intertrust®

EBOOK

Securing DER ecosystems with PKI

Advantages of managed PKI for enhanced security and trust

Building trust for a connected world.

Contents

PKI's role in securing DER ecosystems

Distributed energy resources (DERs) such as solar panels, wind turbines, and battery storage systems are becoming increasingly integrated into power grids worldwide. As the number of these devices grows, ensuring their security becomes critical.

Public Key Infrastructure (PKI) plays a vital role in securing DER ecosystems by providing a framework for authenticating devices, encrypting communications, and ensuring data integrity.

In DER networks, devices often communicate across wide geographic areas and interact with a variety of stakeholders, such as utility providers, manufacturers, and regulatory bodies.

3 Critical security measures for PKI

1. Device authentication

PKI enables each DER device to possess a unique digital identity, ensuring that only authorized devices can connect to the grid.

2. Data encryption

With PKI, data transmitted between devices and central systems is encrypted and protected from tampering.

3. Integrity verification

PKI safeguards the integrity of the data being exchanged, ensuring that it has not been altered during transmission.

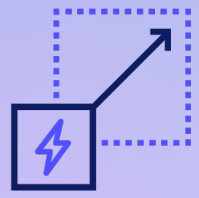
Overview of managed PKI services

Turnkey PKI management

A managed PKI service gives organizations an outsourced solution for PKI deployment, management, and maintenance. It offers a comprehensive, turnkey approach that covers everything from certificate issuance to secure key management, allowing organizations to focus on their core competencies while maintaining robust security.

Scalable PKI for DERs

By leveraging managed PKI service, organizations can build a secure and scalable infrastructure to support the growing number of DER devices. Managed PKI services are particularly advantageous in this context, as they offer streamlined deployment and management, allowing organizations to focus on operational efficiency while maintaining high levels of security.



Efficient and secure PKI

Organizations that adopt managed PKI services can efficiently manage large DER networks, providing seamless device authentication, secure data exchanges, and simplified compliance processes. Companies report reduced operational costs and enhanced security levels due to the streamlined and automated nature of managed PKI services.

Important features of modern PKI

Advanced certificate management and PKI architecture

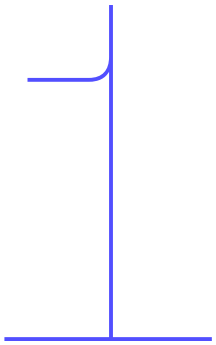
A modern managed PKI service supports diverse certificate formats and encryption standards. It also provides:

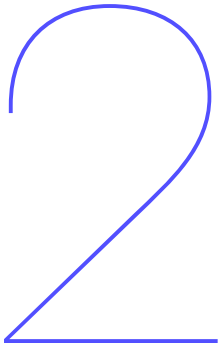
- Scalable and redundant architecture for certificate management
- Automated certificate renewal, revocation, and management
- High availability to minimize downtime and secure communication channels

Robust key management and security protocols

Key management is at the core of PKI security. Modern managed PKI services offer:

- Secure key storage using hardware security modules (HSMs)
- Automated key rotation and certificate revocation to prevent misuse
- Stringent security to safeguard key management facilities





"Managed PKI allows organizations to focus on core competency while maintaining robust security."

Regulatory compliance and continuous audits

A modern managed PKI service needs to meet regulatory requirements without difficulty. It should facilitate:

- Certification practices aligned with frameworks like WebTrust
- Regular security audits to identify vulnerabilities and reinforce trust
- Strong identity verification protocols to prevent unauthorized access

Seamless user experience and integration

Streamlined processes and ease of use are a priority in modern PKI services, which offer:

- Integration capabilities with existing IT systems, simplifying adoption
- Training and support services for staff to ensure efficient management of PKI processes
- Automated alerts and monitoring for proactive threat management

Security dangers and inadequacy of in-house PKI

"There are major risks associated with in-house PKI, especially for DERs."

High costs and complexity

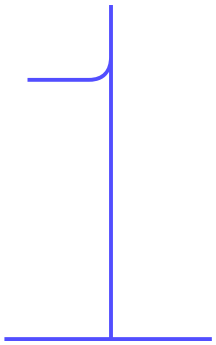
Building an in-house PKI for DERs requires significant investment and operational challenges for organizations, including:

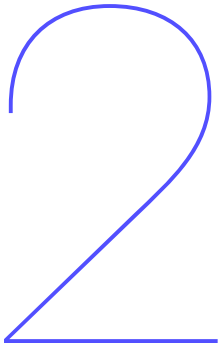
- Infrastructure needs specialized hardware for cryptographic operations
- Software demands continuous security framework development
- Personnel must include skilled cybersecurity professionals

Risk of mismanagement and outdated technology

Without specialized expertise, organizations may struggle to maintain a secure PKI. Common challenges include:

- Inadequate key rotation practices, leaving the system vulnerable to attacks
- Insufficient monitoring, resulting in undetected breaches
- Difficulty scaling the PKI system as the DER network grows





Market insights

75%

of organizations are understaffed for in-house PKI management.

