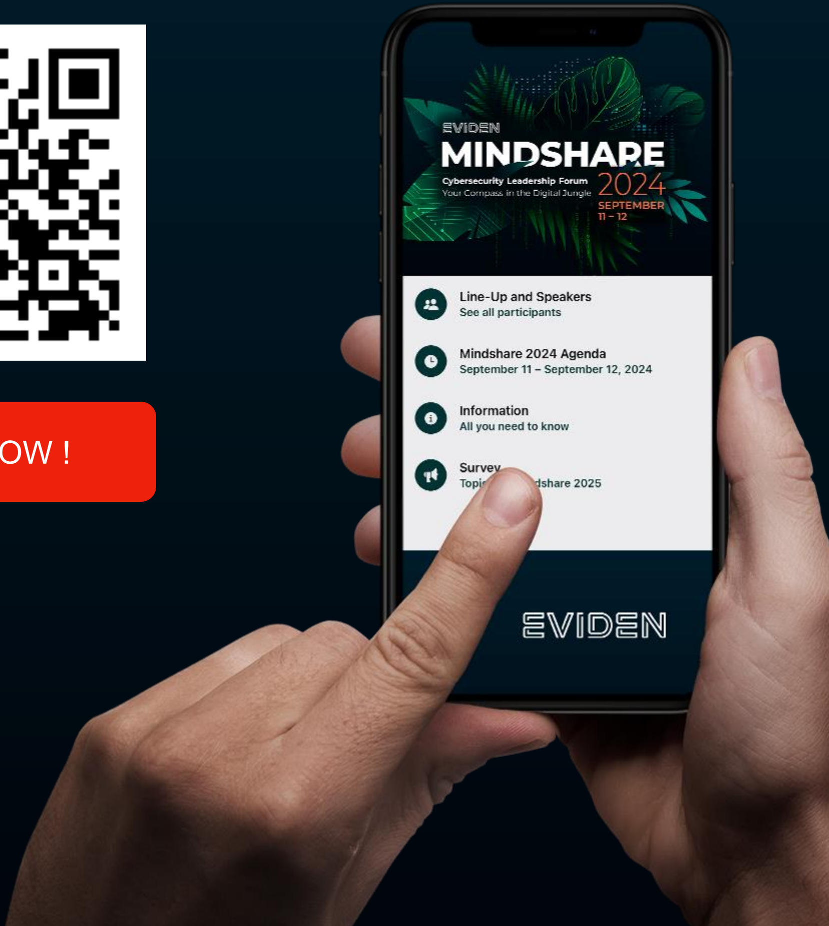
MINDSHARE 2024
AGENDA

SCAN NOW !



EVIDEN

MINDSHARE

Cybersecurity Leadership Forum

Your Compass in the Digital Jungle

2024

SEPTEMBER
11 – 12

Line-Up and Speakers
See all participants

Mindshare 2024 Agenda
September 11 – September 12, 2024

Information
All you need to know

Survey
Topi dshare 2025

EVIDEN

EVIDEN DirX

EVIDEN
MINDSHARE
2024

How to secure your confidential communication and important assets using

Multi Factor Authentication - MFA

Ralf Knöringer, Vahid Asadi - EVIDEN

Phishing is a major threat vector

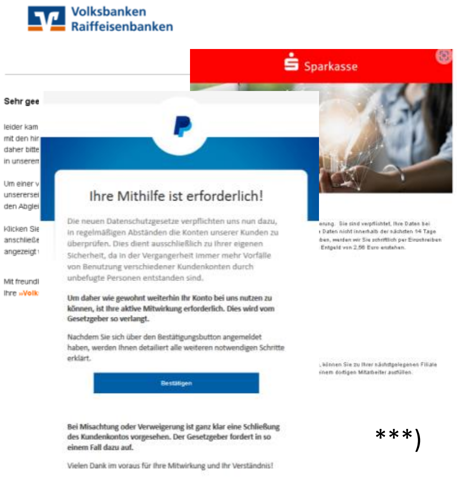
Fake emails or messenger messages lure the recipient to a fraudulent website. There users are asked to enter secret information, which ends up in the hands of the attacker.

Colonial Pipeline >3 Mrd. $US

Phishing & Ransomware attack
Shut down of fuel delivery US Eastcoast for a week in May 2021 *)

New trend in Europe

“please check your credentials because due to DSGVO/GDPR !” 😈



Sehr gee

leider kam
mit den hin
daher bitte
in unserem

Um einer v
unserersei
den Abglei

Klicken Sie
anschließe
angezeigt

Mit freundl
Ihre »Volk

Ihre Mithilfe ist erforderlich!

