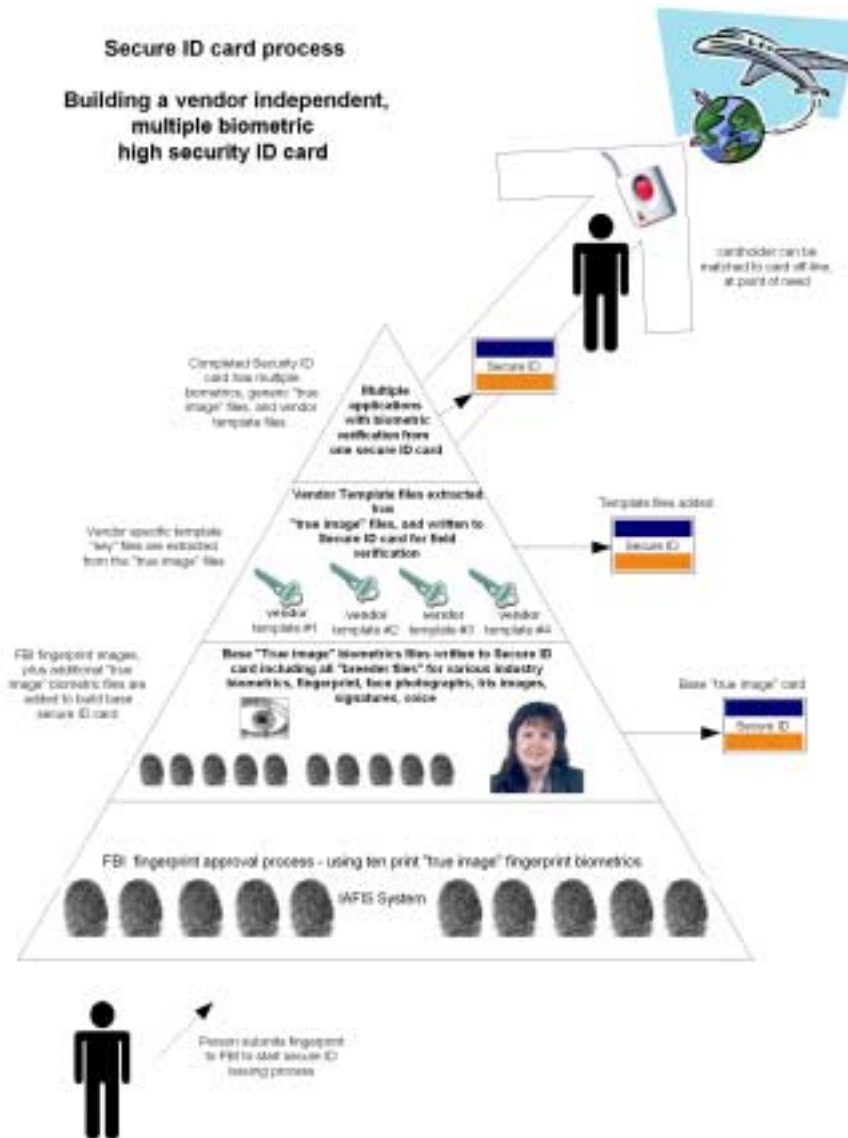


Verifying a person's true identity requires:

1. A secure identification card that cannot be easily counterfeited;
2. One or more biometric means to link the person to that card with absolute certainty; and
3. A secure, automated interface to verify that the person and card links are valid.

