On-Card Matching, Match-On Card

MOBILITY & IDENTITY AUTHENTICATION & SECURITY & PRIVACY

DIGENT

R1.0 2015-03

Definition

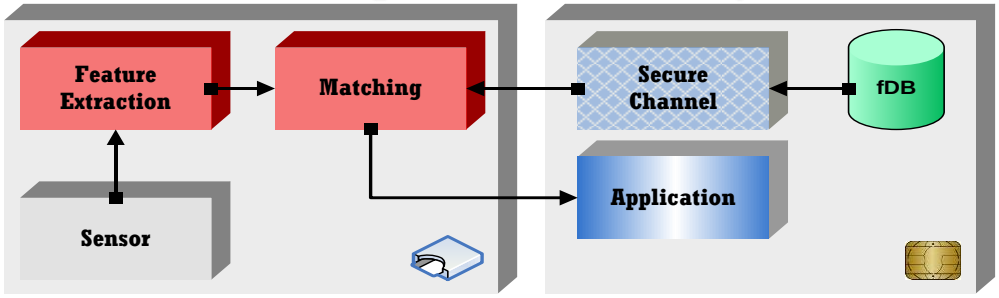
Biometric technology is becoming increasingly popular as a means of accurate **identity authentication**. To further enhance the **security** and **privacy** of biometric technology, the biometric match-on-card technology is proposed.

- The process of biometric data acquisition and feature extraction is done at the reader while the matching is done inside the smartcard.
- During the initial enrolment stage, the original template constructed at the reader is stored inside the smartcard.
- During matching, the reader will construct the query template which is then sent to the smartcard for matching.
- The final matching decision is computed inside the smartcard itself and the entire original template is thus not released from the smartcard.

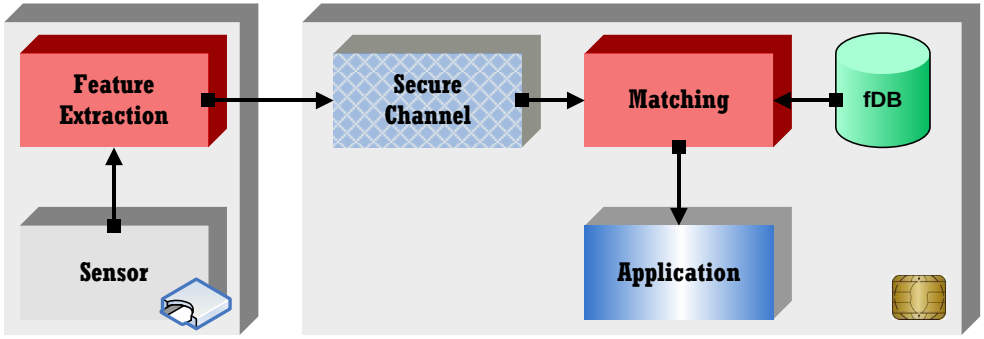
Technology

The combination of biometric and smartcard offers the advantages of **mobility**, **security** and **strong identity authentication** capability and at the same time, offers the owner a high degree of control over who has access to that biometric data. **Privacy** concern is hence minimised.

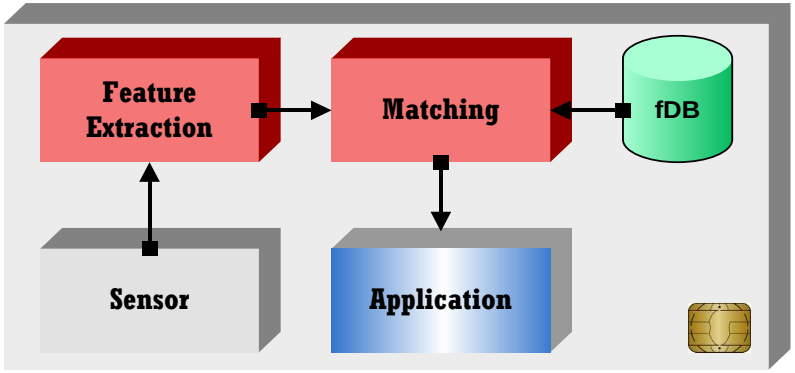
- **Off-Card Matching, Store-On Card, Template-On Card**



- **On-Card Matching, Sensor-Off Card, Match-On Card**



- **System-On Card, Sensor-On Card**



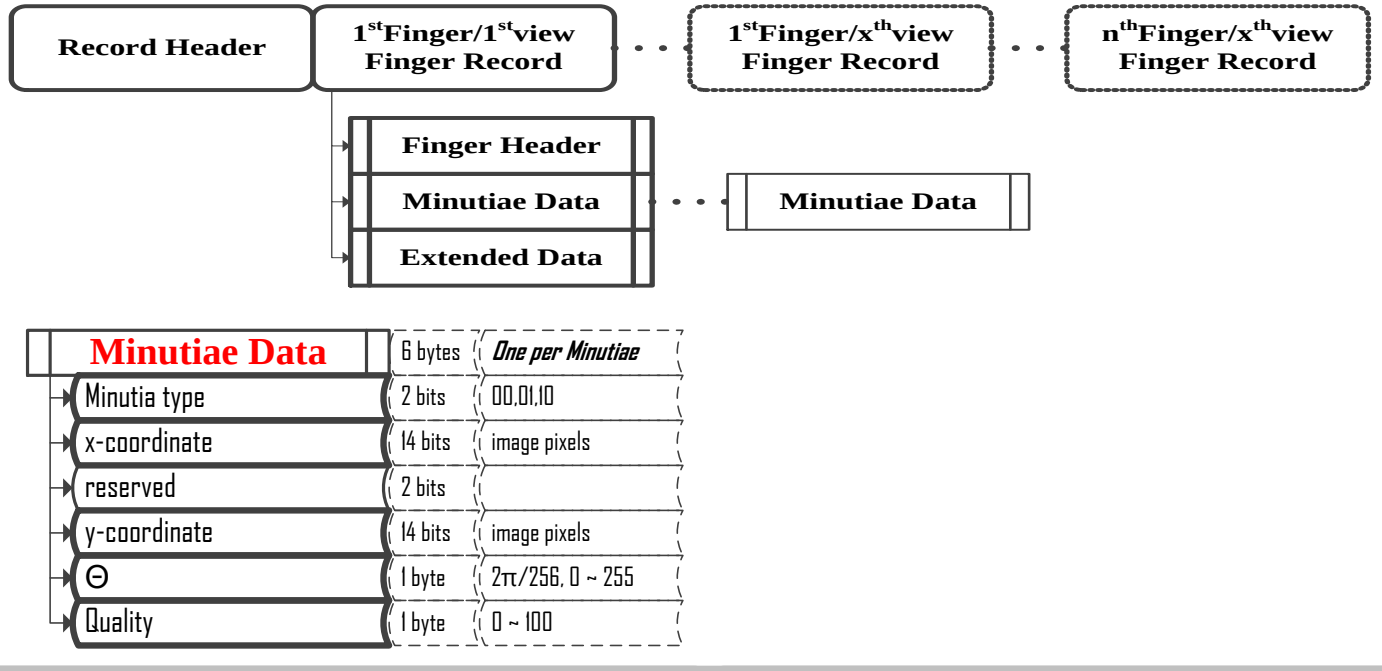
Standard (1)

