Towards harmonizing ISO/IEC 24727 with FIDO and Web Crypto API in order to enable strong authentication and trustworthy identities for the Open Web Platform

Dr. Detlef Hühnlein

ecsec GmbH, Sudetenstrasse 16, 96247 Michelau, Germany
detlef.huehnlein@ecsec.de

Abstract: The ISO/IEC 24727 series of standards **[ISO24727]** define architectures and application programming interfaces for electronic identity (eID) cards, the Universal Authentication Framework (UAF) **[FIDO-UAF]** and Universal Second Factor (U2F) **[FIDO-U2F]** **[FIDO-U2F]**specifications of the FIDO Alliance provide means for strong authentication in the internet and W3C's Web Cryptography API **[Web-Crypto]** describes a JavaScript API for performing basic cryptographic operations in web applications. We argue that these three approaches should be harmonized and combined in order enable strong authentication and trustworthy identities for the Open Web Platform.

Against the background of the US Government Smart Card Interoperability Specification **[NIST-GSCIS]** and the activities around the Personal Identity Verification (PIV) program **[NIST-PIV]** the National Institute of Standards and Technology (NIST) initiated the development of the ISO/IEC 24727 series of standards **[ISO24727]** which defines architectures and application programming interfaces for electronic identity cards (eID) as an abstraction of the widely deployed smart card standard ISO/IEC 7816 **[ISO7816]**. ISO/IEC 24727 also forms the basis of the European Citizen Card specification **[CEN15480]**, the German eCard-API-Framework **[BSI-TR03112]** and the National Smartcard Framework of the Australian Government **[AG-NSF]** and hence is used in various eID projects around the Globe. The Open eCard project (http://openecard.org) provides an open source implementation of this standard, which allows to support arbitrary eID cards and similar cryptographic tokens, which are described by a standardized XML-based CardInfo file. Furthermore, as ISO/IEC 24727 is generic and extensible[1] with respect to cryptographic mechanisms and authentication protocols it would also be possible to support the biometric authentication mechanisms addressed in **[FIDO-UAF]**, use cryptographic tokens conforming to **[FIDO-UAF]** and provide a Web Cryptography API conform wrapper around the ISO/IEC 24727 stack.

[1] Please refer to **[WHP+13]** for details with respect to the extension mechanisms of ISO/IEC 24727 and the corresponding implementation within the Open eCard project.

Indeed a closer analysis of ISO/IEC 24727, the available drafts of the FIDO specifications and the Web Cryptography API reveals that three approaches share many similarities and could easily be harmonized to provide a common framework which would enable strong authentication and trustworthy identities for the Open Web Platform.

The proposed contribution briefly recalls the most important aspects of ISO/IEC 24727, the FIDO specifications and the Web Cryptography API and discusses possible path towards a future harmonization of these specifications and the compelling advantages of this approach.

References

[AG-NSF] Australian Government: *National Smartcard Framework*, http://www.finance.gov.au/policy-guides-procurement/authentication-and-identity-management/national-smartcard-framework/

[BSI-TR03112] German Office for Information Security: *eCard-API-Framework*, Technical Directive Nr. 03112, BSI TR-03112, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03112/index_htm.html

[CEN15480] CEN: *Identification card systems — European Citizen Card*, CEN TS 15480 (Part 1-4), 2007

[FIDO-U2F] FIDO-Alliance: *Universal Second Factor (U2F) Specifications*, 2014, https://fidoalliance.org/specs/fido-u2f-v1.0-rd-20140209.zip

[FIDO-UAF] FIDO-Alliance: *Universal Authentication Framework (UAF) Specifications*, 2014, https://fidoalliance.org/specs/fido-uaf-v1.0-rd-20140209.zip

[ISO7816] ISO/IEC: *Identification cards – Integrated circuit cards*, ISO/IEC 7816 (Part 1-13 & 15)

[ISO24727] ISO/IEC: *Identification cards – Integrated circuit cards programming interfaces*, ISO/IEC 24727 (Part 1-6)

[NIST-GSCIS] NIST: *Government Smart Card Interoperability Specification*, Version 2.1., July 2003, http://csrc.nist.gov/publications/nistir/nistir-6887.pdf