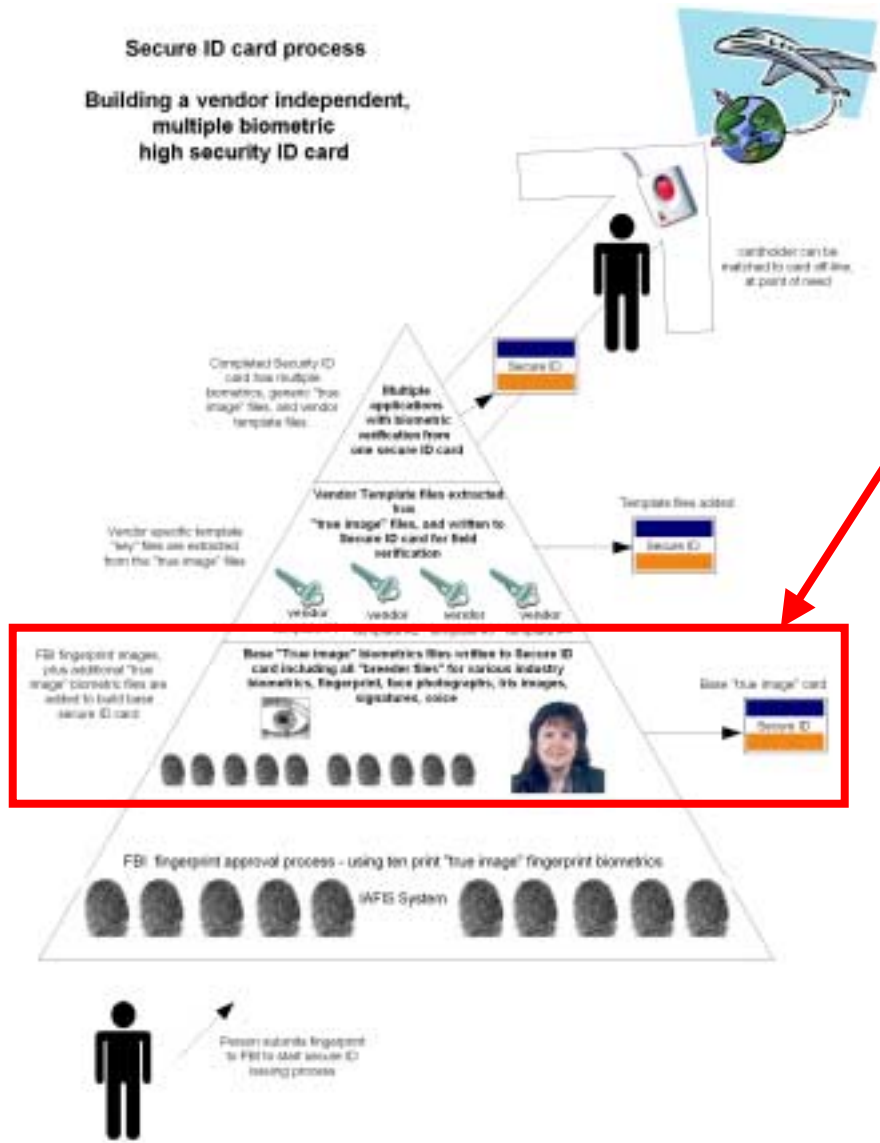
A secure identification card is a personal identification document, which verifies that a person is who he says he is, is not a threat, and has authorization for the requested service or activity.

Biometric ID System



Requirements for an effective biometric ID system:

1. Implement more than one biometric;
2. Allow room to add new biometrics seamlessly;
3. Assure off-line verification ability;
4. Provide for the selection of an appropriate biometric based upon application requirements; and
5. Assure integrity of the biometric files from issuer to user.



