

FIDO APPROACHES: NOK NOK LABS S3 SUITE VS "BUILD YOUR OWN" FIDO

TABLE OF CONTENTS

Executive Summary 3

FIDO Solution Requirements 3

FIDO UAF Client infrastructure 4

FIDO UAF Server Infrastructure..... 4

Summary 6

EXECUTIVE SUMMARY

The FIDO specifications provide an open approach to strong authentication. Industry leaders from across the industry have formed an alliance to cooperate defining technical specifications that deliver strong authentication interoperability. Organizations that deploy consumer-facing applications are able to leverage these FIDO specifications and can choose to deploy the Nok Nok Labs S3 Authentication Suite or

can take a “do it yourself” approach to building FIDO authentication infrastructure. This paper focuses on the FIDO UAF protocol and highlights the main issues that organizations should consider in making this decision. It explains why the Nok Nok Labs S3 Suite provides better value, security and a proven approach to successful FIDO-based solution deployment.

FIDO SOLUTION REQUIREMENTS

Keeping Up With An Evolving FIDO Specification

Like any other protocol, the FIDO specifications will continue to develop over time to add new capabilities and address new use cases. An organization’s ability to leverage updated FIDO capabilities that appear on new FIDO-enabled devices will be dependent on the FIDO server’s support for these new features. An organization that chooses to implement its own FIDO server will need to continue to monitor the evolution of the FIDO specification, and incorporate support for updated features. Without such continued investment, the capabilities of the FIDO server will fall behind the current specifications and may result in reduced functionality and limited interoperability with newer devices featuring FIDO support.

The final draft of the FIDO UAF 1.0 specification was published in December 2014, and that is expected to be superseded by FIDO UAF 1.1 in late 2015, and then another possible “dot” release of FIDO UAF 1.x. In addition, the prospect of “FIDO 2.0” is on the horizon, which may entail further changes to an organization

building their own FIDO deployment. The Nok Nok Labs S3 Suite allows an organization to take advantage of the feature richness of FIDO without having to dedicate considerable development resources to keeping up with FIDO updates and changes.

Development Issues

The FIDO protocol is a specification, not a technology. Deploying a FIDO authentication solution involves resources and costs to implement the specification. While organizations can develop their own FIDO infrastructure to support FIDO-enabled devices and applications, required resources and costs in terms of development, testing and support can quickly mount. This involves both client-side (see Figure 1) and server side (see Figure 2) development. As shown in Figure 1, organizations need to address SDKs for each target platform that interface with the target mobile application and the FIDO client on the device, in addition to the authentication server infrastructure.

