



Encrypt Everything With Public Key Infrastructure (PKI)

A Simple, Scalable Way to
Secure Data and Prevent
Cyber Attacks



Your Network Has Been Compromised. Now What?

Data breaches have become commonplace, and organizations are starting to recognize that it's no longer a question of whether sensitive information will be compromised, but when.

The problem is made more acute by the complexity of the enterprise data environment — and the mountains of data that today's organizations collect, generate and process from both internal and external sources.

Given how difficult it is to define the enterprise data perimeter (let alone secure it), the best way to protect sensitive information is to make sure attackers can't read or use it if they do manage to gain access. Encrypt everything: it's a recommendation that has circulated for years in the enterprise security community.

Unfortunately, according to Forrester, only 13% of global firms encrypt all data. Nearly half (45%) encrypt little to no data. In this eBook, we'll explore why it's so critical to close this security loophole — and how public key infrastructure (PKI) can help you do it simply, efficiently and in a scalable manner.

The Case for Encrypting Everything

Zero Trust frameworks — which encourage organizations to do away with the idea of a defined network perimeter and instead authenticate anyone and everyone who attempt to access network resources — are widely recognized for their power to protect against data breaches.

Forrester research suggests they have been adopted by 74% of global organizations. However, many firms still struggle to operationalize Zero Trust concepts. And no surprise: critical data are sourced not just from internal databases but from cloud providers, vendors and IoT platforms. Employees use personal devices to connect to network resources, along with communications channels like public WiFi that are highly insecure.

That's why encrypting all data is seen as an increasingly critical extension of the Zero Trust philosophy. Even if information is stolen, it can't be exploited. Encrypting everything also streamlines both security and compliance workflows, eliminating complicated and confusing schemes that enforce different levels of protection on different parts of the network. And it helps firms comply with the growing body of regulations aimed at protecting critical public and private infrastructure — like the [White House Executive Order](#) on Improving the Nation's Cybersecurity Infrastructure, which calls on organizations to encrypt data “to the maximum extent consistent with Federal records laws and other applicable laws.”





The Financial Stakes Are Rising

The case for encrypting everything isn't just abstract. Data breaches can and do cause major real-world damage. The Ponemon Institute's Cost of a Data Breach Report 2021 estimates the cost of an average breach at \$4.24 million — the highest it's ever been. Each stolen record of personally identifiable information (PII) costs organizations \$160.

The reputational impact of a breach can also be substantial. 63% of people say a company is always responsible for protecting user data. 80% will defect from a business if their information is compromised.

According to Ponemon, however, the average cost of a breach was \$1.76 million less at organizations with a mature Zero Trust approach. At organizations that encrypted data at rest and in motion using high standard encryption (at least 256 AES), it was \$1.25 million less.

What's more, because encrypted data are not considered PII, their loss is often not considered a "breach" under the law — sparing organizations the expense and reputational risk of having to notify customers.

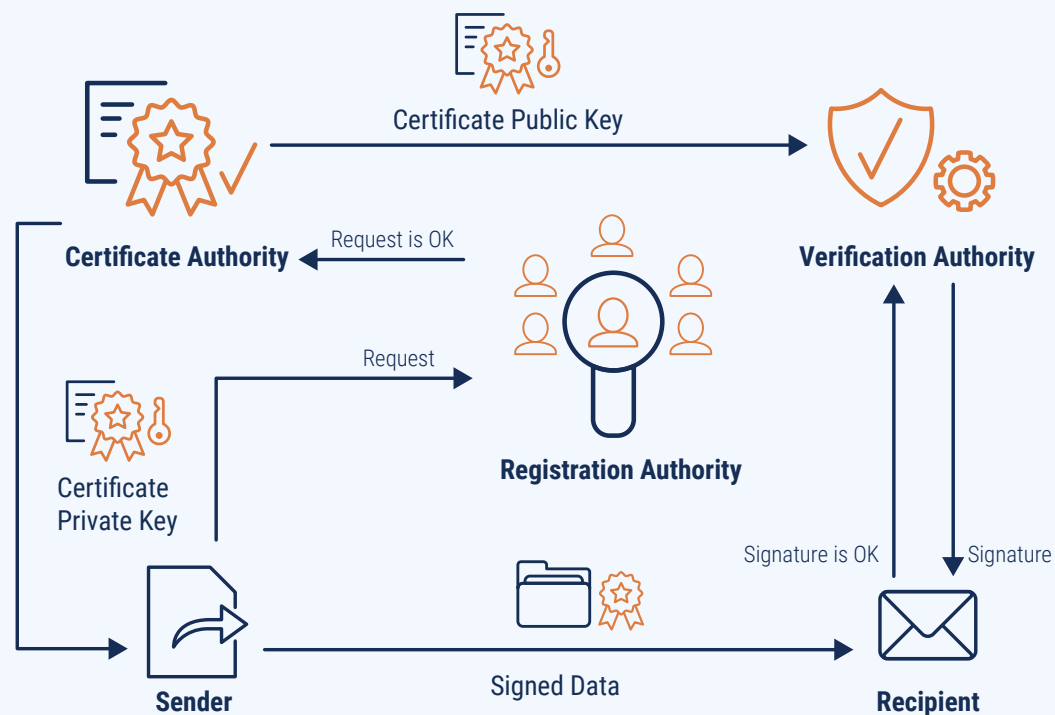
PKI Provides Scalable, Efficient Data Protection