Die neuen Datenschutzgesetze verpflichten uns nun dazu, in regelmäßigen Abständen die Konten unserer Kunden zu überprüfen. Dies dient ausschließlich zu Ihrer eigenen Sicherheit, da in der Vergangerheit immer mehr Vorfälle von Benutzung verschiedener Kundenkonten durch unbefugte Personen entstanden sind.

Um daher wie gewohnt weiterhin Ihr Konto bei uns nutzen zu können, ist Ihre aktive Mitwirkung erforderlich. Dies wird vom Gesetzgeber so verlangt.

Nachdem Sie sich über den Bestätigungsbutton angemeldet haben, werden Ihnen detailiert alle weiteren notwendigen Schritte erklärt.

Bei Misachtung oder Verweigerung ist ganz klar eine Schließung des Kundenkontos vorgesehen. Der Gesetzgeber fordert in so einem Fall dazu auf.

Vielen Dank im voraus für Ihre Mitwirkung und Ihr Verständnis!

enung. Sie sind verpflichtet, Ihre Daten bei
Daten nicht innerhalb der nächsten 14 Tage
ben, werden wir Sie schriftlich per Einschreiben
Entgeld von 2,56 Euro enstehen.

, können Sie zu Ihrer nächstgelegenen Filiale
inem dortigen Mitarbeiter ausfüllen.

***)

Some Statistics

- Phishing is the most common form of cyber crime, with an estimated 3.4 billion spam emails sent every day
- Google alone blocks around 100 million phishing emails every day.
- Millennials and Gen-Z internet users (18-40 year olds) are most likely to fall victim to phishing attacks **)

*) www.itgovernance.eu, **) www.aag-it.com/the-latest-phishing-statistics, ***) www.bsi.bund.de

Phishing is a major threat vector

Colonial Pipeline >3 Mrd. $US

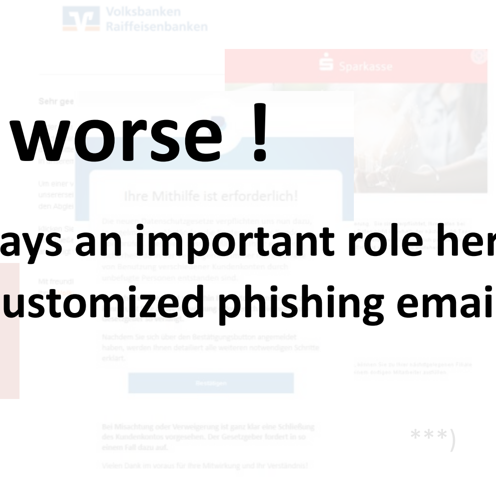
Phishing & Ransomware attack
Shut down of fuel delivery US East Coast for a week
in May 2021 *)

and it’s getting worse !

Artificial intelligence (AI) plays an important role here and enables attackers to create hundreds of thousands of customized phishing emails and fake websites within a very short space of time.

New trend in Europe

“please check your credentials
because due to DSGVO / GDPR”


Volksbanken Raiffeisenbanken

Sparkasse

Sehr gee

Ihre Mithilfe ist erforderlich!

Die neuen Datenschutzgesetze verpflichten uns nun dazu,

von Benutzung verschiedener Kundenkonten durch unbefugte Personen entstanden sind.

Gesetzgeber so verlangt.

Nachdem Sie sich über den Bestätigungsbutton angemeldet haben, werden Ihnen detailiert alle weiteren notwendigen Schritte erklärt.

Bestätigen

Bei Missachtung oder Verweigerung ist ganz klar eine Schließung des Kundenkontos vorgesehen. Der Gesetzgeber fordert in so einem Fall dazu auf.

Vielen Dank im voraus für Ihre Mitwirkung und Ihr Verständnis!

