A Study on Biometric Standards for Adaptation of the National Infrastructure

Yong-Nyuo Shin[1], Dong-Kyun Lim[1] and Seung-Jung Shin[2]

[1]*Dept.of Computer Engineering, Hanyang Cyber University, Seoul, Korea*
[2]*Hansei University, Gyeonggi-do, Korea*
ynshin@hycu.ac.kr, eiger07@hycu.ac.kr, expersin@hansei.ac.kr

Abstract

Biometric technology based on the biometric hardware security module is more frequently used: in various areas which requires a high level of reliability such as, banking, procurement services. Korea Biometric Test Center[1] are providing the services to check whether the biometric products are implemented in conformance with the international standard BioAPI v2.0 on which recent products are based since 2006. The BioAPI standard conformance test provides the benefits that standard conformance testing encourages the biometric technology product developer to comply with relevant standards. This paper is designed to provide the test methodology for operating biometric hardware security module which can evaluate BioAPI standard conformance of the BSP implementation object and to introduce the biometric hardware security module which is standardizing in ITU-T SG17 for adaptation of the national infrastructure.

Keywords: *Biometric Hardware Security Module, BioAPI, ISO/IEC 24709*

1. Introduction

The BioAPI specification is one of a set of International Standards produced jointly by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) under their Joint Technical Committee 1 (JTC1), Subcommittee SC37 Biometrics[2]. The standard was based on some early work done in the United States of America and by the BioAPI Consortium which was called BioAPI 1.0 and BioAPI 1.1, but these specifications were heavily revised to correct bugs and to provide enhancements when the work was introduced to ISO/IEC. The first international version was therefore called BioAPI 2.0. A subsequent international version of BioAPI containing extensions of the user interface-related features and other enhancements produced a BioApi 2.1. Further enhancements to BioAPI are expected. BioAPI 2.0 is specified in ISO/IEC 19784-1 and was first published on 1 May 2006. The BioAPI standard conformance test provides the following benefits. Firstly, standard conformance testing improves the security of the developer or product user in the reliability of the product. Secondly, standard conformance testing guarantees compatibility between standards-based products and systems. Finally, standard conformance testing encourages the biometric technology product developer to comply with relevant standards. As many biometric technology products are being released in the market and used widely, it has become important to check whether these products are implemented in conformance with the international standard BioAPI v2.0. NIST/ITL's BioAPI CTS implementation [3] and DoD BMO BioAPI CTS(Conformance Test Suites) study [4] are the

representative BioAPI standard conformity studies. NIST/ITL's BioAPI CTS implementation is based on the INCITS Project 1703-D – "Information Technology Conformance Testing Methodology for ANSI INCITS 358-2002"[5]. The CTS evaluation tool is implemented with C++ and Java, and contains the execution engine that performs evaluation by reading the XML-type test assertion code. DoD BMO BioAPI CTS also performs standard conformance testing of the BSP product according to the INCITS Project 1703-D – "Information Technology Conformance Testing Methodology for ANSI INCITS 358-2002". It also contains some of the standard conformance testing function for BioAPI applications. The conformance testing methodology for BioAPI version 2.0 using test assertion language was not included in these studies either, because ISO/IEC 24709 was selected as an international standard in 2007. A biometric hardware security module (BHSM) is a physical device that traditionally come in the form of smartcard or some other USB type security token is composed with biometric sensor and microcontroller unit (MCU)[6]. These modules are designed to process key generation and electronic signature generation inside of the device (so that the security token can safely save and store confidential information, like the electronic signature generation key and the biometric sensing information). This paper is designed to implement BioAPI v2.0 CTS for operating Biometric Hardware Security Module which can evaluate BioAPI standard conformance of the BSP implementation object according to the method described in ISO/IEC 24709.Chapter 2 explains the conformance test methodology to evaluate BioAPI v2.0 conformance of the test target. Chapter 3 explains the biometric hardware security module. Finally, a conclusion is drawn and future study tasks are reviewed.

2. Conformance Test Methodology

Standard conformance testing of the BSP module is started when the BSP module vendor submits the BSP module, parameters, and BCS (BioAPI Conformity Statement) to the evaluation agency. The evaluation agency inputs the received data into the CTS evaluation tool and performs evaluation based on the data. The person in charge at the evaluation agency checks the evaluation result and reports it to the vendor. If necessary, the test report can be sent to the vendor, so that the vendor can understand the reason and timing of the problem's occurrence. Evaluation is performed through the following steps.