- **ISO/IEC 19794-2** - Finger Minutiae data
  - ♦ Finger Minutiae Record Format
  - ♦ Finger Minutiae Card Format
    - Normal Size Finger Minutiae Format
    - Compact Size Finger Minutiae Format
- **ISO/IEC 7816-11** - Personal verification through biometric methods
- **ISO/IEC 19785-1** - Common Biometric Exchange Formats Framework
- **ISO/IEC 24787** - On-Card biometric comparison

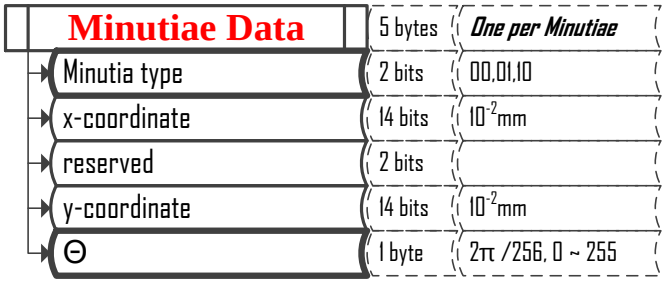
- **ANSI INCITS 378** - Finger Minutiae Format for Data Interchange
- **ANSI INCITS 398** - Common Biometric Exchange Formats Framework

Standard (2)

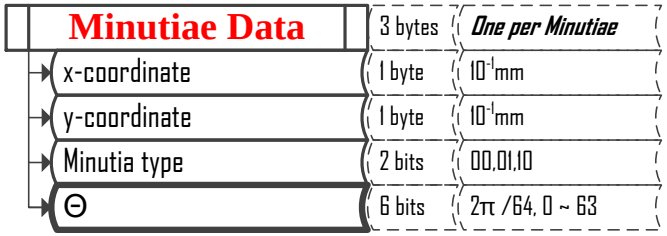
♦ **ISO/IEC 19794-2** - Finger Minutiae data ; **Finger Minutiae Record Format**



