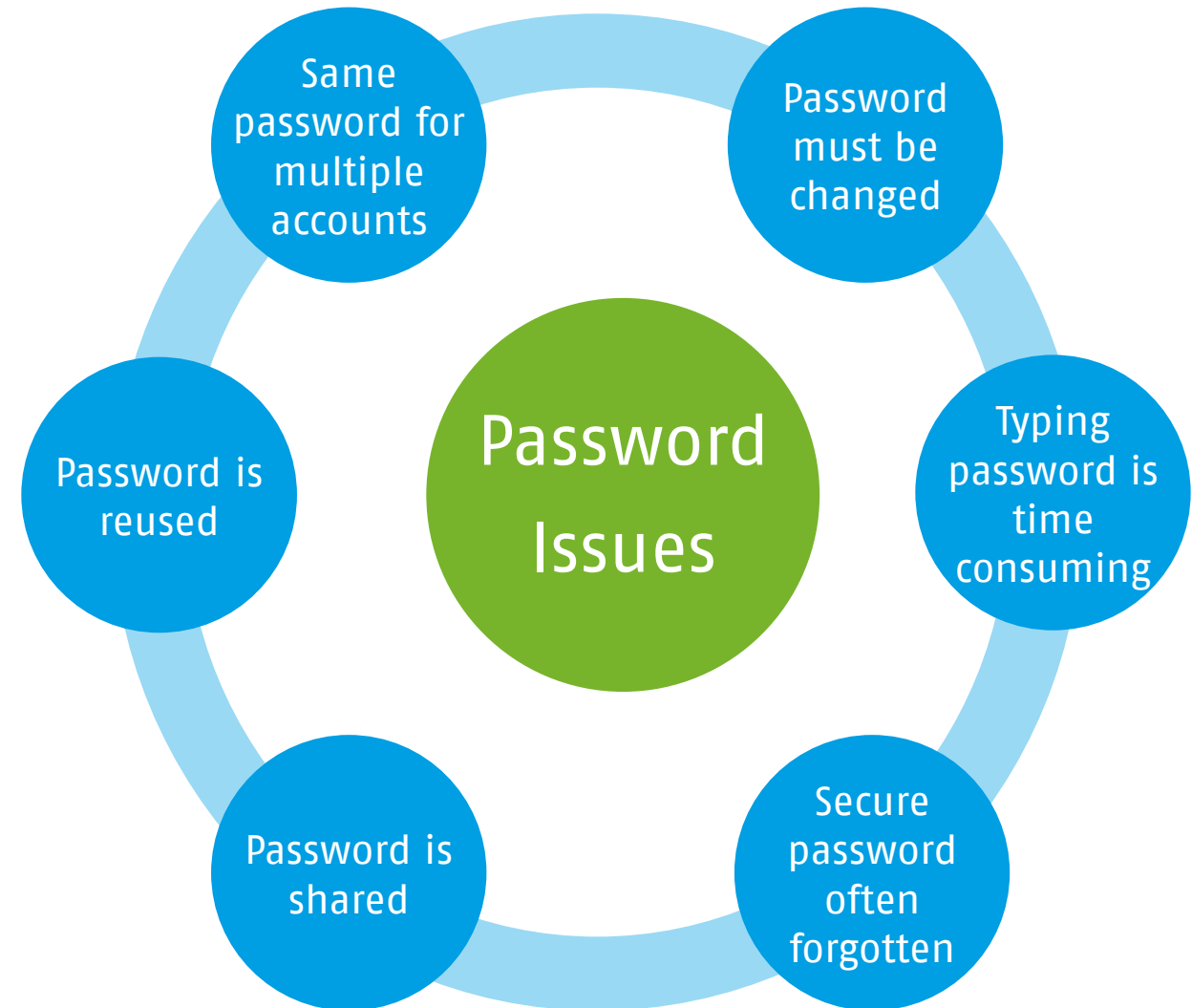


Protecting Online Accounts with Strongest and Most Trusted Hardware Authentication

Swissbit iShield FIDO2 USB-A / NFC security key for simple, secure and flexible authentication.





KRATIKAL

CYBER AWARENESS

Cyber Criminal Attempted to Poison Water Supply in Florida

February 11, 2021 - 4 mins read

A Proactive Civil Servant Saved the Town from Mass Poisoning

www.kratikal.com

BBC Sign in Home News Sport Reel Worklife Travel

NEWS

Home Coronavirus Video World UK Business Tech Science Stories Entertainment & Arts Health

World Africa Asia Australia Europe Latin America Middle East **US & Canada**

US companies hit by 'colossal' cyber-attack

3 July

ZDNet EDITOR: EU

CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY SPAIN MORE

MUST READ: Windows 11: Everything you need to know

Hacker leaks 15 million records from Tokopedia, Indonesia's largest online store

The Tokopedia data has been published on a well-known hacking forum.

Breach Report #13: Phishing, Ransomware, & Supply Chain Attacks Dominate The 2021 Threat Landscape

April 20 – May 04, 2021

日本経済新聞

Morning and evening editions LIVE My nekkei company

Top Breaking news opinion Economy Politics business Finance market Money Manabi Tech international Sports Sc

Cyber attack on Nikkei Personal information leaked for 12,514 employees

Society / living

May 12, 2020 16:30

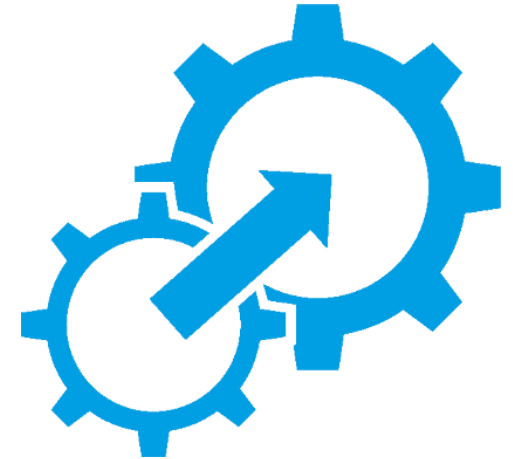
Swissbit allows users to protect online accounts – private and professional – by securely accessing websites, applications and online services with strongest & most trusted authentication – Made in Germany –, that is:



Simple



Secure



Flexible



Made in Germany

fido™
CERTIFIED

FIDO2

Protecting Online Accounts with Strongest
and Most Trusted Hardware Authentication

swissbit

SECURED BY

swissbit

www.swissbit.com

Enterprise IT

Simple and fast deployment across entire enterprise.

