FIDO Impact Analysis Report (FIAR)

Version 1.0

April 2018

Revision History

Date	Version	Description
2017-10-02	0.1	Initial draft version
2017-11-03	0.2	Content creation covering chapters 1 and 2.1

2017-11-14	0.3	Content creation of chapters 2.x
2017-11-24	0.4	Completion and General updates
2018-04-10	1.0	Updates including the new logo and new levels naming

Contents

1 Introduction

1.1 Concept

1.2 Audience

1.3 Confidentiality & Copyright notice

1.4 Contact

1.4.1 FIDO Security Secretariat

1.4.2 FIDO Certification Secretariat

1.4.3 FIDO Accredited Laboratory

1.4.4 Vendor, Sponsor, Developer

1.5 FIAR Review Process

1.6 Derivative FIDO Authenticator Certification Process

1.7 Delta FIDO Authenticator Certification Process

1.8 FIDO Authenticator re-Certification Process

1.9 Summary of the FIAR and Certification Process

1.10 Evaluation of Changes

1.10.1 NON-INTERFERING Change

1.10.2 MINOR Change

1.10.3 MAJOR Change

1.11 FIAR Structure

2 FIDO Impact Analysis Report - Template

2.1 Introduction

2.1.1 FIAR Document Identification

2.1.2 Certified Authenticator Details

2.1.3 Changed Authenticator Details

2.1.4 Laboratory Details (if applicable)

2.2 Description of the Change(s)

2.3 Impacted FIDO Authenticator Security Requirements

2.3.1 Authenticator Definition and Derived Authenticator Requirements

2.3.2 Key Management and Authenticator Security Parameters

Documentation

Random Number Generation

Signature and Registration Counters

2.3.3 Test for User Presence and User Verification

2.3.4 Privacy

2.3.5 Physical Security, Side Channel Attack Resistance, and Fault Injection Resistance

2.3.6 Attestation

2.3.7 Operating Environment
2.3.8 Self-Tests and Firmware Updates
2.3.9 Manufacturing and Development
2.4 Impacted Evaluation Evidence
2.5 Impacted Metadata Requirements
2.6 Description of Regression Testing & Calibration
2.7 Vendor's Conclusion & Judgement
3 Appendix A: References
4 Appendix B: Terms & Abbreviations

Introduction

This document defines the FIDO Impact Analysis Report (FIAR) template listing the scope and the structure of the expected contents. This report must be completed by the vendor while re-submitting for a Delta FIDO Authenticator Certification. This is a required step to update an existing FIDO Authenticator Certificate and is intended to record the analysis of the impact of changes to the certified FIDO Authenticator.

The guidelines contained herein are intended to provide a common ground and language for both vendors and the security secretariat to conduct a FIDO Authenticator Certification maintenance.

Concept

To enable vendors meeting time-to-market needs while providing the assurance that is required for each FIDO Authenticator Certification level, vendors could request a Derivative or a Delta certification to minimize redundancy in the FIDO Authenticator Certification. The goal being to avoid repeating unnecessary evaluation work previously performed.

The FIAR review process is intended to identify eventual changes to the Certified Authenticator, whereas Derivative/Delta Certification refers to the certification of a Changed Authenticator because the changes to the Certified Authenticator do not adversely affect the FIDO Authenticator Security Requirements.

It is important to note that the Delta Certification process is not intended to provide assurance that the original certified Authenticator is resistant to new attacks discovered since the date of the initial certificate. Such assurance can only be gained through Re-certification. Delta Certification only considers the effect of changes on the FIDO Authenticator Security Requirements.

Nevertheless, the vendor must consider implementing countermeasures against all publicly known vulnerabilities, as of the date of the release of the updated version, before submitting a Changed Authenticator for a Delta Certification process.

Audience

The primary audience of this document are FIDO Authenticator Vendors/Sponsors who have already undergone a FIDO authenticator certification.

The intermediate audience of this document, once it has been completed by the vendor, is the FIDO Security Secretariat to validate the results and trigger next steps of the Delta Certification process.

Confidentiality & Copyright notice

This document must be strictly confidential for only the FIDO certification team, the Accredited Security Laboratory, and the Vendor concerned in the current evaluation.

