+44 20 8123 2220
info@marketpublishers.com

Public Key Infrastructure Market – Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Component (Hardware, Solution, Services), By Deployment Mode (On-premise, Cloud), By Organization Size (Large Enterprise, Small & Medium Enterprise), By Vertical (BFSI, Government & Defense, IT & Telecom, Retail, Healthcare, Manufacturing, Others), By Region, and By Competition, 2018-2028

https://marketpublishers.com/r/PEB64BA0816EEN.html
Date: November 2023
Pages: 189
Price: US$ 4,900.00 (Single User License)
ID: PEB64BA0816EEN

Abstracts

The global Public Key Infrastructure (PKI) market is experiencing significant growth as organizations increasingly prioritize cybersecurity and data protection. PKI serves as a fundamental framework for secure digital communication, authentication, and data encryption. Key factors driving the growth of the PKI market include the rising number of cybersecurity threats, stringent regulatory requirements, and the growing adoption of cloud-based services.

In an era where cyberattacks are becoming more sophisticated and prevalent, PKI solutions are essential for safeguarding sensitive information. Industries such as finance, healthcare, government, and e-commerce rely heavily on PKI to protect customer data, ensure secure transactions, and maintain regulatory compliance. Moreover, the proliferation of Internet of Things (IoT) devices and the need to secure their communications further fuel the demand for PKI.

The market also benefits from the increasing adoption of cloud-based PKI solutions, offering scalability, cost-efficiency, and ease of management. As businesses transition

to hybrid and multi-cloud environments, the need for centralized identity and access management becomes paramount, driving the adoption of PKI.

Additionally, governments and regulatory bodies worldwide are introducing stricter data protection regulations, such as GDPR and CCPA, compelling organizations to implement robust security measures, including PKI. This regulatory landscape is expected to sustain market growth.

However, the PKI market faces challenges related to the complexity of implementation, the need for skilled professionals, and interoperability issues. Despite these challenges, the global PKI market is poised for steady growth as organizations recognize the critical role of PKI in securing digital assets and ensuring trust in an increasingly connected and data-driven world.

Key Market Drivers

Increasing Cybersecurity Threats and Data Breaches

The escalating frequency and sophistication of cyberattacks and data breaches have become a primary driver for the adoption of PKI solutions. Organizations across industries are grappling with the ever-present threat of data theft, identity fraud, and unauthorized access. PKI plays a crucial role in enhancing cybersecurity by providing robust encryption, authentication, and digital signature capabilities. As organizations strive to protect sensitive data and secure their digital transactions, the demand for PKI solutions has surged. PKI helps establish trust and confidentiality in online communication, making it a fundamental component of modern cybersecurity strategies.

Regulatory Compliance and Data Privacy Requirements

The stringent regulatory landscape, with laws such as the General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the United States, mandates the protection of sensitive data and privacy. PKI enables organizations to meet these compliance requirements by ensuring the secure transmission and storage of personal and confidential information. Digital certificates issued by trusted certificate authorities (CAs) are used to verify the identity of entities and encrypt data in transit. Compliance mandates are driving organizations to implement PKI as a means to demonstrate their commitment to data protection and privacy, further propelling market growth.

+44 20 8123 2220
info@marketpublishers.com

Expansion of IoT Devices and Applications

The rapid proliferation of Internet of Things (IoT) devices and applications is a significant driver for the PKI market. IoT devices, ranging from smart thermostats to connected vehicles, require secure communication and authentication to protect against unauthorized access and data breaches. PKI provides a scalable and secure framework for authenticating IoT devices, ensuring data integrity, and encrypting communications. As IoT adoption continues to expand across industries such as healthcare, manufacturing, and smart cities, the demand for PKI solutions to secure these interconnected ecosystems is on the rise.

Growing E-commerce and Online Transactions

The global shift toward e-commerce and online transactions has been accelerated by the convenience of digital shopping, banking, and payment services. However, this trend also exposes individuals and businesses to cyber threats, including online fraud and identity theft. PKI technology is at the heart of secure online transactions, enabling secure payment processing, e-signatures, and identity verification. With the continued growth of the e-commerce sector, particularly in emerging markets, the demand for PKI solutions that guarantee the integrity and security of online transactions is expected to surge.

