The Ultimate Protection against Phishing Attacks

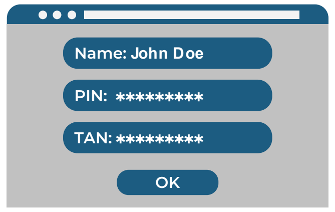
The limits of multi-factor authentication and effective measures

Over 90% of all cyber-attacks start with a phishing email

A phishing attack usually begins with a fake email or messenger message that lures the recipient to a fraudulent website. There they are asked to enter their username, password and possibly other secret information, which ends up in the hands of the attacker.

The probability of success of such an attack increases if the message appears to come from a known provider or work colleague. In recent years, the IT world has seen an alarming rise in phishing attacks, making this technique one of the most significant forms of cybercrime. According to Forbes, this method caused over $500 million in damage in 2022 alone.[1] CNBC also reports a 61% increase in phishing attacks between May and October 2022 compared to the previous year.[2] Over 90% of all cyberattacks begin with a phishing email.

Of the many thousands of phishing messages sent by an attacker, often only one is successful – but that can be enough for an effective attack. Tools have long been available to automate phishing, with "phishing as a service" also being offered on the market. Artificial intelligence (AI) plays an important role here and enables attackers to create hundreds of thousands of customised phishing emails and fake websites within a very short space of time.



Name: John Doe

PIN: *********

TAN: *********

OK

Figure 1: Multi-factor authentication requires at least two independent methods to be used together for authentication, for example PIN and TAN.

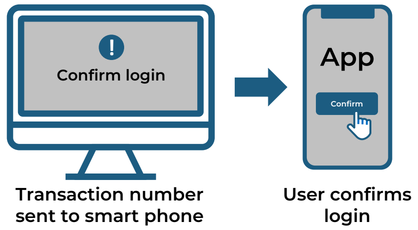


Figure 2: One of the factors in multi-factor authentication can be a transaction number that the user has to take from a smartphone app.

Multi-factor authentication does not necessarily protect against phishing

Multi-factor authentication (MFA) is a proven concept that makes authentication more secure. MFA requires the use of at least two independent methods of authentication. Security policies often require the use of MFA, but usually the exact requirements are not defined, although there are significant differences between the different MFA variants.

Not sufficient: Basic MFA: OTP/TAN, mobile app push notification

A traditional method combines the password with a transaction number that is only used once (OTP/TAN). (Figure 1). The transaction number is sent to the user by SMS or e-mail or generated on the user's device (authenticator). The user then enters it in the login screen in addition to the password. Alternatively, a smartphone app can send a push notification requesting confirmation from the user (Figure 2).

However, attackers have adapted to this and are now using "Attacker in the Middle" phishing (AitM phishing) based on a proxy server (Figure 3). AitM phishing 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. The attacker can immediately replay this information on the target website, gaining authentication in place of the victim. Even though the OTP expires every 30 seconds, this provides sufficient time to execute the AitM replay attack. Although a trained user could expose the false identity of the proxy server by checking the certificate, this will rarely happen in practice as few users have the necessary know-how and are willing to accept the associated loss of convenience.

Only signature-based MFA protects against phishing

MFA can only protect against phishing if at least one factor of authentication is based on secret information that is not sent over the network. This is the case if a private key is used that is securely stored and not disclosed but is used to create a digital signature. There are essentially two proven technologies that incorporate signature-based MFA: Authentication based on electronic certificates („Certificate Based Authentication") and FIDO authentication („Fast IDentity Online").

Phishing-proof MFA through private signature keys

Authentication based on digital signatures is an effective measure against phishing, as no secret information is sent over the network. Authentication with digital signatures works as follows (Figure 4):

1. The server sends a request to the client containing a random number, the current time and the server's URL.
2. The client uses its private key locally to create a digital signature. The private key is protected by another factor, such as a PIN or biometric information (fingerprint or facial recognition). The client signs the request from the server and sends it back to the server as a response. The signed challenge is bound to the TLS connection and is therefore only valid on this connection. A phishing attacker, who has to establish a separate TLS connection to the server, cannot do anything with it.
3. The server checks the signature. If it is correct and matches the TLS connection, authentication is successful.