***)

Some Statistics

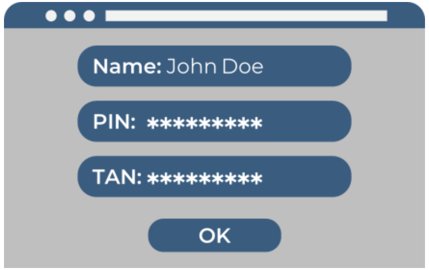
- Phishing is the most common form of cyber crime, with an estimated 3.4 billion spam emails sent every day
- Google alone blocks around 100 million phishing emails every day.
- Millennials and Gen-Z internet users (18-40 years olds) are most likely to fall victim to phishing attacks **)

*) www.itgovernance.eu, **) www.aag-it.com/the-latest-phishing-statistics, ***) www.bsi.bund.de

Good News - Multi Factor Authentication

Multi-factor authentication (MFA) is a proven concept that makes authentication more secure. Basic MFA requires the use of at least two independent methods of authentication.

A traditional method combines the password with a transaction number that is only used once

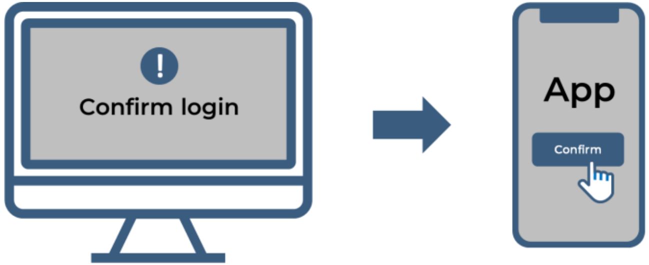


Name: John Doe

PIN: *********

TAN: *********

Alternatively, a smartphone app can send a push notification requesting confirmation from the user



Transaction number sent to smart phone

User confirms login

Bad News – Attacker in the Middle

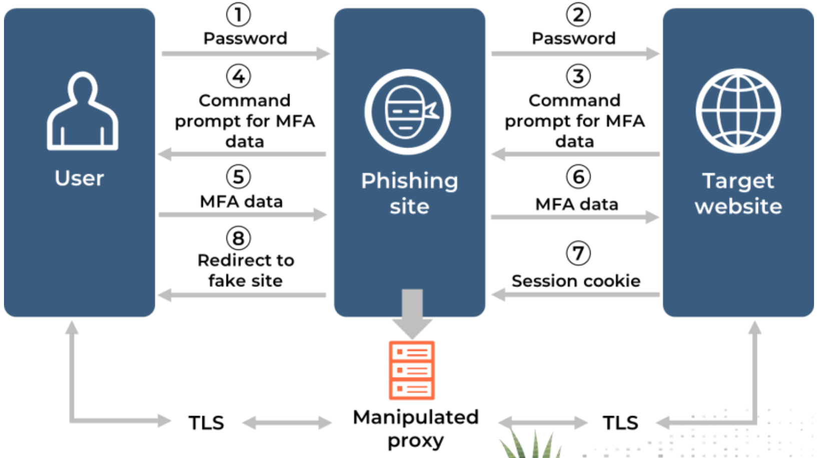
AitM phishing based on a proxy server is now widespread and an integral part of many phishing toolkits.

Using this technique, an attacker can tap into any information that the user enters as part of a phishing attack.

+ In theory users could expose the false identity of the proxy server by checking the site certificate, but

– Normal users are missing the technical know-how

– This reduces the acceptance of the MFA due to reduced convenience



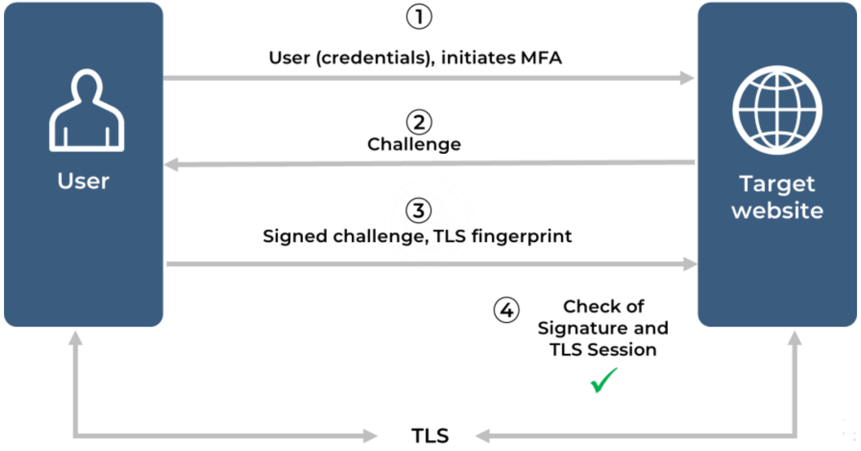
The solution –
Phishing-proof MFA through private signature keys

