cpl.thalesgroup.com

THALES

A Comprehensive Guide to Authentication Technologies and Methods

White Paper

Contents

Introduction – On Digital Identities and Authentication

NIST SP 800-63 defines that "digital authentication establishes that a subject attempting to access a digital service is in control of one or more valid authenticators associated with that subject's digital identity." For services in which return visits are applicable, successfully authenticating provides reasonable risk-based assurances that the subject accessing the service today is the same as that which accessed the service previously.

Digital identity presents a technical challenge because this process often involves proofing individuals over an open network, and always involves the authentication of individual subjects over an open network to access digital services. The processes and technologies to establish and use digital identities offer multiple opportunities for impersonation and other attacks.

There is an increased interest on strong user authentication, as more and more regulations, such as GDPR, the European Payment Directive (PSD2), and standards, such as PCI DSS, oblige strict security requirements for protecting personal information, for electronic payments and the protection of consumers' financial data.

A system can have strong security if it asks in a systematic manner for multiple authentication factors. This kind of user authentication can have opposite results by jeopardizing user convenience. A good security strategy is one where there is the right tradeoff between security and user convenience, which can be achieved by adapting the level of authentication based on a continuous risk assessment.

The purpose of this whitepaper is to present the various authentication methods and how these methods mitigate various attack vectors and match with various levels of authentication assurance.

Methods of Authentication

Authentication establishes confidence that the claimant has possession of one or more authenticators bound to the credential. Authentication does not determine the claimant's authorizations or access privileges – for example, what they are allowed to do once they have successfully been allowed to access a digital service.

The classic paradigm for authentication systems identifies three factors as the cornerstones of authentication:

- Knowledge factor ("something you know"): The system accepts you if you show that you know a certain bit of information. Examples include PINs, answers to security questions, tax return details, etc.
- Possession factor ("something you have"): The system accepts you if you can prove that you have a certain physical device on you. Examples include devices such as smartcards, mobile phones and USB keys.
- Inherence factor ("something you are"): The system accepts you by using a biometric comparison. Examples include fingerprint scanners, retina scanners, voice recognition, and behavioral biometry.

Multi-factor authentication (MFA) refers to the use of more than one of the above factors. The strength of authentication systems is largely determined by the authentication technology deployed and the number of factors incorporated by the system — the more factors employed, the more robust the authentication system. With increasingly complex access environments and more access points than ever before, organizations have every reason to add multi-factor authentication.

In addition to MFA, organizations are adopting passwordless authentication, such as FIDO or Windows Hello, which eliminates the use of a textually based password. Instead of passwords, proof of identity is achieved by replacing the password with other methods of authentication. Passwordless authentication can provide varying levels of assurance and convenience based on how it is implemented, and it has gained traction because of its significant benefits in easing the login experience for users and overcoming the inherent vulnerabilities of text-based passwords.

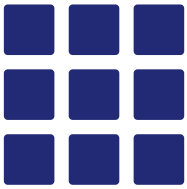
Adaptive Authentication

Technological innovations, such as the proliferation of mobile devices with integrated biometrics, geolocation and other sensors, have led to the development of 'adaptive' or 'contextual' authentication. By assessing a range of attributes such as location, network or device, type of transactions and historical data, adaptive authentication can verify a person's identity to a reasonable degree when they log into an application. In fact, it can do so without the user having to take any action, which is why this method is increasingly popular.

The model of adaptive authentication can be used in low risk situations, or in conjunction with other stronger methods of authentication when needed. Businesses are eager to adopt adaptive authentication solutions since they offer greater flexibility in risk management while improving user experience.

Passwords: Memorized Secrets

Passwords are secret values intended to be chosen and memorized by the user. Passwords need to be of enough complexity and secrecy that it would be impractical for an attacker to guess or otherwise discover the correct secret value. The limitations and drawbacks of passwords are well known—complex password management, easily stolen and hard to remember, and as such are typically not chosen well. Attempts to make this method more secure by requiring longer, more complex passwords further undermine their effectiveness, as often this leads to passwords being written down, making them vulnerable to exposure.



