FEITIAN Technologies

# THE FUTURE OF PASSWORDLESS AUTHENTICATION AND THE STATUS OF FIDO IMPLEMENTATION IN OVERSEAS COMPANIES

FEITIAN Technologies Co,. Ltd
www.ftsafe.com

# THE EVOLUTION OF AUTHENTICATION

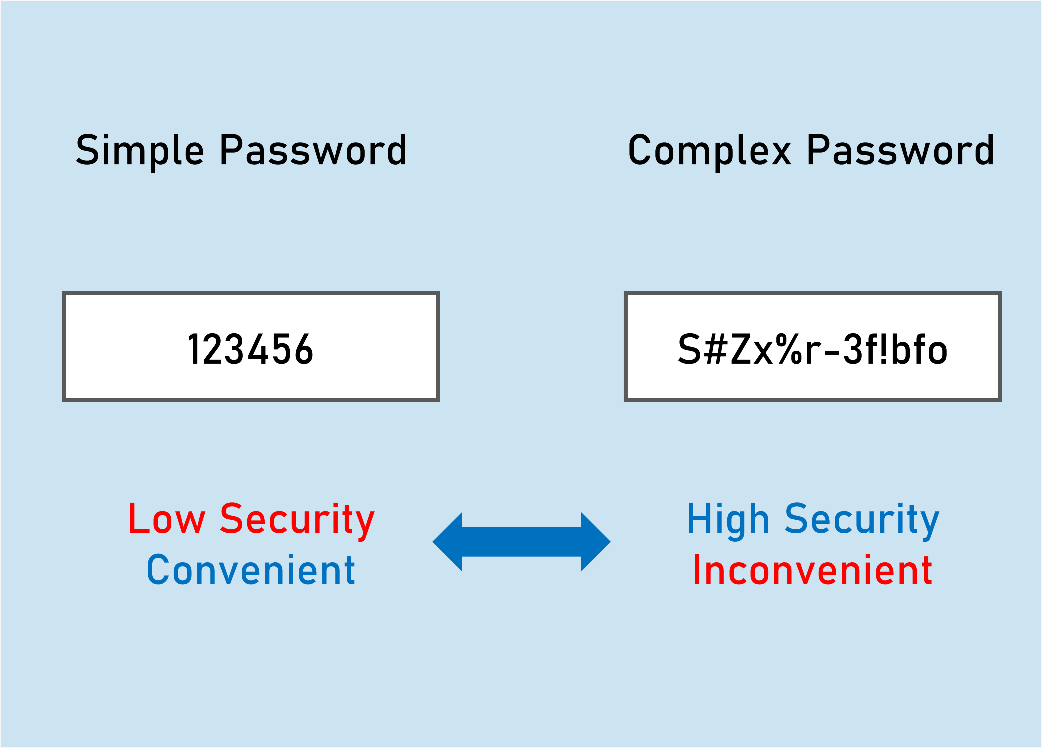
From Password to MFA to Passwordless

FEITIAN Technologies Co,. Ltd
www.ftsafe.com

# Password Authentication

Problem 1

**Security vs. Convenience**



Simple Password

123456

Low Security
Convenient

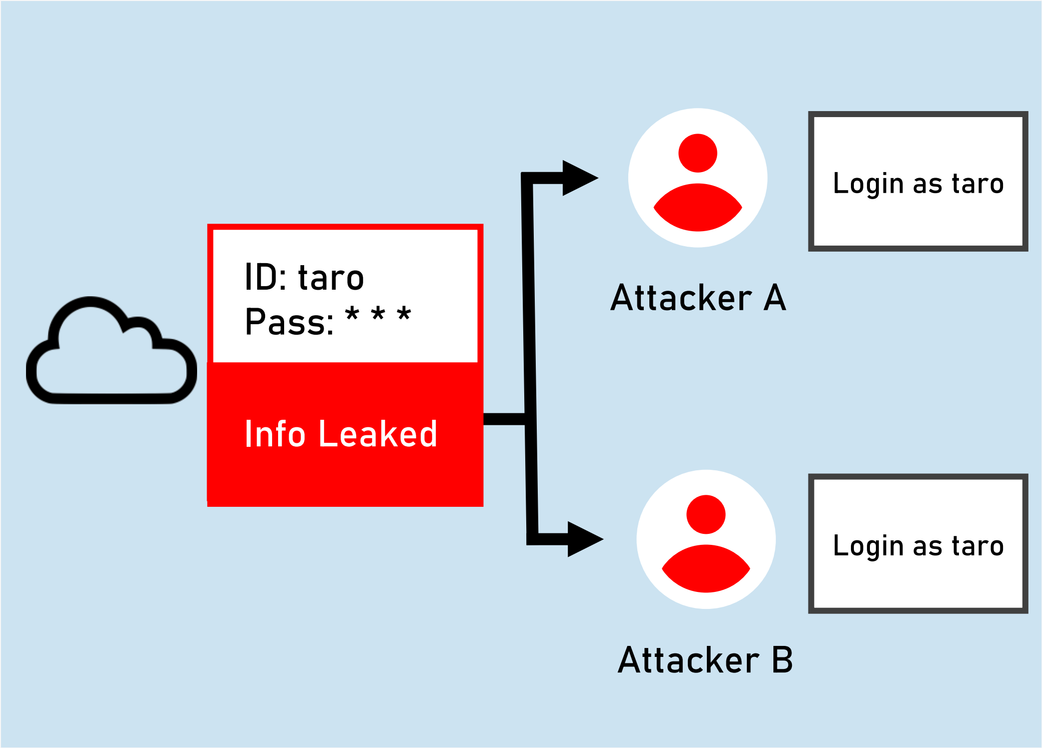
Complex Password

S#Zx%r-3f!bfo

High Security
Inconvenient

Problem 2

**Vulnerable to attacks**



ID: taro
Pass: * * *