• Card ; **Normal Size Finger Minutiae Format**

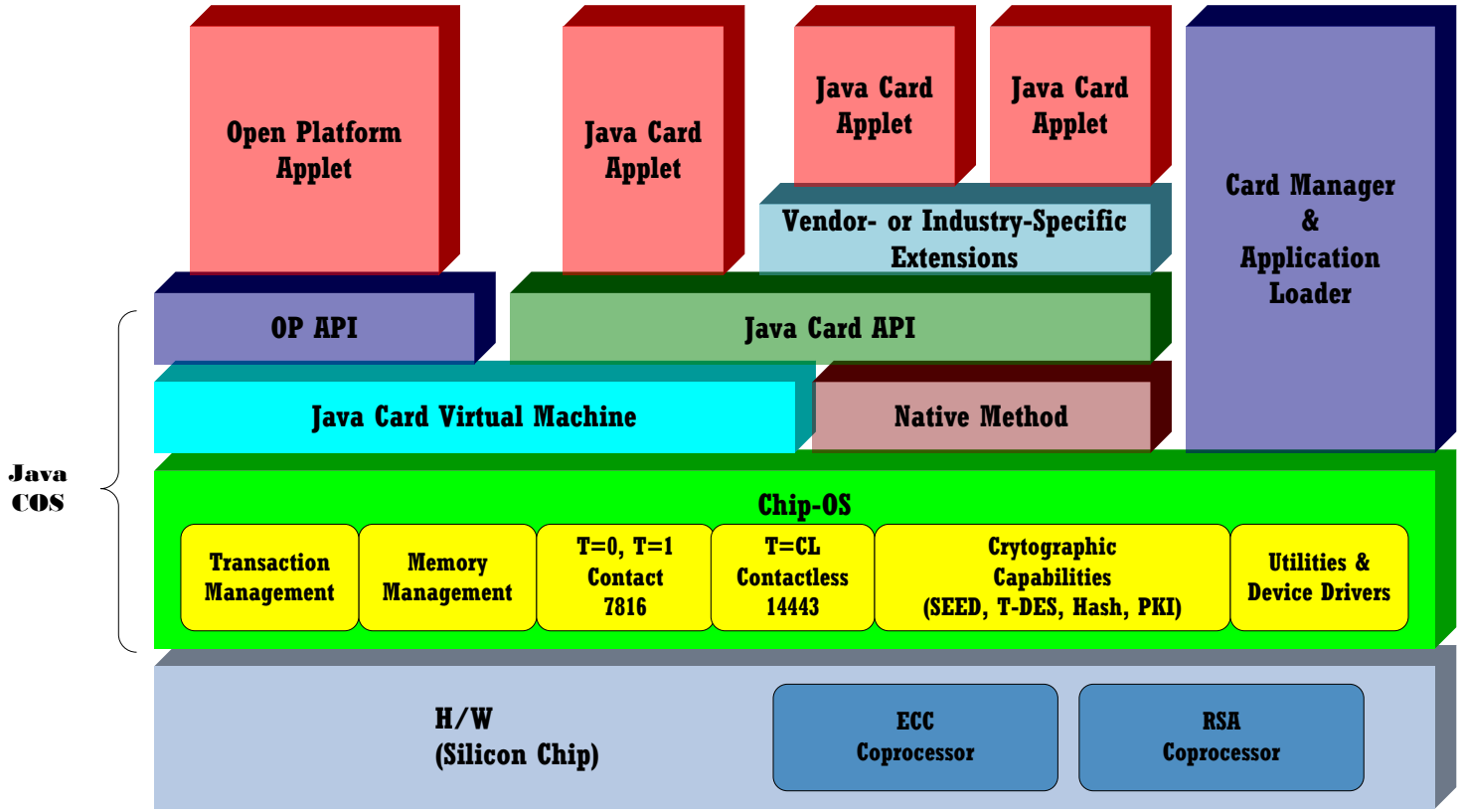


• Card ; **Compact Size Finger Minutiae Format**



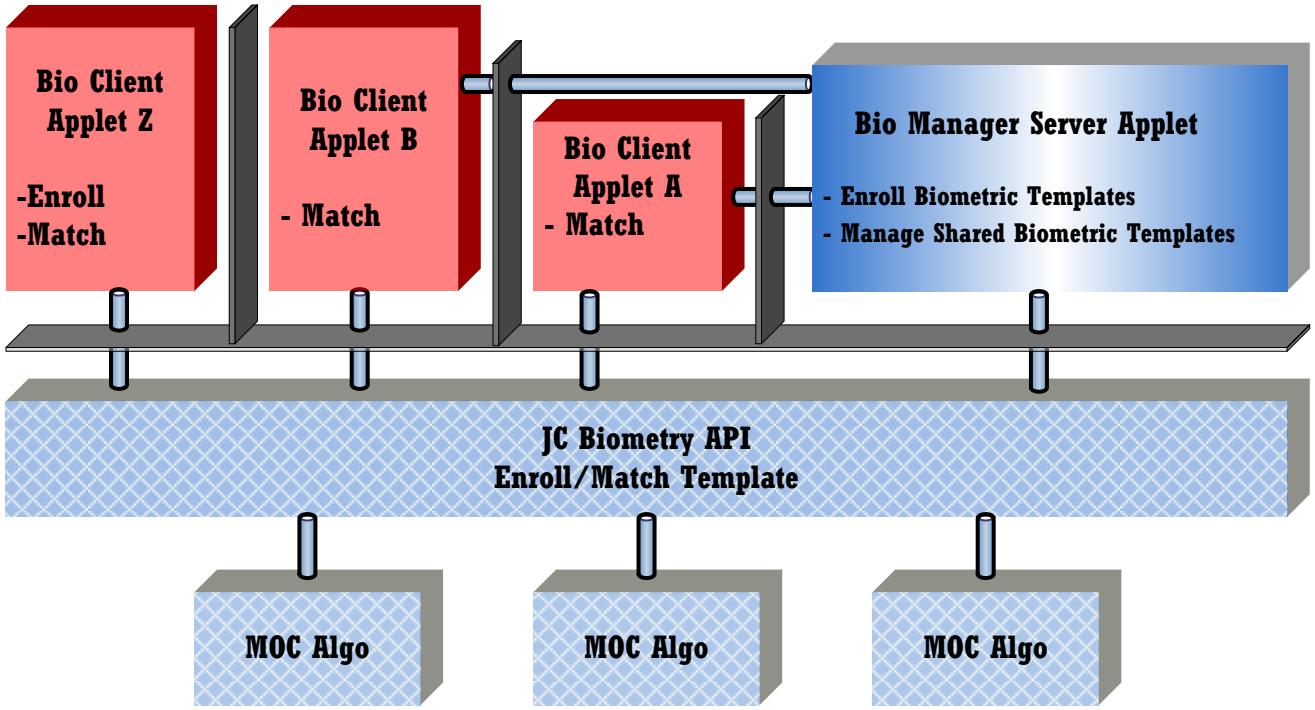
MOC Framework (1)

- JavaCard Functional Configuration



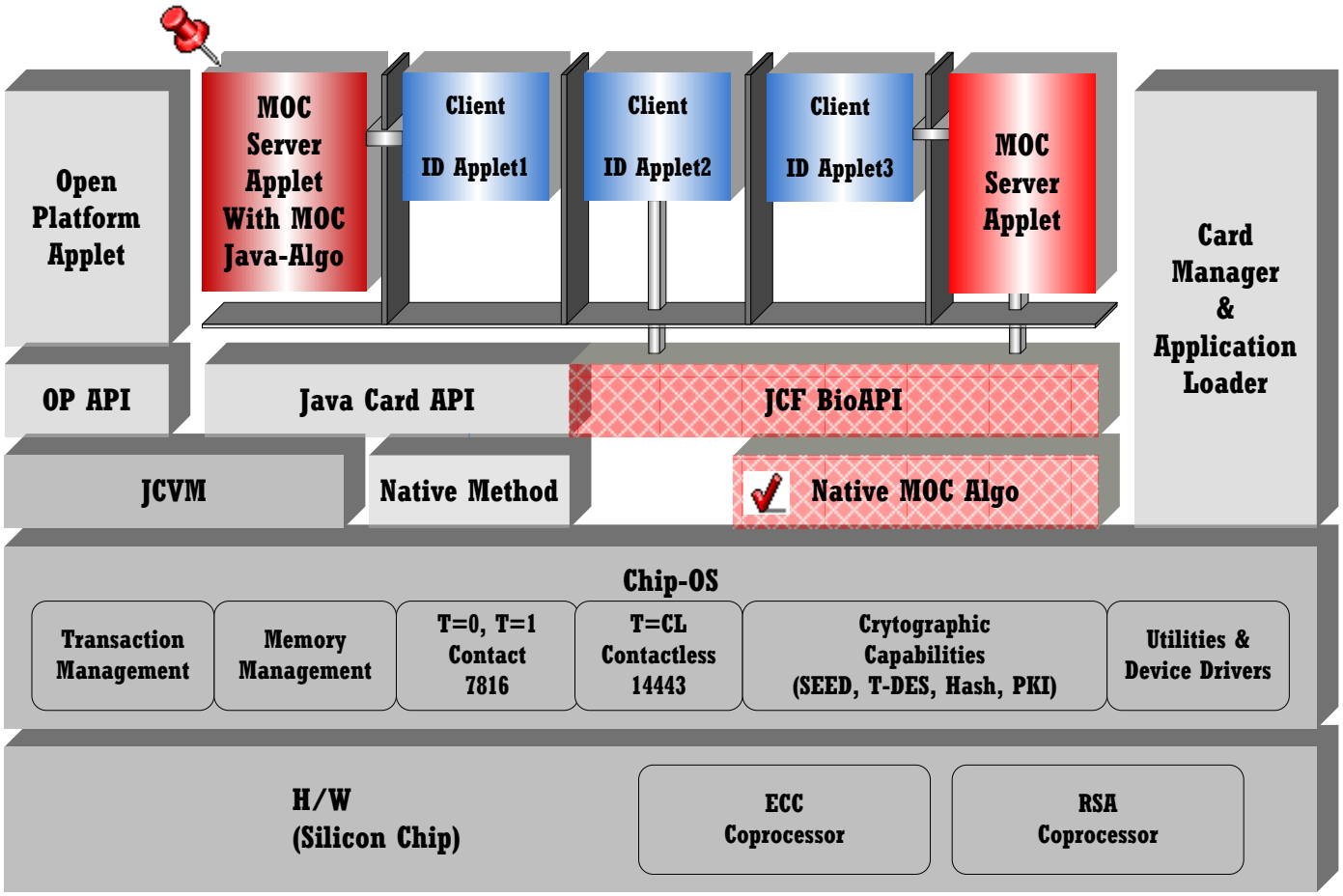
MOC Framework (2)