1 User request access to web site or resource..

2 challenge containing a random number, the current time and the server's URL

3 Client digital signature bound to PIN or biometric information. Challenge bound to session.

4 The server checks the signature. If it is correct and matches the TLS connection, authentication is successful.


User
Target website
① User (credentials), initiates MFA
② Challenge
③ Signed challenge, TLS fingerprint
④ Check of Signature and TLS Session ✓
TLS

The solution –
Phishing-proof MFA through private signature keys

1 2 User enters credentials, forwarded by Proxy

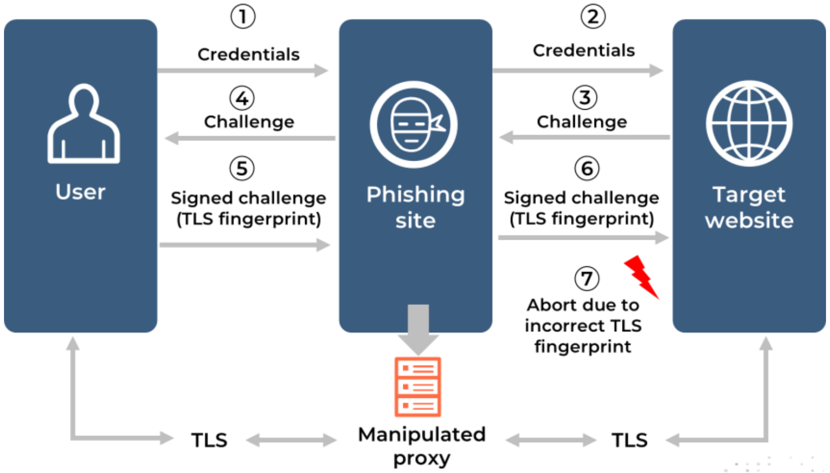
3 4 challenge containing a random number, the current time and the server's URL

Phishing Site re-sends challenge

5 6 Client signature bound to PIN or biometric information. Challenge bound to session.

Phishing site re-sends signed challenge

7 **Target Web Site checks the signed challenge. TLS session is changed – ABORT !**


User
① Credentials
④ Challenge
⑤ Signed challenge (TLS fingerprint)
Phishing site
② Credentials
③ Challenge
⑥ Signed challenge (TLS fingerprint)
⑦ Abort due to incorrect TLS fingerprint
Target website
TLS
Manipulated proxy
TLS

The associated public signature keys must be trustworthy !!!

Most secure technologies – PKI and FIDO2

- Both certificates and FIDO2 are suitable for achieving the highest Authenticator Assurance Level 3 (AAL3) and the Authentication Level of Assurance 4 (LoA4) (enables eIDAS Identity Assurance HIGH)

But what are the differentiators ?

- The **centralized** nature of **PKI** allows any service that trusts given PKI infrastructure to authenticate users through the corresponding certificate.
- Implementing a PKI infrastructure also empowers end-users to utilize certificates for secure connection setup, digital signatures, and other cryptographic functions.
- Smartcards/PKI-Tokens are **usually company-owned** and distributed to employees.

- **FIDO** credentials are **designed specific to a single service**. Combined with an identity providers with single sign-on capabilities, the FIDO approach closely resembles the centralized one of PKI.
- The principle of FIDO is to separate the user authentication process from the technical protocol between server and client.
- FIDO allows for a Bring Your Own Device approach without compromising security