Info Leaked

Attacker A

Login as taro

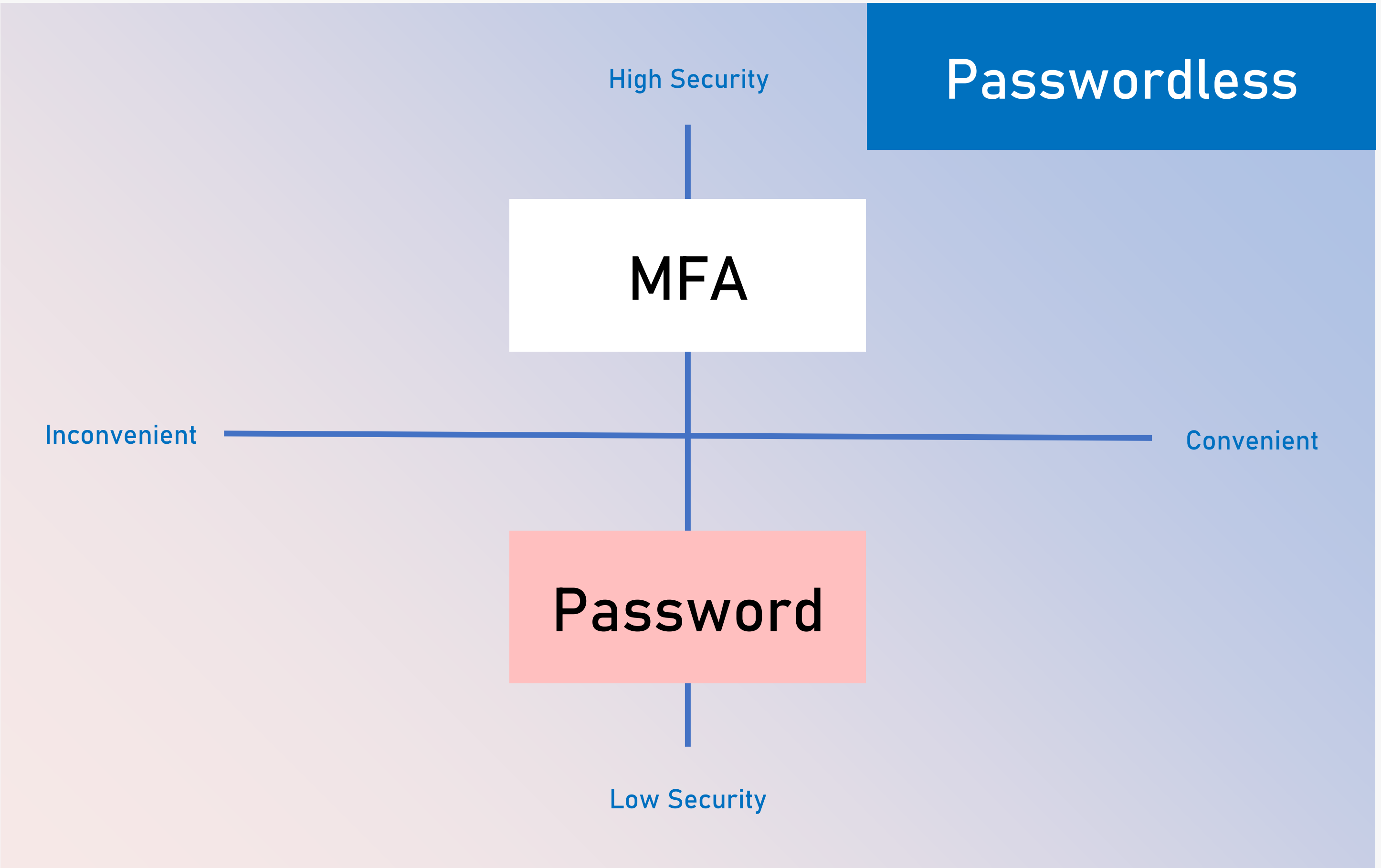
Attacker B

Login as taro

# Multi-factor Authentication（MFA）

Authentication factors

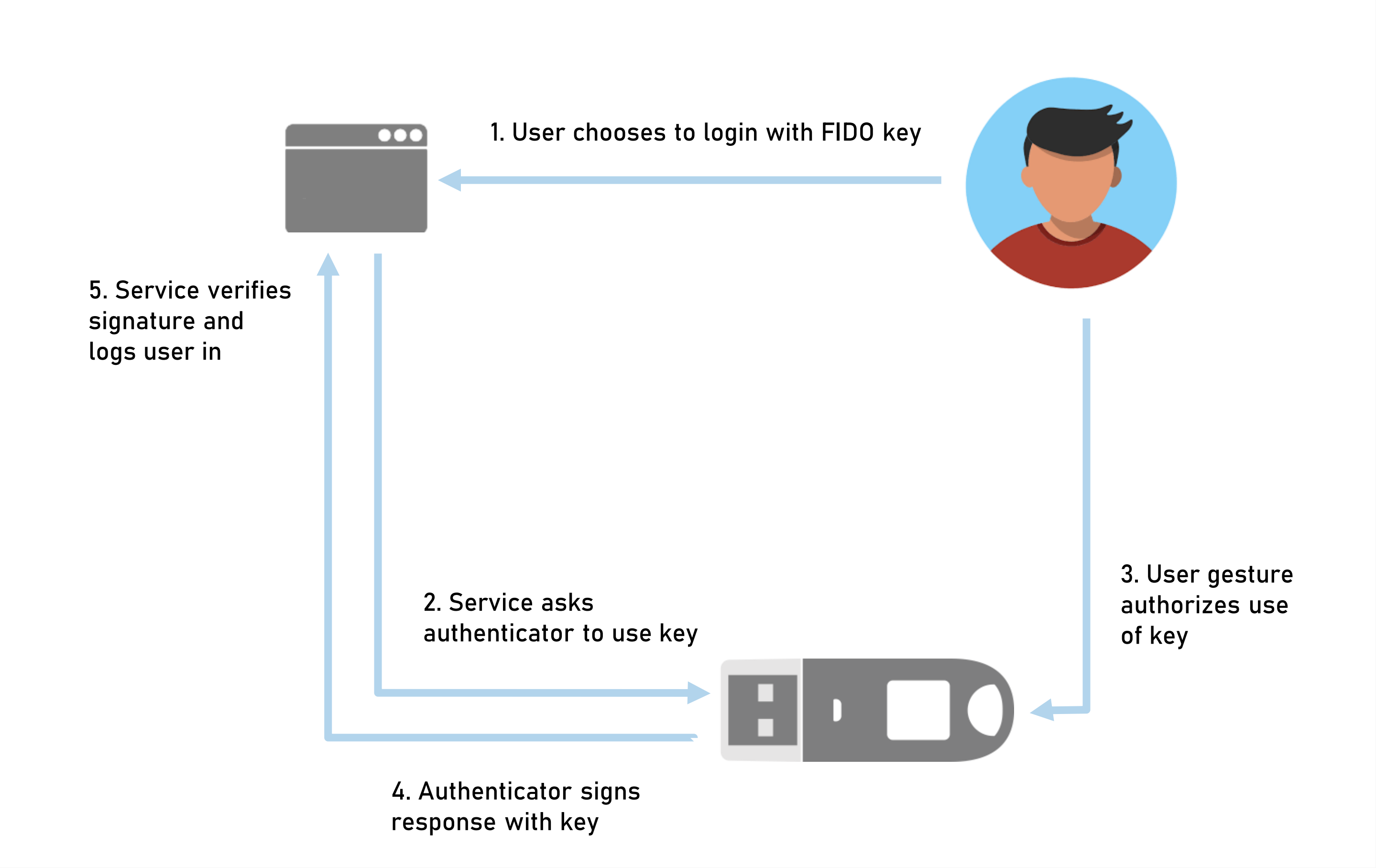
| | |
|---|---|
| Factor 1 | Something you know<br>(knowledge information) |
| Factor 2 | Something you have<br>(possession information) |
| Factor 3 | Something you are<br>(biometric information) |



# Secure and Convenient Passwordless Authentication

fido

fast identity online



1. User chooses to login with FIDO key

2. Service asks authenticator to use key

3. User gesture authorizes use of key

4. Authenticator signs response with key

5. Service verifies signature and logs user in

# FIDO2, a Passwordless World

### Passwordless

FIDO2 can be used as single factor authentication, 2nd factor authentication and multi-factor authentication. FIDO2 enables customers to do passwordless logon to their accounts including Microsoft Azure Active Directory.

### High Security

FIDO2 is designed to replace weak account-passwords mechanism with strong hardware-based authentication using public key crypto to protect against phishing, session hijacking, man-in-the-middle, and malware attacks. No secrets are shared between services.