[NIST-PIV] NIST: *Personal Identity Verification (PIV) of Federal Employees and Contractors*, FIPS PUB 201-1, March 2006, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

[PAOS-v1.1] Liberty Alliance Project: *Liberty Reverse HTTP Binding for SOAP Specification*, Version v1.1, via http://www.projectliberty.org/liberty/content/download/1219/7957/file/liberty-paos-v1.1.pdf

[SOAP-v1.1] W3C Note: *Simple Object Access Protocol (SOAP) 1.1*, 08 May 2000, via http://www.w3.org/TR/2000/NOTE-SOAP-20000508

[Web-Crypto] W3C: *Web Cryptography API*, W3C Last Call Working Draft 25 March 2014, http://www.w3.org/TR/WebCryptoAPI/

[WHP+13] T. Wich, M. Horsch, D. Petrautzki, J. Schmölz, D. Hühnlein, T. Wieland: *An extensible platform for eID, signatures and more*, In: Proceedings of Open Identity Summit 2013, LNI, vol. 223, 2013. pp. 55–68, http://www.ecsec.de/pub/2013_OID_Platform.pdf

Annex – Background on ISO/IEC 24727

We assume that the attendees of the workshop are familiar with the FIDO specifications and the Web Cryptography API, but not with ISO/IEC 24727 and hence we will provide some background information with respect to this standard.

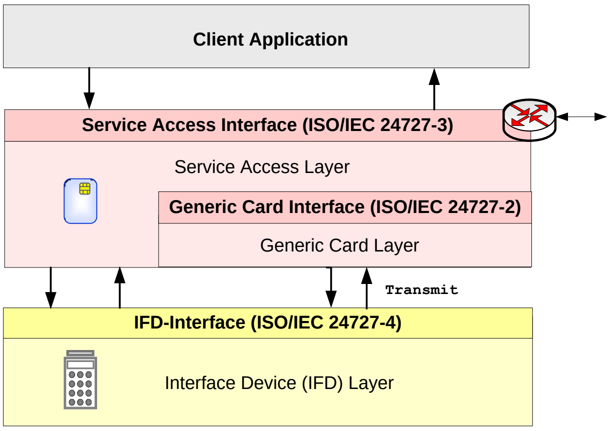
Client Application
Service Access Interface (ISO/IEC 24727-3)
Service Access Layer
Generic Card Interface (ISO/IEC 24727-2)
Generic Card Layer
Transmit
IFD-Interface (ISO/IEC 24727-4)
Interface Device (IFD) Layer

Figure 1: ISO/IEC 24727 Architecture

The architecture defined in Part 1 of **[ISO24727]** and depicted in Figure 1 assumes that a Client Application uses the functionality of cryptographic tokens using the *Service Access Interface* defined in Part 3 of the standard series.

This interface comprises generic functions which allow to establish (cryptographically protected) connections to card-applications, manage those card-applications, store and retrieve data, perform cryptographic operations, manage the related key material (so called Differential-Identities (DID)) and manage access rights for data, keys and services provided by card-applications.

The Service Access Layer (SAL) maps the generic requests at the Service Access Interface to APDUs of the *Generic Card Interface* defined in Part 2, which allows a subset of the commands and options defined in **[ISO7816]** (Part 4, 8 and 9). If the cryptographic token does not support those standard-commands directly they may be translated by the Generic Card Layer before they are sent to the Interface Device (IFD) Layer using the `Transmit`-command, which is – as other IFD-related commands in the IFD-API – defined in Part 4 of **[ISO24727]**. The IFD-API allows to use different card terminal technologies and secure elements available in mobile phones in a transparent fashion. If the cryptographic token under consideration does not support the APDUs defined in Part 2 of **[ISO24727]**, but only the underlying base standard **[ISO7816]** it is possible to describe the mapping in an XML-based CardInfo file and hence ISO/IEC 24727 is also capable to support legacy cards which are already rolled out.

Furthermore there is a “dispatcher”, which redirects web service requests to remote software stacks and establishes trusted channels using TLS or similar protocols. The dispatcher supports different web service bindings, based on SOAP or PAOS and it is possible to add more lightweight bindings based on REST and JSON or YAML in the future.