- JavaCard JC Biometry API(javacardx.biometry)

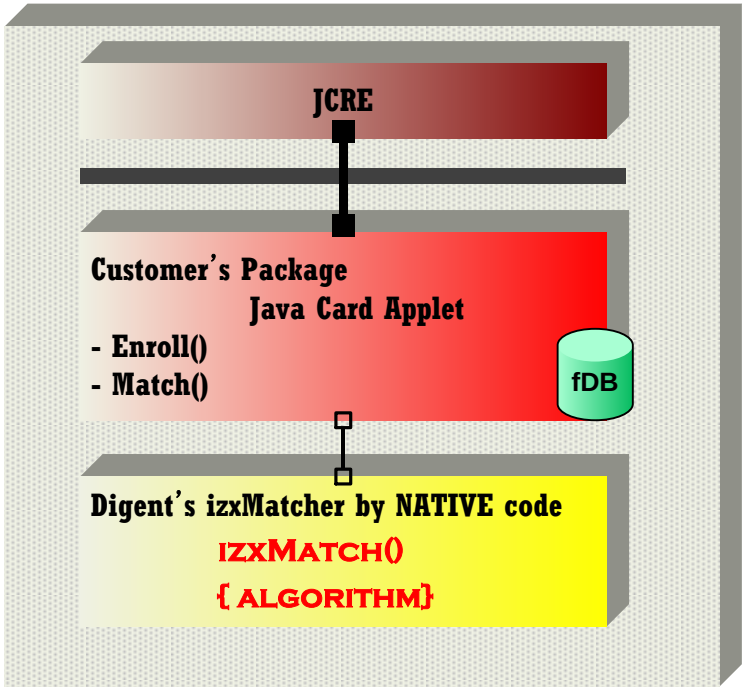


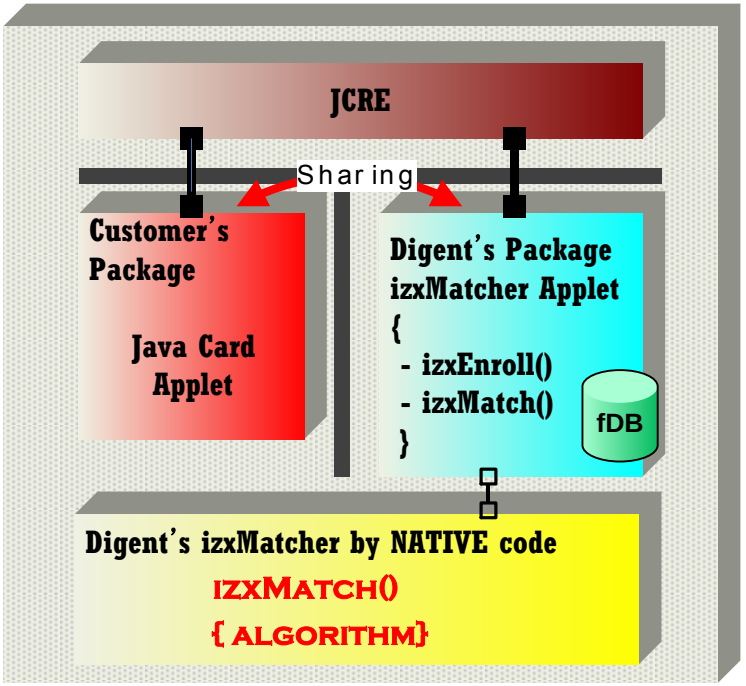
MOC Framework (3)

