White Paper

Cogito Group

PKI vs FIDO

PKI vs FIDO

Cogito's Jellyfish platform supports both PKI and FIDO tokens, but what is the difference between the two? Both are based on asymmetric key cryptography.

PKI (Public Key Infrastructure) and FIDO (Fast IDentity Online) are both authentication technologies, but they serve different purposes and are structured differently. Here's a comparison between the two:

1. Purpose and Use Case:

PKI:

- Designed for securing communications and verifying identities using digital certificates.
- Used for a wide variety of use cases including secure email, VPN authentication, document signing, and securing network communications (like SSL/TLS).
- PKI is broader in scope and used for both user and device authentication, encryption, and integrity checking.

FIDO:

- Designed for secure, passwordless authentication.
- Primarily used to authenticate users to web applications and services.
- FIDO protocols (like FIDO2/WebAuthn and U2F) are aimed at improving the security of user authentication and reducing the reliance on passwords.
- Popular for consumer authentication (e.g., logging into online services) and enterprise security.

2. Authentication Method:

PKI:

- Also based on asymmetric cryptography.
- Involves digital certificates issued by a trusted Certificate Authority (CA) that binds a public key to an identity (person, organization, or device).
- Used not only for user authentication but also for securing data in transit (e.g., SSL certificates for websites).

FIDO:

- Based on asymmetric cryptography (public/private key pairs).
- User's private key is stored in a secure hardware device (such as a FIDO security key or biometric device), and a public key is registered with the service.
- Provides phishing-resistant authentication as it verifies both the server and the user.

3. Deployment and Management:

PKI:

- More complex to deploy and manage, requiring infrastructure such as Certificate Authorities (CAs), Registration Authorities (RAs), and certificate revocation and validation services. Jellyfish PKIaaS capability can reduce this overhead.
- Certificates need to be issued, renewed, and managed, which can be time-consuming and costly. This can be mitigated with Jellyfish PKIaaS that allows automated deployment reducing this overhead to less than that of a FIDO token.
- Central management is possible allowing organisations to maintain full control over authentication credentials including the ability to revoke the credentials.

FIDO:

- Easier to deploy for single user authentication.
- Focuses on passwordless authentication, removing the need to manage complex passwords.
- Typically involves enrolling the user's FIDO device (e.g., a security key) with the service.

- No central management possible and an organisation has no ability to revoke credentials centrally. Removal of a lost token, stolen or non-returned token must be done at each account and service if they are known. It is unlikely all will be known. Cogito's Jellyfish platform can mitigate this risk for organisations.
- Organisations can struggle to know what their tokens are used for. Cogito's Jellyfish platform can mitigate this risk.

4. Security:

PKI:

- Provides robust security through encryption, digital signatures, and certificate-based authentication.
- PKI is highly flexible and scalable, supporting various use cases. It is best implemented with secure storage of private keys (which can be in software or hardware).

FIDO:

- Strong security against phishing attacks since it binds the authentication process to the service, preventing man-in-the-middle attacks.
- Private keys are securely stored on hardware, and user authentication can involve biometrics or PINs.
- No central revocation controlled by an organisation is possible. Cogito's Jellyfish platform can mitigate this risk.

5. Usability:

PKI:

- More complex for end-users, especially when managing certificates. Cogito's Jellyfish platform removes this issue and makes PKI as easy to use as FIDO.
- Involves the use of digital certificates, which may require technical understanding or assistance to manage. Cogito's Jellyfish platform removes this issue and makes PKI as easy to use as FIDO.

FIDO:

- User-friendly and eliminates the need for passwords.
- Supports multi-factor authentication (e.g., hardware key + biometric), making it easy for users to authenticate securely.

6. Standards:

PKI:

- Based on long-established standards such as X.509 certificates, RSA, and ECC cryptography.
- Used in many protocols like TLS/SSL, S/MIME, and VPN authentication.

FIDO:

- FIDO Alliance develops standards like FIDO2 and U2F.
- Focuses on web authentication (supported by most major browsers) and standardized authentication flows.

7. Applications:

PKI:

- Securing email, digital signatures, VPN access, code signing, and SSL certificates for websites.
- Trusted device and user authentication across networks and systems.

FIDO:

- Web authentication (e.g., logging into accounts like Google, Facebook, etc.).
- Enterprise applications, single sign-on (SSO), and mobile device login.

Conclusion:

- **PKI** is a more versatile framework used for securing communications, signing data, and authenticating users and devices across a broad range of systems and networks and can be simple to use and maintain with the assistance of Cogito's Jellyfish platform, which has been designed specifically for this purpose.

- **FIDO** is more focused on simplifying and securing user authentication, especially in web applications, without passwords, while providing phishing resistance, but is more limited in it's use cases. It also has no central management, but Cogito's Jellyfish platform can mitigate these issues.

