YESsafe Mobile Token+

Turn any mobile device into a personal trusted device for authentication and authorization

YESsafe Mobile Token+ is a new generation all-in-one mobile security token using One Time Password (OTP), PKI / Digital Certificate and FIDO technologies for strong authentication and transaction authorization. It not only provides transaction signing to provide non-repudiation and data integrity protection, it also leverages the advanced features of mobile devices to offer security protection and ease of use.

Features:

All-In-One Mobile OTP and PKI Token

Supports both OTP and PKI for authentication and transaction signing with "What you see What you sign" features. Its OTP features include:

- Response Only OTP Token
- Challenge Response OTP Token
- Transaction Signing OTP Token

Smart Transaction Data Capture

Leverages the camera, Bluetooth, NFC and data connection of a mobile device to capture the transaction content via QR Code or Push Notification to transfer transaction information from any of the delivery channels to the mobile token for authentication and authorization without the need for users in keying the necessary information as in the traditional tokens.

Trust elevation and step-up authentication

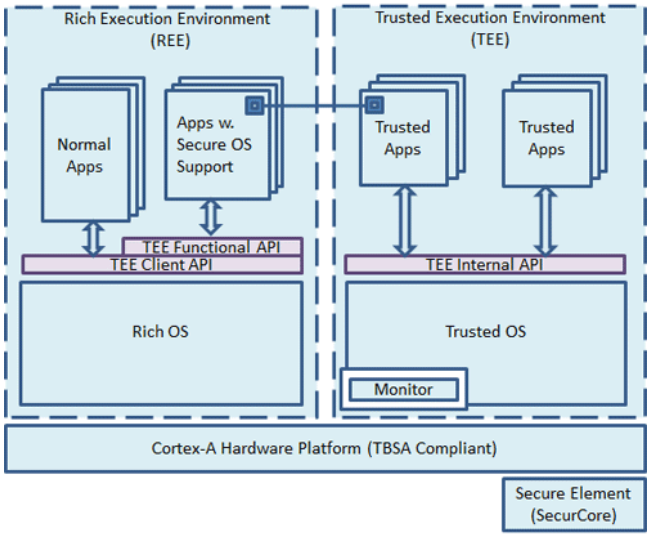
Applies the step-up authentication process for accessing resources with higher trust level requirements.

FIDO Certified

Certified to compliance with the FIDO (Fast IDentity Online) standard which is the new generation of biometric identification technology to enable seamless authentication integration with different online services.

TEE Protection Option

Integrates with TEE (Trusted Execution Environment) to provide a trusted environment for sensitive application and data by providing isolated secure and non-secure zone directly on the CPU hardware; TEE is able to build a mini operating system that isolated from Android and iOS to run the sensitive apps with security and privacy concerns. This solution fulfils the banks, military and political units that require high security requirements.



Powered by i-Sprint

Contextual Authentication Ready

Integrates with AccessMatrix UAS Server offers contextual authentication features to leverage a wide variety of identity-relevant contextual data (for example, geographic location, time-of-day and endpoint identity) to elevate the trust in the authentication process. It extends the current credential and attributes based approach to verify the user's claimed identity during the user authentication process.

Rule-based Risk-Scoring Engine

Incorporates a rule based risk scoring engine to determine the risk level and use the appropriate authentication method(s) based on the contextual of the authentication process.

Out-of-Band Authentication and Authorization

Takes advantage of the data connectivity of the mobile device to transfer authentication and/or authorization information such as OTP, transaction signing data using a 2nd channel which is different from the transaction initiation channel for authentication and authorization.

Complete Token Management and Authentication Solution

Integrated with the battle-tested AccessMatrix Universal Authentication Server to provide a complete Token Management and Authentication solution with contextual authentication capabilities.

Flexible Self Service Features

Delivers a Mobile SSO platform on mobile devices to enable users to enjoy the SSO convenience within the portal and SSO to other applications on the same mobile device.

Configurable Token Layout Design

Provides a Token Design Tool for organizations to customize their token layout:

- Layout and Color Scheme
- Card Verification Features
- Labeling – System and User Defined Fields for data integration

Geolocation and Time-Based Restrictions

Determines the geo-location based on the mobile devices using external information such as GSM location, IP address, location detection device such as iBeacon and time-based information to determine the authentication requirements.

Device Fingerprinting

Captures the unique information about the mobile device for device identification purpose and leverages the same information for data encryption and prevention of device and application cloning. It also detects the state of the mobile device e.g. Jail Break, OS version, etc to determine the appropriate authentication requirements.

i-Sprint's unique world leading IAM and IDM solutions include :

- Complete IDM Life Cycle Management Platform for User Administration, Authentication, Single Sign-On and Authorization.
- Proven Secure E2E Encryption (E2EE) Authentication and Data Protection solutions for securing credentials and transactions during transit.
- Bank grade versatile strong authentication (biometrics, multi-factor authentication and more) and credential management platform to secure multiple access channels based on an unified integrated security platform.

Global Headquarters
Blk 750D Chai Chee Road #08-01
ESR BizPark @ Chai Chee (Lobby 1)
Singapore 469004
Global: +65 6244 3900
enquiry@i-sprint.com
www.i-sprint.com

For a complete list of our offices in China, Hong Kong, Japan, Malaysia, Thailand & United States, please visit
www.i-sprint.com/contactus

i-Sprint
Trust without Boundaries