- JavaCard Match-On Card

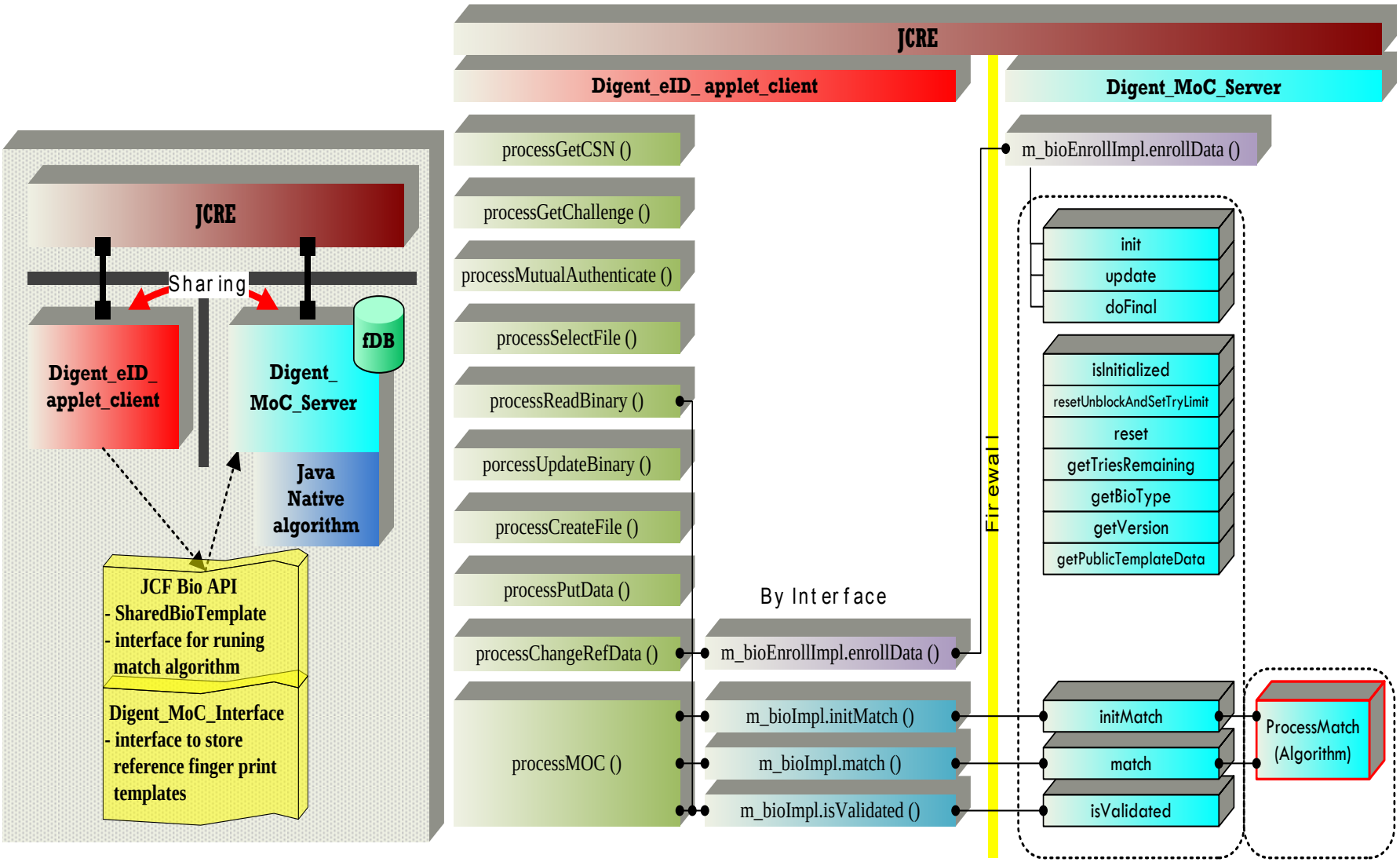


JC Implementation (1)