Pattern-based Authentication

A pattern-based authentication makes use of a physical or electronic record that stores a set of secrets shared between the individual and the verifier. The claimant uses the authenticator to look up the appropriate secret(s) needed to respond to a prompt from the verifier. In the case of electronic authenticators, the secrets are generated by an approved random bit generator.

Magic Links

Magic links are authenticated URLs, which can be sent to the consumer in the form of SMS/email that helps them to log in to the system with just one click of the link without any human interaction. Magic links are step towards passwordless authentication, and they remove all the friction points of user authentication. However, there are certain concerns for their security, since a malicious actor impersonating a legitimate user or having hijacked a mail account can gain access through a magic link to sensitive information.

Out-of-Band Authentication

An out-of-band (OOB) authentication uses a physical device, usually a mobile device or dedicated authentication device that is uniquely addressable and can communicate securely with the verifier over a distinct communications channel, referred to as the secondary channel. The device is possessed and controlled by the claimant and supports private communication over this secondary channel, separate from the primary channel for e-authentication. OOB voice and SMS modes are popular, but vulnerable to a variety of attacks, such as SIM swapping attacks.

In fact, the National Institute of Standards and Technology (NIST) has published guidance that recommends against companies and government agencies using SMS as the channel for OOB verification. While a password coupled with SMS has a much higher level of protection, it is considered less secure than other methods of strong authentication. It's not just the vulnerability of someone stealing your phone, it's more related to the SMS being sent over unsecured mobile networking channels to your phone. What is more, NIST states that "methods that do not prove possession of a specific device, such as voice-over-IP (VOIP) or email, SHALL NOT be used for out-of-band authentication."

Other approaches, for example, push-based OTP (sending a code to a mobile device via an authenticator app), which is cryptographically signed and not delivered via the SMS mobile networking channel, avoids those vulnerabilities. Hence, OOB push modes, which offer better security, as well as better UX are gaining traction.

One-Time Password Tokens

One-Time Password (OTP) tokens are generated either by hardware devices or software-based OTP generators installed on devices such as mobile phones. These devices have an embedded secret that is used as the seed for generation of OTPs. The OTP is displayed on the device and manually input for transmission to the verifier or displayed as a push OTP, thereby proving possession and control of the device.

OTP authentication can be used to replace legacy passwords as the sole authentication factor or used together with an additional authentication method to provide multi-factor authentication. Used in combination with a local PIN or device-native biometric, OTP tokens can create sufficient trust in many cases.

When OTP authentication is used, it is important to strongly protect the symmetric key used by the authenticator against compromise. NIST states that "the verifier SHALL use approved encryption and an authenticated protected channel when collecting the OTP in order to provide resistance to eavesdropping and MitM attacks".

Certificate-based (X.509) Authentication

Certificate-based authentication, also referred to as PKI authentication - may use either software or hardware tokens. Authentication is accomplished by proving possession and control of the key. When a software cryptographic authenticator is used, the certificate should be stored securely within a device's secure element – TPM - so that it cannot be compromised. In this configuration, authentication is single factor, since the certificate used to validate the user's identity is not separate from the access device. A more secure multi-factor implementation of certificate-based authentication is when the certificate is secured in smart card chip that is embedded on an independent device such as a USB token or smart card form factor.

FIDO Authenticators

The Fast Identity Online (FIDO) alliance was created to offer a secure way for consumers to authenticate to online services. The notion behind FIDO was to separate the actual authentication mechanisms from the authentication process itself, so that authentications could run over a variety of hardware infrastructure, software apps, and digital identity methods.

The FIDO protocols provide what are essentially passwordless, multifactor cryptographic tokens. A FIDO authenticator embeds one or more private keys, each dedicated to one online account. The protocols require a "user gesture" — a PIN, biometric method or authentication token — before the private key can be used to sign a response to an authentication challenge.