Increasing Adoption of Cloud Services

The adoption of cloud computing services continues to expand as organizations seek scalability, flexibility, and cost-effectiveness in their IT operations. However, the migration to the cloud introduces new security challenges, including data protection, access control, and identity management. PKI addresses these challenges by providing a trusted framework for authentication and encryption in cloud environments. Cloud-based PKI services offer organizations the ability to centrally manage digital certificates and keys, ensuring the secure and seamless integration of cloud services into their IT infrastructure. As more businesses embrace cloud computing, the demand for PKI solutions that enhance cloud security and identity management is expected to grow.

Key Market Challenges

Complexity of Implementation and Management

One of the significant challenges in the adoption of PKI is the complexity associated

+44 20 8123 2220
info@marketpublishers.com

with its implementation and management. Deploying a PKI infrastructure involves multiple components, including certificate authorities (CAs), registration authorities (RAs), hardware security modules (HSMs), and secure key management. Setting up and configuring these components can be a daunting task for organizations, especially smaller ones without dedicated IT security teams. Moreover, managing the lifecycle of digital certificates, including issuance, renewal, and revocation, requires specialized skills and resources. The complexity of PKI can lead to misconfigurations, security vulnerabilities, and operational inefficiencies if not managed properly.

High Costs and Resource Intensiveness

Another significant challenge in the PKI market is the cost associated with implementing and maintaining a PKI infrastructure. Organizations must invest in hardware, software, and personnel with expertise in PKI to set up and operate the system effectively. Hardware security modules (HSMs), which are essential for protecting private keys, can be expensive. Additionally, the costs of obtaining and renewing digital certificates from trusted certificate authorities (CAs) can add up over time. Smaller organizations may find it challenging to allocate the necessary financial resources and skilled staff for PKI, leading to concerns about affordability and ROI.

Certificate Lifecycle Management

Managing the lifecycle of digital certificates is a complex and critical aspect of PKI. Certificates have finite lifespans and must be renewed or replaced regularly to maintain security. Keeping track of certificate expiration dates, ensuring timely renewals, and managing certificate revocations can be a resource-intensive process. Failure to manage certificates effectively can result in service disruptions, security vulnerabilities, and compliance issues. Organizations need robust certificate lifecycle management (CLM) solutions to automate these tasks and ensure the continuous validity of certificates. However, implementing CLM solutions can be challenging and may require integration with existing IT systems.

Evolving Security Threats and Vulnerabilities

The security landscape is continually evolving, with cyber threats becoming more sophisticated and persistent. PKI, while a robust security framework, is not immune to vulnerabilities and attacks. Vulnerabilities in PKI implementations can be exploited by malicious actors to compromise the confidentiality and integrity of digital certificates and private keys. Recent incidents, such as the compromise of certificate authorities (CAs),

have raised concerns about the trustworthiness of digital certificates. Organizations must stay vigilant, regularly patch and update PKI components, and monitor for potential security threats and vulnerabilities. Additionally, the emergence of quantum computing poses a long-term challenge to PKI, as quantum computers could potentially break current encryption algorithms.

Interoperability and Standards

PKI relies on standards to ensure interoperability between different PKI components and systems. However, the landscape of PKI standards can be complex and fragmented, leading to interoperability challenges. Organizations may face difficulties when integrating PKI solutions from different vendors or when working with partners or customers who use different PKI standards. This can result in compatibility issues, increased implementation costs, and operational inefficiencies. Efforts to promote standardization and interoperability in the PKI market are ongoing, but achieving universal compatibility remains a challenge.

Key Market Trends

Growing Emphasis on Data Security and Privacy

In today's interconnected digital landscape, data security and privacy have become paramount concerns for governments, organizations, and individuals. This heightened awareness is driving the adoption of Public Key Infrastructure (PKI) solutions. PKI provides a robust framework for securing data, communications, and identities through the use of encryption and digital signatures. The trend towards stricter data protection regulations, such as the European Union's GDPR and various data breach incidents, has fueled the demand for PKI as organizations seek to safeguard sensitive information.

The Rise of IoT and PKI

The Internet of Things (IoT) has witnessed explosive growth in recent years, with billions of connected devices now part of our daily lives. This proliferation of IoT devices has introduced new security challenges, as these devices often transmit sensitive data. PKI is emerging as a key technology to address IoT security concerns. It allows for the secure authentication of devices, encryption of data, and the establishment of trusted connections between devices and servers. As IoT continues to expand into various industries, the PKI market is poised for significant growth.

