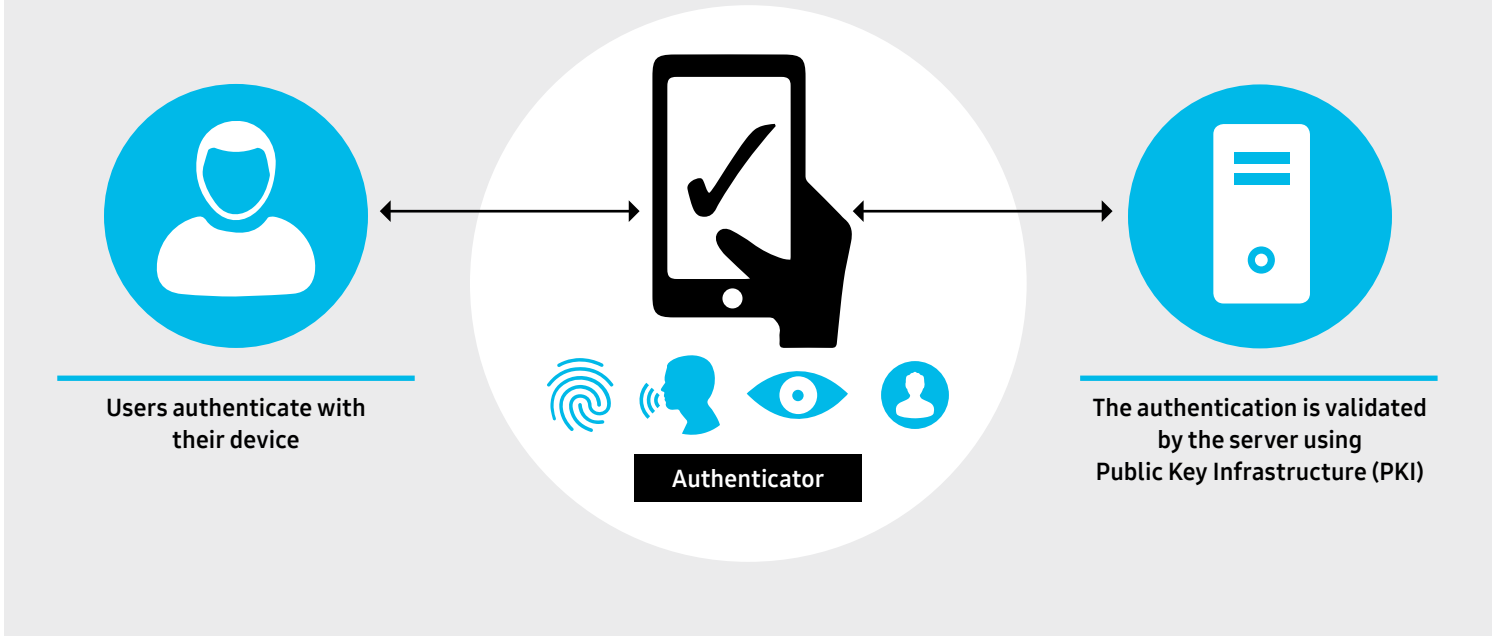
TECH BRIEF

Samsung SDS Nexsign™

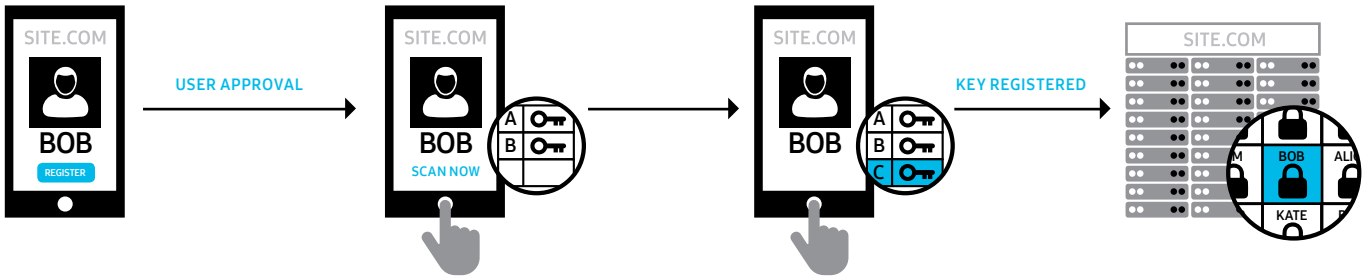
An authentication solution that verifies identities with biometric information like a fingerprint, face, or voice.

Samsung SDS is a member of the FIDO Alliance, an association that facilitates the interoperability of hardware, mobile, and biometric authentication by empowering enterprises and service providers to create more secure solutions that minimize the reliance on passwords as well as PINs and defend against cyber-attacks that use stolen passwords.