While FIDO authentication offers the advantage of multi-factor security, the protocol does not address the issue of identity proofing or credential life-cycle management. These are two elements that are key to enterprise authentication use cases. Identity proofing ensures that a validated individual is enrolling a token while credential life cycle management ensures that enterprise IT systems can revoke credentials in the event that a token is lost or stolen.

fido™

Passwordless Authentication

Passwordless authentication replaces passwords with other methods of identity proof improving the levels of assurance and convenience. This type of authentication has gained traction because of its significant benefits in easing the login experience for users and overcoming the inherent vulnerabilities of text-based passwords. These advantages include less friction, a greater level of security that's offered for each application and—best of all—the elimination of the legacy password.

There are various layers of passwordless authentication that offer varying levels of security. Implementation of a specific model depends on the level of identity, authentication and federation an enterprise wishes to apply based on the business and security risks and the sensitivity of the data to be protected.

Zero-factor passwordless authentication involves rules to analyze the network, devices and location indicators as familiarity signals. If the familiarity signals are unavailable or do not provide confidence in the identity claim, the tool must be able to prompt for an orthodox authentication method (passwordless or not); otherwise, access must be denied. The drawback of zero-factor authentication is that it cannot completely ensure identity validation and should ideally be used as a backup method or in conjunction with other authentication methods.

Multi-factor passwordless authentication schemes allow organizations to replace passwords as a factor in an MFA deployment with a combination of an OTP device or a certificate-based solution and PIN or biometrics. It must be noted that according to NIST SP 800-63-3, a biometric is recognized as a factor, but not recognized as an authenticator by itself. Therefore, when conducting authentication with a biometric, it is necessary to use two authenticators because the associated device serves as "something you have," while the biometric serves as "something you are."

Continuous Authentication

The evolution of authentication technologies reflects an ongoing tension between the need to offer users an easy logon experience while still maintaining access security. To this end, the desire to eliminate passwords has been enabled by new authentication technologies such as adaptive authentication, and mobile devices. These authentication decisions, however, are taken at a particular point in time for a single access request.

Traditional authentication methods allow users to log in an application or a service by creating a web session. The user is then able to perform actions based on granted permissions. The problem with session-based authentication is that it does not consider contextual changes, such as the user moving from a trusted network to a public one while maintaining the same session. Considering all different environments a user may find himself/herself, session-based authentication may not provide enough security and may require a continuous authentication until the user is logged out from the service.

The premise of continuous authentication is to continuously validate the user's identity as he / she carries out tasks within an application, while taking the security – convenience equation further. For example, may have been authenticated initially but now wants to download a sensitive file. Within the continuous authentication framework, the application would then trigger additional authentication to ensure the user's authenticity before he or she goes ahead.

Classes of Attacks on Authentication Mechanisms

Before selecting an authentication method, it is important to have a thorough understanding of the threat landscape. Cyber threat intelligence combined with traditional intelligence can become the most valuable asset in an organization's arsenal to assess and mitigate emerging threats to user authentication.

Organizations and agencies such as CISA and ENISA provide in an annual basis a taxonomy of the most predominant and noteworthy attack vectors. MITRE notes that "the approach or attack vector outlines the specifics behind how the adversary would like to attack the target." The table below provides a taxonomy of the most common attack vectors in 2018, according to ENISA . A full knowledge base of cyber adversary behavior and taxonomy for adversarial actions maintained by MITRE is available at ATT&CK website.

High-Level Attack Vector	Vectors	Authentication Threat
Attacking the human element	Social engineering	✓
	Phishing/Spear-phishing	✓
	Business Email Compromise (BEC)	✓
	Email spams	✓
	Scams	✓
Web and Browser based	Drive-by downloads	✓
	Cryptojacking	x
	Malicious scripts	✓
	SQL injection	x
	Watering hole attacks	x
Internet exposed	Uprotected assets (IoT)	x
	Default/weak credentials	✓
	Password reuse	✓
Exploitation of vulnerabilities and cryptographic flaws		✓
Supply chain attacks	Software manipulation	✓
	Hardware manipulation	x
DNS attacks	DNS hijacking/poisoning	✓
Privilege or user credentials misuse	Access token manipulation	✓
	Sticky-keys	✓
	Account manipulation	✓
Fileless attacks	Malicious PowerShell and XSL scripts	✓