+44 20 8123 2220
info@marketpublishers.com

Increased Adoption of Cloud-Based PKI Solutions

Enterprises are increasingly adopting cloud-based PKI solutions due to their scalability, cost-effectiveness, and ease of management. Cloud-based PKI offers organizations the flexibility to manage digital certificates and keys centrally while eliminating the need for on-premises hardware and maintenance. This trend is particularly pronounced among small and medium-sized enterprises (SMEs) that may lack the resources to maintain complex on-premises PKI infrastructure. Cloud-based PKI providers are continuously enhancing their offerings to meet the evolving security needs of organizations in an ever-changing threat landscape.

Integration of PKI with Identity and Access Management (IAM)

Identity and Access Management (IAM) solutions are crucial for controlling and managing user access to digital resources. The integration of PKI with IAM systems is a growing trend, as it enhances security by enabling strong authentication methods like multi-factor authentication (MFA). PKI can provide the digital certificates necessary for secure authentication and access control. This integration helps organizations streamline their security processes, reduce the risk of unauthorized access, and ensure compliance with security policies and regulations.

Evolving PKI-as-a-Service (PKIaaS) Models

PKI-as-a-Service (PKIaaS) is gaining traction as a cost-effective and efficient way for organizations to implement PKI solutions. PKIaaS providers offer a range of services, including certificate issuance, revocation, and management, as well as compliance monitoring. This trend is particularly appealing to organizations looking to quickly deploy PKI without the need for extensive in-house expertise or infrastructure. PKIaaS providers are also enhancing their offerings to support emerging use cases, such as code signing and securing containers in DevOps environments.

Segmental Insights

Component Insights

Solution segment dominates in the global public key infrastructure market in 2022. PKI solutions encompass a wide range of security features and functionalities, making them a comprehensive choice for organizations looking to secure their digital assets. These solutions include digital certificates, certificate authorities, registration authorities, and

+44 20 8123 2220
info@marketpublishers.com

key management systems, all of which work together to establish a trusted and secure communication framework.

In an increasingly digital world, establishing and managing digital identities is paramount. PKI solutions play a pivotal role in this aspect by enabling the creation and management of digital certificates. These certificates are used to verify the identity of users, devices, and entities in online transactions and interactions, enhancing security and trust.

Data security is a top priority for organizations across industries. PKI solutions provide robust encryption capabilities that ensure data confidentiality and integrity. This is particularly crucial for sectors such as finance, healthcare, and government, where sensitive information must be safeguarded.

Many industries are subject to stringent regulatory requirements concerning data security and privacy. PKI solutions help organizations achieve compliance with regulations like GDPR, HIPAA, and PCI DSS by providing the necessary tools for secure data handling and user authentication.

Deployment Mode Insights

Cloud segment dominates in the global public key infrastructure market in 2022. Cloud-based PKI solutions offer unparalleled scalability, allowing organizations to adjust their resources according to their needs. Whether it's adding new digital certificates, expanding user bases, or accommodating IoT devices, cloud-based PKI can seamlessly scale to meet these requirements.

Cloud deployment eliminates the need for significant upfront capital investments in hardware and infrastructure. Organizations can opt for a pay-as-you-go model, reducing the total cost of ownership and ensuring cost-efficiency. This makes PKI accessible to businesses of all sizes, including small and medium enterprises.

Cloud-based PKI solutions provide global accessibility to users and devices, allowing secure access and authentication from anywhere with an internet connection. This is crucial in today's interconnected world, where remote work, mobile access, and global collaborations are commonplace.

Regional Insights

+44 20 8123 2220
info@marketpublishers.com

North America dominates the Global Public Key Infrastructure Market in 2022. North America, particularly the United States, has a history of early technology adoption and innovation. This forward-thinking approach has led to the emergence of technology pioneers, both in the public and private sectors. Government agencies, financial institutions, and tech giants in North America were among the first to recognize the potential of PKI for securing digital communications, and they played a pivotal role in shaping the market.

The United States, in particular, has well-defined regulations that require the use of PKI for securing sensitive data and ensuring compliance. Regulations like the Health Insurance Portability and Accountability Act (HIPAA) for healthcare and the Federal Information Security Management Act (FISMA) for federal agencies mandate the use of PKI for data protection and secure communication. This has driven widespread adoption of PKI solutions across various industries.