Step 1. The vendor of the BSP product for testing submits the following to the evaluation agency.

- BSP product to test
- Biometric terminal (fingerprint recognition device, iris recognition device, etc.)
- Terminal driver (for Windows OS)
- BCS and test assertion parameter values

Step 2. The evaluator connects the received biometric terminal and installs the driver, and then checks whether the terminal operates normally.

Step 3. The evaluator inputs the BCS detail and test assertion parameters into the CTS evaluation tool, and saves them in the database.

Step 4. The list of test assertions to run the CTS evaluation tool will be calculated, depending on the entered BCS detail.

Step 5. Perform a standard conformance evaluation by using the CTS evaluation tool.

Step 6. The evaluator checks the evaluation process and result.

Step 7. The evaluation result and test report are reported to the vendor.

Step 8. If the evaluation result is not "pass" the vendor analyzes the reason by referring to the test report, and then modifies the BSP module and requests a re-evaluation.

Step 9. If the evaluation result is "pass" the evaluation agency issues a certificate for the product in question.

The BCS information to be submitted by the vendor is described in detail in ISO/IEC 24709-2. Major components of the BCS are as follows.

- Vendor information
- Product information
- BioAPI conformance class for testing
- BioAPI conformance subclass for testing
- Additional BSP functions provided by the BSP product for testing
- Additional functions provided by the BSP product for testing
- Additional information related to BSP product

The list of test assertions for standard conformance testing is determined by the submitted BCS detail. The CTS evaluation tool can be considered as a kind of interpreter that reads and executes each test assertion in the list. The execution result of each test assertion can be classified as PASS/ FAIL/ UNDECIDED. PASS means that the BSP product runs normally for each test item, whereas FAIL means that the BSP product doesn't run properly, or the expected response is not received. UNDECIDED means that the test was not carried out properly because a problem occurred with an item other than the testing function. For the tested BSP product to pass the standard conformance test, the execution result of all test assertions included in the list should be "PASS." If any item is evaluated as FAIL or UNDECIDED, the product cannot pass the standard conformance test.

3. Biometric Hardware Security Module

A hardware security module is a type of secure cryptoprocessor at managing digital keys in terms of digital signings and for providing strong authentication to access critical keys. They are physical devices that traditionally come in the form of smartcard

or some other USB type security token that can be attached directly to general purpose computer. The cryptographic materials handled by most HSMs are asymmetric key pairs (and certificates) used in public-key cryptography related to X.509 certificate. HSMs can be employed in any application that uses digital keys. Typically the keys must be of significant meaning, negative impact to the owner of the key occurs if it were compromised. The access control of the HSM, however, is usually performed by the password which can be disclosed by attackers. That is the reason why biometric technologies are required for the access control of the HSM. Moreover, HSM containing X.509 certificate can be used for personal authentication by using the private key with PKI. In this case, the verifier can only check the holder of X.509 certificate not owner of it who is the registered at RA. Sometimes, the ownership is intentionally transferred to others for gaining malicious profit. That is one of main reasons why biometric HSM is required for verifying the ownership of the X.509 certificate in the telebiometric environment.