Contact

FIDO Security Secretariat

The FIDO Security Secretariat is FIDO Staff responsible for reviewing applications, questionnaires, monitoring security threats, and acts as an independent FIDO security expert for the FIDO Security Certification Program.

For help and support, visit the FIDO Website [FIDO Cert] or contact the FIDO Security Secretariat at security-secretariat@fidoalliance.org.

FIDO Certification Secretariat

The FIDO Certification Secretariat is FIDO Staff responsible for implementing, operating, and managing all FIDO Certification Programs.

For help and support, visit the FIDO Website [FIDO Cert] or contact the FIDO Certification Secretariat at certification@fidoalliance.org.

FIDO Accredited Laboratory

FIDO Accredited Laboratories are Laboratories that have successfully completed the FIDO Laboratory Accreditation Process and have a valid Certificate of Accreditation.

Vendor, Sponsor, Developer

Implementers seeking Certification may be FIDO member organizations or non-member organizations.

FIAR Review Process

The FIAR review process is composed of 3 steps:

- The FIAR submission step: The vendor submits a complete FIAR document based on the template described in Chapter 2 of this document.
- The FIAR review step: FIDO security secretariat reviews the submitted FIAR report for completeness and analysis the changes to determine their impact on the FIDO Authenticator Security Requirements.
- The FIAR conclusion step: FIDO security secretariat will provide a judgement based on the characteristics of the chances made to the Certified Authenticator. The outcome would be either that the changes are **Non-INTERFERING** or **MINOR** or **MAJOR**.

Derivative FIDO Authenticator Certification Process

A **Derivative FIDO Authenticator Certification** process is conducted on an Authenticator that has been already certified in earlier versions. In the case where the Security Secretariat concluded that changes reflected in the IAR have **NON-INTERFERING** impacts on FIDO Security Requirements coverage after reviewing the FIAR provided by the Vendor, then an addendum to the existing certificate is created. It is made publicly available by the end of this process.

Delta FIDO Authenticator Certification Process

A **Delta FIDO Authenticator Certification** is conducted on an Authenticator that has been already certified in earlier versions. In the case where the Security Secretariat concluded that changes reflected in the FIAR have **MINOR** impacts to the FIDO Authenticator Security Requirements coverage, then the following must apply:

- For L1 Certifications: FIDO Security Secretariat will review only the updates made to the VQ and approves it, then an addendum to the existing certificate is created and made publicly available by the end of the process.
- For L1.5 Certification and above: The Accredited Lab will review only the updates made to the VQ, conduct the delta tests and updates the relevant FER to reflect the new version. Then, an addendum to the existing certificate is created by FIDO Security Secretariat and made public by the end of the process.

FIDO Authenticator re-Certification Process

A **FIDO Authenticator re-Certification** is conducted on an Authenticator that has been already certified in earlier versions. In the case where the Security Secretariat concluded that changes reflected in the FIAR have **MAJOR** impacts to the FIDO Authenticator Security Requirements coverage, then the following must apply:

- For L1 Certifications: FIDO Security Secretariat will review completely the VQ while reusing previous certification results to the maximum extent possible to minimize duplication of effort. Then approves it, and issue a new certificate which will replace the existing one. This new certificate will be made publicly available by the end of the process.
- For L1.5 Certification and above: The Accredited Lab will review completely the VQ and re-conduct testing while reusing previous certification results to the maximum extent possible to minimize duplication of effort. Then updates the FER to reflect the new results before submitting it to FIDO Security Secretariat. That latter will validate the FER and issue a new certificate which will replace the existing one. This new certificate will be made publicly available by the end of the process.

Summary of the FIAR and Certification Process

The starting point for these processes is when a change is made to an existing certified Authenticator. This change might be a patch designed to correct a discovered flaw, an enhancement to a feature, the addition of a new feature, a clarification in the guidance documentation, or any other change to the Authenticator Hardware and/or Software.

The following Figure 1 shows the FIAR & Certification Process flow.

Figure 1: FIAR & Certification Process Flow

Evaluation of Changes

After completing the FIAR, the vendor submits the report to FIDO Security Secretariat who analysis the changes described in order to determine their impact upon the FIDO Security Requirements coverage.