Table 1: Attack Vector Taxonomy (source: ENISA Threat Landscape 2018)

Malicious actors may leverage above attack vectors to jeopardize the authentication mechanisms of an organization. These vectors may lead up to launching a man-in-the-middle (MITM) attack. MITM attacks happen when an unauthorized actor manages to intercept and decipher communications between two parties and monitors or manipulates the exchanged information for malicious purposes. For instance, hackers can stage MITM attacks to steal sensitive data, such as account credentials or credit card information, or they can use them to deliver malware-inflicted files and applications while posing as legitimate sources.

MITM attacks come in different forms. Conceptually, they're similar, but technically, they're different and they leverage various vulnerabilities in security practices. The table below provides a brief overview of the various MITM attack vectors.

Attack Vector	Definition
IP Spoofing	A malicious actor masks their identity by presenting themselves with the IP address of a legitimate device to gain access to resources that would otherwise be beyond their reach.
DNS Spoofing	A malicious actor intercepts DNS request and returns the address that leads to its own server instead of the real address.
HTTPS Spoofing	A malicious actor replaces characters in the targeted site's domain with other non-ASCII characters that are very similar in appearance.
Man-in-the-Browser	An attacker inserts himself into the communications channel between two trusting parties by compromising a Web browser used by one of the parties, for the purpose of eavesdropping, data theft and/or session tampering.
SSL Stripping	The attackers downgrade the communications between the client and server into unencrypted format to be able to stage a MITM attack. When a victim wants to connect to a server, the attacker intercepts the request and creates an independent, legitimate connection to the server through HTTPS protocol.
Email Hijacking	The hacker compromises and gains access to a target's email account. The attacker then silently monitors the communications between the client and the provider and uses the information for malicious purposes.
Wi-Fi Eavesdropping	The malicious actor tricks unsuspecting victims into connecting to a malicious Wi-Fi network. To perform Wi-Fi eavesdropping, a hacker sets up a Wi-Fi hotspot near a location where people usually connect to a public Wi-Fi network.
Session Hijacking	The hacker steals the user's session token and uses it to access the user's account. There are several ways that an attacker can stage a session hijacking attack, such as inflicting the user's device with a malware that monitors and steals session data. Another method is the use of cross-site scripting attacks, in which an attacker uploads a programming script into a webpage that the user frequently visits and forces the user's computer to send the session cookie data to the server.

Table 2: Man-In-The-Middle (MITM) Attack Vectors

At the network level, insiders can pose a significant threat to enterprise network integrity and confidentiality. Administrators and DevOps users are privileged accounts. Authenticating the access of privileged users, such as administrators and DevOps users, allows establishing trust and can help limiting the risks of insider attacks. Attacks can also be launched from a person external to the enterprise, exploiting known vulnerabilities and then performing lateral movements with the network. These attacks leverage weaknesses in authentication mechanisms, such as the use of weak or compromised passwords. Employing strong authentication mechanisms that leverage network security protection can mitigate these external threats.

At the application level, launching an attack is not an easy task, especially when communications are encrypted in accordance with standards and regulations. For a malicious actor to perform a successful attack it would require either to:

- Spoof and redirect the user through a malicious server, which will act as a proxy between the user and the legitimate service provider
- Succeed in manipulate the TLS connection and make it trustable by the browser (TLS stripping attacks, cookie poisoning, etc.). The same effect can be achieved by using a compromised or rogue certificate (bought in the dark web, after a CA cryptographic incident, etc.).
- Compromise the network through identity theft via phishing/spear phishing attacks, public Wi-Fi interception, etc.

Whatever the attack vector, it is important to select an authentication method that is immune to these vectors, both at the network and application level. The level of immunity is based on the authentication factors that comprise a given method.

