

## Match-on-Card Technology

*Björn Nordin, April 2004*

### SCOPE

Precise Match-on-Card™ brings even higher degrees of security to the biometric solution, reducing the risk that data can be misused to an absolute minimum by storing *and matching* the biometric template in the sealed and tamper-proof environment of a smart card.

With Precise Match-on-Card™, your biometric template will never leave the card, and thus constitutes the ideal solution for preserving privacy while gaining maximum security.

### SECURITY, PRIVACY AND SCALABILITY

#### Security

A smart card is a very well protected and closed environment, suitable for storage of personal or confidential information. To access that information it is practical to use biometrics. But does it suffice to simply tell the smart card that some biometric verification has granted someone access? Is it really foolproof?

If the biometric verification is performed outside the closed environment of the smart card, the verification is put at risk. Communication between the smart card and the decision-making unit may be disrupted. The biometric template may be manipulated (and copied!). The very decision to grant or deny access may be altered. Even if the biometric template is protected by another security mechanism, the open environment must be considered the weakest link.

For many years now, smart cards have been protected by PIN, but the validation of the PIN have always been done by the smart card (who would ever think of validating the PIN outside the smart card?). Match-on-Card replaces PIN with biometrics, and yet keeps the smart card in charge of security. That's why the smart card itself must make the decision to grant or deny access! This is the only way to really protect information on a smart card and this is what Match-on-Card is all about.

## Privacy

With Match-on-Card, the owner of the smart card controls the only record of his or her biometric template. There is no need for an external fingerprint database, which is good from two perspectives: smart card owners can enjoy the privacy of not giving away biometric information, and smart card issuers don't have to worry about updating and maintaining databases.

Even if a smart card is stolen or lost, the biometric template can't be extracted. It is securely stored in the smart card along with the data it protects.

Match-on-Card and PKI is an efficient combination, where the smart card keeps the private key protected, and Match-on-Card ensures secure authentication to the smart card.

## Scalability

Match-on-Card creates a highly scaleable, distributed, and transportable database with each biometric asset maintained in its own secure smart card environment. Match-on-Card is suitable for large systems, where maintaining databases of biometric records would be expensive. For example, national ID-card systems must handle not only thousands of users, but also many millions of users. Since each citizen carries her own biometric record, Match-on-Card offers a neat and powerful solution.

## PRECISE MATCH-ON-CARD™ TECHNOLOGY

### Terminology

The *biometric template* is the data that represents an enrolled fingerprint. It consists of two parts; the *biometric header*, which contains data about type and version of the biometric algorithms, and the *reference data*, which contains the actual fingerprint characteristics.

When performing a verification, *verification data* is sent to the smart card. The verification data is compared with the reference on the smart card in order to measure similarity, and depending on the similarity score, grant or deny access.

### Overview

Match-on-Card can be described with the following three steps:

- a) The fingerprint is read from the sensor
- b) Verification data from the fingerprint is extracted (with Precise BioCORE™ II, a PC or another host).
- c) The smart card decides if the verification data corresponds with the stored reference data.

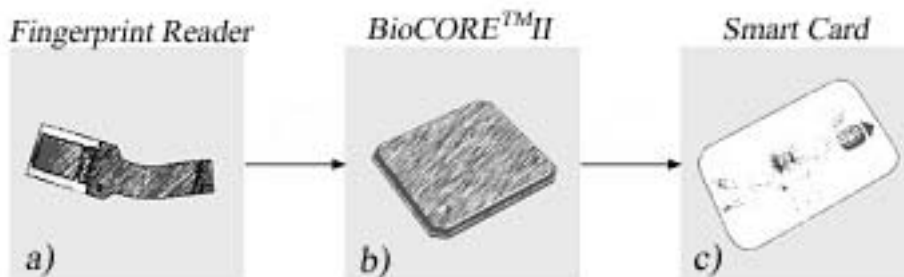


Figure 1: Match-on-Card process.

## Two Techniques

Two patented techniques are used to decide if the verification data really corresponds with the reference data. Even though both techniques can be run separately, the best result is achieved when combining them. One is based on minutia matching (local details) and the other is based on pattern matching (global structure). The workings of these techniques are explained in more detail under respective heading.