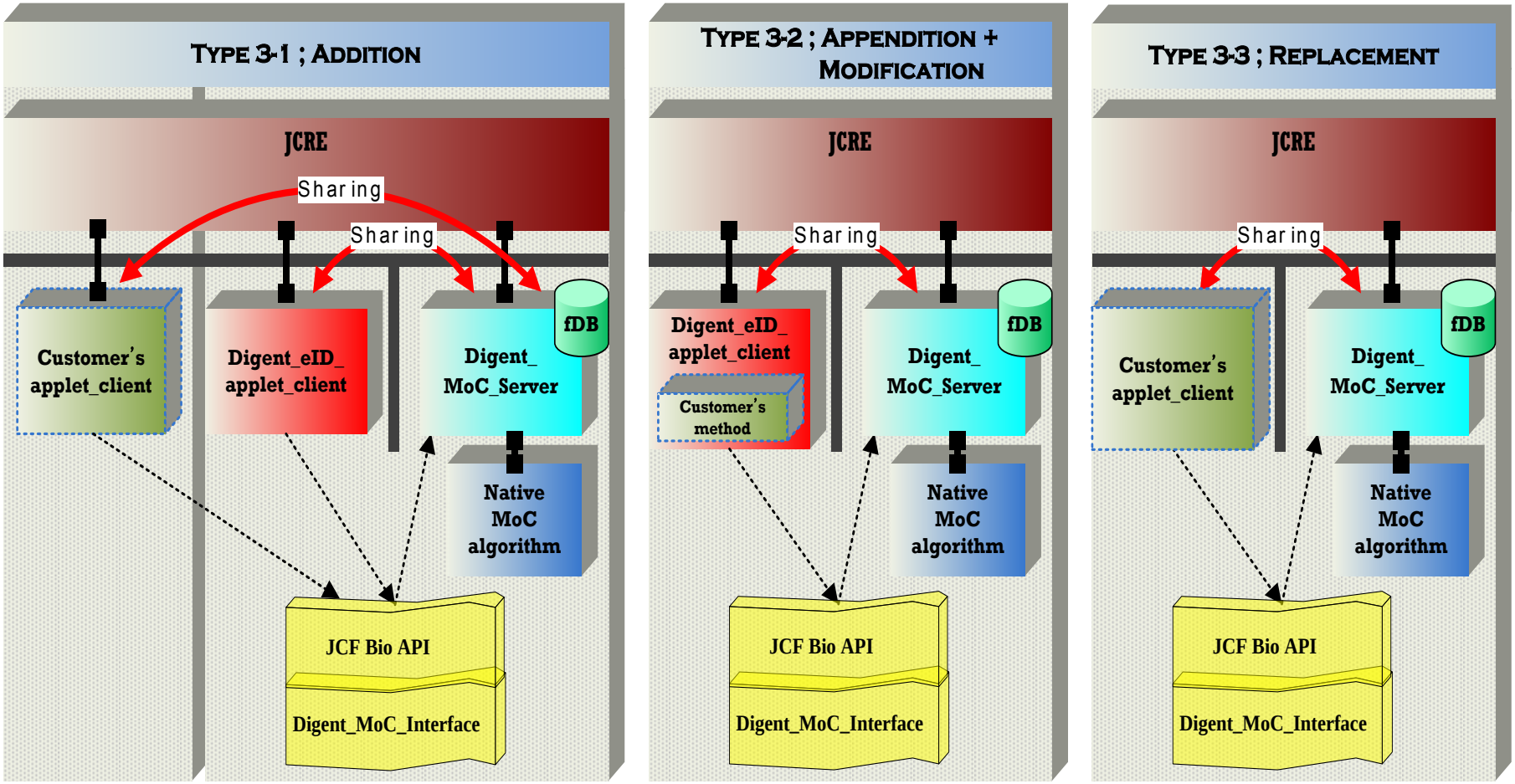




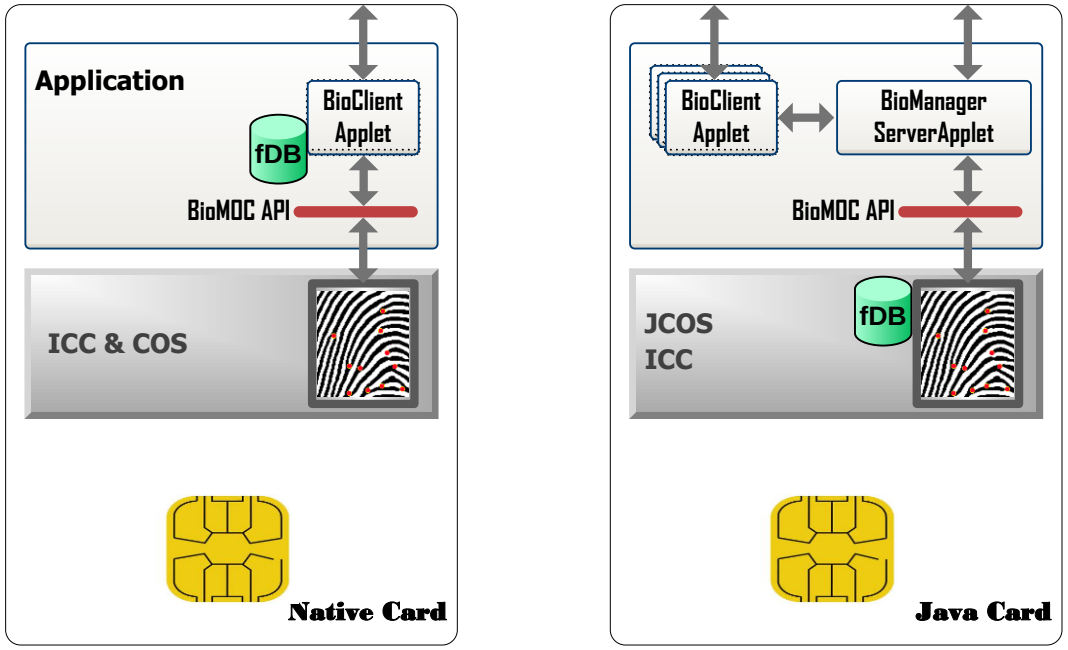
JC Implementation (2) – example1



JC Implementation (2) – example2



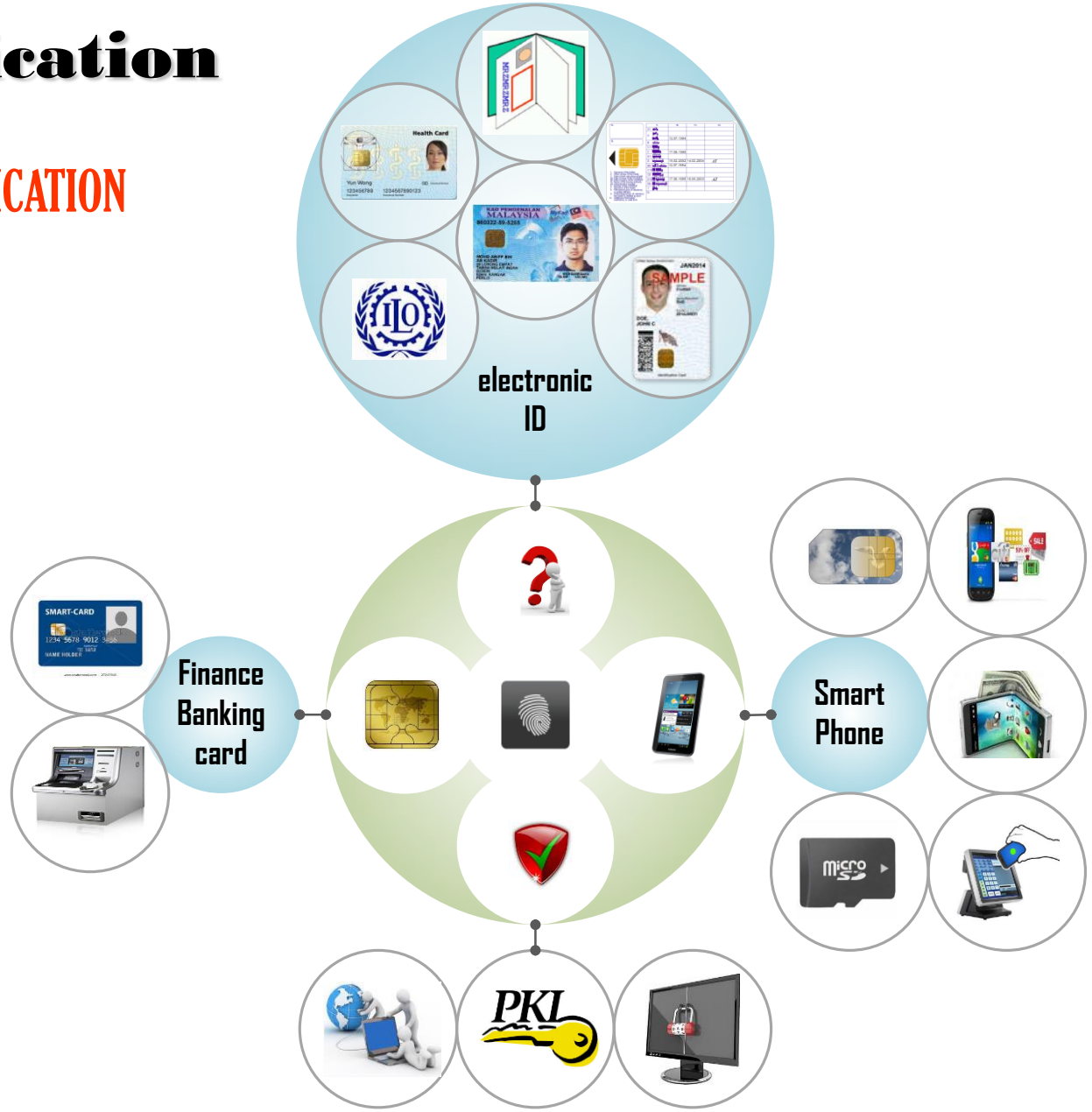
Implementation – Native & JavaCard



Application

AUTHENTICATION

SECURITY

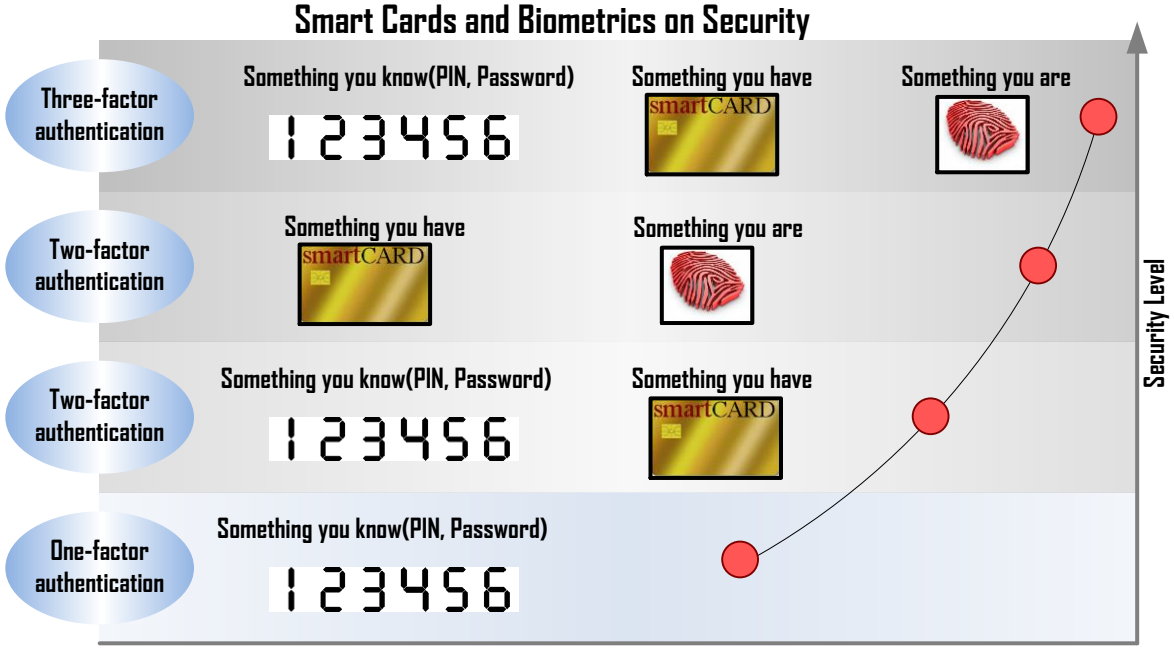


PRIVACY

MOBILITY

Benefits of Combining Smart Card Technology and Biometrics

- Enhanced Privacy
- Enhanced Security
- Improved System Performance and Availability
- Improved Efficiency
- Upgradability and Flexibility



Biometric MOC technology

- holds great promise in offering **good security** and **privacy protection**.

- has come a long way to become feasible today at an attractive cost and more can be done to make it better and cheaper.

- provides a **good platform** for the launch of a **nation-wide strong identity authentication capability** and this will open up many other new applications and business possibilities that provide better convenience, security and protection to the users as compared to what is available today.

- has also gained a foothold in the global push for **machine readable travel documents** which will hopefully lead to a global opportunity.

[Technical notes]

▪ Enhanced Privacy

Using smart card technology significantly enhances privacy in biometric ID systems. The smart card provides the individual with a personal database, a personal firewall and a personal terminal. It secures personal information on the card through advanced cryptography and digital signatures to prevent alteration or replacement of biometric data and to prevent cloning of the card. This allows the individual to control access to their biometric information and eliminates the need for central database access during identity verification.

When used in combination with biometrics, a smart card ID becomes even more personal and private. A biometric provides a strong and unique binding between the cardholder and the personal database on the card, identifying the cardholder as the rightful owner of this card. The biometric cannot be borrowed, lost, or stolen like a PIN or a password, and so strengthens the authentication of an individual's identity. A smart card-based ID system also gives the cardholder control over who can access personal information stored on the card. A biometric further enhances this control, ensuring that only the rightful cardholder can authorize access to personal information.