How it Works*

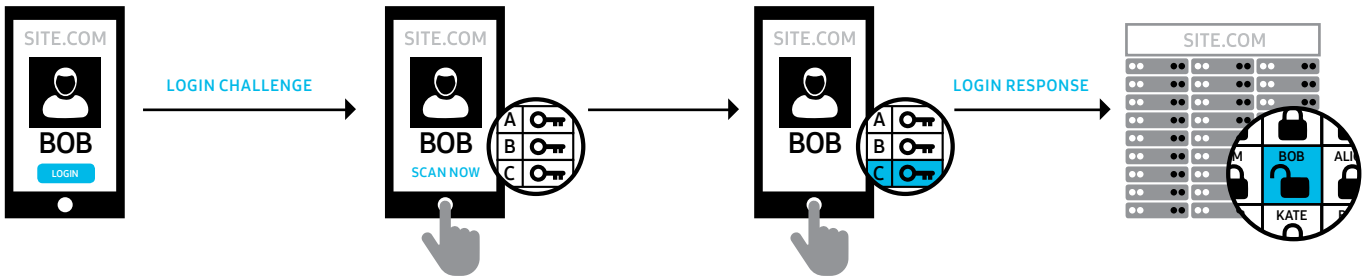


Registration*



1. **Registration Begins:** User is prompted to choose an available FIDO authenticator that matches the online service's acceptance policy.
2. **User Approval:** User unlocks the FIDO authenticator using his or her biometric information.
3. **New Key Created:** User's device creates a new public/private key pair unique for the local device, online service, and user's account.
4. **Registration Complete:** The public key is sent to the Nexsign server behind the enterprise firewall and associated with the user's account. The private key and biometric templates never leave the local device.

FIDO Login*



1. **Login:** Online service challenges the user to login with a previously registered device that matches the service's acceptance policy.
2. **User Approval:** User unlocks the FIDO authenticator using the same method used at the registration stage.
3. **Login Response:** Device uses the user's account identifier provided by the server to select the correct key and sign the service's challenge.
4. **Login Complete:** Client device sends the signed challenge back to the service, which verifies it with the stored public key, and logs in the user.

Simple and Easy System Configuration

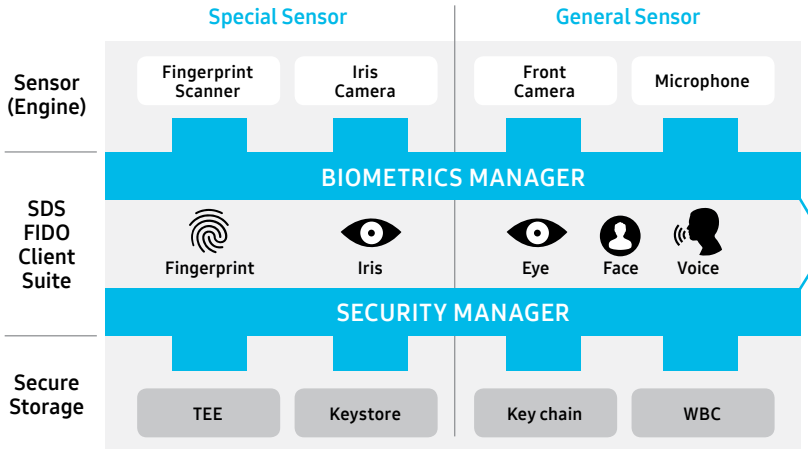
*All information from FIDO Alliance website

Biometric Modalities & Capabilities

Modalities Currently Supported

- Face, Iris**
- Voice
- Fingerprint
- Behavioral**

In addition, the platform can support any FIDO-compliant authenticator.



BIOMETRICS MANAGER

- Various biometric methods supported (fingerprint/ eye/face/voice)
- Pluggable local authentication with biometric method

SECURITY MANAGER

- Interact with the various types of device storage through standarized APIs
- Provide encryption, decryption, key generation, signing functionalities

Integration

Nexsign includes the following modules for both the Client and the Server.

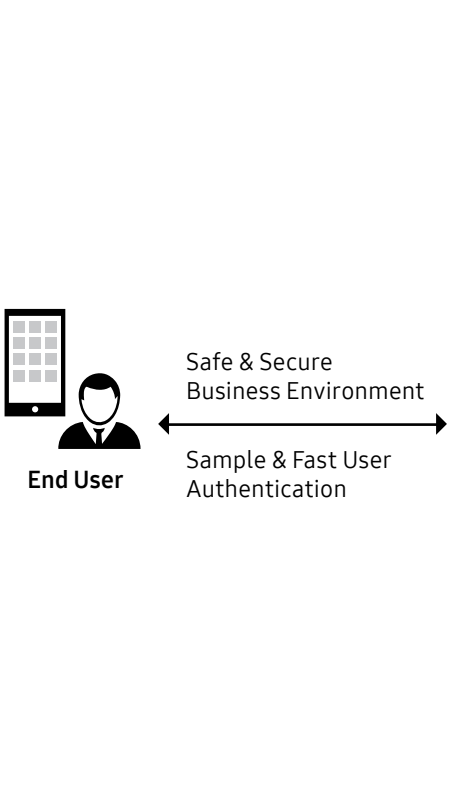
Client

- Nexsign Client SDK (includes face and voice authenticators) for both Android and iOS; SDK also includes the FIDO Client and the FIDO Authenticators
- Sample Client app along with associated source code and documentation for both Android and iOS