### Open Authentication Standard

Consists of W3C's Web Authentication Specification (WebAuthn) and FIDO's corresponding Client-to-Authenticator Protocol (CTAP).

* Click here to watch the video clip about FEITIAN BioPass Security Key.

FEITIAN
WE BUILD SECURITY

# CASE REFERENCE

Microsoft

# CASE REFERENCE

Microsoft

## Microsoft Believes Employees' Passwords Are a Problem

81% of breaches leverage stolen or weak passwords.

The average help desk labor cost for a single password reset is $70 (around 7,700 JP¥).

20% - 50% of all help desk calls are for password resets.

Multi-factor authentication (MFA) protocols that require users to enter a known password or answer a knowledge-based question are risky and do not fully ensure the security of company data and accounts.

For enterprises with Microsoft accounts, including Azure Active Directory or Windows Hello for Business, biometrics are the key to unlocking a faster, highly reliable single sign-on (SSO) experience to access on-premises and cloud-hosted resources.

# CASE REFERENCE

Microsoft

## The Reason Microsoft Uses FEITIAN Products

### 1. Enhance Security and Privacy

Online accounts, systems, and applications are vulnerable to attack and credential theft is at an all time high.

Employees reusing passwords increases the likelihood of phishing attacks, MTM attacks, and severe credential breaches. No business wants to risk a data breach given the steep financial consequences and toll on a brand's reputation.

By using FIDO2-certified fingerprint-enabled security keys or cards as part of multi-factor authentication process, only the correct user in possession of their biometric device can gain access to systems, leaving no chance for hackers to manipulate credentials.

# CASE REFERENCE

Microsoft

## The Reason Microsoft Uses FEITIAN Products

### 2. Decrease IT Management Costs

Most IT help desk support calls are for password resets. And resetting an employee's password is more complex than a quick, one-click action.

IT department has more important tasks to perform, like ensuring business continuity and optimizing operations. By going passwordless, an organization no longer needs to expend support resources to manage employee credentials and assist with password resets.

Cut costs further by combining multiple functions on one security key or card, including authentication, identity verification, physical access, and payment processes.

FEITIAN passwordless security keys and smart cards are designed to meet FIDO and WebAuthn standards with Bluetooth for PC and mobile, as well as a variety of interfaces to fit Microsoft's needs.

# CASE REFERENCE

Microsoft

## The Reason Microsoft Uses FEITIAN Products

### 3. Streamline Employee Productivity

Employee productivity suffers when the authentication experience requires time-consuming, complex processes.

No one wants to memorize and keep track of new passwords. And tedious multi-factor authentication protocols, including traditional one-time password (OTP) methods, can often be anxiety - inducing and cause user friction.

Satisfy multi-factor authentication needs quickly by combining biometric security keys and cards with Azure AD MFA. With a simple touch, built-in sensors can verify employee's fingerprint and automatically unlock employee's device, allowing easy access to company resources from anywhere.