[1] https://www.forbes.com/advisor/business/phishing-statistics/

[2] https://www.cnbc.com/2023/01/07/phishing-attacks-are-increasing-and-getting-more-sophisticated.html

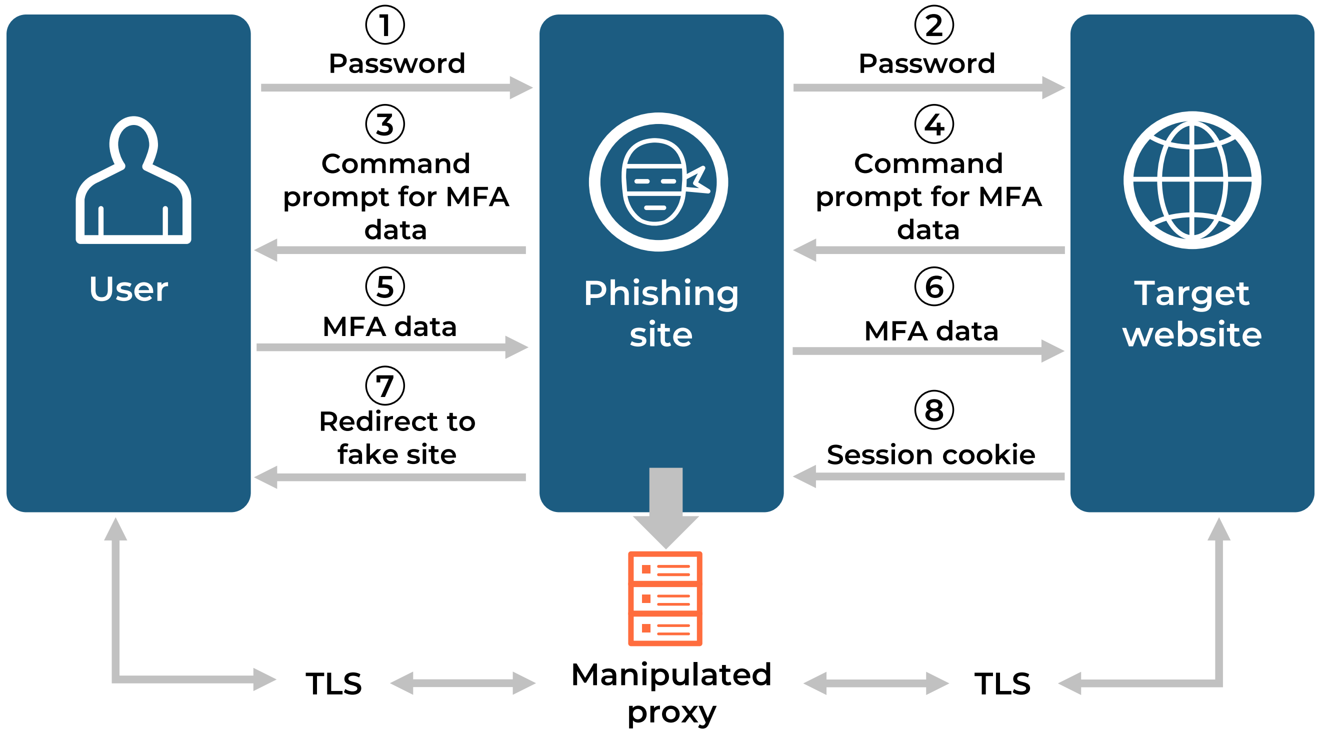


Figure 3: An attacker successfully authenticates to a target website via "Attacker in the Middle" phishing with replay of information on both sides.