North America boasts a robust ecosystem of cybersecurity companies, research institutions, and professionals. This ecosystem is continuously focused on developing and implementing cutting-edge security solutions. PKI plays a crucial role in this landscape, and the presence of cybersecurity experts and thought leaders in the region has contributed to its dominance.

North America is home to a multitude of large-scale enterprises, including Fortune 500 companies, which have substantial cybersecurity needs. Additionally, government contracts and initiatives related to national security have propelled the adoption of PKI solutions. Government agencies and defense organizations require highly secure and scalable PKI infrastructure, further fueling the market's growth.

North America has a powerful financial sector, with Wall Street serving as the global financial hub. Financial institutions rely heavily on PKI to secure online banking, transactions, and communication. The need for robust security solutions to protect against financial fraud and cyberattacks has driven substantial investment in PKI technologies.

Key Market Players

Thales

Entrust Datacard

+44 20 8123 2220
info@marketpublishers.com

DigiCert

GlobalSign

Let's Encrypt

GoDaddy

Cloudflare

Amazon Web Services

Microsoft Azure

Google Cloud Platform

Report Scope:

In this report, the Global Public Key Infrastructure Market has been segmented into the following categories, in addition to the industry trends which have also been detailed below:

Public Key Infrastructure Market, By Component:

Hardware

Solution

Services

Public Key Infrastructure Market, By Deployment Mode:

On-premise

Cloud

Public Key Infrastructure Market, By Organization Size:

Large Enterprise

+44 20 8123 2220
info@marketpublishers.com

Small & Medium Enterprise

Public Key Infrastructure Market, By Vertical:

BFSI

Government & Defense

IT & Telecom

Retail

Healthcare

Manufacturing

Others

Public Key Infrastructure Market, By Region:

North America

United States

Canada

Mexico

Europe

Germany

France

United Kingdom

Italy

+44 20 8123 2220
info@marketpublishers.com

Spain

South America

Brazil

Argentina

Colombia

Asia-Pacific

China

India

Japan

South Korea

Australia

Middle East & Africa

Saudi Arabia

UAE

South Africa

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global Public Key Infrastructure Market.

Available Customizations:

Global Public Key Infrastructure Market report with the given market data, Tech Sci

+44 20 8123 2220
info@marketpublishers.com

Research offers customizations according to a company's specific needs. The following customization options are available for the report:

Company Information

Detailed analysis and profiling of additional market players (up to five).

+44 20 8123 2220
info@marketpublishers.com

Contents

+44 20 8123 2220
info@marketpublishers.com

8. NORTH AMERICA PUBLIC KEY INFRASTRUCTURE MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

9. EUROPE PUBLIC KEY INFRASTRUCTURE MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

10. SOUTH AMERICA PUBLIC KEY INFRASTRUCTURE MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

11. MIDDLE EAST & AFRICA PUBLIC KEY INFRASTRUCTURE MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

12. ASIA PACIFIC PUBLIC KEY INFRASTRUCTURE MARKET OUTLOOK

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

I would like to order

Product name: Public Key Infrastructure Market – Global Industry Size, Share, Trends, Opportunity, and Forecast, Segmented By Component (Hardware, Solution, Services), By Deployment Mode (On-premise, Cloud), By Organization Size (Large Enterprise, Small & Medium Enterprise), By Vertical (BFSI, Government & Defense, IT & Telecom, Retail, Healthcare, Manufacturing, Others), By Region, and By Competition, 2018-2028

Product link: https://marketpublishers.com/r/PEB64BA0816EEN.html

Price: US$ 4,900.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:
info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page https://marketpublishers.com/r/PEB64BA0816EEN.html

To pay by Wire Transfer, please, fill in your contact details in the form below:

First name:
Last name:
Email:
Company:
Address:
City:
Zip code:
Country:
Tel:
Fax:
Your message:

**All fields are required

Custumer signature _____

Please, note that by ordering from marketpublishers.com you are agreeing to our Terms & Conditions at https://marketpublishers.com/docs/terms.html

+44 20 8123 2220
info@marketpublishers.com

To place an order via fax simply print this form, fill in the information below and fax the completed form to +44 20 7900 3970