The "Something you know" factor, such as a password, may be disclosed to an attacker, who might guess the password or perform a dictionary attack on a hash of that value. An attacker may observe the entry of a PIN or passcode by installing malicious software (e.g., a keyboard logger) to capture the secret. Additionally, an attacker may determine the secret through offline attacks on a password database maintained by the verifier.

The "Something you have" factor, may be lost, damaged, stolen from the owner, or cloned by an attacker. For example, an attacker who gains access to the owner's computer might copy a software authenticator. A hardware authenticator might be stolen, tampered with, or duplicated. Out-of-band secrets may be intercepted by an attacker and used to authenticate their own session.

Finally, the "Something you are" factor may be replicated. For example, an attacker may obtain a copy of the subscriber's fingerprint and construct a replica.

Analysis of Authentication Mechanisms

NIST SP 800-63-3 specifies that the strength of an authentication transaction is characterized by an ordinal measurement known as the Authentication Assurance Level (AAL). Stronger authentication (a higher AAL) requires malicious actors to have better capabilities and expend greater resources in order to successfully subvert the authentication process. Authentication at higher AALs can effectively reduce the risk of attacks and place greater trust in the authentication method.

Authenticator Assurance Level 1: AAL1 provides some assurance that the claimant controls an authenticator bound to the subscriber's account. AAL1 requires either single-factor or multi-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol. The trust level of the authentication methods is low.

Authenticator Assurance Level 2: AAL2 provides high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Proof of possession and control of two different authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are required at AAL2 and above. The trust level of the authentication methods is medium.

Authenticator Assurance Level 3: AAL3 provides very high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication requires a hardware-based authenticator and an authenticator that provides verifier impersonation resistance; the same device may fulfill both these requirements. In order to authenticate at AAL3, claimants are required to prove possession and control of two distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques are required. The trust level of the authentication methods is high.

The table below provides a mapping of the authentication methods with the assurance and trust levels.

Authentication Method	AAL1 – Low Trust	AAL2 – Medium Trust	AAL3 – High Trust
Passwords	✓	x	x
Pattern-based	✓	x	x
SMS Out-of-Band	✓	x	x
OTP Tokens	✓	x	x
FIDO security key	-	✓	x
Certificate-based PKI	-	✓	x
Pattern + Password	-	✓	x
Mobile push + Biometrics	-	✓	x
Mobile OTP + Biometrics	-	✓	x
Mobile OTP + Password	-	✓	x
FIDO + Password/Biometrics	-	-	✓
Hardware OTP + Password	-	-	✓
Crypto + Password	-	-	✓
OTP + Crypto	-	-	✓

Table 3: Mapping of Authentication Methods with Assurance Levels

To determine the appropriate level of authentication assurance, enterprises must assess the potential risks and sensitivity of the resource being access, as well as compliance regulations related to the type of data being accessed.

Categories of harm and impact because of weak authentication include:

1. Identity theft and theft of personal information such as social security numbers, bank account information etc.

2. Personal executive liability and financial loss

3. Harm to government agency programs or public interests

4. Unauthorized release of sensitive information

5. Fines and penalties imposed on organizations from regulatory bodies

NIST offers guidelines regarding required assurance levels for digital transactions, which are determined by assessing the potential impact of each of the above categories. While these are geared toward organizations that need to comply with US Federal security guidelines, they also offer an effective framework for all organizations. The three potential impact values are explained in the table below:

Low	The loss of confidentiality, integrity and availability could be expected to have a limited adverse effect on organizational operations, organization assets or individuals.
Moderate	The loss of confidentiality, integrity and availability could be expected to have a serious adverse effect on organizational operations, organization assets or individuals.
High	The loss of confidentiality, integrity and availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organization assets or individuals.

Table 4: Impact Values according to FIPS 199

The maximum potential impacts for each assurance level are shown in the table below.