Businesses

Easy integration into own system and application to allow users to protect access to accounts offering various security options.

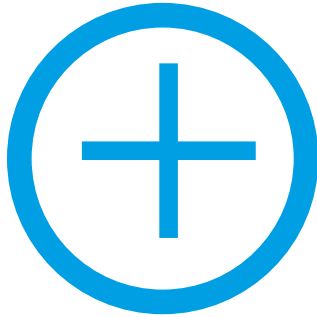
Individuals

All-in-one security key allowing users to securely access websites, applications and services, such as Google, Microsoft, Facebook and many more other services.

Swissbit iShield FID02 offers strong hardware-based authentication – Made in Germany –, that is simple, secure and flexible. It protects users against online attacks, such as phishing, social engineering or account takeover.



Made in Germany



Unparalleled Advantages over OTPs / Mobile Authentication

Hardware-based authentication:

- increases usability with faster login process
- offers strongest security
- increases productivity due to less account lockouts

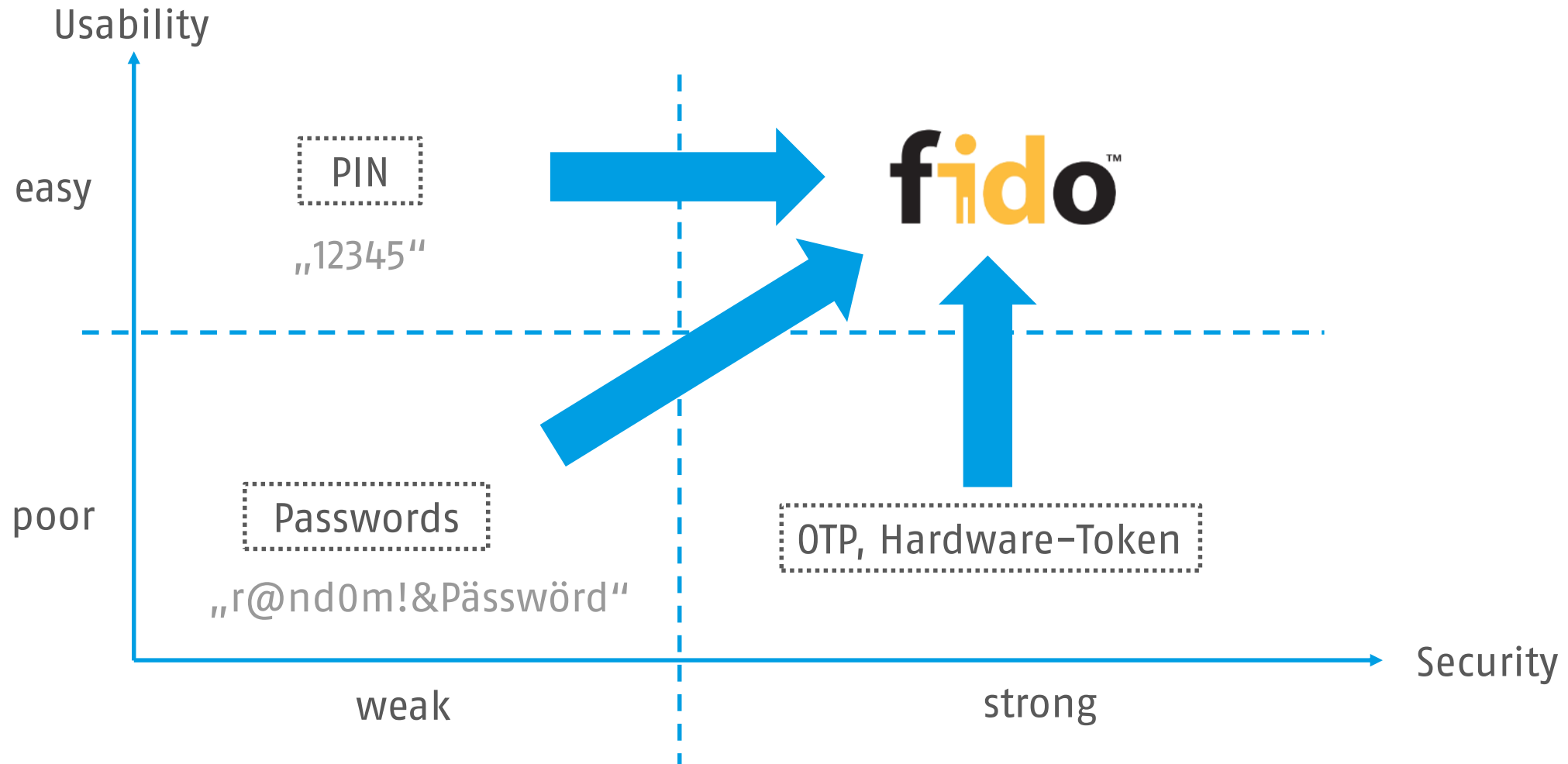


Supports Zero Trust Strategy

Zero Trust Strategy: Phishing-resistant multi-factor authentication (MFA) , such as FIDO Authentication, now specified for US agencies*.