FIDO = Fast Identity Online

Eviden – Your One-Stop Shop for Security

DirX Identity
Management,
Governance &
Compliance

CardOS Secure ID
Smart Cards & Tokens

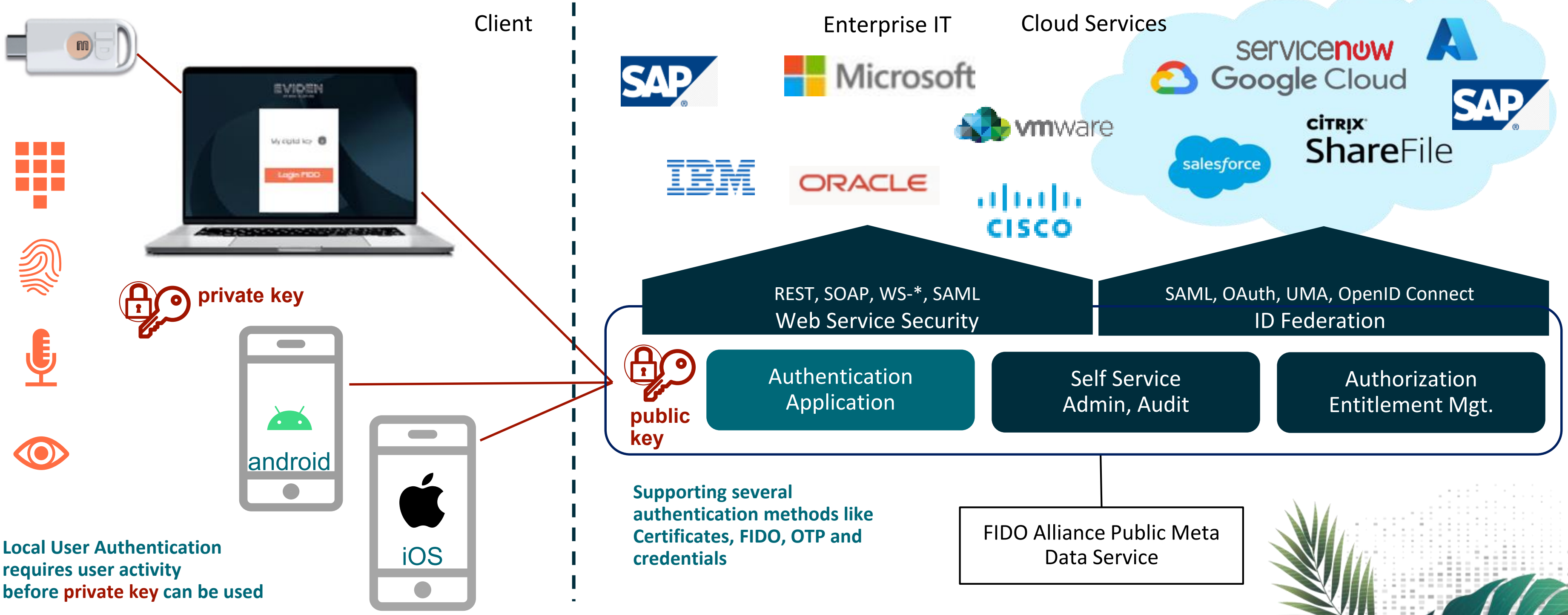
DirX Access
Management,
Single-Sign-On &
Federation

Cryptovision Greenshield
Email (S/MIME) & Document
Encryption

Live Demo – CardOS FIDO2 Token in DirX Identity Mgt. and SSO Infrastructure

FIDO2 Credentials on CardOS Security Token

FIDO2 Architecture with SSO IDP / DirX Identity & Access Management



Local User Authentication requires user activity before private key can be used

Supporting several authentication methods like Certificates, FIDO, OTP and credentials

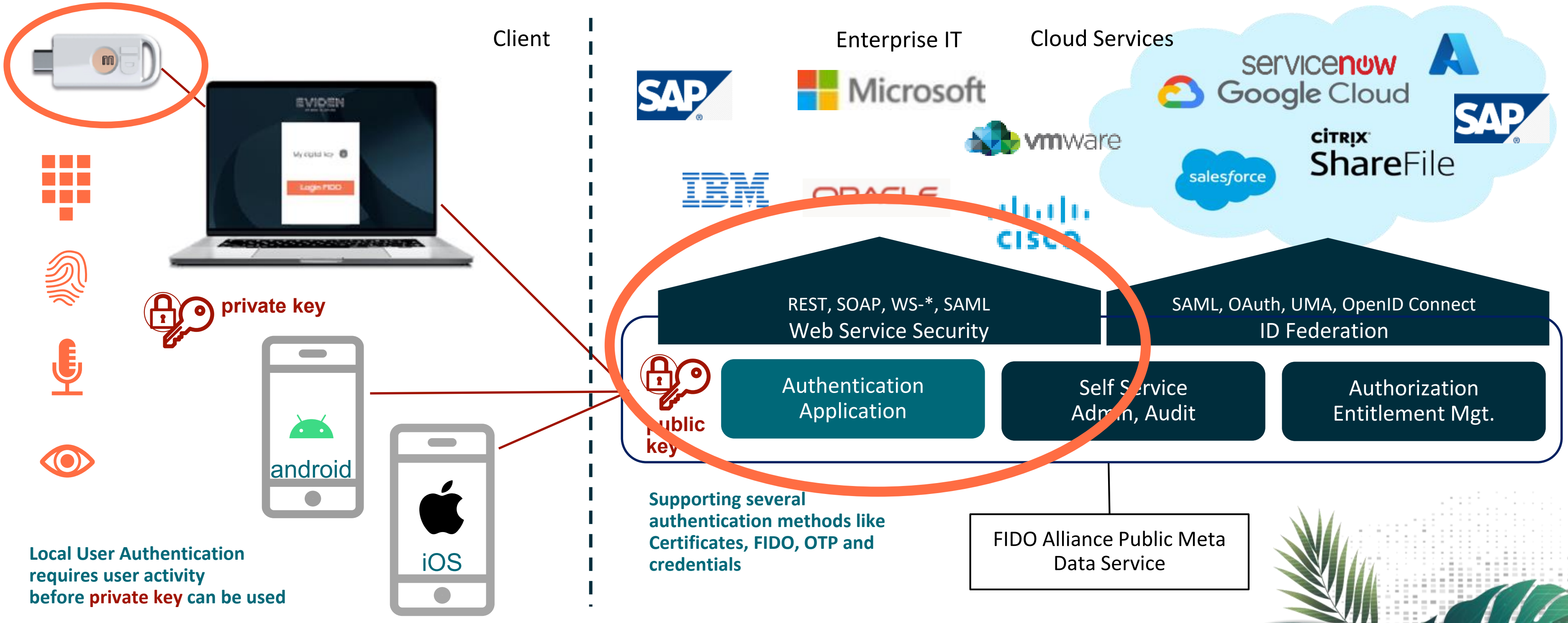
MINDSHARE
Cybersecurity Leadership Forum
Your Compass in the Digital Jungle 2024