Impact Category	AAL1/Low Trust	AAL2/Medium Trust	AAL3/High Trust
Inconvenience, distress or damage to standing or reputation	Low	Moderate	High
Financial loss or organizational liability	Low	Moderate	High
Harm to organization programs or public interests	N/A	Low/Moderate	High
Unauthorized release of sensitive information	N/A	Low/Moderate	High
Personal safety	N/A	Low	Moderate/High
Civil or criminal violations	N/A	Low/Moderate	High

Table 5: Maximum Potential Impacts for Each Assurance Level

In analyzing risks, an organization should consider all the expected direct and indirect results of an authentication failure, including the possibility that there will be more than one failure, or harms to more than one person or organization.

Selecting the appropriate level of authentication will help your organization to mitigate the various attack vectors described in this paper. NIST SP 800-63-3 provides a thorough guidance on selecting authentication mechanisms that are threat resistant. The table below summarizes the NIST guidelines.

Authentication Level	Token Requirements	Authentication Protection Requirements
AAL1 **Low Trust**	Allows single-factor authentication. Passwords are the norm at this level.	Little effort to protect session from offline attacks or eavesdropper is required.
AAL2 **Medium Trust**	Multi-factor authentication, typically a password or biometric factor used in combination with a 1) software token, 2) hardware token, or 3) one-time password device token	On-line guessing, replay, eavesdropper, impersonation and man-in-the-middle attack are prevented. Cryptography must be validated at FIPS 140-2 Level 1 overall with Level 2 validation for physical security.
AAL3 **High Trust**	Multi-factor authentication with a hardware crypto token.	On-line guessing, replay, eavesdropper, impersonation, man-in-the-middle, and session hijacking attacks are prevented. Cryptography in the hardware token must be validated at FIPS 140-2 level 2 overall, with level 3 validation for physical security

Table 6: Authentication Levels, Mechanisms and Threat Mitigation

Key Considerations for Selecting an Authentication Method

Selecting an authentication method involves maintaining a balance between trust, user experience and total cost of ownership. However, the process of selecting the appropriate method should involve a structured approach, centered on the need to balance between security and convenience. The table below summarizes the considerations for selecting an authentication method.

Topic	Considerations
Principles	• Risk-appropriate authentication • End-to-end security: how to protect your users and the authentication infrastructure • Low friction and superior user experience • Minimalism: a single authentication method for all use cases with similar characteristics
Authentication Requirements	• Authentication scenarios • Adaptive access • End-user devices: desktop vs mobile device, Windows vs MacOS, BYOD vs Corporate-owned, etc.
Constraints	• Compliance • User experience • Integration with application architecture • User constituencies (management, office workers, contractors, privileged users, etc.)

Table 7: Structured Approach for Authentication Selection

Conclusion

Authentication of individuals over internet or disperse corporate networks presents multiple opportunities for impersonation and other man-in-the-middle attacks which can lead to fraudulent claims of an individual's digital identity. For this reason, the integrity of our digital lives and our ability to operate online relies on the ability to successfully authenticate an individual accessing online services and applications by ascertaining with a high degree of certainty that he/she is who they claim to be.

In today's environment, an organization's authentication solution need not to be monolithic. The variety of available authentication methods allows organizations and agencies to employ standards-based, pluggable authentication solutions based on mission need. Stronger authentication, adopting methods with higher Authentication Assurance Level, requires malicious actors to have better capabilities and expend greater resources to successfully subvert the authentication access. Stronger authentication can effectively reduce the risk of attacks.

Authentication Method	AAL/Trust Level	Impact Level	Threats
Passwords	AAL1 / Low	Low	Susceptible to MITM attacks, phishing
Pattern-based	AAL1 / Low	Low	
Out-of-Band	AAL1 / Low	Low	Susceptible to SIM swap, MITM attacks
OTP Tokens	AAL1 / Low	Low	Susceptible to cryptographic attacks, session hijacking, key compromise. Prevent MITM, eavesdropping.
FIDO security key	AAL2 / Medium	Moderate	
Cryptographic	AAL2 / Medium	Moderate	
Pattern + Password	AAL2 / Medium	Moderate	Susceptible to session hijacking, and key compromise. Prevent MITM, eavesdropping
Mobile OTP + Biometrics	AAL2 / Medium	Moderate	
Mobile OTP + Password	AAL2 / Medium	Moderate	
FIDO + Password/ Biometrics	AAL3 / High	High	Susceptible to CA cryptographic incidents or key compromise
Hardware OTP + Password	AAL3 / High	High	
Crypto + Password	AAL3 / High	High	
OTP + Crypto	AAL3 / High	High	