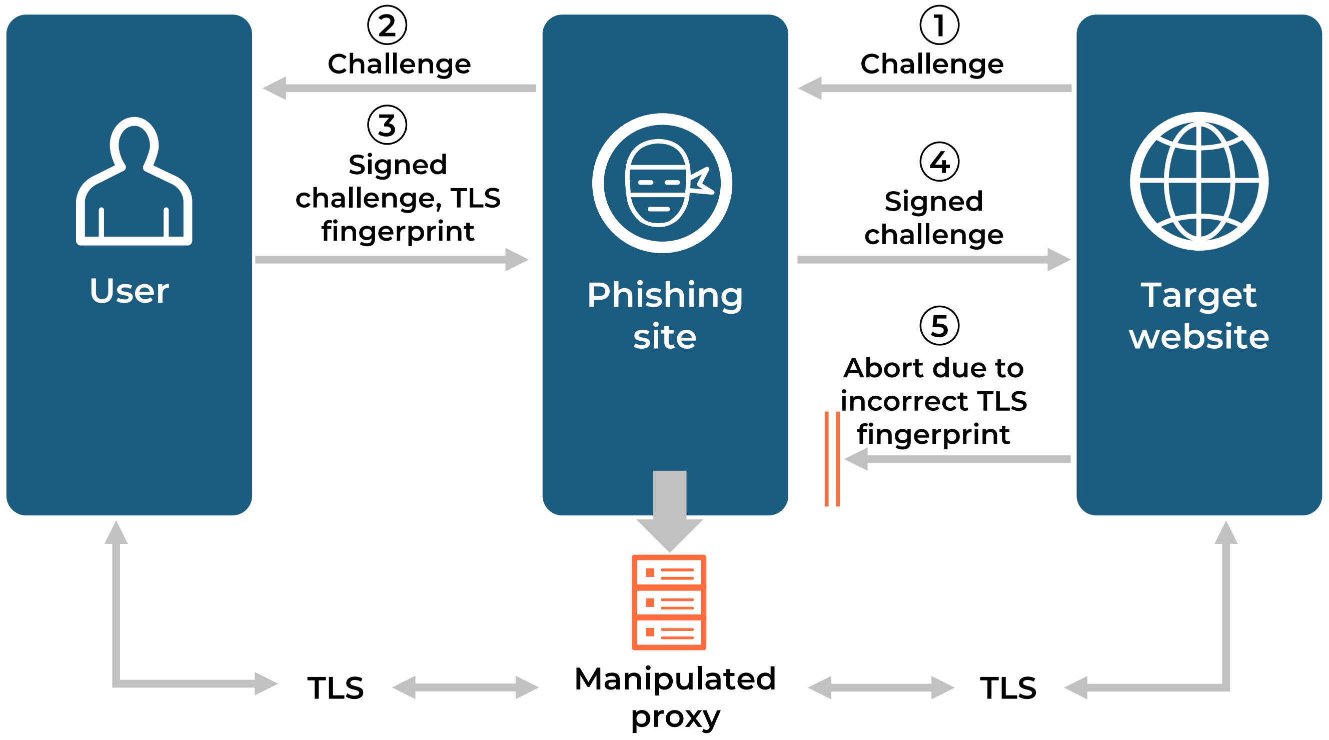


Figure 4: Phishing-proof MFA protects from "Attacker in the Middle" attacks.

Phishing-proof MFA authentication

Certificate-based authentication

- ✓ Not based on passwords
- ! Requires public key infrastructure
- ✓ Digital certificates (signed by certification authority) ensure authenticity
- ✓ Supported by numerous operating systems, browsers and other components
- ✓ Centralised revocation of digital certificates possible
- ✓ Can be used for email and file encryption
- ✓ Can also be used for trusted digital signatures
- ✓ Centralized management
- ✓ Different smartcard form factors supported
- ✓ Key recovery possible

FIDO authentication

- ✓ Not based on passwords
- ! Requires out-of-band trust relationship
- ✗ Separate key pairs for each communication partner
- ✗ No central blocking of public keys
- ✗ Cannot be used for email and file encryption
- ✗ Cannot be used for trusted digital signatures
- ✗ No centralised management
- ✓ Different smartcard form factors supported
- ✗ No key recovery possible

For an MFA to work with private signature keys, the associated public signature keys must be trustworthy. There are two approaches for this purpose: On the one hand, digital certificates and a public key infrastructure (PKI) can be used. On the other hand, the FIDO framework can be used. The advantages and disadvantages of both variants are described in the table above.

Both certificates and FIDO are suitable for achieving the highest Authenticator Assurance Level 3 (AAL3), which is defined in the NIST SP 800-63 Digital Identity Guidelines, and the Authentication Level of Assurance 4 (LoA4), which is defined in the ISO/IEC 29115 standard that enables eIDAS Identity Assurance HIGH.

High security is affordable and uncomplicated

Certificate-based authentication used to be seen as an expensive solution that was mainly used by authorities with high security requirements and in the defence sector. However, this view is now outdated.[3] Eviden offers a subscription-based PKI that requires little initial investment. Automation tools for issuing, renewing and managing certificates have reduced the need for specialised staff and lowered operating costs. Eviden Virtual Smartcards can utilise the Trusted Platform Module (TPM) found in laptops to protect private keys, eliminating the need to purchase smartcards or tokens.

Multi-factor authentication can pay for itself in the first year. One of the reasons for this is that users save time by not having to memorise passwords: Research shows that the financial burden of password management is significant. Forrester Research has determined that each password reset costs 70 dollars.[4]

The IT department also benefits from passwordless multi-factor authentication, as the number of helpdesk calls due to forgotten or blocked passwords is reduced. Digital certificates also offer other advantages. In particular, they can be used for digital signing, a technology that streamlines workflows by eliminating the need for physical document handling. Implementing digital signatures can assist organizations in meeting process and regulatory requirements.