True Image Biometrics

Store original, high resolution biometric image files on the ID card

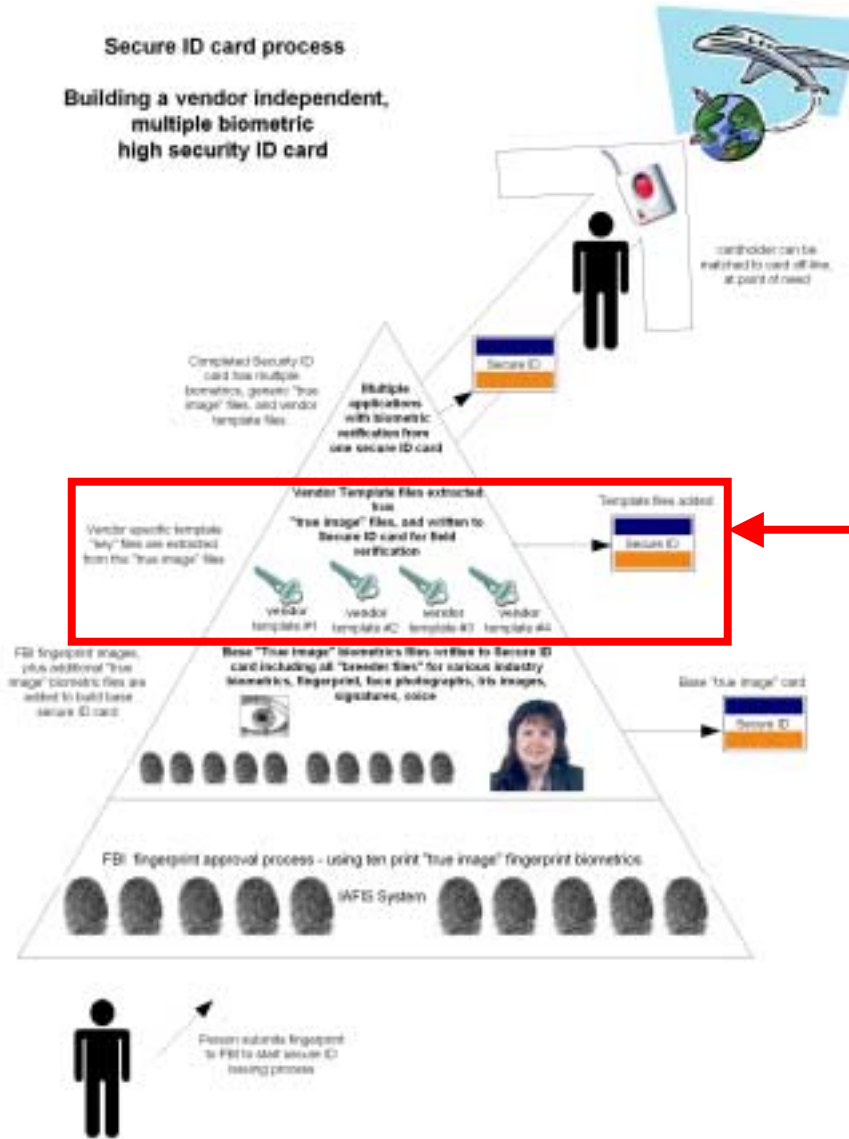
For example, store ...

... the complete FBI-quality DPI gray-scale fingerprint image ...

... high resolution face scans, iris scans, voice prints, signatures, and other selected biometrics.

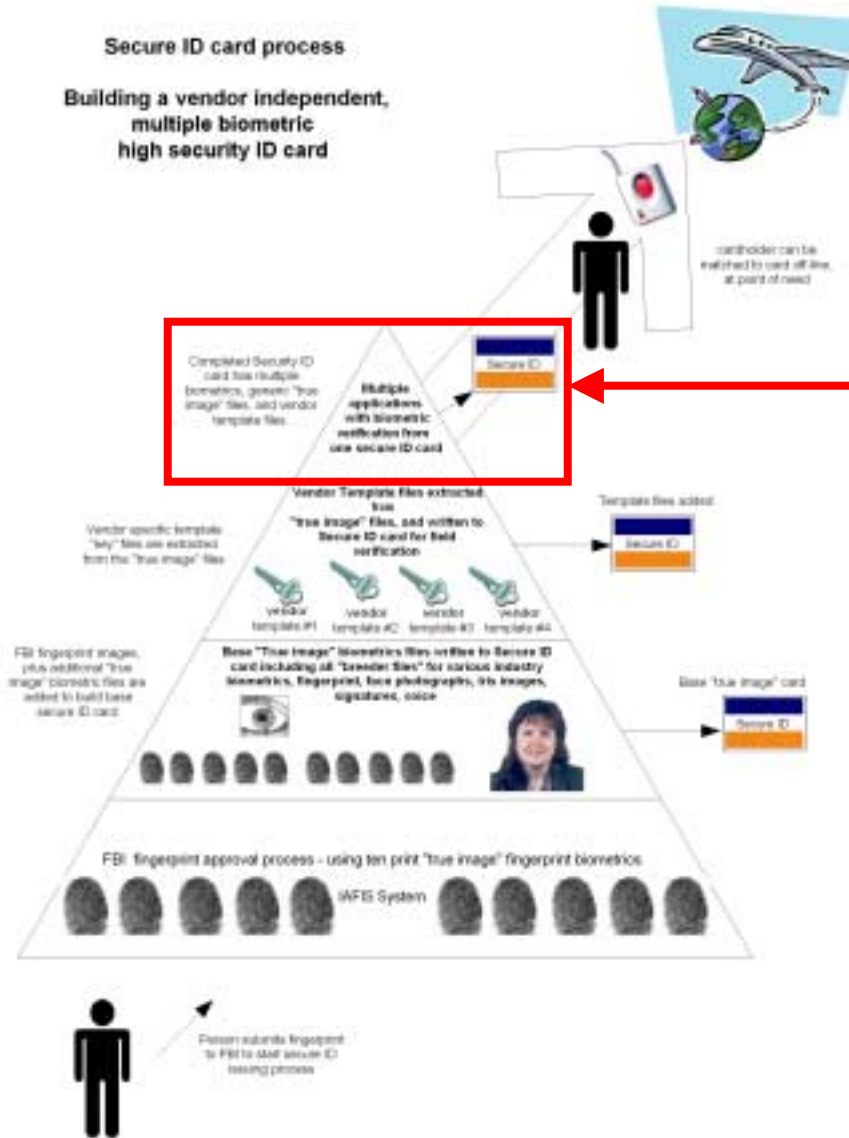
This "base" biometric approach of storing "true images" maintains a broad open architecture for the use of multiple biometric systems that are vendor independent.