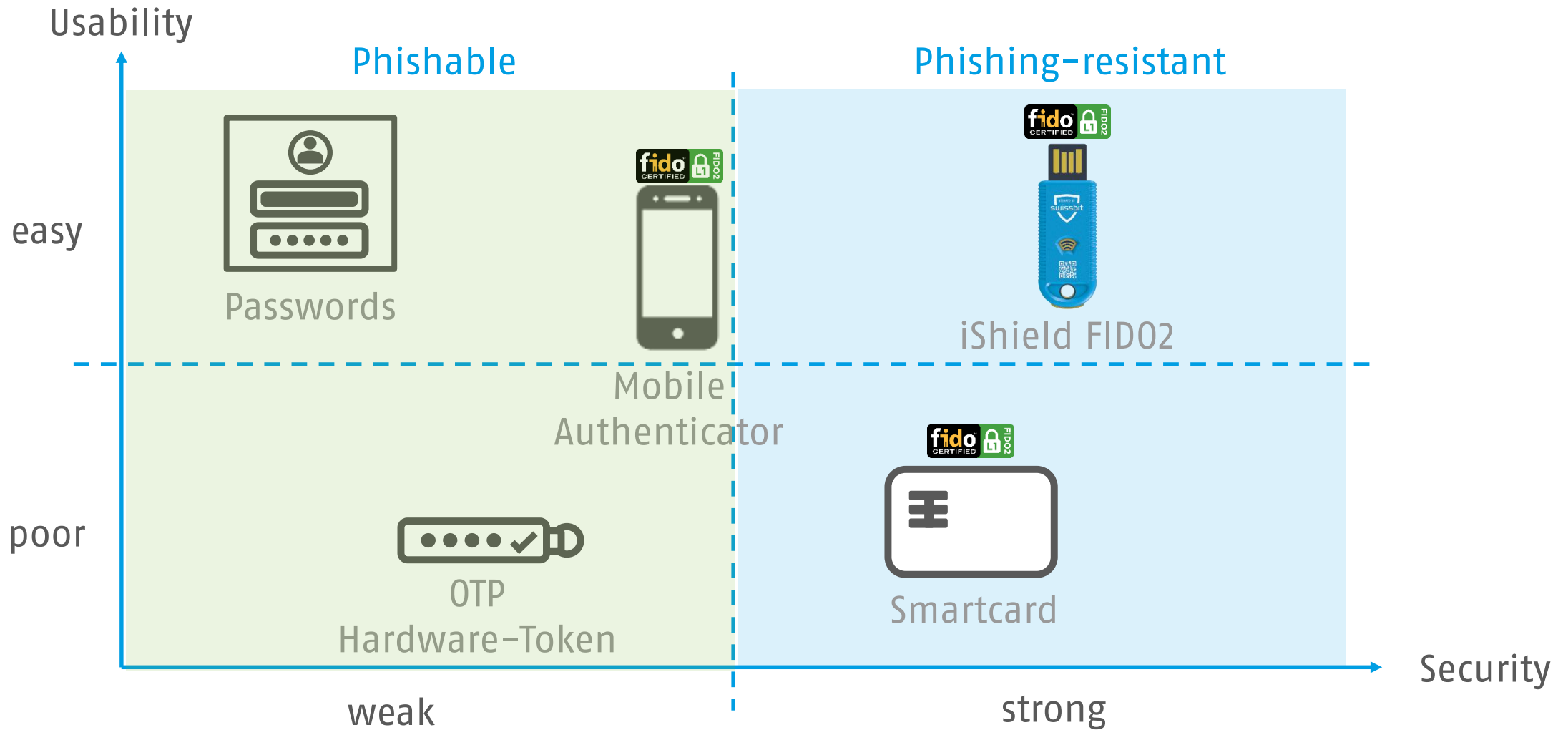
*: <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>

