

M1/06-0350

InterNational Committee for Information Technology Standards  
INCITS Secretariat, Information Technology Industry Council (ITI)  
1250 Eye St. NW, Room 200, Washington, DC 20005  
Telephone 202-737-8888; Fax 202-638-4922  
email: [incits@itic.org](mailto:incits@itic.org)

---

Date: 1 March 2006

Submitted by: James Cambier (Iridian Technologies)

Email: [jcambier@iridiantech.com](mailto:jcambier@iridiantech.com)

Title: Contributions to AHGBEA Study Report on Biometrics in E-Authentication dated 6 February 2006

---

p. 17 *Biometric Identification*

following existing text on “Considerations”

Although identification-based authentication may have limited use in applications requiring a claimed identity and/or multiple authentication factors, it offers some capabilities that are uniquely valuable in some situations. As part of the enrollment process, an identification search can be performed to determine whether an enrollment already exists for the applicant in the database. This eliminates duplicate enrollments and can prevent the establishment of fraudulent identities. Identification also offers an opportunity for “anonymous authentication” in applications where the mere existence of an enrollment in the database confers a privilege or benefit, without the need to record any personal identifying information. The authentication system need only confirm that the person is in the database in order to authorize the privilege associated with enrollment. Finally, identification is essential in “watch list” applications. Here the presence of an enrollment record in the database indicates the individual is “of interest” due to previous activity, or perhaps is to be denied some benefit because it has already been received at the time of enrollment.

p. 42 Cancelable Biometrics

One proposed solution to the problem of compromised templates is the introduction of predefined distortions of raw biometric data or extracted features [1]. When applied to image-based biometrics like fingerprints or facial recognition, this technique has the potential for enabling re-issuance of templates. Because the transformations are intended to be nonreversible, however, the possibility of converting a database from one specialized format to another may be limited. In addition, it is necessary at least in some cases to reverse the transformation prior to matching; this exposes the original biometric data to hacking during the matching process and may represent a significant vulnerability.

An alternative technique [2] is based on the definition of unique, application- (or even transaction-) specific formats for biometric templates that prevent the unauthorized

M1/06-0350

exchange of templates across multiple applications, yet provide a mechanism for authorized transfer across applications. In addition they support the re-issuance of compromised templates without re-enrollment. Finally, the template matching operations are invariant across the transformations, so there is no need to return templates to a vulnerable “nontransformed” state in order to perform authentication.

1. Ratha, N. and Connell, J., “Cancelable Biometrics”, presented at Biometric Consortium 2000 Conference, Sept. 13-14, 2000.
2. Braithwaite, M., Cahn von Seelen, U., Cambier, J., Daugman, J., Moore R., Scott, I. “Application-Specific Biometric Templates”, Proceedings IEEE AutoID’02 Workshop on Automatic Identification Advanced Technologies, IEEE, 2002