## Pattern Matching

Pattern matching is the process of comparing selected regions in the fingerprint, and their relative position.

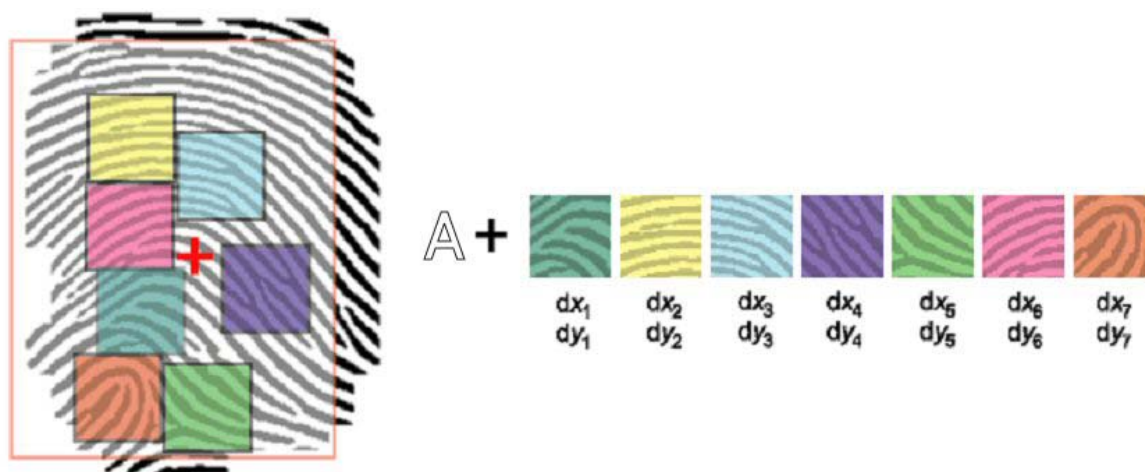


Figure 2: Pattern matching with seven regions (in this example). The biometric template consists of alignment information (A) and the selected regions with relative positions. A red cross marks the alignment center.

A number of representative regions are selected from the fingerprint at enrollment. These regions are processed and compressed, and constitutes the pattern matching part of the reference data. In order to identify these regions again when verifying, the verification fingerprint image must be aligned with the reference data stored on the smart card. Information of how to align the image is stored in the biometric header on the smart card.

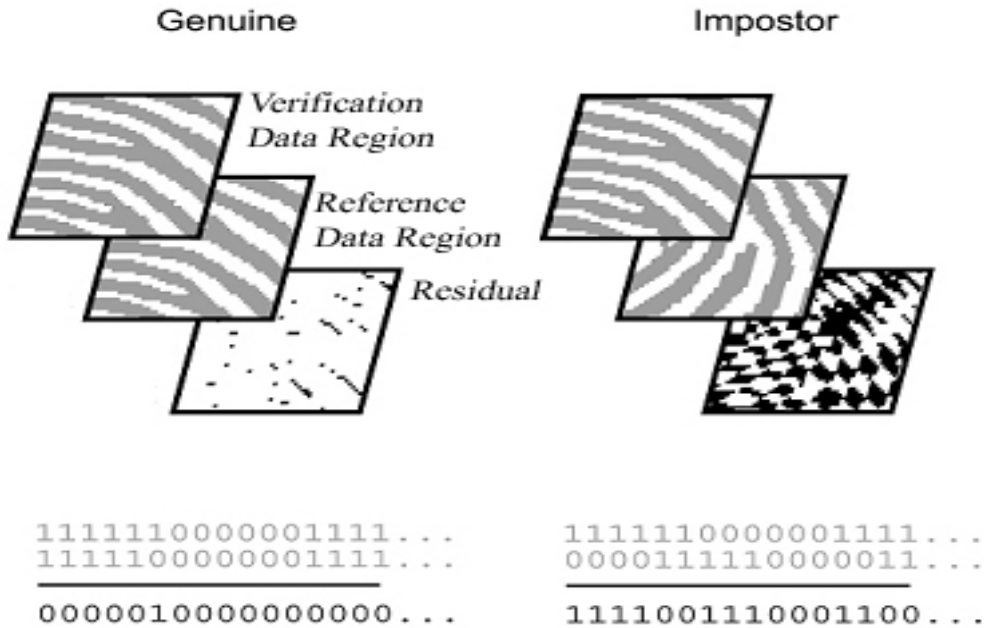


Figure 3: Verification data regions are matched with reference data regions.