Why FIDO2: Providing the Strongest Authentication



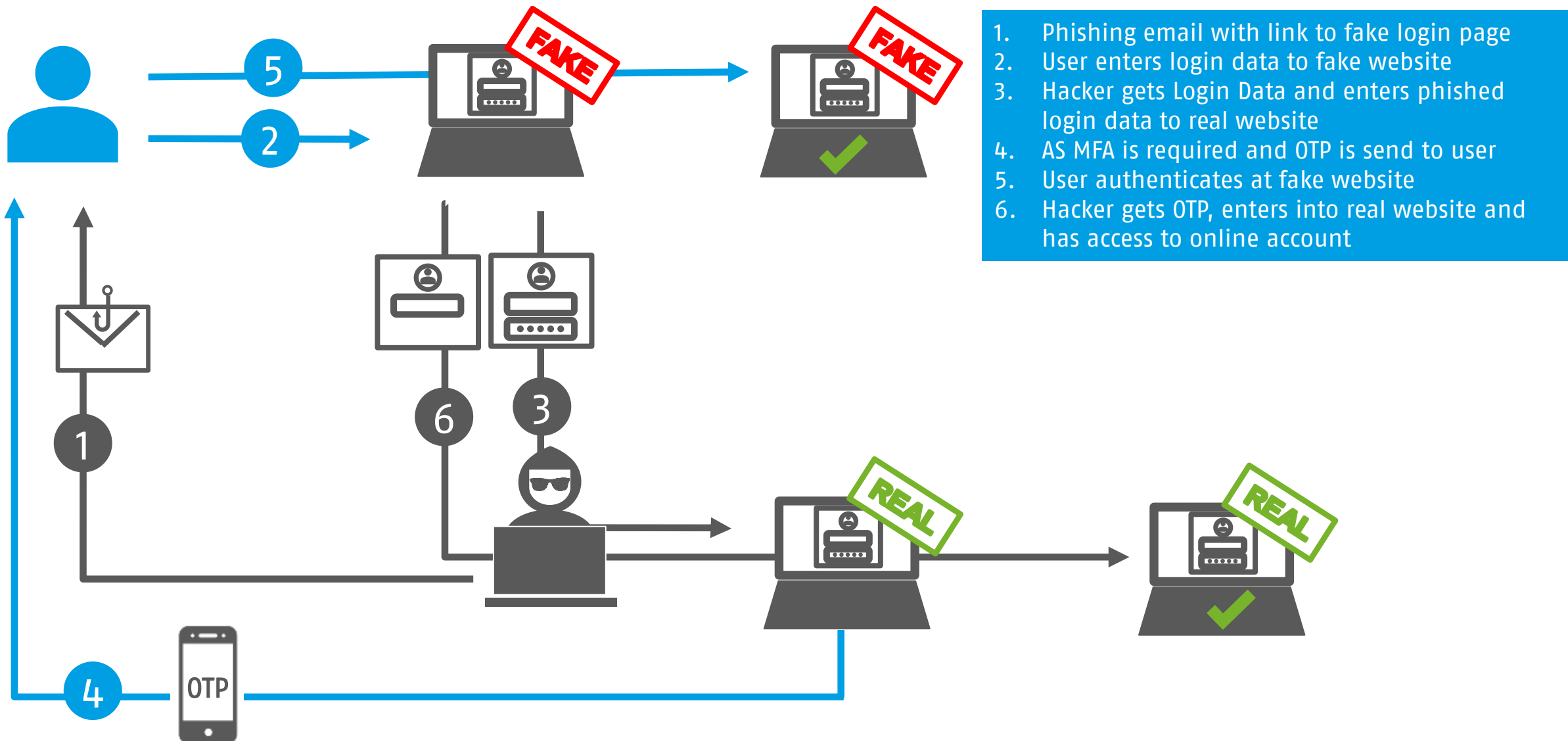
Source / inspired by: <https://engineering.linecorp.com/en/blog/fido-at-line/>

Why iShield FIDO2: Easy-to-use & Phishing-Resistant



Inspired by: <https://engineering.linecorp.com/en/blog/fido-at-line/>

Phishing Even With Mobile-based Authenticators

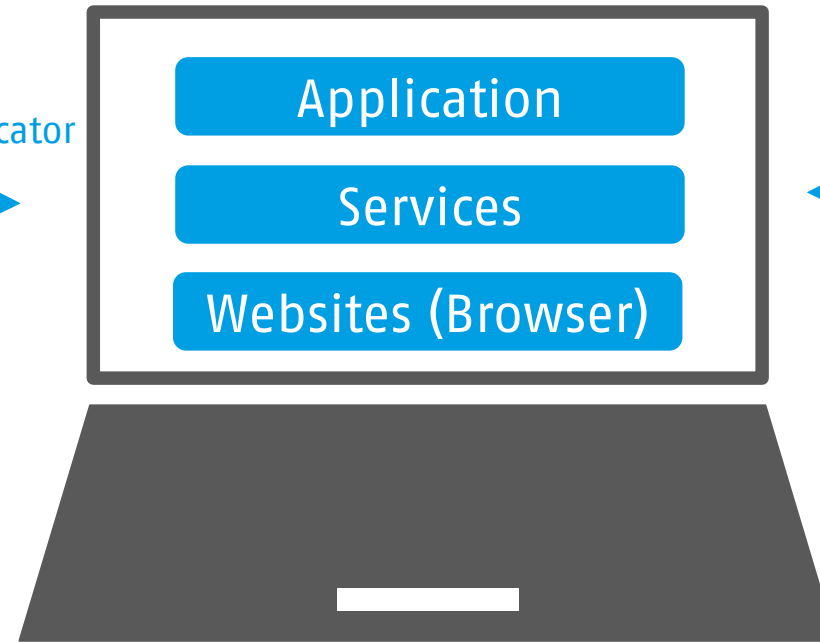


The FIDO Principle: Hardware-based Authentication

FIDO2 Hardware Authenticator



CTAP
(Client-to-Authenticator
Protocol)