Because of their cryptographic processing capabilities, smart cards can be used in ID systems to increase the trustworthiness of terminals. This can translate into increased privacy for individuals and can allow cardholders to use anonymous devices as personal terminals. The increase in terminal trustworthiness is especially critical for biometric systems. Biometric ID systems rely on terminals to perform live-sample captures of some biometric trait. The ID system should be able to trust the biometric reader to capture and process a user's biometric. If it cannot, the integrity of the whole authentication process is compromised.

Smart card technology can help to address this vulnerability. Using well-established security protocols, a smart card can participate in the exchange of digital certificates (or cryptographic secrets) with a terminal to determine its authenticity and trustworthiness. In essence, the smart card asks the terminal to prove that it is certified by the ID system. The terminal, in turn, asks the card to prove that it is a genuine member of the system. Once trust is established between the terminal and the smart card, it can then be extended to include the cardholder. By using biometric data captured from the cardholder at the point of use, the system can perform a match against enrollment data stored on the smart card. The ID system can thus authenticate that this user is the rightful owner of this card, and that the personal information stored on this card belongs to this cardholder. This completes the trust relationship between the user, the card, the terminal being used, and the ID system.

Enhanced Security

Biometric technologies are used with smart card technology for ID system applications specifically due to their ability to identify people with minimal ambiguity. A biometric-based ID allows for the verification of "who you claim to be" (information about the cardholder printed or stored in the card) based on "who you are" (the biometric information stored in the smart card), instead of, or possibly in addition to, checking "what you know" (such as a PIN). This increases the security of the overall ID system and improves the accuracy, speed, and control of cardholder authentication.

Each ID application needs to determine the level of risk management required to counter security threats and then choose the level of technology appropriate for the desired level of assurance.

