



## The FIDO Alliance: Strong, Simple Authentication for Financial Transactions

Biometric techniques (fingerprint, facial, and voice) and other forms of multifactor authentication provide access to private data that is more secure and easier to use than passwords. These technologies require custom software, proprietary interfaces, and considerable work to integrate into financial services applications. In contrast, the FIDO Alliance provides trusted convenience by making strong authentication easy for both IT and end users to deploy and use.

### WHAT IS THE FIDO ALLIANCE?

The FIDO Alliance is an industry standards body that is changing the nature of authentication by:

- Developing technical specifications that define an open, scalable, interoperable set of mechanisms that reduce the reliance on passwords to authenticate users
- Providing operating programs to help ensure worldwide adoption of the specifications
- Submitting the specifications to standards development organizations for formal standardization



# FIDO ADVANTAGES FOR FINANCIAL SERVICES

By complying with FIDO standards, financial services organizations can more easily take advantage of a full range of multifactor authentication techniques to deliver powerful security and convenience to their employees and customers.



## STRONG SECURITY

Samsung SDS FIDO (Fast Identity Online) is more secure than passwords. Multifactor authentication combines a FIDO-certified hardware device, such as a smartphone, with a second factor, such as a or fingerprint. When a user registers to use a FIDO device with an online server, the device generates a new key-pair of encryption keys used and known only by that server. Because no identifying information is sent to the service, hackers breaking into the service cannot obtain complete authentication information.



## COMPREHENSIVE

Without complex programming, financial services' online or on-premise applications that support FIDO standards can leverage any type of authentication available on each end user's device:

- Biometrics—fingerprint scanners, voice, and facial recognition
- Existing standards—Trusted Platform Modules (TPM), USB Security Tokens, embedded Secure Elements (eSE), Smart Cards, Bluetooth Low Energy (BLE), and Near Field Communication (NFC)
- Future innovation—standards are extensible



## CONVENIENT

Once FIDO standards are commonly deployed, users will be able to use one device and or biometrics to log into any number of services. FIDO eliminates the need for users to remember large numbers of complex passwords or struggle with multiple authentication mechanisms.

## SAMSUNG SUPPORT FOR FIDO

The Samsung SDS America Biometric solution provides fingerprint, facial, and voice biometric authentication. Its client, server and authenticator comply with the FIDO Universal Authentication Framework (UAF).

To learn more about our FIDO solution visit [www.samsungsdsa.com](http://www.samsungsdsa.com) or email us at [bd.sdsa@samsung.com](mailto:bd.sdsa@samsung.com).

## ABOUT SAMSUNG SDS AMERICA, INC.

Samsung SDS America (SDSA) is the U.S. subsidiary of Samsung SDS, a global IT solutions company. SDSA provides purpose-built technology solutions in the areas of enterprise mobility, security, advanced analytics, mobile sales productivity, and training. We enable our customers in the public sector, finance, retail and other industries to achieve greater freedom, operational efficiency and smarter decision making as the driving force for their competitive advantage. SDSA is headquartered in Ridgefield Park, NJ with offices in Herndon VA and San Jose CA.

Copyright © 2016 Samsung SDS America, Inc. All rights reserved.

Samsung SDS FIDO is the trademark or registered trademark of Samsung SDS America, Inc. or Samsung SDS Co., Ltd. Other company and product names mentioned are trademarks of their respective owners. This document is provided for information purposes only. The contents of this document are subject to change without notice.