# CASE REFERENCE

Microsoft

## FEITIAN Products Adopted by Microsoft

BioPass FIDO

BioPass FIDO

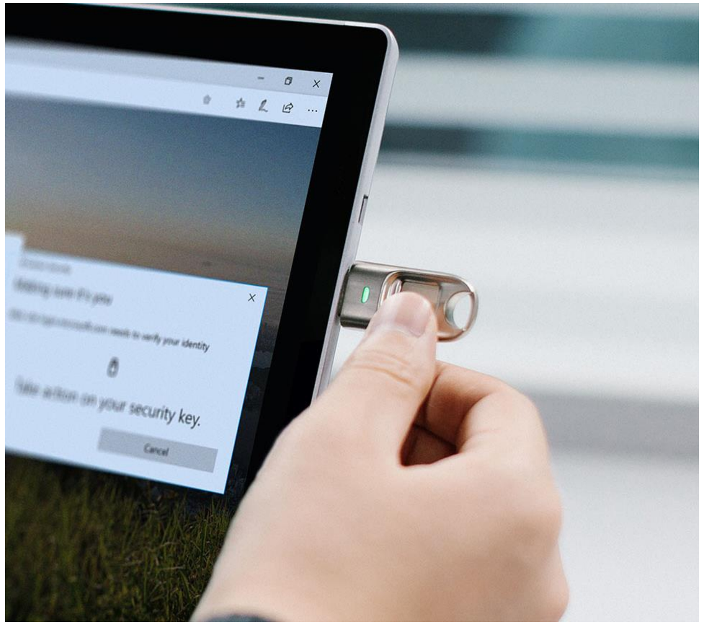
AllinPass FIDO

* Click HERE to know more about these products

# CASE REFERENCE

Microsoft

FEITIAN Products Adopted by Microsoft



Login to Azure AD with
Biometric Security Key

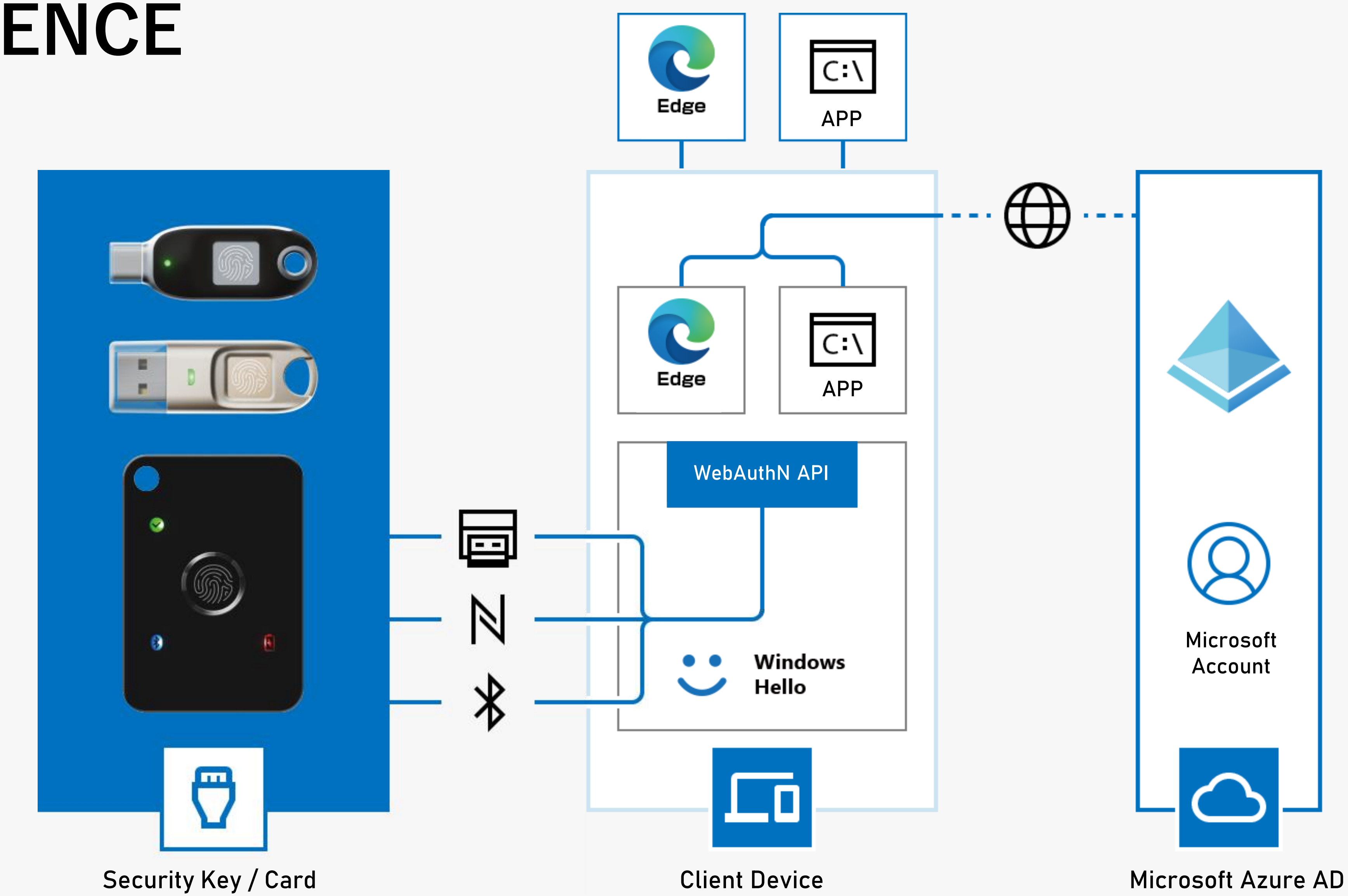
Door access with Fingerprint Card

* Click **HERE** to know more about FEITIAN FIDO2 Fingerprint Card

# CASE REFERENCE

Microsoft

Solution Provided by FEITIAN



FEITIAN Technologies Co,. Ltd
www.ftsafe.com

# CASE REFERENCE

Google

# CASE REFERENCE

Google

## Google Demands for a Second Factor Device to Improve Privacy, Security, and Usability

Account takeovers have highlighted the challenge of securing user data online: accounts are often protected by no more than a weak password for the online service provider to distinguish legitimate users from account hijackers.

Researches have produced numerous proposals to move away from passwords, but in practice such efforts have largely been unsuccessful. Instead, many service providers augment password-based authentication with a second factor in the form of a one-time password (OTP). Unfortunately, OTPs as a second factor are still vulnerable to relatively common attacks such as phishing.

In addition, OTPs have a number of usability drawbacks. These factors limit the success and deployment of OTPs as a reliable and secure second factor.

