PRECISE™
BIOMETRICS

White Paper

Match-on-Card for Java Cards

Jonas Nilsson and Michael Harris, April 2004

INTRODUCTION

Biometric verification has the advantage of ensuring that only the correct physical user can gain access to certain information or physical locations. The biometric identity can never be borrowed, and it is up to the security administrator of a system to decide who is to be granted or denied access.

The biometric process can be divided into two functions - enrollment and verification. For enrollment, unique features are extracted from the initial sample image, converted to biometric data and stored in a biometric template. During verification, data is extracted from the live raw image data to be compared with the previously stored template.

As the biometric template maintains the user's digital identity, it is of high importance that this data be stored securely. From a user's perspective, it may also be of high importance that the personal data integrity is being safeguarded and the acceptance of having one's biometric data stored on a server might cause security trust problems. When deploying biometrics in an enterprise network, a server solution may also introduce limitations in terms of scalability.

The solution to these privacy, security and scalability challenges is to perform biometric verification inside the smart card, so that the storing and verifying of identity is accomplished directly on the card.

MATCH-ON-CARD

The ideal way to verify that a fingerprint presented to a fingerprint reader, actually matches the template stored from an earlier enrollment session, is to do the matching on the smart card, using the embedded smart card processor. By using Match-on-Card you gain five distinct advantages:

Privacy	The template never leaves the smart card [1]
Security	Two-factor authentication and on-card biometric matching
Interoperability	Open Standards compliance offers adaptability & low cost readers
Scalability	Matching performed in the card – unlimited scalability gives lower administration costs
Easy Integration	Fits to existing infrastructure and requires minimum memory usage

White Paper

JAVA CARD FORUM

The major smart card manufacturers started Java Card Forum[2] (JCF) with the goal of promoting Java Cards as the preferred platform for multi-application smart card solutions. The primary purpose for the JCF is the development and recommendation of a standardized specification to the existing Java Card API.
Today, the Java Card Forum Biometry API defines the industry standard for Java Card implementations of Match-on-Card.

PRECISE BIOMATCH™ ON ALL JAVA CARDS

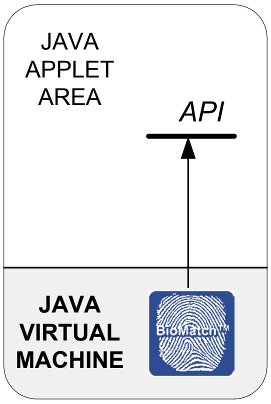
Precise BioMatch™ is a hybrid fingerprint-matching algorithm optimized for secure one-to-one matching. The hybrid technology combines the benefits of traditional minutia extraction with those of advanced pattern matching to maximize the information collection from a fingerprint. Precise BioMatch™ runs on all types of Java cards, providing identical external interface characteristics and biometric matching functionality.

Major smart card vendors currently provide Precise BioMatch™ as an integrated function within their *Java Card Operating System*, thereby saving applet memory space and improving performance in terms of biometric verification speed.

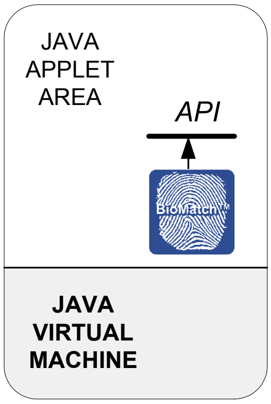
For Java cards from vendors that have not yet integrated Precise BioMatch™, a Java library, called Precise BioMatch™ J, is available for easy downloading.

Precise BioMatch™ supports the Java Card Forum Biometry API. The API is identical for all Java cards, regardless if the card has native support for Precise BioMatch™, or if the Precise BioMatch™ Java library is used.

The JCF-API biometry specification enables transparent integration of Java libraries or Java Card native OS implementations. This effectively eliminates vendor lock-in by providing a framework that accepts isolated applets or native OS code modules across varying Java Card smart card platforms.



Precise BioMatch™ integrated by card vendor



Precise BioMatch™ downloaded as a library

MATCH-ON-CARD CHARACTERISTICS

Privacy

With Match-On-Card, the fingerprint template is stored within the card, unavailable to external applications and the outside world. In addition, the matching decision is securely authenticated internally by the smart card itself.

