MINDSHARE 2025
10–11 SEP
CYBERSECURITY LEADERSHIP FORUM
Securing Identity for our Digital Future

infineon

Nicole Wagner, Infineon Technologies AG

From Good to Great with Modern Auth & Timeless Trust: A Hybrid FIDO2 – PKI Blueprint

PKI Explained

Introduced with RSA algorithm

1970s

Standardized through X.509 certificates

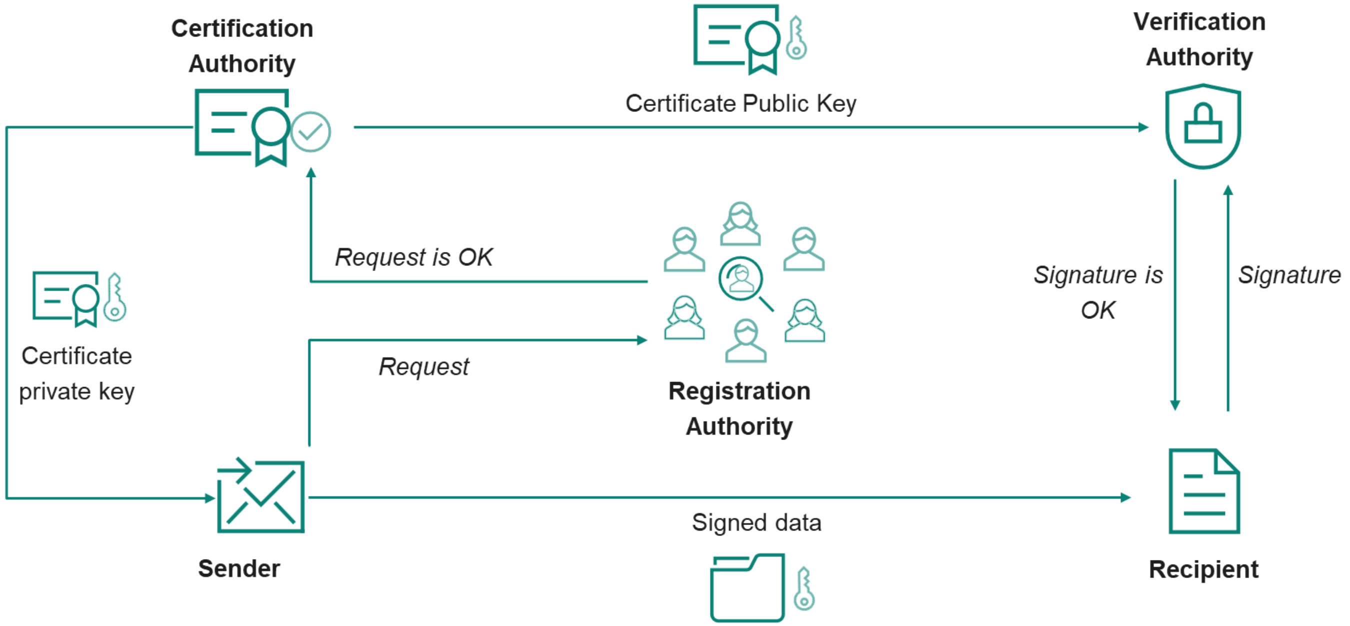
1990s

What is PKI?

- Maps a public key to an identity, creates a link between physical and digital ID
- Manages public-key encryption and digital certificates
- Establishes trust and security in digital transactions and communications

Mechanism: Certificate-Based Authentication

- Relies on asymmetric cryptography
- Relies on certificate authorities for binding between ID and public key