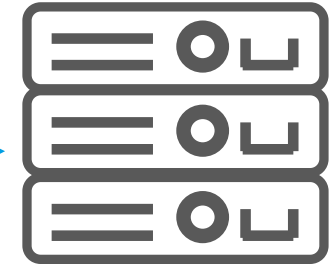


PC, Notebook or Mobile

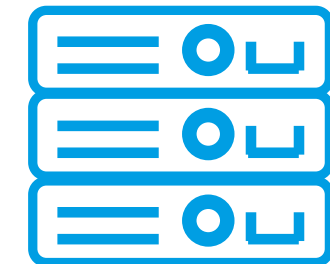


WebAuthN
Authentication

App Server /
Company Network



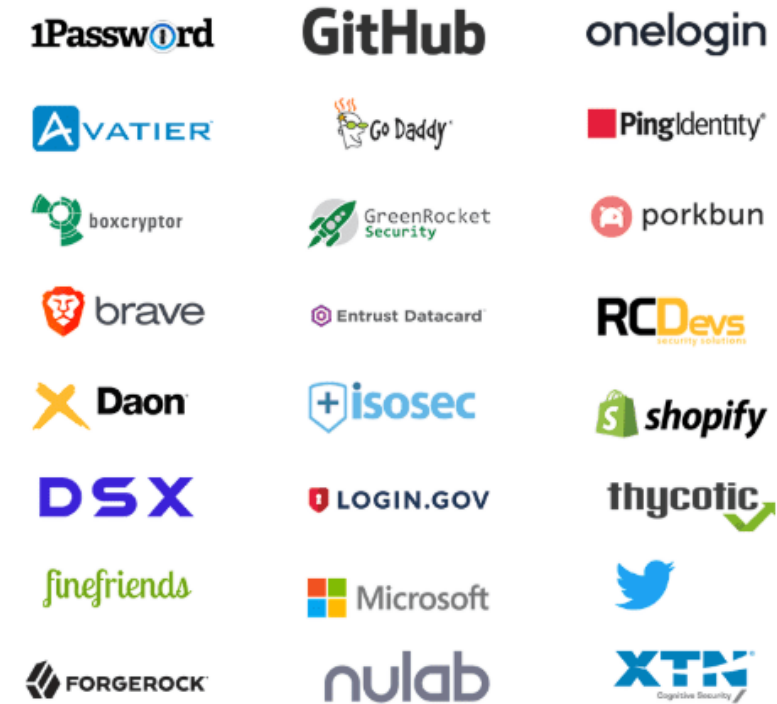
FIDO Server



U2F Services



FIDO2 Services



...and many other services.

The Benefits We Provide

swissbit®

Secure access to websites, applications and online services

Using strongest hardware-based authentication with various security options (passwordless, two-factor/ 2FA or multi-factor authentication/ MFA) replacing weak password authentication.

Future-proof solution based on open standards

AI-in-one security key works with any FIDO2 compatible websites and services including password-less sign-in to a Windows 10 desktop.

Protecting private & professional online accounts as well as user identity

AI-in-one security key protects users against online attacks, such as phishing, social engineering or account takeover, thus protecting user identity.



The Services We Provide: Custom Form Factor and Branding



Own production facility provides a trusted supply chain und unique services: We offer customization of form factors and branding as well as assembly and testing.


Made in Germany





Trusted Partner for 20 years

- Own Production & Products "Made in Germany"
- Worldwide leader of industrial storage and security solutions

Proven Security Competence

- Over 10 years of field proven security products and solutions to protect data and devices
- Trusted Supply Chain

Best Service & Support

- Custom form factor and custom branding possible
- Unique sales & worldwide technical support

About FID02 Standard



- Passwordless authentication

Strong single factor authentication using a hardware authenticator replaces weak password-based authentication.

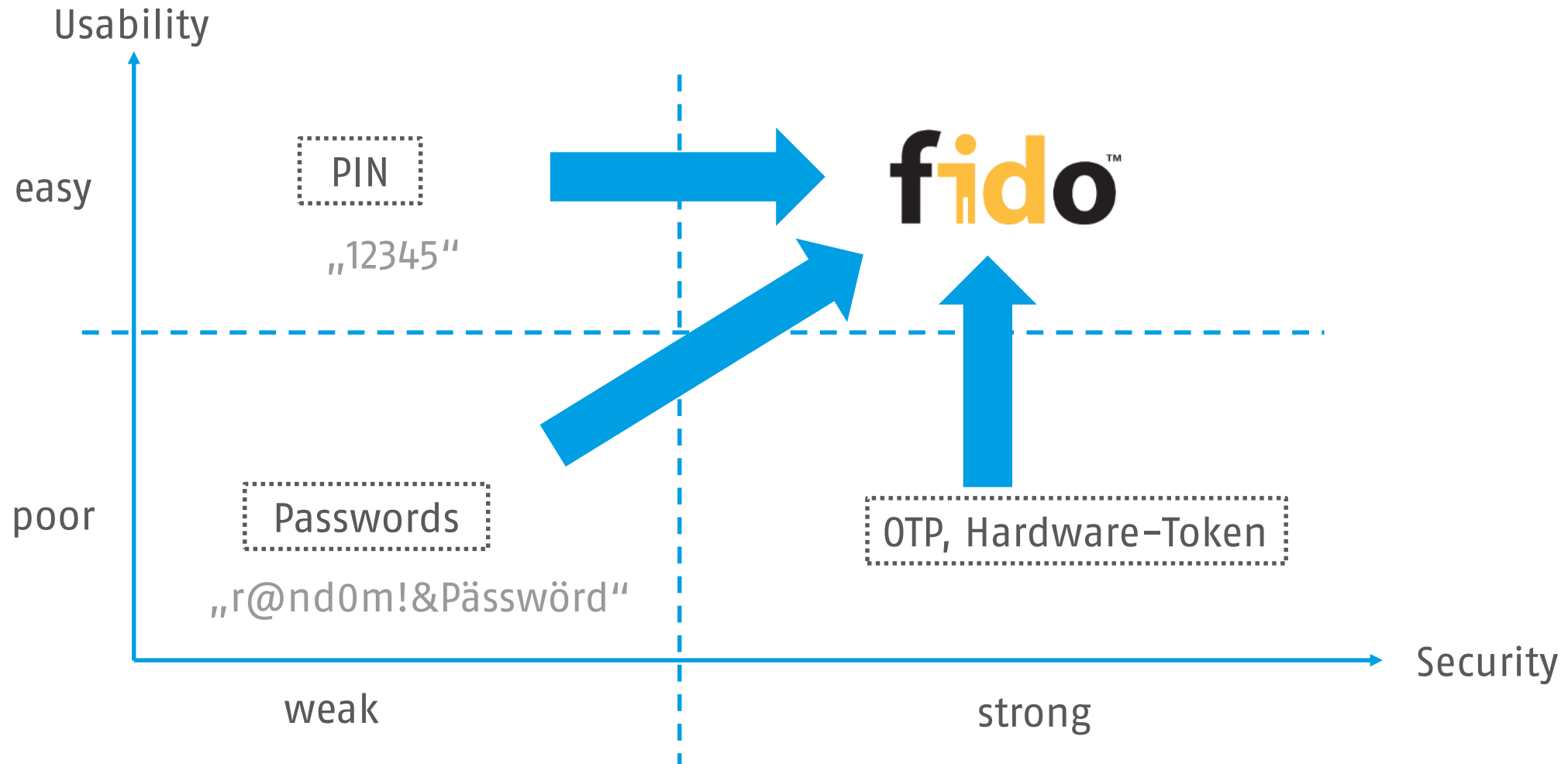
- Two-factor authentication

Strong two-factor authentication using a hardware authenticator as an extra layer of protection beyond a password

