Sanchez-Reillo R., Mueller R. (2015) Biometric System-on-Card, Standardization. In: Li S.Z., Jain A.K. (eds.) *Encyclopedia of Biometrics*. Springer, Boston, MA.

DOI: https://doi.org/10.1007/978-1-4899-7488-4_1042

Metadata of the chapter that will be visualized online

Chapter Title	Biometric System-on-Card, Standardization	
Copyright Year	2014	
Copyright Holder	Springer Science+Business Media New York	
Corresponding Author	Family Name	**Sanchez-Reillo**
	Particle	
	Given Name	**Raul**
	Suffix	
	Division	GUTI (University Group for Identification Technologies)
	Organization	Carlos III University of Madrid
	Address	28911, Avda. Universidad, 30, Leganes, Madrid, Spain
	Email	rsreillo@ing.uc3m.es
	Email	raul.sanchezreillo@gmail.com
Corresponding Author	Family Name	**Mueller**
	Particle	
	Given Name	**Robert**
	Suffix	
	Organization	Giesecke & Devrient GmbH
	Address	Prinzregentenstraße, Muenchen, Germany
	Email	raul.sanchezreillo@gmail.com

Encyclopedia of Biometrics
DOI 10.1007/978-3-642-27733-7_1042-3

Biometric System-on-Card, Standardization

Raul Sanchez-Reillo*[a] and Robert Mueller†[b]
[a]GUTI (University Group for Identification Technologies), Carlos III University of Madrid, Leganes, Madrid, Spain
[b]Giesecke & Devrient GmbH, Muenchen, Germany

Q1

Synonyms

BSoC; Sensor-on-card

Definition

Smartcard that contains capabilities for performing the on-card comparison of a biometric record and also embeds the biometric capture device in the card body. In a biometric system-on-card (BSoC), the sample to be compared with the stored biometric reference is obtained directly from the embedded sensor, and all biometric processing steps are performed in the smartcard.

Introduction

The International Standard ISO/IEC 24787:2010 [1] developed by WG 11, *Application of biometrics to cards and personal identification* of ISO/IEC SC 17*, Cards and personal identification* [2], defines several architectures to integrate biometrics with smartcards, including the storage-on-card alternative (i.e., the biometric reference is stored securely in the smartcard memory and read by the external world when the verification is needed) and the on-card biometric comparison (i.e., the biometric feature vector is sent to the smartcard for performing an internal comparison with the stored biometric reference). The biometric system-on-card (BSoC) is a functional extension to the on-card biometric comparison where the whole biometric process is executed inside the card, including the capture of the biometric sample. This architecture is being standardized by ISO/IEC JTC1/SC17 WG11 in the ISO/IEC 17839 multipart international standard [3–5].

As it can be seen in Fig. 1, a BSoC includes the sensor (biometric capture device) in the smartcard, together with the signal processing and feature extraction algorithms, plus the same services as offered by an on-card biometric comparison smartcard. While the decision takes place in the BSoC, it can provide information to the outer world to allow recording the process in the application. This information shall be minimal, as to not allow hill-climbing attacks. It is important to note that the main difference of a BSoC with other kind of biometric dongles is that a BSoC is actually a smartcard. Therefore, it provides all the security mechanisms traditionally available in a smartcard, including a tamperproof security controller and operating system.

*E-mail: rsreillo@ing.uc3m.es, raul.sanchezreillo@gmail.com
†E-mail: raul.sanchezreillo@gmail.com

Encyclopedia of Biometrics
DOI 10.1007/978-3-642-27733-7_1042-3

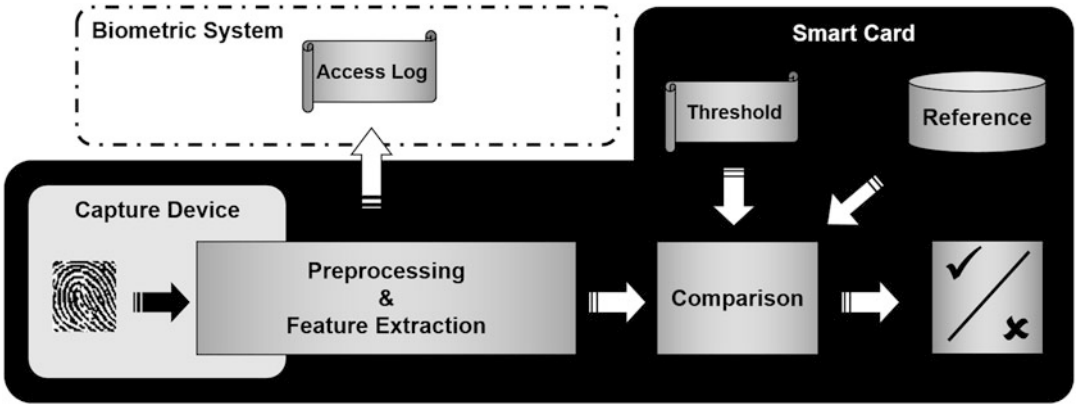

Fig. 1 Block diagram of a BSoC

BSoC Architecture

The development of BSoCs is on the very edge of current technology. The integration of a biometric sensor in an ISO/IEC 7810 [6] compliant smartcard is challenging. The card thickness and the bending and stiffness requirements are currently not addressable in a mass production context. The rest of the specifications can be satisfied, and therefore ISO/IEC 17839-1 [3] defines two possible system architectures for a BSoC. These two architectures are defined as:

- Type S1: this architecture is a fully flexible card compliant with ISO/IEC 7810.
- Type S2: architecture that intentionally deviates from the requirements of Type S1, by defining a thicker card body and easing the requirements to torsion, bending, and stiffness.

Type S1 may communicate with the external world by any of the smartcard communication interfaces, either with contacts (e.g., ISO/IEC 7816-3 [7] or the USB connection defined in ISO/IEC 7816-12 [8]) or contactless (e.g., ISO/IEC 14443 [9] or ISO/IEC 15693 [10]). In the case of Type S2, in order to avoid the creation of new readers that accept thicker cards, the communication interface is limited to contactless, either by using proximity cards (i.e., ISO/IEC 14443 [9]) or vicinity cards (i.e., ISO/IEC 15693 [10]). Type S2 is also motivated by the fact that the BSoC anyhow has to be contactless with most card readers to allow physically touching the embedded sensor. The thickness of Type S2 is defined to ease integration of components and to avoid damaging currently deployed card readers.

Although the first products will likely rely on fingerprint recognition, the BSoC standard is not limited by the biometric modality, allowing other capture devices to be embedded in the card as soon as technology allows it. Due to ergonomics, it seems logical that for some modalities (e.g., face recognition), only contactless interfaces would be available, as capturing the face of the cardholder with the smartcard already inserted in the reader may not be physically possible.

For the correct operation of the BSoC, the cardholder may require some feedback to signal when the data capture is in progress and when the acquisition is already complete. For some kind of sensors, such as fingerprint sweep sensors, further feedback for helping the cardholder during the process of data capture may be needed. Such feedback shall be provided without compromising the security and integrity of the BSoC and its data, i.e., avoiding hill-climbing attacks.

Encyclopedia of Biometrics
DOI 10.1007/978-3-642-27733-7_1042-3

In order to improve performance, a BSoC may be designed in a way that the enrolment is performed using sensors and algorithms outside of the smartcard, in order to obtain biometric reference data of superior quality.

Last but not least, power to the BSoC can be supplied either from the contact interface, from the contactless field, or using internal power supply devices such as a battery or a capacitor.

Physical Specifications for BSoC

Part 2 of ISO/IEC 17839 [4] defines the physical characteristics of the card including the dimensions of the card body, the location of the sensor, ergonomic requirements depending on the biometric modality, and the coexistence with other ID technologies included in the smartcard, plus other storage and operating conditions, such as temperature.

As previously mentioned, the Type S1 card shall be in accordance to the ID-1 specification in ISO/IEC 7810. In the case of Type S2, the physical characteristics are defined in the ID-T card format also defined in a forthcoming revision of ISO/IEC 7810. No other physical dimensions are in the scope of ISO/IEC 17839.

In any of these cases, but particularly in Type S1 when using a contact interface, the location of the sensor shall be carefully decided as not to limit the use of the card. Therefore, if the contact interface is used, the sensor shall be located in the right edge of the card, as to allow, for example, the placement of the finger with half of the card inserted in the reader.

In addition, the sensor shall be separated from the edges of the card, as to limit potential damage. A minimum margin from each of the edges is defined.

Biometric capture devices can coexist with other identification technologies already defined for smartcards, such as magnetic stripes, photographs, bar codes, or even embossing. The only limitation is that the introduction of such identification data shall not limit the functionality of the sensor, either mechanically (e.g., with traditional embossing technologies) or by ergonomics.

Commands and Security Mechanisms

In order to reach interoperability between BSoC and external applications, not only physical characteristics shall be defined but also the way information is exchanged and managed. This includes instruction codes for the card, logical data structures, and security mechanisms. Part 3 of ISO/IEC 17839 [5] provides solutions to all these needs, in accordance with the rest of the smartcard standards such as ISO/IEC 24787 [1], ISO/IEC 7816-11 [11], ISO/IEC 7816-4 [12], and the recent development works on the future International Standard ISO/IEC 18328.

This third part of ISO/IEC 17839 provides the mechanisms for the external world to recognize that a connected card (either inserted or in the field) is a BSoC card, plus additional information such as the biometric modality and the functionality and security mechanisms offered to the external world. One of the important aspects when using a BSoC is the security link between the application and the integrity and validity of the biometric data capture and comparison process. Therefore, integrity and authentication mechanisms are defined.