FIDO UAF CLIENT INFRASTRUCTURE

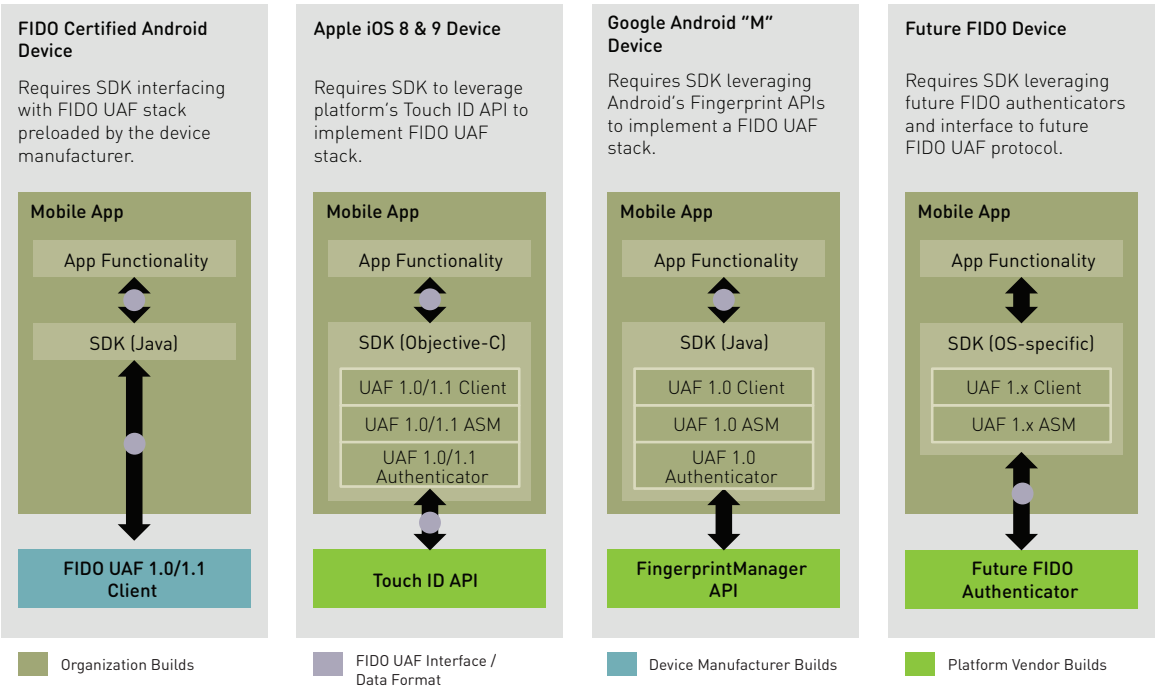


Figure 1

FIDO UAF SERVER INFRASTRUCTURE

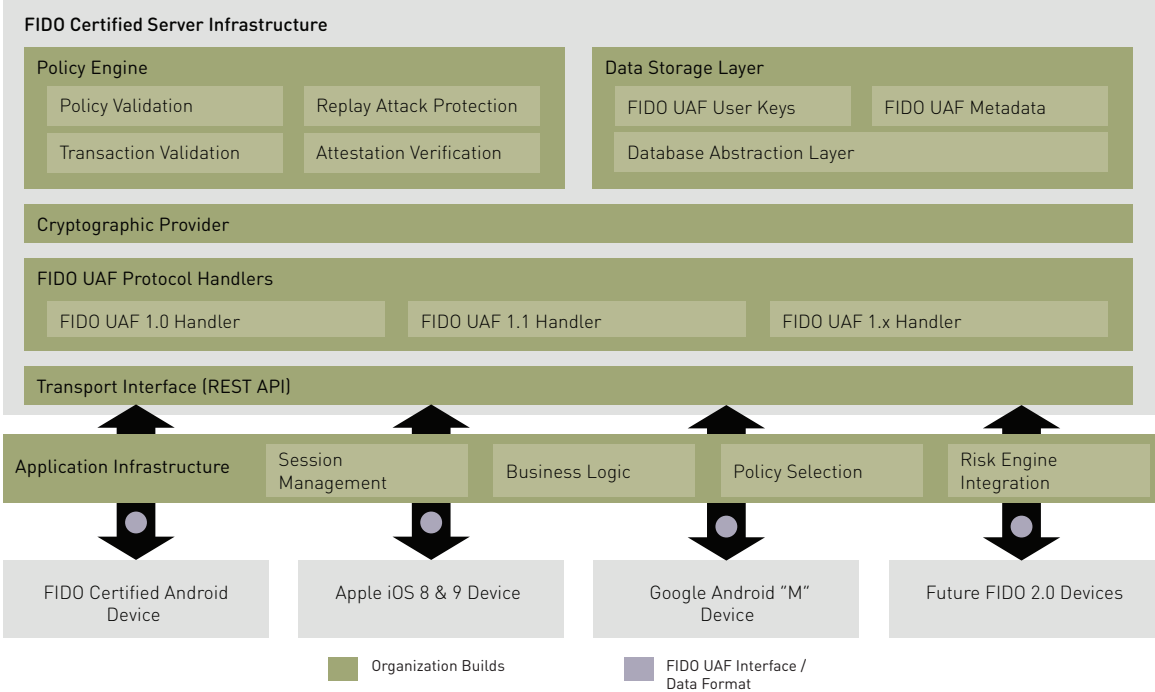


Figure 2

The FIDO specifications include a number of “non-normative” elements that are left to the FIDO developer/implementor to design and deploy. Examples include how to (i) handle replay attack prevention, (ii) track information across authentications, and (iii) represent and manage policy on the server. The developer/implementor is required to address these issues, among others, which reside outside of the FIDO protocol. The Nok Nok Labs S3 addresses these elements so the deploying organization can deploy more quickly and with lower risk.

While the FIDO specifications provide a roadmap to developing an authentication server, organizations need to consider a variety of design decisions when building their own FIDO server solution. The Nok Nok Labs S3 Suite provides a proven solution for both the client and the server that accelerates deployment, lowers project risk and avoids development costs.

Heterogeneous Platform & Device Support

Organizations deploying FIDO solutions will want to support a broad number of devices and authenticators in order to avoid “authentication silos” and reduce costs. While organizations deploying their own FIDO solution can take advantage of any FIDO Certified™ device, the Nok Nok Labs S3 Suite also provides support for any device, not just FIDO Certified™ devices. For example, Nok Nok Labs App SDK supports iOS and Apple Touch ID.