- Multi-factor authentication

Strong multi-factor authentication using a hardware authenticator and a PIN or biometric when performing critical transactions

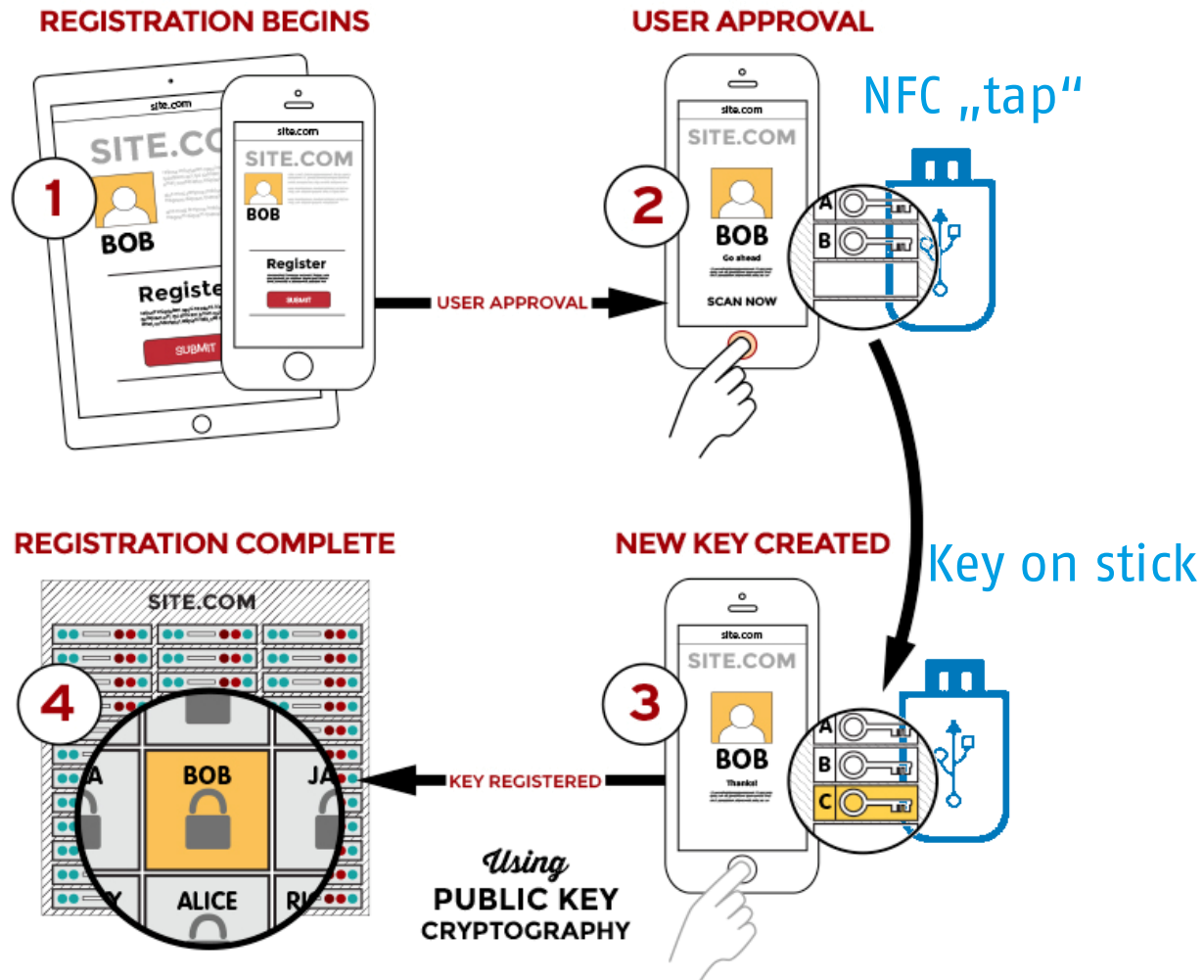
The FIDO Standard Defining The Strongest Authentication