Why have PKI over FIDO in the enterprise

There are several reasons why an enterprise might choose PKI (Public Key Infrastructure) over FIDO (Fast Identity Online), depending on the specific needs, use cases, and existing infrastructure. Here are some key reasons why an enterprise would favor PKI over FIDO:

1. Broad Range of Use Cases:

- PKI is more versatile and can be applied to many different use cases beyond user authentication. It provides:
  - **Encryption** for data in transit and at rest.
  - **Digital signatures** for documents, code signing, email encryption (S/MIME), etc.
  - **Device authentication** for secure communications between servers, clients, or IoT devices.
- FIDO, on the other hand, is more specialized and focused primarily on user authentication and reducing password reliance.

2. Securing Non-Human Identities:

- PKI is ideal for securing non-human identities like **servers, devices, and applications**. Certificates issued under PKI can be used to authenticate and encrypt communications between systems (e.g., SSL/TLS for web servers or VPN authentication).
- FIDO is mainly designed for **human user authentication**, with limited capabilities for securing devices or applications.

3. Legacy Compatibility:

- Many enterprise systems and applications have been built to rely on PKI-based authentication, such as **VPNs, secure email (S/MIME), document signing**, and network communications using SSL/TLS.
- PKI has been the industry standard for decades, and many legacy systems are tightly integrated with PKI-based frameworks. Replacing or upgrading these systems to support FIDO might require significant effort and resources.

4. Compliance and Regulatory Requirements:

- PKI is often required in industries with strict regulatory or compliance needs, such as **finance, healthcare, government,** and **defence**. For example:
  - **Digital signatures** using PKI certificates are recognized by many regulations (e.g., eIDAS in Europe) for document signing and electronic transactions.
  - PKI can help meet compliance with security standards such as **ISO27001, PCI-DSS,** and **HIPAA**.
- While FIDO is excellent for reducing phishing and securing user authentication, it may not fully meet compliance needs for use cases requiring **encryption, signing, and secure communication**.

5. Encryption Capabilities:

- PKI supports **encryption and signing** beyond just user authentication. It's essential for securing data at rest and in transit (e.g., SSL/TLS certificates for web servers).
- FIDO focuses on **authentication**, and while it uses encryption for authentication flows, it doesn't cover broader encryption requirements across the enterprise.

6. Granular Certificate Management:

- PKI provides a **hierarchical trust model** with **Certificate Authorities (CAs)**, allowing for the issuance, renewal, and revocation of certificates. This allows for better lifecycle management of certificates, which is critical in enterprise settings where certificate trust chains are central to maintaining security.
- **Certificate revocation lists (CRLs)** and **Online Certificate Status Protocol (OCSP)** in PKI ensure that compromised or expired certificates can be identified and invalidated.

7. Control and Ownership:

- Enterprises that implement PKI can operate their own **Certificate Authorities (CAs)**, providing full control over the issuance and lifecycle of certificates. This is especially important for enterprises that require complete control over security infrastructure, such as those handling highly sensitive data.
- With FIDO, there is no centralised management. While it enhances security, enterprises depend on third-party services (like FIDO2 and WebAuthn implementations) and **hardware tokens** managed by users, giving them less control over the authentication process. Cogito's Jellyfish platform can help mitigate these issues.

8. Device Management and Secure Communications:

- PKI enables **secure device management** and **machine-to-machine (M2M) communications**, particularly in large enterprise networks with distributed systems or IoT environments. PKI certificates ensure trusted communications between devices and networks.
- FIDO is focused on **user-centric authentication**, so it doesn't offer the same level of support for securing internal device communications.

9. Certificate-Based VPN and Wi-Fi Authentication:

- Many enterprises use **PKI-based certificates** to authenticate users and devices to internal VPNs or secure Wi-Fi networks. PKI certificates provide strong, **mutual authentication** for secure remote access.
- While FIDO can enhance VPN access via passwordless user authentication, it doesn't directly support certificate-based VPN or Wi-Fi access authentication.

10. Digital Signature Requirements:

- Enterprises often need to sign contracts, code, or sensitive documents digitally. PKI supports **digital signatures** that can provide non-repudiation, ensuring that the signature is legally binding and traceable to the specific signer.
- FIDO is not designed for **document signing** or code signing; its focus is primarily on authentication.

11. Enterprise-Scale Identity Management:

- PKI can integrate with **Active Directory** or other directory services for enterprise-scale identity management, allowing large organizations to centrally manage and issue certificates to thousands of users, devices, and services.
- While FIDO works well in web-based or specific enterprise use cases, it lacks the **full identity lifecycle management** capabilities that PKI provides.

12. Customizable Security Policies:

- PKI offers enterprises the flexibility to define security policies, such as enforcing certificate expiration times, choosing cryptographic algorithms, and setting custom validation rules (e.g., for TLS sessions).
- FIDO standards are generally **more standardised** and may offer less flexibility for defining custom security policies at an enterprise scale.

Summary:

While FIDO is a great solution for modernizing user authentication and eliminating passwords, PKI can perform the same roles as FIDO, but also offers broader capabilities that are necessary for many enterprise use cases, such as secure communications, compliance, device authentication, and digital signatures. Enterprises that want better control over credentials, need to secure both human and machine identities, maintain granular control over their security infrastructure, and comply with stringent regulations typically choose PKI over FIDO for its **flexibility, control,** and **comprehensive security** features.

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.