Meanwhile, secure authentication factors, which use challenge/response-based cryptographic protocols, have their own barriers to deployment. National ID cards and smart cards require custom reader hardware and/or driver software to be installed prior to use. Depending on the implementation, these systems also make it challenging for users to protect their privacy.

# CASE REFERENCE

Google

## The Reason Google Uses FEITIAN Products

Google turned to FEITIAN FIDO Secure Keys – multi-factor authentication devices that improve practicality in terms of privacy, security and usability.

The Security Keys were designed from the ground up to be practical: simple to implement and deploy, straightforward to use, privacy preserving, and protect against strong attacks. Google has supported Security Keys in its Chrome browser, deployed it within its internal sign-in system, and has enabled Security Keys as an available MFA in its web services.

After the deployment of FEITIAN FIDO Security Keys, Google has achieved both increased level of security and user satisfaction as well as reduced support cost.

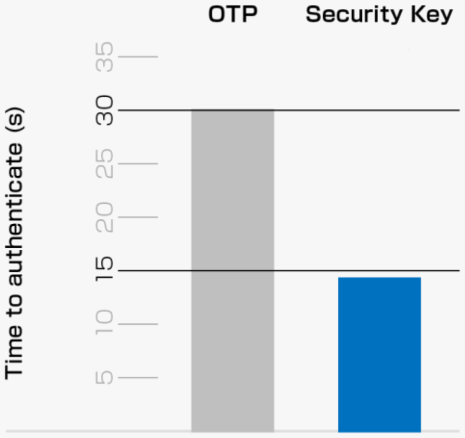
# CASE REFERENCE

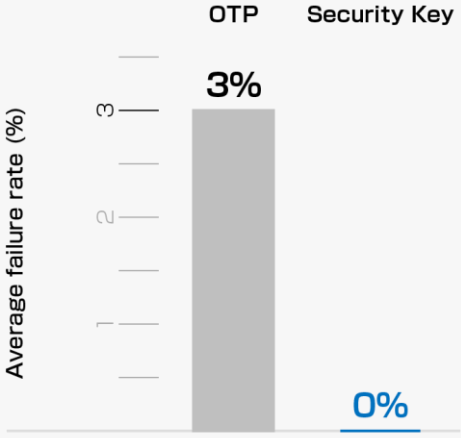
Google

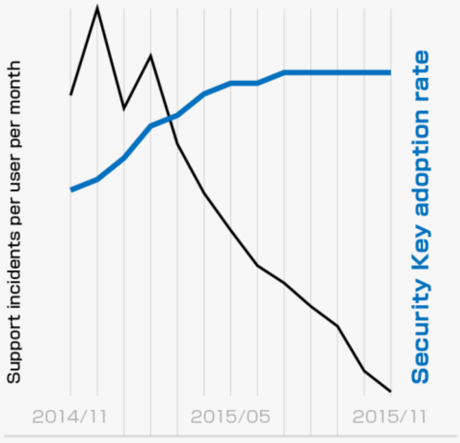
## The Reason Google Uses FEITIAN Products

“Security Keys are mandatory at Google, they provide superior protection against phishing not possible with many alternative two factor authentication solutions.”

“FIDO Security Keys provide strong authentication that’s resistant to many forms of advanced phishing attacks that traditional 2FA doesn’t protect against, it also provides for a much better user experience.”







# CASE REFERENCE

Google

FEITIAN Products
Adopted by Google

**MultiPass FIDO**

(Click HERE to know more)