Table 8: Overview of Authentication Methods vis-a-vis Assurance Levels, Threats and Potential Impact of Weak Authentication

Before selecting the optimal authentication method(s) for your organization, it is recommended to review the available authentication methods in the market, the level of assurance they provide, and their susceptibility to known threats (see Table 7 above), and taking into account key considerations and how they pertain to your organization. It is highly advisable to start planning your approach to reducing your organization's reliance on passwords, by embracing adaptive approaches and analytics which increase trust while reducing friction for end users.

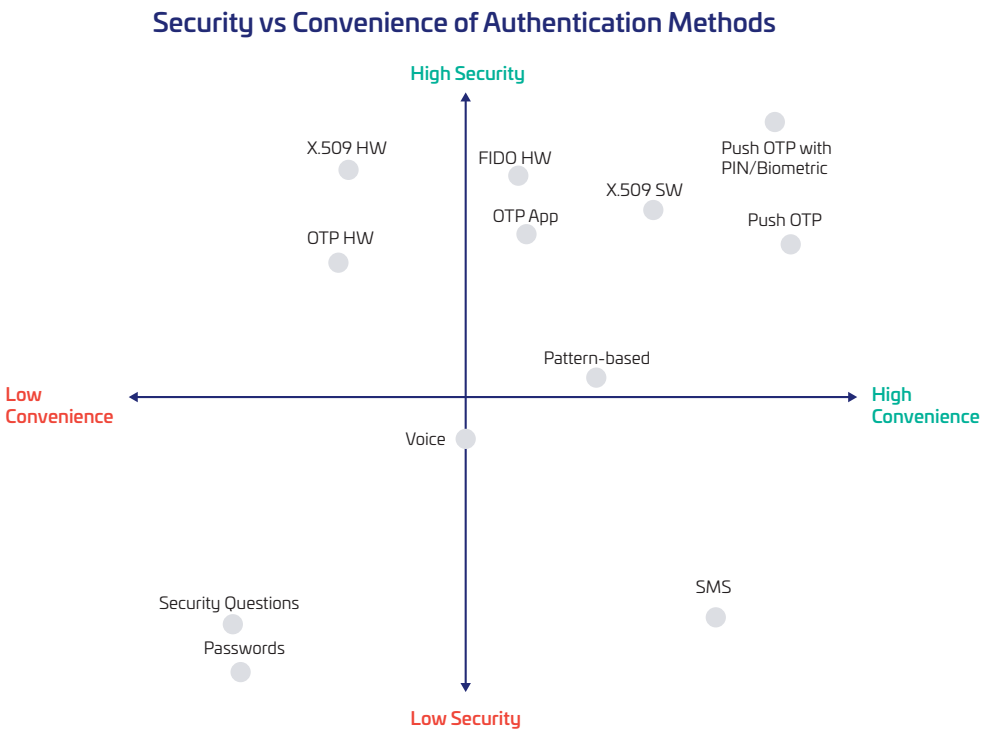


Figure 1: Security vs User Experience of Authentication Methods

Together with policy-based access and single sign on, authentication is a key component of access management. Indeed, the ability to optimize convenience and security is made possible by implementing authentication via a policy-based access management solution. Access management solutions allow organizations to incorporate a broad range of authentication methods into access policies. This allows for the configuration of different policies, each with its own authentication or combination of authentication methods, for specific access scenarios. The combination of access policies combined with smart Single-Sign-On further optimizes security and convenience by offering end users a single sign on experience, requiring them to authenticate once and provide additional authentication as needed.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

THALES

Americas
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

Asia Pacific – Thales Transport & Security (HK) Ltd
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 8141 | E-mail: apacsales.cpl@thalesgroup.com

Europe, Middle East, Africa
350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> cpl.thalesgroup.com <