Vendor Template Files



- Extract vendor-specific “minutiae” template files from “base” biometric files
- Any number of such vendor-specific template files could be extracted and stored on the same card along with the card holder’s set of “true image” base files.
- This approach eliminates the need to select one vendor’s biometric template for a specific application.

Multiple Applications

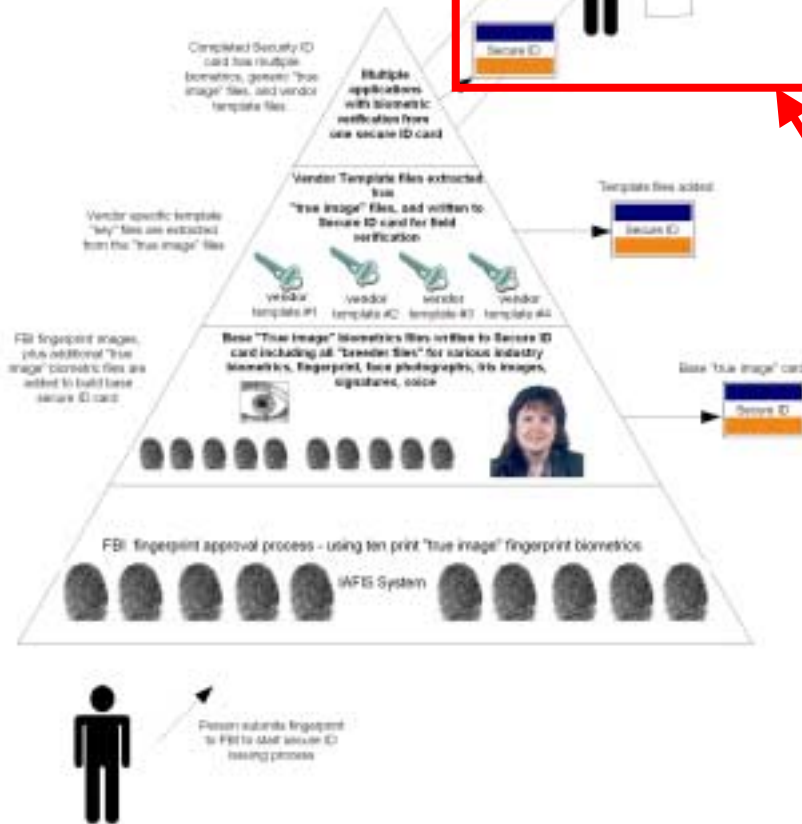


Use different biometrics for different screening requirements

- There is no perfect biometric system. Each has its strengths, weaknesses, and vulnerabilities.
- To avoid false rejection as well as the possibility that someone might try to defeat a one-biometric system, multiple biometric identifiers should be used.
- Not all locations will want to use the same method of biometric identification.
- New biometrics may need to be added as they become available.