Server

- Nexsign Server & Nexsign Server SDK
- Sample Relying Party App and associated source code and documentation
- Administration Portal to manage Authenticators, Service Providers Trusted Facets, and Policies
- Admin User Guide

Samsung SDS Nexsign Architecture



** Included in 2018

Server Architecture

Nexsign Server

- Java application based on Play framework
- JEE WAS is not required
- Non-blocking I/O
- Java 7.0 is required

Nexsign SDK

- API set to use the FIDO protocol
- JDK 7.0 is required
- Fail-over using SDK should be considered for High Availability between RP and Nexsign Server (Web server fail-over can be utilized as an alternative)

RP App Server

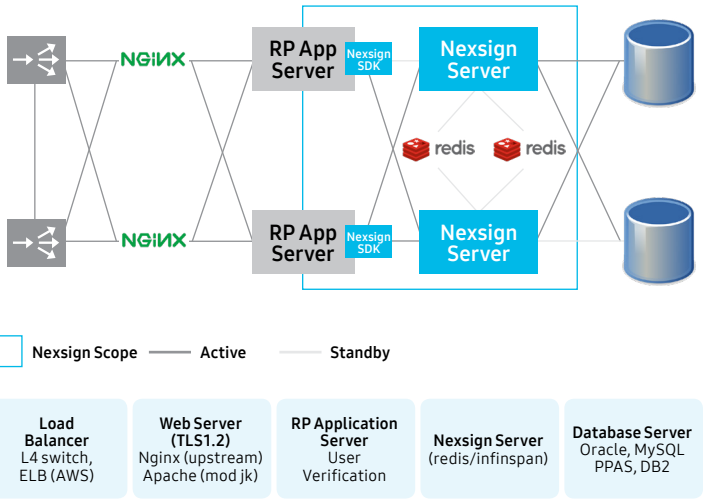
- HTTP protocol service based on Java
- Normally, JEE server
- Authentication/ Authorization

Cache Server

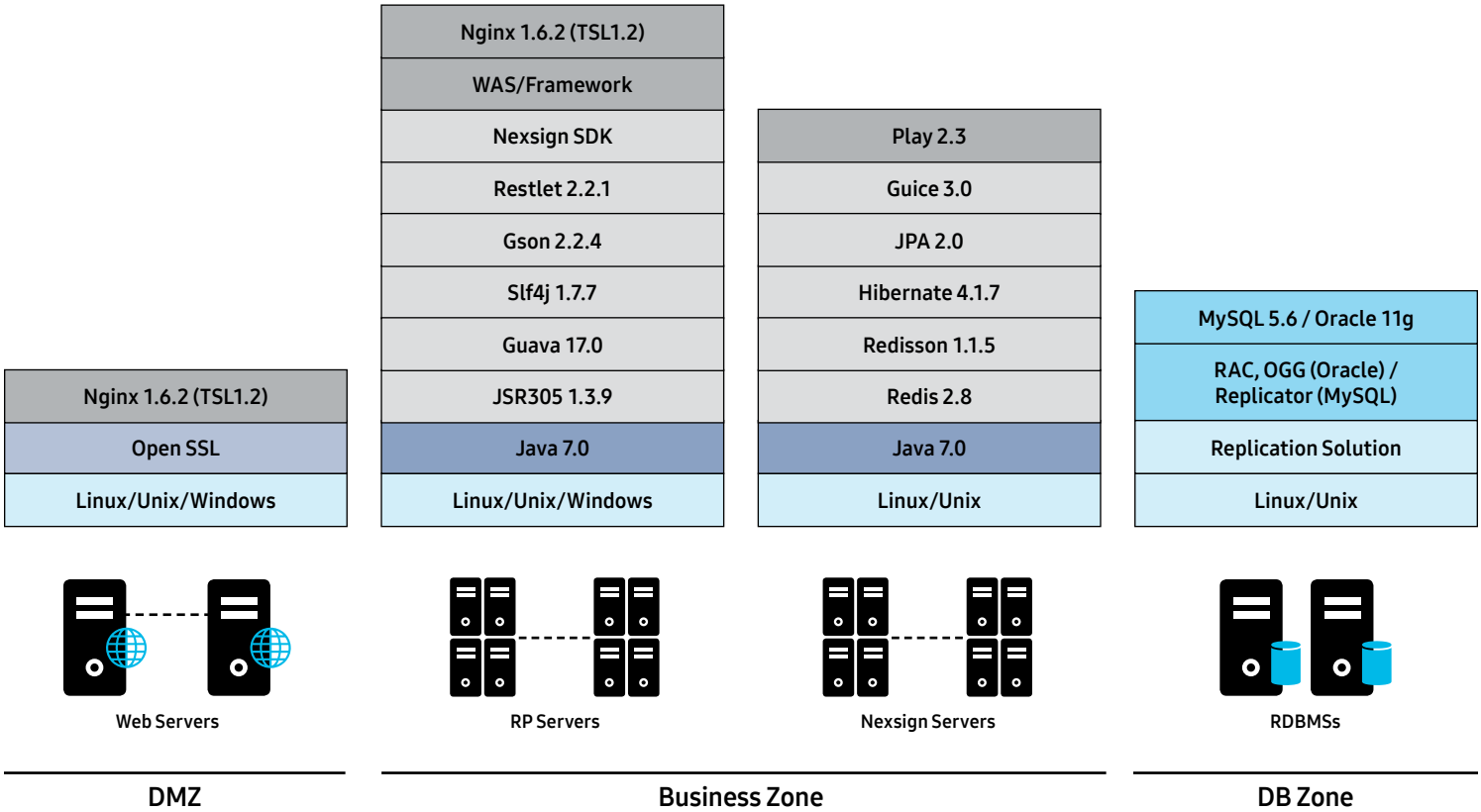
- Memory cache server for quick response
- Active-Standby configuration by Sentinel (standby server is read-only)
- Cluster configuration by Infinispan