At verification, once the respective regions have been found, the smart card matches regions in the verification data with regions in the reference data, as showed in Figure 3. Each matched region produces a residual, which is small for genuine verification attempts and large for impostor verification attempts. Finally, a score is calculated based on the residual of all matched regions. This is the “Pattern Score”.

Using Pattern Matching only, the size of the reference data is below 600 Bytes. The size of the biometric header is approximately 100 Bytes.

### Minutia Matching

Minutia matching is the process of comparing location and direction of ridge endings and ridge bifurcations in a fingerprint.

At both enrollment and verification, minutia-points are extracted from the fingerprint. For every minutia-point, a connection is made to all other minutia-points, forming a large number of minutia-point pairs.

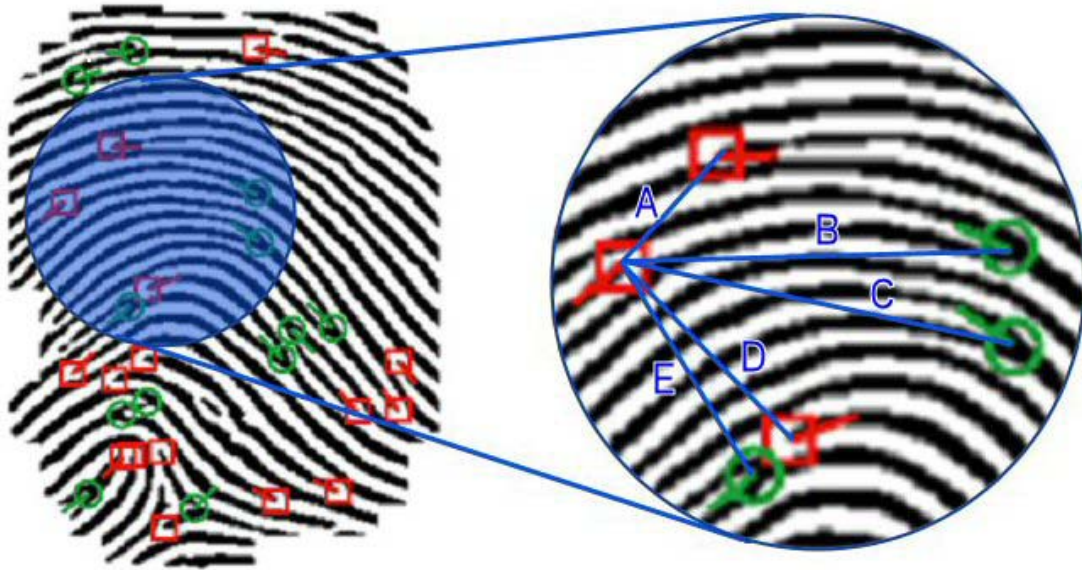


Figure 4: The minutia-points are connected in pairs. Five different pairs (A,B,C,D,E) are shown in the magnification to the right.

Data from every such minutia-point pair is extracted and ordered into a structure  $S$  that is independent of fingerprint translation and rotation. Hence, minutia matching does not need alignment. The smart card compares reference data structure  $S_R$  with verification data structure  $S_V$  by calculating the total residual:

$$residual = \sum |S_V - S_R|$$

Using Minutia Matching only, the size of the reference data is approximately 150 Bytes. The size of the biometric header is below 10 Bytes.

