A Study on BioAPI Conformance Test for operating Biometric Hardware Security Module

Yong-Nyuo Shin[1], Dong-Kyun Lim[1], 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. 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.

Keywords: Conformance Test, BioAPI, Biometric Hardware Security Module

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. 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]. 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.

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.

4 Conclusion

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. The existing model is not consistent with the basic purpose of the hardware device, designed to process key generation and digital signature generation inside of the device (so that the security token can safely save and store privacy information, like an digital signature generation key). 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.

References

1. Korea Biometric Test Center, http://knbtc.kisa.or.kr/kor/guide/guide01.jsp, Jan 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, May 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.