DBMS

- High Availability should be considered with customer's own HA solution (Oracle RAC/ OGG, MySQL LVS/ Replication)



System Architecture (Software)



Management Tools

Samsung SDS Nexsign comes with a web-based Admin and Tenant portal. All admin functions are also accessible via APIs to help integrate
with customer's existing portals.

Features

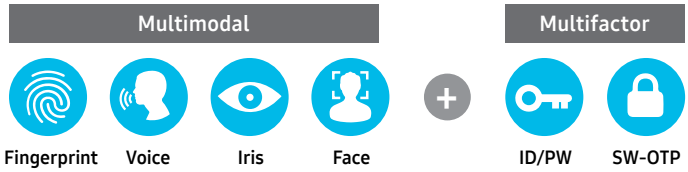
- System managment functions (e.g., user authority, server master data management)
- Service history check
- Statistics and reports
- Solution license management functions
- Service provider management

Policy Management

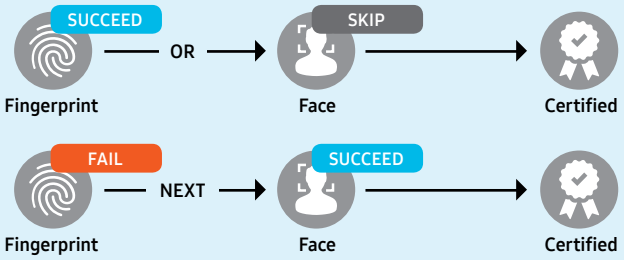
Nexsign allows for and/or business logic when defining policies for Step-up/Multifactor authentication. Policies are managed via the Nexsign Administration Portal.

Support Multifactor Authentication

- Multimodal authentication using various biometrics such as fingerprint, voice, iris, and face
  - Simple and secure FIDO solution
- Multifactor authentication using traditional authentication methods such as ID/PW and SW-OTP
  - FIDO authentication available to general users



Generality (OR/NEXT policy)



Security (AND policy)

Specifications

Operating System
Red Hat Enterprise Linux / AIX / HP-UX / Solaris / Windows

Database
Oracle / MySQL / RDS

Web Server
Nginx / Apache

FIDO Protocols
UAF FIDO V1.0 Certified

Java Application Server
Apache Tomcat

Algorithms
TLS 1.2 / SHA-256 / ECDSA-256 with P256 curve (SECP256R1) / RSA

CPU
PENTIUM 4 (2.6 GHz)

Memory
8GB

Storage
100GB HDD

OS
Ubuntu Server 14.04.1 LTS
RHEL 5.8
HP-UX B11.31
SunOS 11.1 SPARC
AIX 6.1.0.0

JDK
Java Development Kit 1.7 (Oracle ONLY)

DBMS
MySQL 5.6.20
Oracle 11g
PPAS 9.3.5.14

CACHE DB
Redis 2.8
Infinispan 7.2.3 Final

WAS
J2EE compliant Web Application Server

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.

Contact Us

To learn more about this solution and many others, head to www.samsungsds.com or email us at bd.sdsa@samsung.com today.