Source: www.fortunebusinessinsights.com/public-key-infrastructure-market-110435

Compliance and audit challenges

In-house systems often struggle to keep up with regulatory requirements, creating organizational exposure. Key risks include:

- Compliance risks from outdated systems violating regulatory standards
- Delayed issue detection due to inadequate auditing practices
- Increased exposure to non-compliance penalties and legal consequences

Impact on operational efficiency and security risks

Organizations lacking robust PKI expertise face significant cybersecurity risks that can compromise their entire DER network, including:

- Unplanned downtime and disruptions severely impact critical infrastructure
- DER networks become prime targets for cyberattacks with potentially dire consequences
- Vulnerable entry points expose networks to breaches and systemic integrity failures

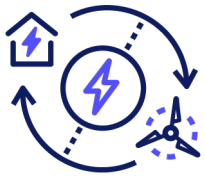
Unique value of Intertrust's managed PKI service

Intertrust PKI service addresses the challenges and security inadequacies of traditional PKI systems by providing a robust, scalable, and compliant solution for securing DER ecosystems.

"Intertrust PKI empowers organizations to protect their assets while remaining agile and responsive to new security threats."

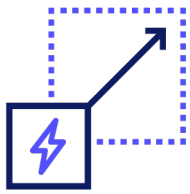
Expertise and end-to-end management

Intertrust's iPKI offers specialized expertise, reducing the burden of in-house PKI management. By handling every aspect of PKI deployment, from initial setup to certificate lifecycle management, Intertrust ensures a secure and compliant environment for DER operations. With continuous support and proactive maintenance, iPKI mitigates the risks of mismanaged certificates and key exposure, keeping systems secure and up-to-date.



Scalable and future-ready solutions

Designed to accommodate the rapid growth of DER networks, Intertrust's iPKI service scales seamlessly as organizations expand. This flexibility allows energy providers to add devices and services without compromising security. Additionally, iPKI supports emerging technologies and is prepared for future security challenges, including the integration of quantum-safe cryptography to address next-generation threats.



Enhanced key protection and secure infrastructure

Intertrust uses advanced HSMs and multi-layered cryptographic techniques to ensure that keys remain secure. Their facilities are fortified with strict access controls and physical security measures, minimizing the risk of insider threats and unauthorized access. By incorporating automated key rotation and certificate renewal processes, iPKI enhances security while reducing the administrative workload for organizations.

Compliance with industry standards

Intertrust iPKI is designed to meet regulatory requirements, ensuring compliance with industry standards like NERC CIP, WebTrust, and other critical frameworks. The managed service includes regular audits, comprehensive reporting, and policy enforcement, helping organizations avoid fines and maintain a strong security posture. This compliance assurance enables energy providers to focus on their core operations without worrying about regulatory issues.

Proactive threat monitoring and incident response

Intertrust's iPKI continuously monitors for potential threats and vulnerabilities, providing real-time alerts and swift incident response. The service's proactive approach minimizes the risk of cyberattacks and ensures that any issues are addressed before they can cause significant damage. By partnering with Intertrust, organizations gain access to 24/7 support and expertise, ensuring that their DER networks remain secure and resilient against evolving threats.

Why Intertrust managed PKI is the future of DER security

Intertrust's managed PKI service offers a differentiated value proposition with its combination of specialized DER security expertise, advanced monitoring systems, and future-ready technology, including quantum-safe cryptography.

Intertrust's iPKI is the choice for organizations seeking to secure their DER ecosystems efficiently and effectively. By investing in Intertrust, energy providers can ensure that their operations remain protected against current and future threats, maintaining grid stability and enhancing operational resilience.

"The future of energy security lies in managed PKI solutions that combine expertise, advanced technology, and scalable design."

Why Intertrust PKI?

Beyond cloud-only PKI services, here's what sets apart Intertrust PKI:

Streamlined management

- Secure operations with bonded, vetted staff and multi-custody protocols
- Robust certificate management with auto-renewal for short-lived certificates
- Comprehensive registration authority for diverse device ecosystems

Resilient infrastructure

- Advanced HSMs with automated key rotation and certificate renewal
- Air-gapped, TEMPEST-shielded rooms with badge and biometric authentication
- 24/7 operations with multi-region disaster recovery

Learn more: intertrust.com
Contact us: energy@intertrust.com

intertrust®

Building trust for a connected world.