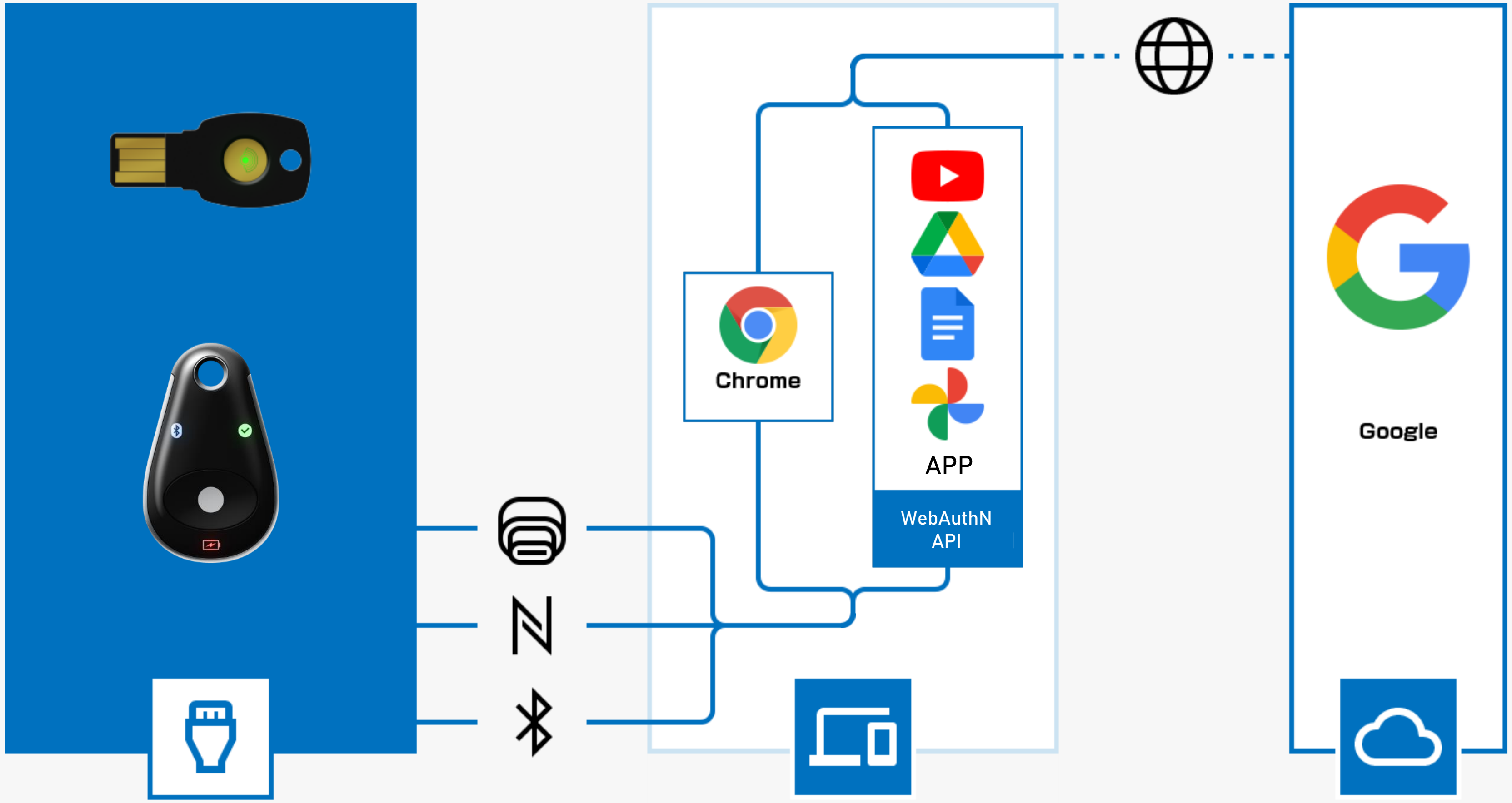
**ePass FIDO -NFC**

(Click HERE to know more)

# CASE REFERENCE

Google

Solution Provided by FEITIAN



Security Key / Card

Client Device

Google Online Service

FEITIAN Technologies Co,. Ltd
www.ftsafe.com

# CASE REFERENCE

An European Bank

# CASE REFERENCE

[redacted]

## The Bank Is Concerned About Its Customers' Account Safety

The development of the Internet has led to the development of the information industry, but also brought about increasingly serious information security problems, and identity authentication, as the first gate of information security protection, has assumed a vital role. However, at present, neither static passwords nor strong authentication methods can fully meet the authentication needs of users and enterprises.

Many banking applications are still using the authentication method of username/static password, and the security is completely dependent on the password. Static passwords are not only inconvenient to use but also not easy to remember, while users try to use common and easy-to-remember numbers such as birthdays and anniversaries as passwords, which are easy to be cracked and stolen and insecure.

To improve the security of application services, many stronger authentication methods are generated. Such as: One Time Password token, USB Key, SMS password, etc. Compared with the simple username/password authentication method, the security is improved. However, with the development of technology, these authentication methods also become more and more easy to be cracked.

# CASE REFERENCE

[redacted]

## The Reason the Bank Uses FEITIAN Products

FIDO as a universal identity authentication protocol, has been gradually adopted by major banks.

As a board member of FIDO Alliance, FEITIAN has participated in the development of FIDO related protocols and policies. FEITIAN has manufactured a variety of FIDO Security Key products to meet the different needs of many banks, as well as the supporting FIDO Server, so it has the ability to provide a complete set of solution for banks.

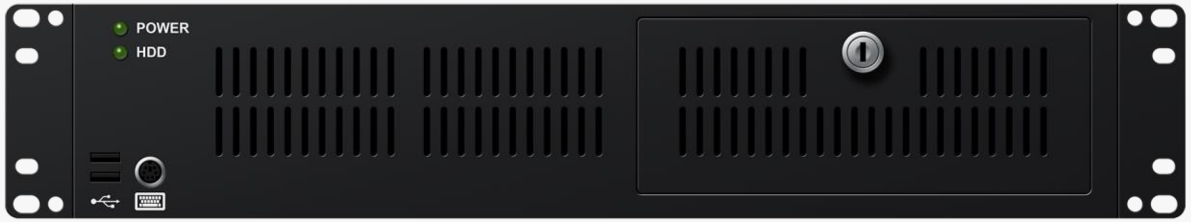
FEITIAN FIDO Security Key and FIDO Server have been certified by FIDO Alliance and hold nearly 100 FIDO related international patents, which provide assurance for customers from the security point of view.