Secure ID card process

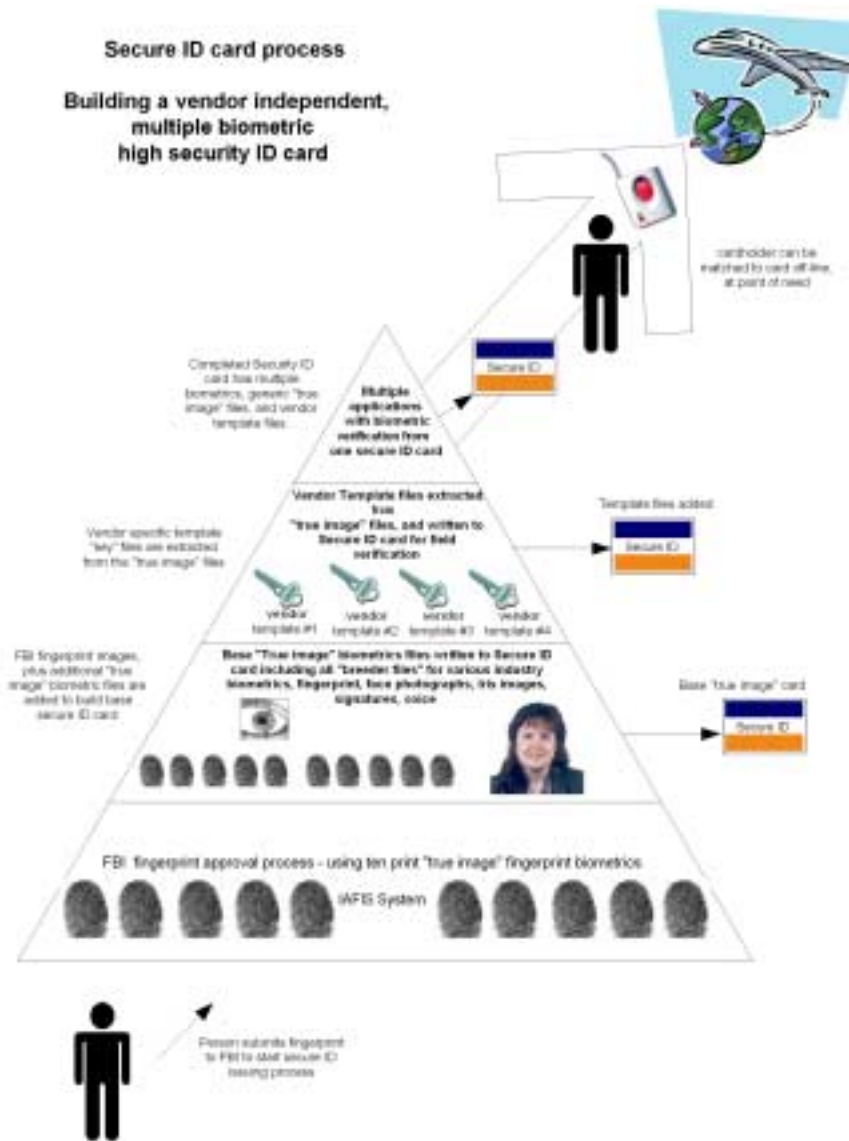
Building a vendor independent,
multiple biometric
high security ID card



Off-Line Verification

Minimize privacy concerns while maximizing accuracy of personal identification

- Personal information remains in the control of the card holder.
- Highly centralized, on-line systems are subject to overload, system-related failures, hacking, and cyber-terrorism.
- A central database, national identification system that is always on-line could provide a single point of failure for our entire society if our enemies ever targeted it.



Optical Card Solution

An Optical Memory Card provides:

- Sufficient unalterable memory capacity on one card to store multiple "true image" biometrics plus multiple, unique vendor templates.
- The capability to create a vendor-independent biometric solution for each application or screening requirement.
- The world's most counterfeit-resistant identification card.

Using Biometrics Effectively

- Implement more than one type of biometric;
- Provide sufficient memory capacity to add new biometrics seamlessly;
- Assure off-line verification capability;
- Provide for selection of the appropriate biometric based upon requirements of the application; and
- Assure the integrity of the biometric files from issuer to user.

More information is available about Biometric Applications using the Optical Memory Card ...

- **Developing user requirements**
- **Technical issues and challenges**
- **Prototyping issues and challenges**
- **Application development lessons learned**
- **Specific application summaries**

www.lasercard.com