Match-On-Card must not be confused with merely storing the biometric template on a smart card and performing the match decision outside the card on a server or a client PC. Such a solution does not add any security or controlled access to the information stored on the card.

Precise Match-on-Card enables PKI identification within the network for increased security while maintaining the biometric privacy and integrity of the end-user.

Security

The Match-on-Card technology is far more secure than matching on PC or server[3], as the fingerprint never leaves the secure environment of the smart card and no biometric data ever has to be transmitted over an open network.

The Match-on-Card procedure can be divided into two separate operations.

Pre-processing - the fingerprint image is enhanced and the characteristic information areas to be matched are located. These operations require greater processing power, but do not utilize the biometric template, allowing the operation to be safely done outside of the smart card.

Matching - This operation requires the biometric template and must be performed in the secure environment of the smart card. Through the optimised design of the BioMatch algorithm, the matching can be done quickly on the smart card chip, without degrading matching accuracy or performance.

In terms of accuracy (FAR/FRR[1]) the matching performance is comparable, whether processed on the smart card or in the PC. Similarly, matching speed is equivalent, although the lower overhead (e.g. no network traffic) associated with Match-on-Card often yields faster overall results.

Interoperability

The Precise Match-on-Card process does not require any special capabilities of the biometric or Smart Card reader. A combination reader (fingerprint + smart card) might be used as well as different heterogeneous brands of independent fingerprint readers and smart card readers. For example, a biometric-only reader can be used along with a separate generic PC/SC smart card reader or a combination reader can be used.

Precise Biometrics provides this flexibility by staunchly supporting and adhering to the diverse smart card and biometric standards. Additionally, Precise Biometrics offers Biometric Service Provider (BSP) solutions that can work transparently with other certified biometric vendor’s products.

[1] FAR - False Acceptance Rate. FRR - False Rejection Rate.

Scalability

In contrast to a server based system, there is no limitation in the number of possible users when utilizing Match-on-Card. All fingerprint verification is performed locally on the smart card without any need for network resources or server processing. Match-on-Card, in effect, reduces administration costs and creates a highly scaleable, distributed, and transportable database with each biometric asset maintained in it's own secure smart card environment.

Easy Integration

The Match-on-Card algorithm requires minimal code space. Typically, when implemented as a library for Java Card™ or MULTOS™, the algorithm uses approximately 1500-bytes of on-card EEPROM memory. Conversely, when the Match-on-Card algorithm is implemented natively in the card's operating system the card's ROM area is utilized. In either case, additional memory space is required for each template stored on the card. The template size is dependent on how the algorithm is configured and varies between 150 and 1000 bytes.

The small memory footprint of the algorithm as well as the flexible template sizing makes it possible to add biometric functionality to most existing smart cards. This valuable feature offers the implementation capability for higher-security (multiple-matching) or alternate finger matching. Alternate finger matching can be useful for damaged fingers or when the implementation requires tying fingers to specific applications.

The Precise Match-on-Card for Java Cards does not interfere with other card applications. An applet utilizing the Match-on-Card library will work side-by-side with any other smart card application such as loyalty, banking, or identification programs.

Additionally, other applications on the card, have the capability to take advantage of the on card biometrics through the sharable interfaces defined by the Java Card Forum - thereby easily adding biometric security to their independent functionality.

CONCLUSION

The Precise Match-on-Card for Java cards has several advantages compared to a server based biometric system:

Ensured privacy
Increased security
Interoperability with various smart card and fingerprint readers
Scalability gives decreased costs
Easy integration with existing infrastructure

Standards Compliancy
ISO/IEC 7816-11
ISO/IEC 14443-A
NISTIR 6529 (CBEFF)
NISTIR 6887 (GSA Interop. Spec.)
FIPS 140-2
Java Card Forum v2.2
Open Card Framework
BioAPI enrollment

REFERENCES

WWW

[2] Java Card Forum, JCF—http://www.javacardforum.org/

Precise Biometrics White Papers

[1] Ensuring integrity with fingerprint verification—http://www.precisebiometrics.com

[3] How secure is your biometric solution—http://www.precisebiometrics.com

Precise BioMatch™ —http://www.precisebiometrics.com

The Match-on-Card technology—http://www.precisebiometrics.com