An ID system using contact or contactless smart card technology, cryptographic functions and biometrics has significant security advantages:

- The biometric template can be digitally signed and stored on the smart card at the time of enrollment and checked between the biometric capture device and the smart card itself each time the card is used.
- The template and other personal information stored on the smart cards can be encrypted to improve security against external attacks.
- Cardholder authentication can be performed by the smart card comparing the live template with the template stored in the card. The biometric template never leaves the card, protecting the information from being accessed during transmission and helping to address the user's privacy concerns.
- A smart card-based ID can authenticate its legitimacy, and that of the reader, by creating a mutually authenticated cryptographic challenge between the ID card and the reader before identity verification is started. Once that process has been accomplished, access to a specific application can be granted. This ensures a very high level of privacy for the cardholder, prevents inappropriate disclosure of sensitive data, and helps to thwart "skimming" of data that might be used for identity theft. The smart card-based ID can also challenge the biometric reader to ensure that a previously captured template is not being retransmitted in a form of playback attack.
- Smart cards have sufficient memory to store growing amounts of data including programs, one or more biometric templates, and multiple cryptographic keys to restrict data access and ensure that data is not modified, deleted, or appended.
- The smart card can also be used to prove the digital identity of its cardholder using cryptographic keys and algorithms stored in its protected memory, making smart cards ideal for applications that need both physical and logical authentication.

▪ Improved System Performance and Availability

Storing the biometric template on a smart card increases overall system performance and cardholder convenience by allowing local identity verification.

The identity of an individual is established and validated at the time the smart card is issued and the individual has proven eligibility to receive the identity card. From that point on, the user's identity is authenticated through the presentation of the smart card to a card reader, without the need to perform a search and match against a remote database over a network. This local processing can reduce the time to authenticate an individual's identity to one second or less, allowing faster security checks, and reduce the need for the card readers to be online with a central system.

The question may arise regarding how to handle a comparison failure (i.e., false rejection) without accessing a remote database. With smart card technology, it is straightforward for the security staff to revert to a visual comparison of a digitally signed, digitized photo or backup biometric also stored on the card. In the event of a false rejection, the cardholder can simply repeat the process.

For applications where fast and frequent use is necessary (e.g., controlling access to buildings and at airports), contactless smart cards can speed the transfer of biometric templates and eliminate the need to make a physical connection. Low cost, contactless smart cards with high communication speeds are now available that have enough memory to store a unique fingerprint template or photographic representation. This means higher security biometrics-based ID systems can use contactless smart card technology to achieve a range of security, throughput and cost goals. When biometric data is transmitted over a contactless interface between a smart card and a reader device, it is advised that the data transmission or data be encrypted to avoid any chance of unauthorized reading of the biometric data through eavesdropping or other surveillance methods.

Improved Efficiency

Using the combination of smart card technology with biometrics for identification and authentication of individuals provides the most efficient implementation of a secure authentication system.

Several ID and security technologies can be combined with a smart card, allowing deployment of different authentication mechanisms based on the degree of security required and the budget available for implementation. Biometrics may be absolutely essential for those security checkpoints in the system where the user must be firmly linked to their ID card as the rightful owner and a password or PIN is not secure enough or lacks ease of use. Examples of systems requiring this stronger verification of identity include airport security gates or border crossings. A government or corporate enterprise identification system may include a variety of physical and logical access checkpoints that have different levels of security requirements. Biometric readers may be required at main entrances to the buildings, but internal access doors may only require the use of a magnetic stripe on the back of a smart card. When on a network, accessing different types of information may also have different security requirements. Some information may only require a password to access (which the smart card can store and remember for the user); other more sensitive information may require the use of a biometric; still other transactions may require the use of features on the smart card to digitally sign the transaction.

Contactless smart card technology can be used in environments where high usage or environmental conditions are expected to affect the cost of maintaining the system. Because the contactless card chip and the reader communicate using radio waves, there is no need to physically make an electrical connection; however, this may require the communication to be encrypted or, at least, not be able to be replayed. Maintenance of readers is minimized while reliability is improved since there are no worn contacts to be replaced or openings to be protected. Cards also last longer because removing them from their regular carrying place is not necessary for use. Readers or kiosks can be sealed, allowing contactless ID systems to be deployed in almost any environment.

Smart cards uniquely provide a single device that can function as an individual's identity card and allow the combination of several technologies to cost-effectively address varying security needs of a system.

Upgradability and Flexibility

A key requirement for any identification system is the ability for the system to be upgraded without needing large investments in new infrastructure. For example, there may be a need to modify the system without replacing the individual ID cards if a security scheme is compromised or if enhanced capabilities become available. Because smart cards contain rewritable data storage, and in some cases rewritable program storage, they allow the most flexibility for updates to card data and card-system interaction algorithms and for secure management of multiple applications on a single card.

When used in biometric-based identity systems, a smart card ID can be upgraded, after issuance, as follows:

- Smart card-based IDs can have sufficient storage to upgrade or add new biometric content (e.g., new or different biometric templates).
- Smart card-based IDs can have on-card content partitioned into mutually private sections to be used by several different secure ID systems. For example, physical access activities and card content may be kept separate from transaction authentication activities and content. With a single multi-partition-capable identity card, new and private uses of the biometric content may be added to the card by any authorized issuing entity at any time.

This last capability makes use of another key smart card attribute – flexibility. Smart cards, due to their on-card processor and software, have the best ability to adapt to varying and evolving requirements.

- Their ability to be both securely read and written by authorized issuers adds system capabilities unavailable with other technologies.
- Their ability to actively detect tampering with information stored on the card is also unavailable except with smart cards.
- A smart card-based ID can support several biometrics: fingerprint, photographic facial image, iris, vascular or hand geometry template, or any combination of these, simultaneously or incrementally over time. Stored reference biometrics can also be updated as needed.
- Smart card-based IDs may have both the traditional contact interface to reader/writer mechanisms and a contactless interface for applications that require high throughput and usage without mechanical wear.
- The same physical smart card can contain multiple storage media, such as a printed photograph, printed bar code, magnetic stripe and/or optical stripe. Thus, a single card can be compatible with many forms of existing infrastructure.

In multi-application smart card-based IDs, each application can have its own degree of challenge and response activity depending upon the respective application's requirements. For example, a simple fingerprint comparison with the stored on-card template may be sufficient to authenticate a person's right to access certain premises, while the same card and fingerprint template may be used in conjunction with an encrypted digital signature exchange to authorize sensitive transaction rights.

In summary, the unique features of smart card technology can deliver enhanced privacy, security, performance, and return on investment to a secure ID system implementation. Their upgradability and flexibility for securely handling multiple applications and accommodating changing requirements over time are unmatched by other ID technology. Smart card technology, coupled with biometrics and privacysensitive architectures and card management processes, provides a proven, cost-effective foundation for a highly secure personal ID system.