As has been previously mentioned, the BSoC can be designed forcing the enrolment to be done with the embedded sensor, or it can allow the biometric reference to be sent from the external world. In the latter case, coding of the imported biometric reference data is also defined in this standard.

Encyclopedia of Biometrics
DOI 10.1007/978-3-642-27733-7_1042-3

Configuration data is also defined in the standard and may contain sensitive operational information, such as comparison thresholds. The configuration data and access regulations are typically provided to the card during personalization. Only part of the data is publically available after issuance of the card. A card may have several biometric references, corresponding to different biometric traits of the cardholder. For example, enrolling two different fingerprints allows usage of the BSoC even in the case of temporary disability, i.e., damage of the finger.

Finally, the commands for performing the biometric system-on-card verification are defined, together with the feedback mechanisms for the human-machine interaction. Feedback data is limited to simple mechanical movement or placement and not providing information about, for example, the quality of the sample being acquired, as to avoid hill-climbing attacks.

Summary

A biometric system-on-card (BSoC) is a smartcard containing a complete set of biometric modules, from the data acquisition to the decision making. This technology is being standardized in the ISO/IEC 17839 series of standards in a modality independent way to allow in the future multiple biometric modalities available in the market.

Related Entries

- On-Card Biometric Comparison
- Storage-on-Card
- Tamperproof Operating System

Q2

References

Q3

1. ISO/IEC JTC1/SC17: ISO/IEC 24787:2010, Information technology – Identification cards – On-card biometric comparison (2010), available at http://www.iso.org/iso/home/store
2. ISO website, ISO/IEC JTC 1/SC 17 Cards and personal identification. http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45144
3. ISO/IEC JTC1/SC17: ISO/IEC DIS 17839-1, Information technology – Identification cards – Biometric system on card – Part 1: functional architecture. (Under development, more information in http://www.iso.org/iso/home/search.htm?qt=17839&published=on&active_tab=standards&sort_by=rel)
4. ISO/IEC JTC1/SC17: ISO/IEC CD 17839-2, Information technology – Identification cards – Biometric system on card – Part 2: physical characteristics. (Under development, more information in http://www.iso.org/iso/home/search.htm?qt=17839&published=on&active_tab=standards&sort_by=rel)
5. ISO/IEC JTC1/SC17: ISO/IEC WD 17839-3, Information technology – Identification cards – Biometric system on card – Part 3: logical information interchange mechanism. (Under development, more information in http://www.iso.org/iso/home/search.htm?qt=17839&published=on&active_tab=standards&sort_by=rel)

Encyclopedia of Biometrics
DOI 10.1007/978-3-642-27733-7_1042-3

6. ISO/IEC JTC1/SC17: ISO/IEC 7810:2003, Identification cards – Physical characteristics (2003), available at http://www.iso.org/iso/home/store. There is a revision in process (more information in http://www.iso.org/iso/home/search.htm?qt=7810&published=on&active_tab=standards&sort_by=rel)
7. ISO/IEC JTC1/SC17: ISO/IEC 7816-3:2006, Identification cards – Integrated circuit cards – Part 3: cards with contacts – Electrical interface and transmission protocols (2006), available at http://www.iso.org/iso/home/store
8. ISO/IEC JTC1/SC17: ISO/IEC 7816-12:2005, Identification cards – Integrated circuit cards – Part 12: cards with contacts – USB electrical interface and operating procedures (2005), available at http://www.iso.org/iso/home/store
9. ISO/IEC JTC1/SC17: ISO/IEC 14443, Identification cards – Contactless integrated circuit cards – Proximity cards (2008–2013), available at http://www.iso.org/iso/home/store
10. ISO/IEC JTC1/SC17: ISO/IEC 15693, Identification cards – Contactless integrated circuit cards – Vicinity cards (2006–2013), available at http://www.iso.org/iso/home/store
11. ISO/IEC JTC1/SC17: ISO/IEC 7816-11:2004, Identification cards – Integrated circuit cards – Part 11: personal verification through biometric methods (2004 – currently under revision, more information in http://www.iso.org/iso/home/search.htm?qt=7816-11&published=on&active_tab=standards&sort_by=rel)
12. ISO/IEC JTC1/SC17: ISO/IEC 7816-4:2013, Identification cards – Integrated circuit cards – Part 4: organization, security and commands for interchange (2013), available at http://www.iso.org/iso/home/store

Encyclopedia of Biometrics
DOI 10.1007/978-3-642-27733-7_1042-3

Author Queries

Query Refs.	Details Required
Q1	Please check if author affiliation is okay.
Q2	The title "On-Card Biometric Comparison," "Storage-on-Card," and "Tamper-proof Operating System" are mismatching with ToC. Please check if we can change the title as per ToC or retain as in MS.
Q3	Reference list has been renumbered to maintain sequence in citations. Please check if okay.