



International Symposium

Borderless Digital Transactions: PKI's Role in a Globalized World

V Srinivasan, Chairperson, Asia PKI Consortium
Bengaluru, India | 28-Nov-2023

1. Introduction
2. Web PKI via SSL/TLS
3. SMIME for Secure emails
4. PKI for Digital Signatures
5. Expanding use cases of Private Trust
6. Progressing forward on PKI
7. Advancements in PKI
8. Summary: PKI for future

The enhanced role of PKI in Digital Transformation & the need to go Borderless

PKI is an essential component of global digital transformation, providing the security infrastructure that underpins a wide range of online activities and services. It plays a critical role in protecting data, ensuring privacy, and enabling trusted digital interactions across the globe.

Where and How?

1. Secure communication and data exchange
2. Strong authentication and access control
3. Digital signatures and non-repudiation
4. Support for emerging technologies
5. Foundation for trusted digital interactions

PKI is indispensable to SSL/TLS security and Web PKI, providing a robust foundation for secure online communication and data protection. It is a critical component of the digital infrastructure, enabling secure and trusted interactions across the internet.

1. **Website Authentication:** PKI enables the authentication of websites and users, ensuring that you are communicating with the intended party and not an imposter. This helps prevent phishing attacks and man-in-the-middle attacks.
2. **Data Encryption:** PKI facilitates the encryption of data exchanged between parties, safeguarding it from interception and unauthorized access. This protects sensitive information such as credit card details and login credentials.
3. **Data Integrity:** PKI ensures the integrity of data, preventing tampering or modification during transmission. This guarantees that the data received is exactly as it was sent.
4. **Non-Repudiation:** PKI provides non-repudiation, meaning that parties cannot deny sending or receiving data. This is crucial for establishing accountability in digital transactions.

Global advancements continue to rely on the Web PKI to trust the internet communications. Browsers are upgrading their risk policies and CA/B Forum has been actively working on necessary improvements in policies and practices by CA.

PKI (Public Key Infrastructure) is of paramount importance in S/MIME (Secure/Multipurpose Internet Mail Extensions), playing a pivotal role in securing email communication and protecting sensitive data. It provides the underlying infrastructure for digital signatures, encryption, and authentication, enabling secure and trusted messaging.

1. **Digital Signatures:** PKI enables digital signatures in S/MIME, ensuring the integrity and authenticity of email messages. This helps prevent email forgery and tampering, guaranteeing that the message content has not been altered.
2. **Encryption:** PKI facilitates the encryption of email messages and attachments, protecting sensitive information from unauthorized access. This safeguards confidential data such as personal information, financial details, and business strategies.
3. **Authentication:** PKI provides authentication mechanisms in S/MIME, verifying the identity of senders and recipients. This helps prevent identity impersonation and phishing attacks, ensuring that you are communicating with the intended party.
4. **Non-Repudiation:** PKI establishes non-repudiation in S/MIME, meaning that parties cannot deny sending or receiving emails. This is crucial for accountability in digital communications and legal proceedings.

CA/B Forum has introduced latest policies on SMIME last year, elevating the security practices and bringing interoperability among SMIME certificates.

Public Key Infrastructure (PKI) plays a crucial role in digital signatures, providing the underlying infrastructure for secure and verifiable electronic signatures. Here are some key points on the use of PKI in digital signatures:

Key benefits include:

1. Authentication and Non-Repudiation
2. Data Integrity
3. Timestamping
4. Long-Term Validity

This are also meeting:

1. Compliance with Legal and Regulatory Requirements
2. Enhanced Trust and Confidence
3. Widespread Adoption and Standardization

Today, this has become a critical component of secure digital transactions and electronic document management.

Expanding use cases of Private Trust

PKI is a critical component of private trust, providing the security infrastructure that underpins trusted interactions and secure data management within private networks and communities. Its role in secure communication, identity management, and access control is essential for protecting sensitive information and enabling trusted collaboration.

Key use cases

1. Internet of Things (IoT) Security / Devices
2. Network Security
3. Secure Shell (SSH) Access
4. Virtual Private Networks (VPNs)
5. Blockchain Security
6. Identity and Access Management (IAM)
7. DevOps Security
8. Access Management

While major use cases are using publicly trusted certificates, there are still numerous areas where private PKI setups are operated across the industry.

Public Key Infrastructure (PKI) is constantly evolving to address new security challenges and meet the demands of an increasingly interconnected digital world. Recent advancements in PKI are focused on enhancing security, improving performance, and expanding its reach to new domains and applications.

Enhanced Security:

1. **Post-Quantum Cryptography (PQC):** PQC algorithms are being developed to protect against future threats from quantum computers that could break current cryptographic algorithms.
2. **Up-to-date Validation Services:** Distribution of OCSP/CRL have been made effective with lower caching period, bringing immediate updates on certificate revocation information.
3. **Effective Certificate Revocation Lists (CRLs):** CRLs are becoming more efficient and scalable, enabling faster revocation of compromised certificates.

Improved Performance:

1. **Elliptic Curve Cryptography (ECC):** ECC offers stronger cryptographic algorithms while maintaining smaller key sizes, improving performance and reducing bandwidth requirements.
2. **Hardware Security Modules (HSMs):** HSMs are being integrated into PKI solutions to provide hardware-based cryptographic acceleration, enhancing performance and security.

The advancements in PKI are paving the way for a more secure, efficient, and scalable digital infrastructure, enabling trusted interactions and protecting sensitive data in an increasingly interconnected world.

Expanding Reach:

1. **Mobile PKI:** PKI solutions are being tailored for mobile devices, enabling secure authentication and communication on smartphones and tablets.
2. **Internet of Things (IoT) Security:** PKI is being adapted to secure IoT devices and networks, protecting against cyberattacks and unauthorized access.
3. **Industrial Internet of Things (IIoT) Security:** PKI is playing a crucial role in securing IIoT systems, protecting critical infrastructure from cyber threats.

Automation and Orchestration:

1. **Automated PKI Management:** Automation tools are being developed to simplify PKI management tasks, reducing manual effort and improving efficiency.
2. **PKI Orchestration Platforms:** PKI orchestration platforms are emerging to integrate PKI with other security infrastructure components, enabling centralized management and policy enforcement.
3. **Self-Service PKI Portals:** Self-service portals are providing users with the ability to manage their own certificates and credentials, reducing administrative overhead.

1. **Adaptability and Resilience:** PKI's ability to adapt to new cryptographic algorithms, incorporate emerging technologies, and address evolving security threats ensures its long-term viability.
2. **Growing Demand for Trusted Interactions:** The increasing reliance on digital interactions and the need for secure data exchange in various industries drive the demand for PKI solutions.
3. **Standardization and Interoperability:** Continuous efforts to standardize PKI protocols and enhance interoperability between different implementations promote widespread adoption and seamless integration.
4. **Integration with Emerging Technologies:** PKI's integration with blockchain, quantum computing, and other emerging technologies expands its applicability and strengthens its role in future security architectures.
5. **Continuous Innovation and Advancements:** Ongoing research and development in PKI, such as post-quantum cryptography and certificate management, ensure its relevance and effectiveness in the ever-changing digital landscape.

Thus, PKI has immense potential for the future & a strong need to go borderless.



THANK YOU