Advantages of PKI over FIDO2

01
Broader Use Cases

02
Comprehensive Security

03
Centralized Management & Control

04
Legally binding digital signatures

05
Securing Non-Human Identities

What is Missing in PKI? – Limitations to Consider

Implementation Challenges

High Complexity

Developer Integration Hurdles

Certificate Management

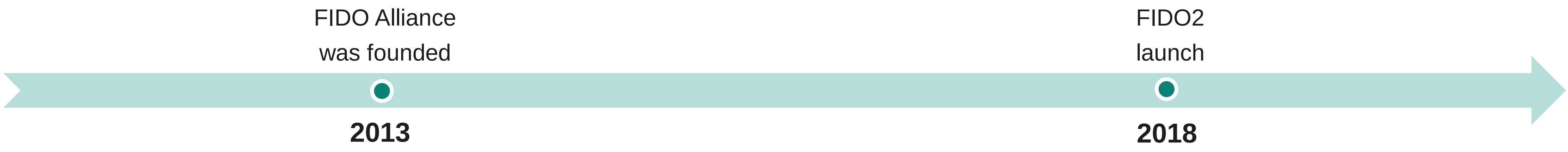
Use Case Limitations

Legacy Application Compatibility

SaaS Environment Restrictions

Management of External Users

FIDO2 Explained

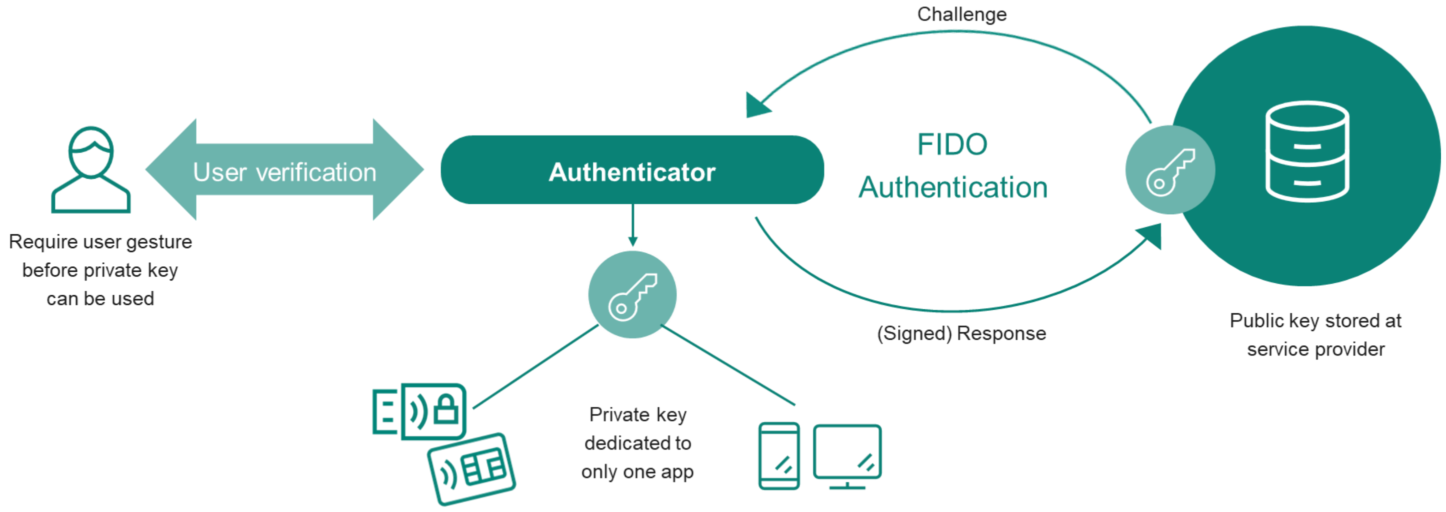


Design goals

- Strong, simple, phishing-resistant, passwordless authentication
- Focus on usability and convenience
- Protects against phishing, replay, credential theft

Mechanism: Cryptographic Authentication

- Relies on asymmetric cryptography
- Registration: scoped key pair creation per service
- Authenticator: separates local user verification and authentication with service


Challenge
User verification
Authenticator
FIDO Authentication
Require user gesture before private key can be used
(Signed) Response
Public key stored at service provider
Private key dedicated to only one app

Advantages of FIDO2 over PKI

01
Enhanced user experience

02
Privacy protection

03
Decentralized trust model

04
Simple & quick implementation

05
Reduced costs & complexity

What is Missing in FIDO2? – Limitations to Consider

Implementation Considerations

Credential Management Complexity

Legacy System Support

Limited X.509 Support

Use Case Limitations Beyond Authentication

Machine Identity Management

Email Signing and Encryption

Document Signing

Consider Using PKI if…

You **already use PKI certificates** for data encryption, digital signatures, or server authentication

You have comprehensive security needs that include **centralized management** and **auditing capabilities**

You need to **support legacy systems** that have native support for PKI

Consider Using FIDO2 if…

You’re **investing in modern authentication** backends

You are looking for a **simplified deployment** for **web** and **mobile** applications

You want to **enhance UX** with biometrics and passkeys for simplified logins

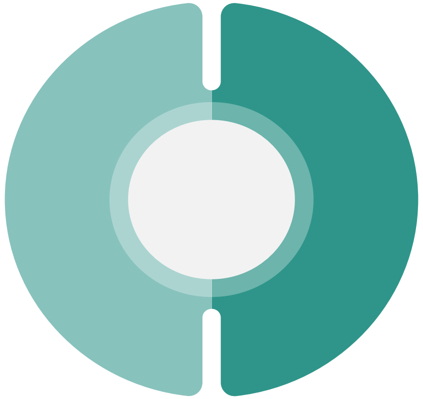
You are looking for a **faster** and more **straightforward implementation** of passwordless authentication

Or Consider a Combined Approach and Leverage All Benefits!

PKI

Ideal for X.509 use cases

- Email Encryption and Signing
- System/Device Identity
- Data Encryption
- Digital Signatures
- EAP-TLS for Wireless Access
- Disk Encryption
- Trust Establishment



FIDO

Ideal where PKI is not issued

- Contractors, temporary employees
- Vendors, partners, guests

Ideal where PKI integration is not feasible

- Mobile
- Cloud & SaaS-based applications
- Legacy systems where PKI can’t be integrated

Leverage the strengths of both technologies to create a more robust and flexible security posture!

The Power of a Combined Approach

- Comprehensive Security Coverage
- Enhanced User Experience
- Future Proof Security Strategy
- Simplified Admin & Auditing
- 1 Authenticator for All Needs

Infineon’s contribution to enable FIDO2, PKI, and hybrid applications

SECORA™ ID for Smart Cards
SECORA™ ID Key for FIDO Security Keys and PKI Tokens

Tamper-resistant, CC EAL 6+ & EMVCo certified, chip

1-stop shop solution incl. JC 3.1 OS, middleware, and applets

Providing highest FIDO Authenticator Security [CTAP2.1, L3+][1]

available with USB interface and as smart card modules

Accelerating your T2M while reducing complexity, costs and your BoM

eIDAS compliant and QSCD listed Infineon eSign applet

[1] certification in process

Key takeaways

- PKI and FIDO2 are complementary, not competing. PKI delivers centralized trust, encryption, and digital signatures for users and machines, FIDO2 a simple, phishing-resistant, user authentication with strong privacy.
- Use PKI when for X.509 use cases, or when centralized management and auditing are mandatory.
- Use FIDO2 to modernize user authentication, reduce helpdesk burden, and deploy quickly without the overhead of user certificate lifecycle management.
- A combined approach closes gaps, improves user experience, and future-proofs your security investments.
- Hybrid tokens and smartcards streamline this strategy. With Infineon you can anchor both FIDO2 and PKI in certified, tamper-resistant chip hardware, while reducing integration effort and cost, and accelerate rollout.

Thank you for your attention!

Questions?