By adopting FEITIAN FIDO Authentication Solution, the bank perfectly overcomes the inconvenient, problematic, complicated, and easily hacked static passwords.

# CASE REFERENCE

[redacted]

FEITIAN Product Adopted by the Bank

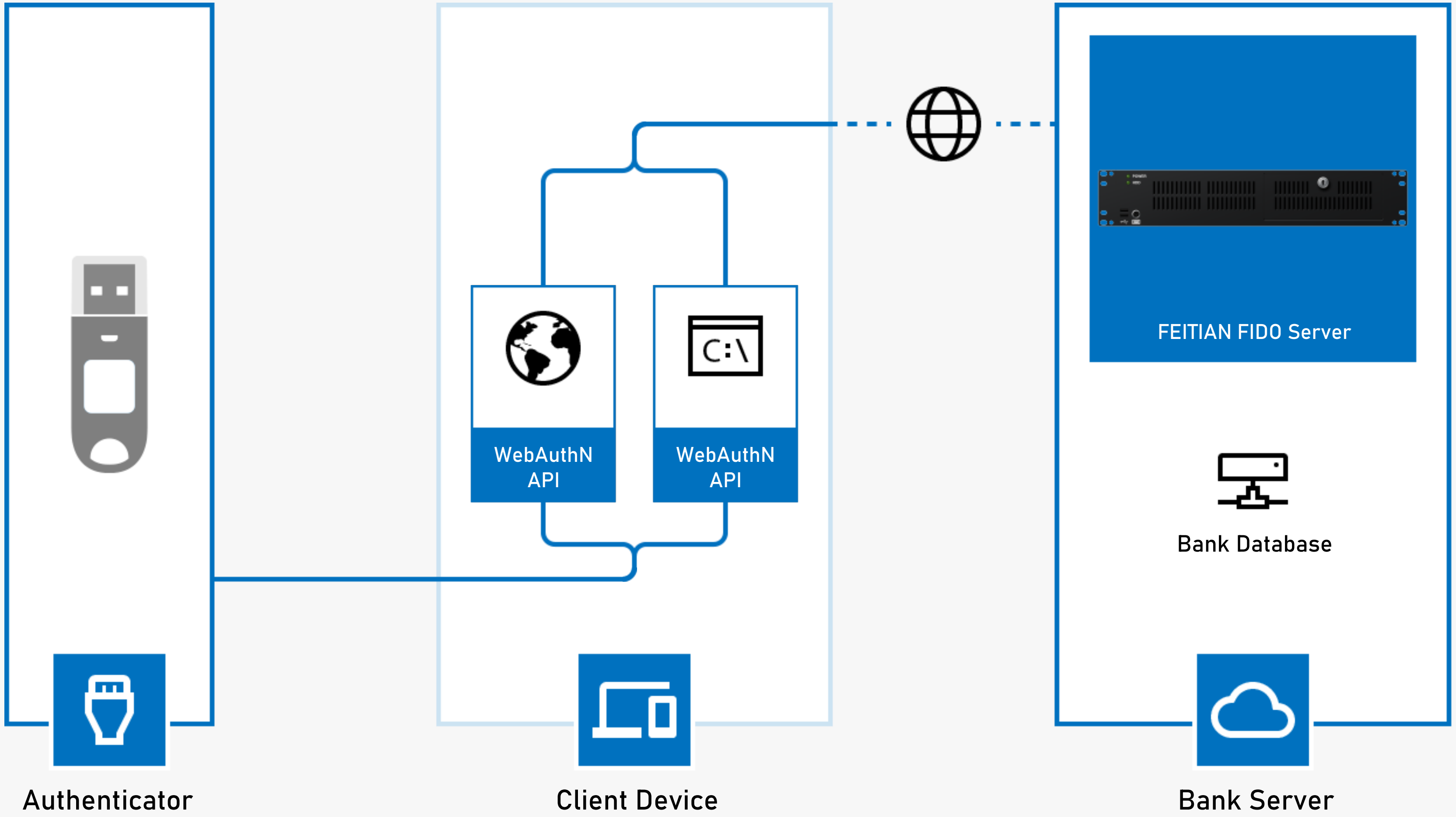


FEITIAN FIDO Server

# CASE REFERENCE

[redacted]

Solution Provided by FEITIAN



# THANK YOU!

Here to contact us for more info: https://www.ftsafe.com/Support/Inquiry

Website: www.ftsafe.com

LinkedIn: www.linkedin.com/company/feitian-technologies-co.-ltd./

YouTube: www.youtube.com/c/FeitianTechnologies