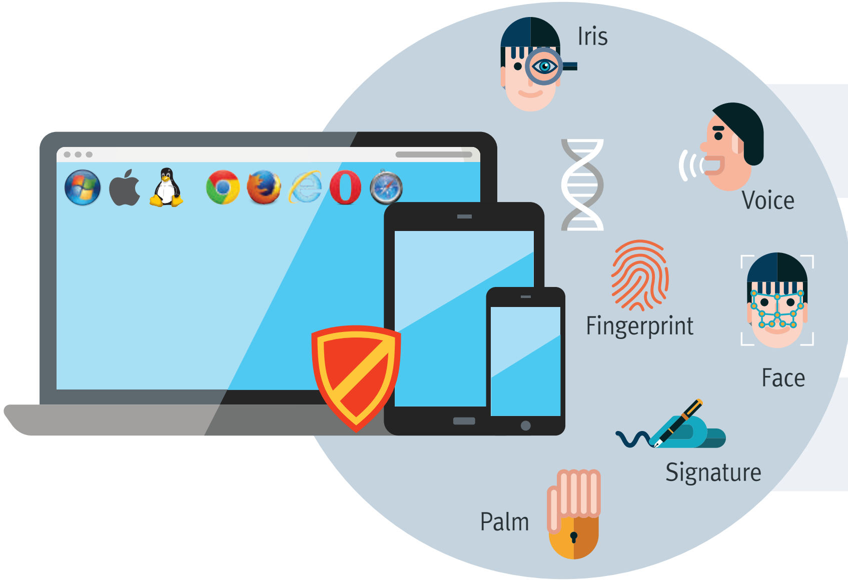
HancomSecure Pass

Biometric-authentication platform solution for Multi-Factor user authentication

HancomSecure Pass is a verified solution passed all mutual integration tests on Server, Client and Authenticator by FIDO Alliance. It complies with FIDO standard and supports a variety of biometric–authentications such as voice, fingerprint (touch and non–touch), face, iris, palm and signature, which is applicable for customers' environments as optimized forms.



Global authentication standard FIDO technology

Biometrics-based Multi-Factor authentication

User convenience with simple authentication

Key Features

Certifications and Standard Compliance

- Acquired FIDO UAF v1.0 certifications
  – Server, Client, Authenticator (Android, iOS)
- Acquired FIDO U2F v1.0 Server certification

Security

- Bio–information is securely saved to the user device instead of sending to the server, which offers high–security on the bio–information
- Enhance user authentication level through Multi–Factor authentication

Convenience

- Improve user convenience with password–less simple authentication
- Support various OS and browsers without separate PC program installation

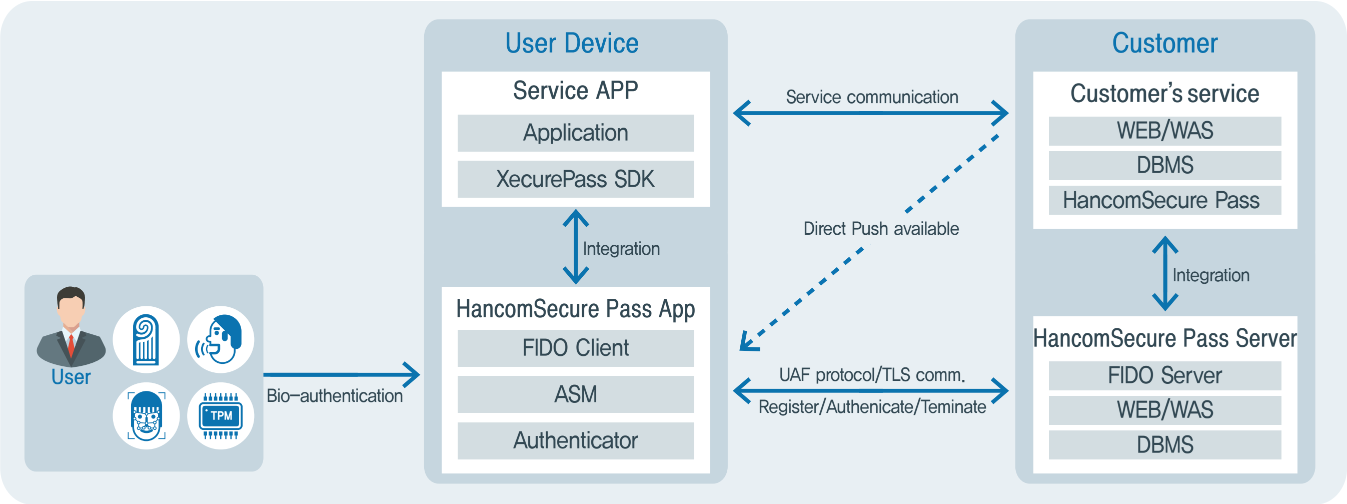
Extendability

- Compatibility on FIDO–compliant biometric–recognition module
- Applicable for bio–authentication to a variety of service environments
- Available to deploy separately required module only (Server, Client, Authenticator)

FIDO UAF Certification

FIDO U2F Certification

Architecture



User

Bio–authentication

User Device

Service APP

Application

XecurePass SDK

Integration

HancomSecure Pass App

FIDO Client

ASM

Authenticator

Service communication

Direct Push available

UAF protocol/TLS comm.

Register/Authenicate/Teminate

Customer

Customer's service

WEB/WAS

DBMS

HancomSecure Pass

Integration

HancomSecure Pass Server

FIDO Server

WEB/WAS

DBMS

Division	Specification		Description
HancomSecure Pass **Server**	O/S		▪ Windows/Solaris Sparc/Solaris x86/HP–UX/HP–IA/AIX/Linux and all other O/S available
	Application Server		▪ JDK 8 or above
	DBMS		▪ MySQL 6.3CE (Other DB support needs to be discussed separately.)
HancomSecure Pass **Client**	Android	Touch fingerprint	▪ Android OS 4.4.1 or above model mounted fingerprint recognition (Galaxy S5, Galaxy S or later)
		Non–touch fingerprint	▪ Android OS 4.4.1 or above all devices available
		Voice, Face, etc.	▪ Android OS 4.4.1 or above all devices available
	iPhone	Tough fingerprint	▪ iOS 8.0 or above suites applied Touch ID (iPhone 5s, iPad Pro or later)
		Non–touch fingerprint	▪ iOS 6.0 or above all devices available
		Voice, Face, etc.	▪ iOS 6.0 or above all devices available

Expected Effects

Non–Plugin & Standard Compliance

- Provide non–plugin environment without separate PC program installation
- Extendability for authentication technologies by complying with FIDO international standard
- Available for web standard–compliant development

Easy Management

- No PC program installation making fault management easy
- Easy extension for FIDO–compliant authenticators without server installation
- Applicable for various service environments
- Authenticator management and monitoring through web–based administrator's page

Security

- Enhance service security through implementation of Multi–Factor authentication
- No risk on leakage by server attacks by saving bio–information to the user's device instead of server

User Convenience

- Easy and low risk on loss and piracy through bio–authentication
- Convenience for users to choose one from various authenticators
- Support a variety of OS and web browsers (IE, Firefox, Safari, Chrome, Opera)

HANCOM
HANCOM SECURE

A: 9FL Hancom Tower, 49, Daewangpangyo–ro 644beon–gil, Bundang–gu, Seongnam–si, Gyeonggi–do, Korea
E: overseas@hsecure.co.kr T:+82–31–622–6321 F: +82–31–622–6277
en.hsecure.co.kr