Poster: A proposal for architecture of biometric authentication products

Asahiko Yamada
Information Technology Research Institute
National Institute of Advanced Industrial Science and Technology (AIST)
Japan
yamada.asahiko@aist.go.jp

***Abstract*—This paper proposes an enhanced architecture of products for biometric authentication which is suitable for policy-based authorization.**

Keywords—application interface; architechture; biometric authentication; biometrics

I. INTRODUCTION

Biometrics has been used mainly for automatic border control and national ID cards. But for these two years it has been becoming widespread into our daily life after FIDO (Fast IDentity Online) Alliance made its specification[1]. Different from the former cases, biometric products used for authentication are owned by the users who are authenticated. Thinking of the trend that policy-based authorization becomes more widely used, the modality (biometric characteristic), such as fingerprint and face, and configuration of the biometric products used at the user's environment should be determined by the consumer of the authentication result such as RP (Relying Party). This paper proposes an overall mechanism of biometric authentication used in the Internet environment which fits policy-based authorization but mainly focuses on the architecture of biometric authentication products. This proposal can be applicable to the case in which the private key of PKI authentication is activated by the result of biometric authentication and also to the case where PKI authentication is not used.

II. CURRENT ARCHITECTURE OF BIOMETRIC PRODUCTS

The oldest architecture of biometric products is BioAPI which was standardized as ISO/IEC 19784-1[2]. It has three layers of biometric products: BioAPI Framework, Biometric Service Provider (BSP) and Biometric Function Provider (BFP). The BioAPI Framework has an interface with the application program. The BSP is the lower layer of the BioAPI Framework and the BFP locates in the lowest of the three. The interfaces specified in BioAPI are mainly targeted to the use of standalone environments. A similar architecture was also given as Biometric API (BAPI) by Microsoft and has evolved to Windows Biometric Framework (WBF) API. Still the use in the Internet environment is not sufficiently considered also in WBF API.

On the other hand, the specification of FIDO Alliance assumes that it is used in the Internet environment. The FIDO Server which authenticates the user shows the criteria of authentication to the FIDO Client whether it satisfies the criteria of the FIDO Server which include the modality used in UAF (Universal Authentication Framework) Authenticator which is the only component for biometric authentication. The interface to UAF Authenticator is specified as commands.

III. POLICIES TO BIOMETRICS USED IN AUTHENTICATION

The modality used in biometric authentication should be determined by the policy of RP as in FIDO Specification since a modality may be more appropriate than another in usability and/or performance. In addition, the configuration of products used for biometric authentication should be also taken into consideration thinking the lifecycle of biometric authentication. Users may change their mobile devices more often than PCs, say once per a year or two. In such cases, they may have to enrol their biometric templates every time they change their mobile devices if the biometric templates are stored in them. That is not convenient for users. But they do not have to re-enrol their biometric templates if they store them in devices other than mobile devices. There are two types of configurations of biometric products for that. One is STOC (STore On Card) configuration and the other is OCBC (On Card Biometric Comparison) configuration. The advantage of the latter is that it is possible for the product which stores the biometric template to execute biometric authentication keeping the biometric template in it from the time of enrolment to the end of life of the product while it is necessary for the former to send the biometric template to another product every time of biometric authentication. In general, the RP prefers the OCBC configuration to the STOC configuration.

How the product is securely implemented may also become a factor of the authorization policy of the RP. For example, a fingerprint recognition product from Morpho has been CC certified on spoofing attack detection from the CC certification body of Germany. If a product used in authentication is CC certified, then the result of authentication may be more trusted than otherwise. If CC certified biometric products become more popular, whether a biometric product is CC certified or not may be included in the authorization policy of the RP. A digital format for CC certificate has been proposed in [5] for the case that the CC certified product is conformant to Protection Profiles (PPs).

IV. Outline of Negotiation

In negotiation for authentication, the modality and configuration of biometric products used which are accepted by the policy of RP are shown to the authentication client. The modalities in FIDO specification are restricted to fingerprint and face but there are other modalities such as vein also appropriate to be used for the applications FIDO specification targets. All the modalities in ISO/IEC 19785-1[3] should be specified in negotiation. The configuration of biometric products is categorized into three: all-in-one configuration type, STOC configuration type and BCOC configuration type. Which types are accepted by the RP shall be negotiated. In the future, whether CC certification is necessary or not would be added in negotiation as CC evaluation of biometric products becomes common.