An organization that builds their own FIDO solution that would like to take advantage of native platform APIs such as Google Android Marshmallow Fingerprint API or Apple Touch ID API will need to develop and maintain software to enable those platform APIs in the context of FIDO. This means building a FIDO Client to embed in an organization’s mobile application, as well as an Authenticator Specific Module (ASM) and the authenticator (e.g. a fingerprint sensor, etc.) that leverages the native platform APIs to perform the underlying FIDO

cryptographic and user verification operations. This development is required for each target platform. The Nok Nok S3 Suite provides a complete solution to support these multiple platforms with heterogeneous devices, saving the organization time and resources.

A key issue when building a FIDO server is ensuring that the implementation complies with the FIDO specifications, and is interoperable with FIDO-enabled devices provided by third parties, such as OEMs. An organization that chooses to build its own FIDO server will need to perform qualification against FIDO-enabled devices to ensure their implementation meets FIDO specifications and is interoperable with other FIDO enabled devices. This may require the organization create a testbed, and then purchase and test a significant inventory of devices against their own FIDO server implementation. Without such rigorous interoperability testing, an organization will not be assured their server will interoperate correctly with third-party FIDO devices.

Deployment Issues

Deploying a FIDO solution requires skill and planning to ensure that the server infrastructure has sufficient scalability and is tuned to deliver exceptionally low latency that optimizes the customer authentication experience. Nok Nok Labs provides a highly tuned Nok Nok Authentication Server that benefits from years of development, testing, tuning and from the “lessons learned” from the many customer deployments that support millions of end users at scale.

Security

Developing a FIDO solution requires security preparations such as penetration testing and auditability. While developing a FIDO server would require such penetration testing, the Nok Nok solution has already completed the necessary penetration testing and avoids auditing.

Intellectual Property Protection

The FIDO Alliance framework involves a contractual intellectual property (IP) regime that relates to the FIDO Alliance specifications. Members of the FIDO Alliance promise not to assert IP rights against other Alliance members, as related to and required by the implementation of the FIDO specifications. An implementor of the FIDO specification who is not a member of the FIDO Alliance does not benefit from this promise not to assert IP rights, and could therefore assume IP risk. Using the Nok Nok Labs S3 Suite provides certain IP protection, because Nok Nok Labs is a founding member of the Alliance, and benefits from the promise not to assert patent rights; Nok Nok Labs has also developed its own patent portfolio to protect its innovations around the implementation of its FIDO solutions.

Additional Feature Requirements

- **Out of Band (OOB) Authentication** – The Nok Nok Labs S3 Suite builds on top of FIDO to enable the use of a FIDO -enabled mobile device as an “Out of Band” method of authentication. With this feature, users can use their phone to authenticate sessions and transactions initiated on another device (such as a desktop web browser, or a kiosk). This unique functionality in the Nok Nok Labs S3 Suite is beyond the scope of FIDO specifications, and is only provided by Nok Nok Labs.
- **Authentication Policies** – The Nok Nok Labs S3 Suite provides lower risk and reduces fraud through dynamic authentication policy options for flexible authentication. Such functionality requires custom code development for an organization that builds its own FIDO server.
- **Infrastructure Integration** - Nok Nok Labs S3 Suite also provides lower costs and simplicity with integration with Identity and Access Management (IAM) and federation systems. Such functionality requires custom code development for an organization building its own FIDO server.

SUMMARY

The Nok Nok Labs S3 Suite is a proven solution that provides simplicity, lower costs, faster deployment and optimal security. While enterprises can develop their own SDKs and authentication servers, this approach increases initial project risk and costs and also carries an ongoing burden required to support and maintain FIDO interoperability as the


specifications evolve. The Nok Nok S3 approach provides functionality beyond basic FIDO support including the ability to support devices from any vendor including Apple and Touch ID. Nok Nok Labs provides the shortest route to successful FIDO-based strong authentication.

ABOUT NOK NOK LABS

Backed by a team of security industry veterans from PGP, Netscape, PayPal, and Phoenix, Nok Nok Labs has deep experience in building internet- scale security protocols and products. Our ambition is to fundamentally transform authentication, by unifying authentication into one standard protocol, giving business the power to make the utmost of the cloud, data, mobile, and business online.

Nok Nok Labs
2100 Geng Road, Suite 105
Palo Alto, CA 94303

www.noknok.com



TO LEARN MORE ABOUT NOK NOK LABS,
VISIT NOKNOK.COM OR CONTACT US
AT INFO@NOKNOK.COM

Nok Nok
LABS

Nok Nok Labs, Nok Nok, and NNL are all trademarks of Nok Nok Labs, Inc. © 2015 Nok Nok Labs, Inc. All Rights Reserved.