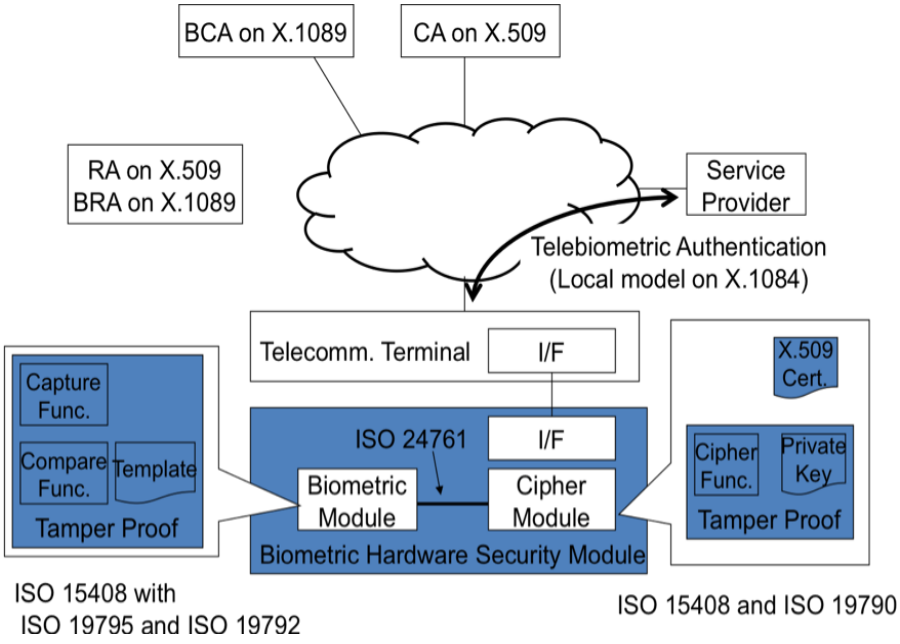

Figure 1. Relation among Standards for the Hardware Security Module

4. Conclusion

ISO/IEC 24709-1[7], the international standard for BioAPI standard conformance testing, stipulates that test assertion definition, data type, grammar, and construction specified in ISO/IEC 24709 should be used for evaluation. That is, the BioAPI CTS(Conformance Test Suites) creates a testing result by accepting the BSP implementation object, which will be a testing target, as well as the test assertion that describes the testing procedure and content. The test assertion for BSP testing is described in ISO/IEC 24709-2[8]. We implemented BioAPI v2.0 which can evaluate BioAPI standard conformance of the BSP implementation object according to the method described in ISO/IEC 24709. Biometric hardware security module can minimize the damage that can be caused by the disclosure of an ID and password, which is used

by the existing personal authentication technique based on the security token, and provide a high level of security and personal authentication techniques that can prevent any intentional misuse of a digital certificate. In this paper, we introduced the biometric hardware security module which is standardizing in ITU-T SG17 for adaptation of the national infrastructure. In the future work, we will provide countermeasures for the implementation problems that ensure security and reliability of the biometrics product based on a biometric hardware security module.

References

[1] Korea Biometric Test Center, http://knbtc.kisa.or.kr/kor/guide/guide01.jsp **(2011)**.

[2] BioAPI, http://en.wikipedia.org/wiki/BioAPI#Procurement_issues **(2012)**.

[3] NIST/ITL's BioAPI CTS Implementation: Overview. NIST/ITL Computer Security Division **(2006)**.

[4] DoD Biometrics Management Office: BioAPI Conformance Test Suite, http://www.biometrics.dod.mil **(2006)**.

[5] ANSI/INCITS 358-2002: Information technology - BioAPI Specification. International Committee for Information Technology Standards **(2002)**.

[6] Yong nyuo shin, "Operational Management for Biometrics Hardware Security Module and PKI.", The Journal of Korea Institute of Information Technology, Vol.9, No.5 **(2011)**.

[7] ISO/IEC 24709-1: 2007: Information technology – Conformance testing for the biometric application programming interface (BioAPI) – Part 1: Methods and procedures **(2007)**.

[8] ISO/IEC 24709-2: 2007: Information technology – Conformance testing for the biometric application programming interface (BioAPI) – Part 2: Test assertions for biometric service providers, **(2007)**.

[9] INCITS Project 1703-D - Conformance Testing Methodology for ANSI INCITS 358-2002, BioAPI Specification **(2002)**.

[10] ISO/IEC 19784-1: 2006: Information technology – Biometric application programming interface – Part 1: BioAPI specification **(2006)**.

Authors

Yong-Nyuo Shin

She received the PhD degree in computer science from Korea University in 2008, Republic of Korea. Currently, she is a professor at Department of Computer Science, Hangyang Cyber University. Also, she is an editor for efforts and continued support in progressing the many standardizations such as ITU-T SG17, ISO/IEC JTC1 SC27 and SC37. Her current research interests are telebiometrics, authentication technologies and privacy.

Dong-Kyun Lim

He received the PhD degree in Electronic Communication from Han yang University in 2002, Republic of Korea. Currently, he is a professor at Department of Computer Science, Hangyang Cyber University. Also, He current research interests are computer education, microprocessor.

Seung-Jung Shin

He received the PhD degree from Kookmin University in 2000, Republic of Korea. Currently, he is a professor at Department of, Hansei University. Also, He current research interests are security, computer education and privacy.