The response of negotiation may be done independently or included in the response of authentication as in FIDO specification.

V. Architecture of Biometric Products

The proposed architecture consists of two layers, the upper Framework Layer and the lower Function Layer. There is only one Framework Layer product in a hardware such as a smart device or a PC. It is less related to biometric authentication and controls the whole process of biometric authentication. In a hardware there may be multiple Function Layer products which are plugged to the Framework Layer product. The relation of Framework Layer product and Function Layer products is depicted in Fig. 1. The profiles of the Function Layer products are registered in the hardware when they are installed and can be searchable by the Framework Layer product.

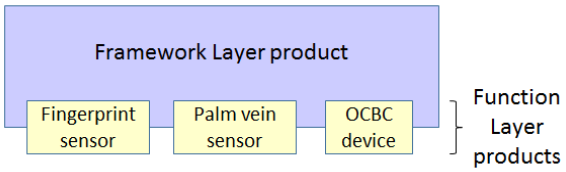

Fig. 1. Framework Layer product and Function Layer products

The Framework Layer product provides two interfaces to applications, one for enrolment and the other for authentication. It is called from the client application with the policy from the RP. It contains the modalities and configurations accepted by the RP. The Function Layer then searches the profiles of Function Layer products plugged to the Framework Layer product which satisfy the policy of the RP. If the policy of RP requires palm vein with OCBC configuration type and the Function Layer products are plugged as in Fig.1 where the OCBC device stores the biometric template of palm vein, then the Framework product concludes that it can satisfy the request from the RP and executes biometric authentication calling the palm vein sensor and the OCBC device.

A Function Layer product is called from the Framework Layer product if it satisfies the policy of RP, executes the processes implemented on the product and returns the result in which the role of the product in biometric execution is also contained together with the modality processed in the product. These form the evidence datum of processes done in the product. For the palm vein sensor in Fig.1, the evidence datum is the couple of "sensor" and "palm vein". For the OCBC device in Fig.1, it is the couple of "OCBC device" and "palm vein".

When the execution of biometric authentication is done successfully, the Framework Layer product returns success with the evidence data from the Function Layer products. If biometric authentication of palm vein with OCBC configuration type is executed, the two evidence data in the above are returned to the server via the client application.

VI. Verification

When the server receives the evidence data from the client, it can verify whether the biometric authentication done at the client satisfies the policy of the RP with the evidence data. In the above example, the modality is known to be palm vein. With "sensor" and "OCBC device", the server can know that biometric authentication under the OCBC configuration type has been done. For other cases, the verification is done similarly. For the evidence data to be trusted, certain assumptions are necessary but omitted here in this paper.

VII. Next Step

The author will define the detailed specification of architecture and also the authentication protocol which can be used with the major specifications of Single Sign-On.

Acknowledgment

The author appreciates Mr. Tatsuro Ikeda of Toshiba Corporation for a lot of discussions related to this work. Without these discussions, the author could not have reached the basic concept of this proposal.

References

[1] FIDO Alliance, FIDO Alliance Universal Authentication Framework (UAF) Specifications, December 2014.

[2] International Organization for Standardization (ISO), International Electrotechnical Com-mittee (IEC). ISO/IEC 19784-1:2006, Information technology — Biometric application programming interface — Part 1: BioAPI specification (2006)

[3] International Organization for Standardization (ISO), International Electrotechnical Committee (IEC). ISO/IEC 19785-1:2006, Information technology - Common Biometric Exchange Formats Framework - Part 1: Data element specification (2006).

[4] International Organization for Standardization (ISO), International Electrotechnical Committee (IEC). ISO/IEC 24761:2009, Information technology - Security techniques - Authentication context for biometrics (2009)

[5] Asahiko Yamada, “A Generalization of ISO/IEC 24761 to Enhance Remote Authentication with Trusted Product at Claimant”, ICT Systems Security and Privacy Protection Volume 455 of the series IFIP Advances in Information and Communication Technology pp 145-158, 2015.