### Hybrid Matching

Minutia matching and pattern matching each have unique expertise, and there are major advantages of combining these two different techniques. One way to visualize this is to let both algorithms work independently on a database of fingerprints to get both Minutia Score and Pattern Score for each verification attempt. Then, in a coordinate system with Minutia Score on one axis and Pattern Score on the other, each genuine verification attempt is represented by a green mark and each impostor verification attempt by a red mark. The red cluster of impostor verification attempts must be separated from the green cluster of genuine verification attempts. Naturally, with a large enough database, it is impossible to separate these clusters totally. A compromise must be made between accepting all genuines and rejecting all impostors. The nature of this compromise is set by adjusting the security-level. However, the compromise can be made in a favorable way.

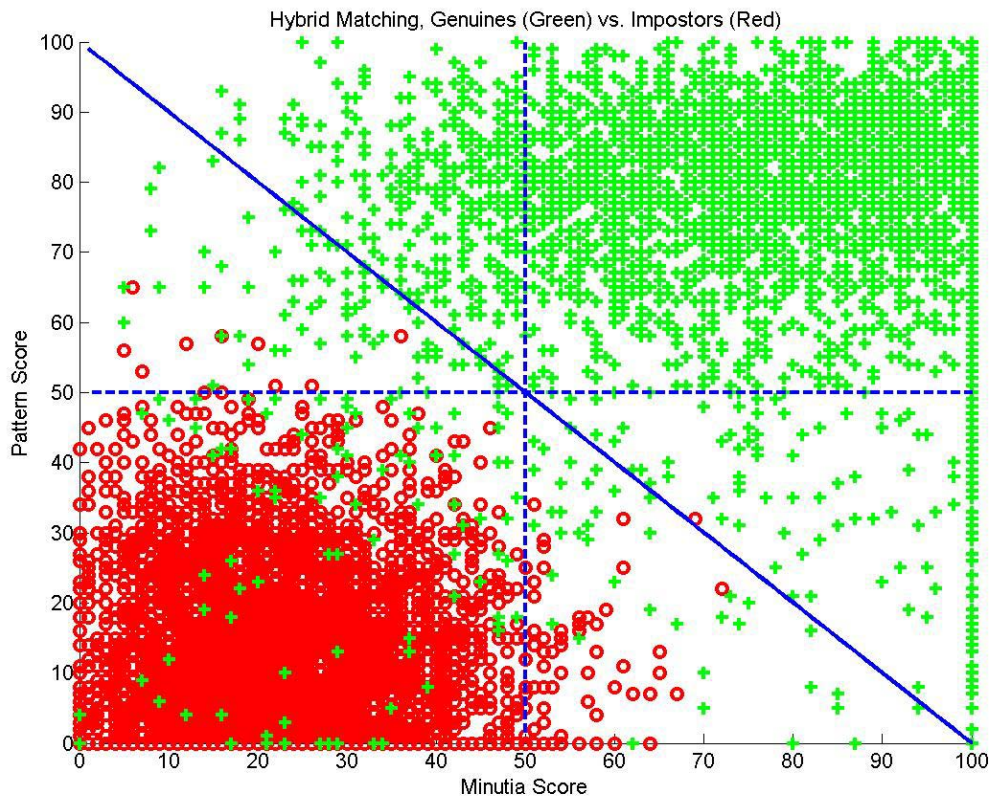


Figure 5: Decision to grant or deny access is based on scores from both techniques.

As can be seen in Figure 5, the best way to separate the green marks of genuine verification attempts from the red marks of impostor verification attempts is a diagonal line in between. If only one technique were used, either a horizontal or a vertical line (depending on selected technique) would separate genuines from impostors.

Using Hybrid Matching, the size of the reference data is approximately 750 Bytes. The size of the biometric header is approximately 100 Bytes.

## Performance

Precise Match-on-Card™ supports security-levels from one false accept in one hundred (1% FAR) to one in a million (0.0001% FAR). Recent independent third-party tests prove strength in performance; EER below 0.1%.

## Standards

Precise Match-on-Card™ is compatible with the following standards and standard drafts:

ISO/IEC 19794-2	Finger Minutiae Data
ISO/IEC 19794-4	Finger Image Data
ISO/IEC 19785	CBEFF
ISO/IEC 19784	BioAPI



## **REFERENCES**

Precise Biometrics white papers—<http://www.precisebiometrics.com/>