Live Demo – CardOS FIDO2 Token in DirX Identity Mgt. and SSO Infrastructure

EVIDEN

FIDO2 Credentials on CardOS Security Token

FIDO2 Architecture with SSO IDP / DirX Identity & Access Management



Local User Authentication requires user activity before private key can be used

Supporting several authentication methods like Certificates, FIDO, OTP and credentials

FIDO Authentication

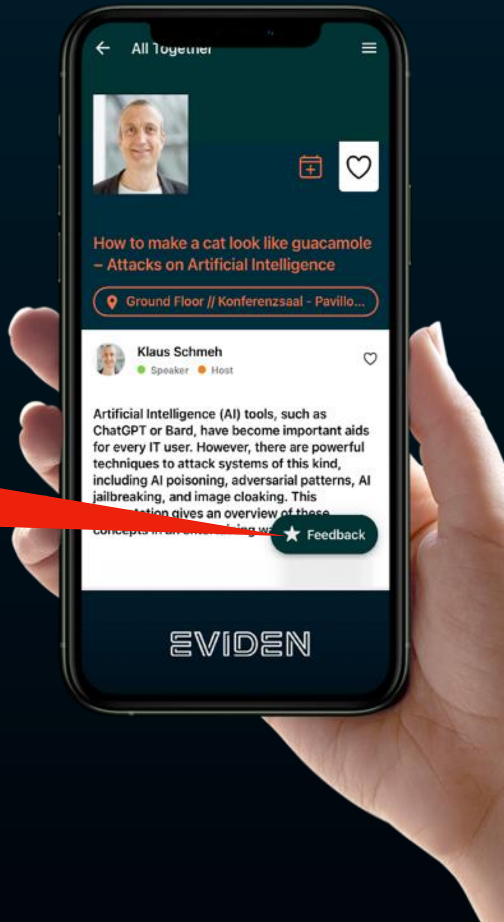
Registration and Authentication Process

- FIDO Registration
  - User is already in IAM and able to login with user and password
  - User registers FIDO token via DirX authentication application
- FIDO Authentication
  - User login to My Company website with user and password
  - User wants to access financial management
  - DirX Access requests the user to step up to FIDO authentication

Questions?

TAKE A MINUTE AND GIVE US FEEDBACK ...

RATE NOW!



How to make a cat look like guacamole – Attacks on Artificial Intelligence

Ground Floor // Konferenzsaal - Pavillo...

Klaus Schmeh
● Speaker ● Host

Artificial Intelligence (AI) tools, such as ChatGPT or Bard, have become important aids for every IT user. However, there are powerful techniques to attack systems of this kind, including AI poisoning, adversarial patterns, AI jailbreaking, and image cloaking. This [illegible]tation gives an overview of these concepts in an [illegible]ing wa