NON-INTERFERING Change

A non-interfering change has NO impacts on the FIDO Security Requirements coverage. Typical changes could be features outside of the Authenticator Boundary or bug fixes related to functional features, performance optimization or an updated name or look.

MINOR Change

A minor change has an impact that is sufficiently minimal to not affect the security assurance level provided by test procedures and calibration requirements to the extent that the Authenticator needs to be re-certified. Changes to the FIDO Security Requirements that DO NOT require Calibration falls typically into this scope, but this is not a restricted case. Typical changes could be bug fixes indirectly related to a security feature or the ASPs, an additional feature interacting with the Authenticator boundary or a security strength optimization.

MAJOR Change

A major change has a potential impact on the security assurance level. Changes to the FIDO Security Requirements that DO require Calibration falls typically into this category. Typical changes could be the addition/remove/replacement of an ASP or a cryptographic algorithm, an implementation of a new countermeasure or a change to the Authenticator boundary security architecture. Note that in some cases, an update including several minor changes could lead to a major impact on security, in that case, the Security Secretariat might consider it as a major change.

FIAR Structure

The FIDO Impact Analysis Report (FIAR) must be completed by the vendor.

Once complete, the FIAR must be delivered to the FIDO Security Secretariat.

The following Chapter includes a template of the document covering the following Sections:

- 2.1 Introduction
- 2.2 Description of the Change(s)
- 2.3 Impacted FIDO Authenticator Security Requirements
- 2.32.4 Impacted Evaluation Evidence2.5 Impacted Metadata Requirements2.6 Description of Regression Testing & Calibration
- 2.7 Vendor’s Conclusion & Judgement

Vendors are required to produce their FIAR following that structure. Details on how to complete each section are included into <> in this template and should be replaced with the vendors inputs.

FIDO Impact Analysis Report - Template
Introduction

<Add a brief introduction of the Delta Certification process, the relevant details identifying the FIDO Authenticator under delta evaluation:

- *Identification of the Hardware part;*
- *Identification of the underlying Software Platform/OS (if applicable)*
- Provide a diagram/picture illustrating the Changed FIDO Authenticator's physical boundary and main logical features while highlighting changes (if they are visible at this level).

And finally complete the following detail tables:>

FIAR Document Identification

Name	
Version	
Creation date	
Author	

Certified Authenticator Details

Vendor Company Name:	
Vendor Contact Name:	
Vendor Contact Email:	
Implementation Name:	
Authenticator Level:	
FIDO Specification:	
FIDO Version:	
Implementation Class:	Authenticator
If UAF, FIDO Transport:	

Changed Authenticator Details

Vendor Company Name:	
Vendor Contact Name:	
Vendor Contact Email:	
Implementation Name:	
Authenticator Level:	
FIDO Specification:	
FIDO Version:	
Implementation Class:	Authenticator
If UAF, FIDO Transport:	

Laboratory Details (if applicable)

Laboratory Name:	
Evaluator(s) Name:	
Evaluation Start Date:	
Evaluation End Date:	

Description of the Change(s)

<Identify and describe the changes relevant to the Authenticator identified above, its development and operational environment. Note that, in this Section, these changes must be described to the level of detail necessary to understand what was done, but no necessarily how it was done.>

Impacted FIDO Authenticator Security Requirements

<Please list the FIDO Security Requirements that are affected by the changes described above. For each impacted SR, please update the rationale to clarify how these changes were addressed, how documentations were updated, how the implementation changed accordingly, how regression tests were performed, etc.>

Authenticator Definition and Derived Authenticator Requirements

SR#:
Updated Rationale/Tests/Evidence:

Key Management and Authenticator Security Parameters

Documentation

SR#
Updated Rationale/Tests/Evidence:

Random Number Generation

SR#
Updated Rationale/Tests/Evidence:

Signature and Registration Counters

SR#
Updated Rationale/Tests/Evidence:

Test for User Presence and User Verification

SR#
Updated Rationale/Tests/Evidence:

Privacy

SR#
Updated Rationale/Tests/Evidence:

Physical Security, Side Channel Attack Resistance, and Fault Injection Resistance

SR#
Updated Rationale/Tests/Evidence:

Attestation

SR#
Updated Rationale/Tests/Evidence:

Operating Environment

SR#
Updated Rationale/Tests/Evidence:

Self-Tests and Firmware Updates

SR#
Updated Rationale/Tests/Evidence:

Manufacturing and Development

SR#
Updated Rationale/Tests/Evidence:

Impacted Evaluation Evidence

<This section shall report for each element provided by the vendor and used as an evaluation evidence the following information:

- *the vendor/developer/author name*
- *the title;*
- *the unique reference (e.g. issue date and version number)>*

Impacted Metadata Requirements

Evaluator Instructions:

<The vendor must thoroughly highlight the updates and verify the consistency of the fields defined in the Metadata with the evaluated implementation.>

SR#
Updated fields:

Description of Regression Testing & Calibration

<if applicable, describe how the regression tests sufficiently address the FIDO Security Requirements>

Vendor’s Conclusion & Judgement

<Provide an overall conclusion of the identified impacts on the FIDO Security Requirements coverage with a rationale supporting whether they were considered NON-INTERFERING, MINOR or MAJOR changes.>

Appendix A: References

Reference	**Title**	**URL**
[Allowed Crypto]	Authenticator Allowed Cryptography List	https://fidoalliance.org/certification/authenticator-certification-levels/
[Allowed ROE]	Authenticator Allowed Restricted Operating Environments List	https://fidoalliance.org/certification/authenticator-certification-levels/
[Certified]	FIDO Certified products	https://fidoalliance.org/certification/fido-certified-products/
[Functional]	FIDO Functional Certification Policy	https://fidoalliance.org/getting-started/

[Application]	Authenticator Certification Application	https://fidoalliance.org/certification/authenticator-certification-levels/
[L2 Requirements]	Authenticator Security Requirements – Level 2	https://fidoalliance.org/certification/authenticator-certification-levels/
[Test Procedures]	Authenticator Security Test Procedures	https://fidoalliance.org/certification/authenticator-certification-levels/
[Lab Accreditation]	FIDO Laboratory Accreditation Program Policy	https://fidoalliance.org/certification/accredited-security-laboratories/
[FIDO Cert]	FIDO Certification Website	https://fidoalliance.org/certification/
[NIAP Assurance]	NIAP Assurance Continuity: Guidance for Maintenance and Re-Evaluation	https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/scheme-pub-6.pdf
[CCRA AC]	Assurance Continuity: CCRA Requirements	https://www.commoncriteriaportal.org/files/operatingprocedures/2012-06-01.pdf
[ANSSI-CC-MAI-P-01/2.EN]	ANSSI – Assurance Continuity	https://www.ssi.gouv.fr/uploads/2014/11/ANSSI-CC-MAI-P-01-Continuit%C3%A9-de-lassurance_v2_EN.pdf

Appendix B: Terms & Abbreviations

Term / Abbreviation	**Definition**
Authenticator Boundary	A vendor-defined boundary according to Security Requirement 1.1.
Certified Authenticator	An Authenticator version that is certified by FIDO Security Secretariat.
Changed Authenticator	An Certified Authenticator that has been changed/updated.
Delta Certified Authenticator	A Changed Authenticator that is certified.
CC	Common Criteria
CWG	Certification Working Group
PP	Protection Profile
FER	FIDO Evaluation Report
RP	Relying Party
SRWG	Security Requirements Working Group

Security Requirements Working Group	FIDO Working Group composed of FIDO member companies that define the requirements for the Security Certification Program and act as Security Experts for FIDO.
Accredited Laboratories	Laboratories that have successfully completed the FIDO Laboratory Accreditation Process and have a valid Certificate of Accreditation.
Vendor	FIDO member organization or non-member organization seeking FIDO Certification.
Security Secretariat	FIDO Staff responsible for reviewing applications, questionnaires, monitoring security threats, and acts as an independent FIDO security expert for the FIDO Security Certification Program.
Accreditation	Formal recognition that a Laboratory is competent to carry out specific tests or calibrations of types of tests or calibrations. Accreditation does not imply any guarantee of Laboratory performance of test/calibration data.
Certificate of Accreditation	Document issued by FIDO to a Laboratory that has been granted FIDO Accreditation.