Source / inspired by: <https://engineering.linecorp.com/en/blog/fido-at-line/>

How FIDO Works: FIDO2 Registration

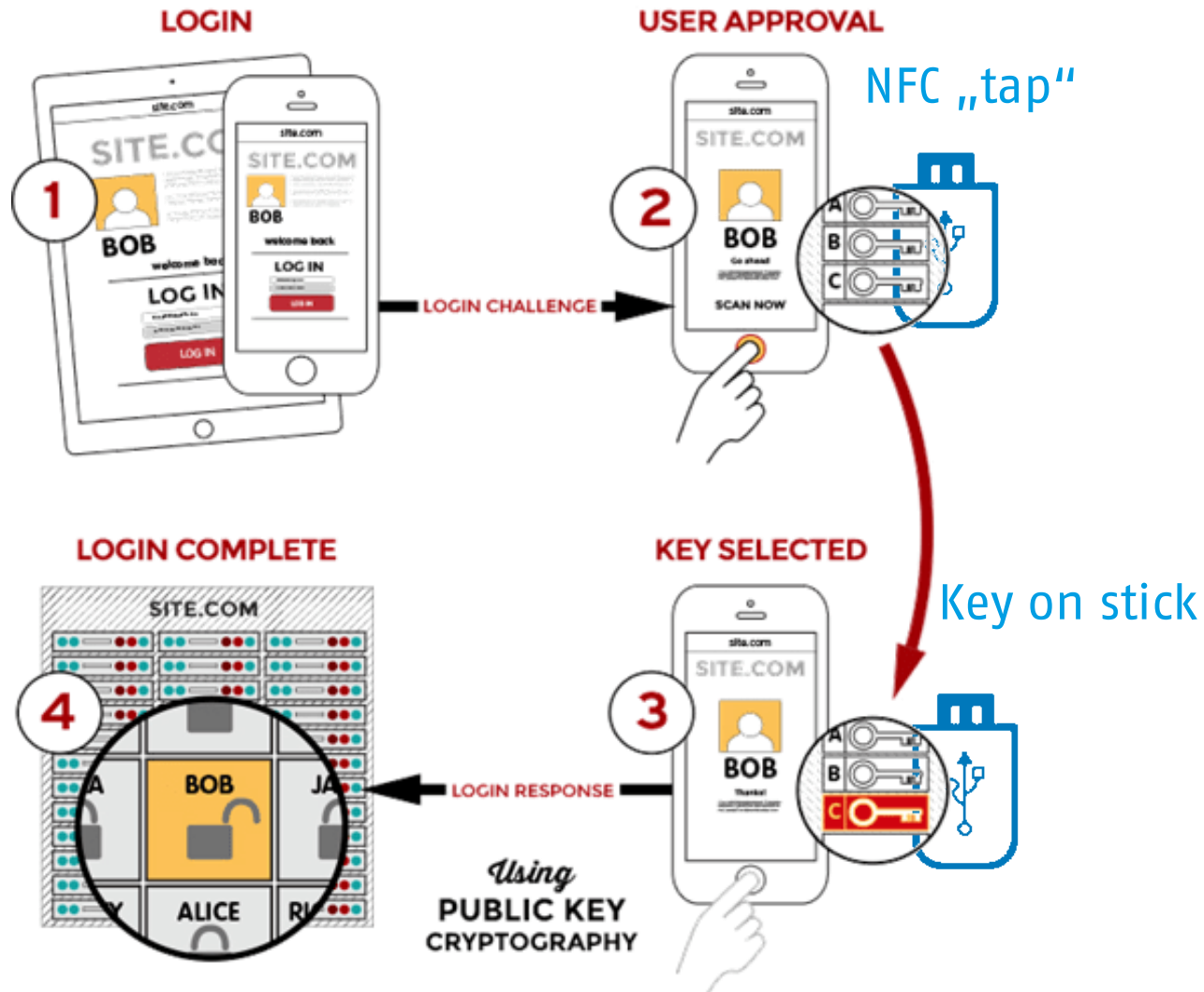
Key Registration



- User is prompted to choose an available FIDO authenticator that matches the online service's acceptance policy.
- User unlocks the FIDO authenticator using a fingerprint reader, a button on a second-factor device, securely-entered PIN or other method.
- User's device creates a new public/private key pair unique for the local device, online service and user's account.
- Public key is sent to the online service and associated with the user's account. The private key and any information about the local authentication method (such as biometric measurements or templates) never leave the local device.

Source: <https://fidoalliance.org/how-fido-works/>

How FIDO Works: FIDO2 Login



Source: <https://fidoalliance.org/how-fido-works/>

- Online service challenges the user to login with a previously registered device that matches the service's acceptance policy.
- User unlocks the FIDO authenticator using the same method as at Registration time.
- Device uses the user's account identifier provided by the service to select the correct key and sign the service's challenge.
- Client device sends the **signed challenge** back to the service, which verifies it with the stored public key and logs in the user.

<https://fido.ishield.cloud>

iShield FIDO2 Token

RegisterLogin

Advanced Settings



What is WebAuthn?

Swissbit made this site to test the functionality of their FIDO2 Sticks in the browsers Chrome, Firefox and Edge with Webauthn. To read more about WebAuthn and what it does, check out webauthn.guide for an introduction.

[Read more at webauthn.guide](https://webauthn.guide)

Use Case DRAC00N File Sharing: Increasing Secure Access & Protecting User Identity

DRACoon



&



Made in Germany

Swissbit FID02 security key provides:

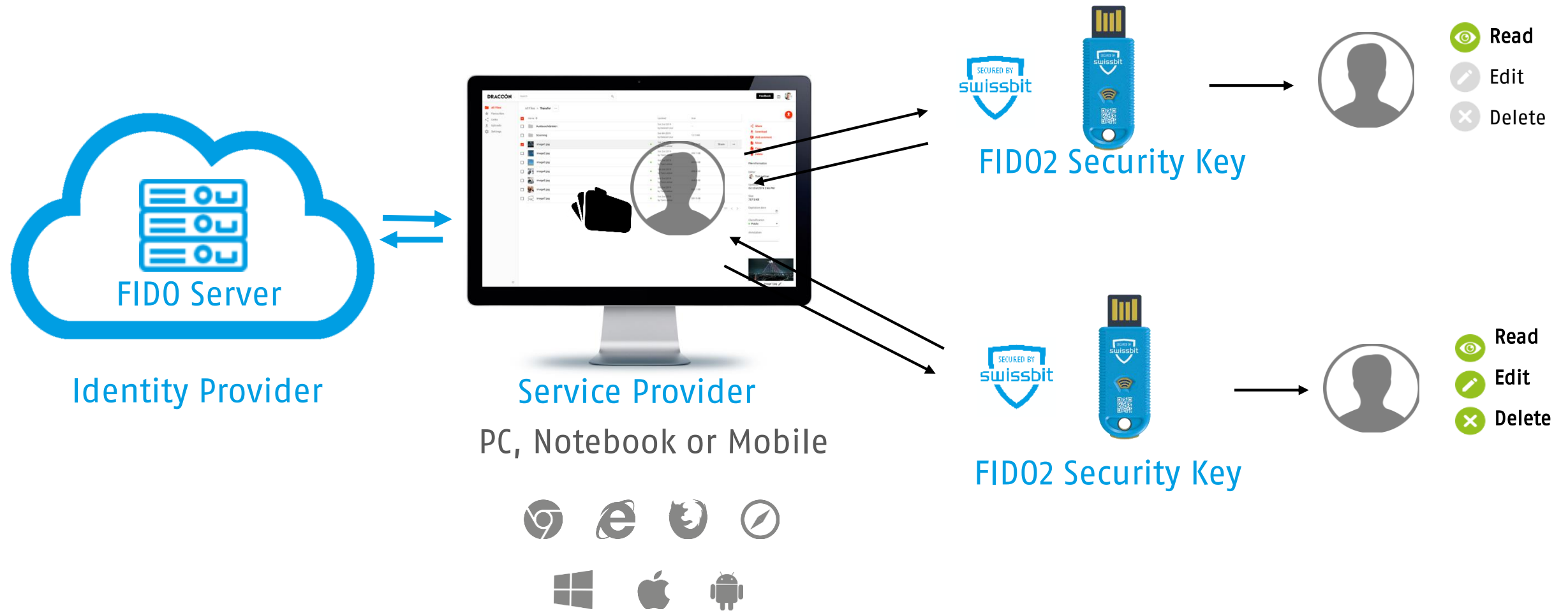
- strongest **hardware-based account and data protection** by offering additional two-factor and multi-factor authentication
- **additional protection of user identity** within a company's network

Use Case DRACoon File Sharing Service used within a company's network:

- Enhanced authentication providing easy connectivity and compatibility through USB and NFC interfaces
- Simple registration and central management of the end devices directly via the DRACoon web interface
- Assignment of a classification (protection requirement classes – high to secret) to users & end devices (context-based access)

Efficient Management of Connected Devices

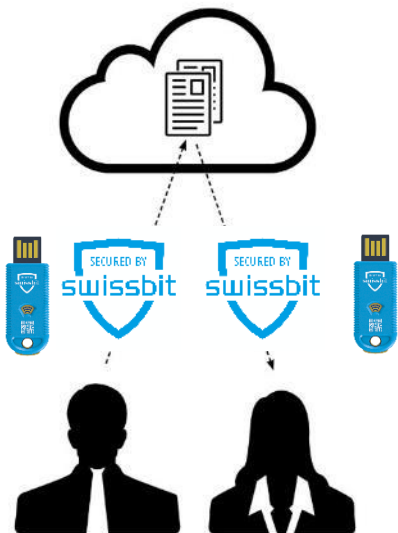
swissbit®



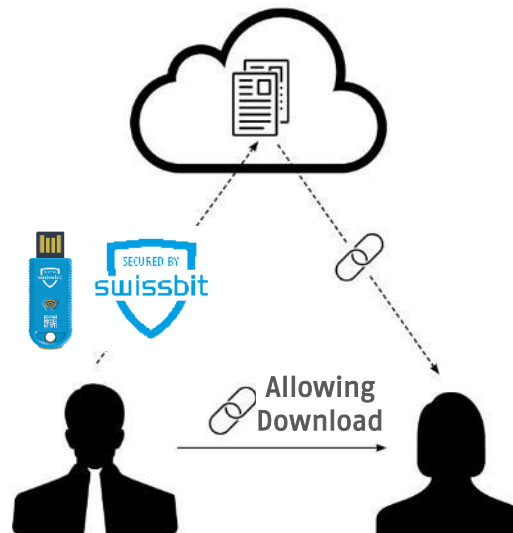
Highly Secure File Sharing Between Users



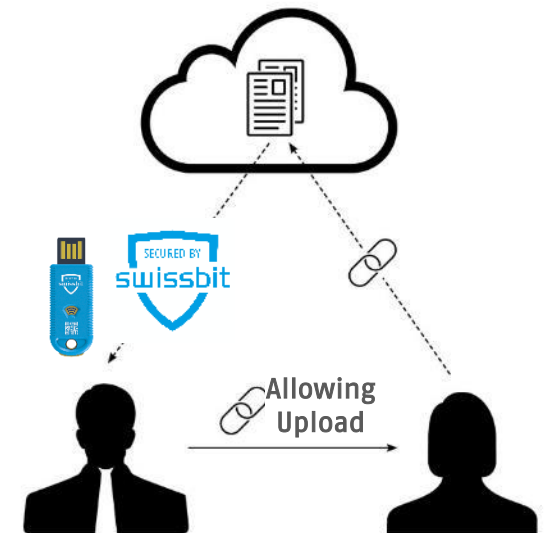
File Sharing
between DRACOON Users



Allowing Download
between DRACOON User
and External User



Allowing Upload
between DRACOON User
and External User



Intelligent User Management & Access Policy



Config Manager
Global Configuration
User and Security Keys
&



Assuring hardware-
based User Identity



User Manager
User & Device
Management



Group Manager
Group Management



Room Manager
Management
Data Rooms
&



Assuring hardware-
based User Identity



Log Auditor
Access to audit log
&
Reporting Security Key
Clients

Role	 Admin Data Room Admin for Data Room	 User Data Room Typical User	 Gets Link Temporary User
Rights and user management within the data rooms	✓		
Secure private room functions	✓		
Uploading, deleting and sending data	✓	✓	
Using download and upload links	✓	✓	✓
Reporting end devices	✓		

Swissbit Security

Protecting Data and Devices in the IoT