[3] https://www.bbc.com/worklife/article/20161219-tech-issues-kill-productivity-but-dont-rush-to-call-it

[4] https://www.forbes.com/sites/forbestechcouncil/2023/03/23/embracing-the-end-of-the-password-here-and-now/

Solutions from Eviden Digital Identity

Eviden is an international company specialising in the digital, cloud, big data and security sectors. As a global leader in data-driven, trusted and sustainable digital transformation, Eviden is a pioneer of the next generation of digital enterprises. The company holds global leadership positions in digital, cloud, data, advanced computing and security.

Eviden Digital Identity offers comprehensive solutions for securing electronic identities with cryptographic technologies and applications.

Phishing-proof MFA authentication from Eviden

Eviden Digital Identity offers a portfolio of solutions for phishing-proof MFA authentication. The customer has a variety of options for integrating these solutions into the existing IT environment.

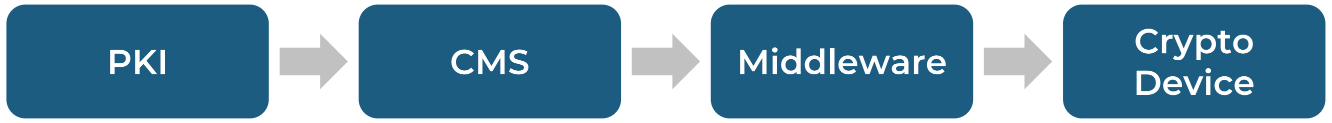


Figure 5: The certificates used for MFA are linked to the cryptographic components using middleware and, if required, a credential management system.

If the customer decides in favor of MFA authentication with digital certificates, an existing PKI can be used. Alternatively, a new PKI can be set up with little effort using IDnomic PKI from Eviden. IDnomic PKI is available as an „on premise“ solution or the customer can use a sovereign cloud-based „software as a service“ model. The certificates are linked to the cryptographic components using middleware and, if required, a credential management system (Figure 5). Depending on the requirements, existing solutions can also be used here. Eviden offers several tried and tested products for this purpose, including the cryptovision SCinterface smartcard middleware and the IDnomic CMS credential management system.

The cryptographic keys required for a public key infrastructure are stored in protected hardware, such as a smartcard. The cryptovision SCinterface VSC middleware also enables the Trusted Platform Module (TPM) in every endpoint to be used for key storage and thus as a virtual smartcard.

For customers who want to use smart cards, the tried-and-tested CardOS product from Eviden is a very secure option with a security chip and smart card operating system designed and certified in the EU. It is available in two form factors: a token with USB and NFC interface and a traditional smart card with contact and NFC interface. CardOS not only supports PKI functions, but can also handle FIDO keys and is certified for this purpose. This means that phishing-proof MFA authentication in the FIDO variant is also possible with CardOS. The two approaches can also be combined: For example, the customer can use certificate-based authentication for resources within the company and also has the option of using FIDO to access systems outside the scope of their own PKI.

Prevent phishing emails with S/MIME

As the majority of phishing attacks are carried out via email, signed emails are becoming increasingly important as a security measure in companies. The format commonly used for this is S/MIME. The signature ensures the integrity of the email and the identity of the sender.

With cryptovision GreenShield, Eviden offers a comprehensive solution for secure and trustworthy e-mail communication. Detailed information on this can be found online.[5]

[5] https://www.cryptovision.com/en/products/security-applications/greenshield/

Would you like to find out more about our services? Please contact us:

cv-info@eviden.com

www.cryptovision.com

Our advisory team will be happy to get in touch with you.

Eviden
cv cryptovision GmbH
Munscheidstr. 14
45886 Gelsenkirchen
Germany
Tel: +49 (0) 2 09 / 1 67 – 24 50
Fax: +49 (0) 2 09 / 1 67 – 24 61

About Eviden[1]

Eviden is a next-gen technology leader in data-driven, trusted and sustainable digital transformation with a strong portfolio of patented technologies. With worldwide leading positions in advanced computing, security, AI, cloud and digital platforms, it provides deep expertise for all industries in more than 47 countries. Bringing together 53,000 world-class talents, Eviden expands the possibilities of data and technology across the digital continuum, now and for generations to come. Eviden is an Atos Group company with an annual revenue of c. € 5 billion.

About Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high-performance computing, the Group provides tailored end-to-end solutions for all industries in 69 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

[1] Eviden business is operated through the following brands: AppCentrica, ATHEA, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Visual BI, Worldgrid, X-Perion. Eviden is a registered trademark. © Eviden SAS, 2023.

eviden.com

20240730