So what's holding back the 45% of firms that don't encrypt most of their data? One common reason is the misguided assumption that encrypting everything will be too complex, too expensive or both.

In truth, PKI — an established technology and the backbone of both Internet and enterprise network security — offers a simple, scalable and efficient way to accomplish the goal.

PKI works by establishing a comprehensive set of roles, policies and procedures that govern centrally-issued digital certificates containing cryptographic keys. These certificates are then inserted into individual devices and applications, where they work to encrypt data and authenticate connected devices and applications. Here's how the process works:

PUBLIC KEY INFRASTRUCTURE



How PKI Encrypts Data

PKI uses asymmetric, mathematically related keys — one public and the other private — to encrypt and decrypt data. The decryption key can only decrypt the same data that the encryption key has encrypted.

If you deploy PKI everywhere on a corporate network, it will automatically encrypt everything that's written to or retrieved from a server or device.

- PKI prevents data in transit from being intercepted by creating a secure channel through which information can pass from one party to another. When you use an SSL/TLS certificate to encrypt the communication channel between a customer's browser and your website's server, you are using this kind of encryption.
- PKI prevents data at rest from being legible by encrypting everything that's stored on a device or database. This renders even stolen data useless to the would-be thieves.

The Benefits of PKI Encryption

Of all the ways to encrypt enterprise data, PKI stands out for its scalability and efficiency.

- PKI is a foundational security technology. It's been around for decades, and it is already deployed in most enterprise IT infrastructures. Support for PKI certificates is already built into a lot of software, from email clients and servers to web servers and operating systems.
- PKI enables organizations not just to encrypt information but also to authenticate its origin using the same security infrastructure. It also detects any tampering — especially relevant when you imagine how changing a key piece of data could impact your critical systems.
- When large amounts of data are to be encrypted and decrypted, symmetric cryptography has to be used, since asymmetric cryptography is too slow. PKI can handle both types, bringing you the security of asymmetric encryption and the simplicity of symmetric encryption.

PKI encryption protects your business by enabling you to secure data from:



Your website and server



Documents



Web development environments



Databases



Emails and messaging platforms





Overcoming Common Challenges

PKI is an established technology, but deployments require careful planning to ensure they meet the needs of your business now and in the future. Challenges include:

- **Complexity** — PKI requires organizations to create, store and distribute digital certificates that map public keys to specific entities and can be used to authenticate them. According to the Ponemon Institute, the average number of certificates that organizations must manage grew to 56,192 in 2020 — a 43% year-over-year increase. Thoughtfully designed certificate hierarchies and lifecycle automation make this process easier.
- **Resources** — The expertise needed to manage PKI certificates is often in short supply: 52% of the security professionals who participated in the Ponemon study said their top challenge was a lack of understanding of their PKI's security capabilities. Vendor-managed PKI solutions — which we'll cover in more depth on the next page — alleviate this issue, delivering best-in-class expertise without additional headcount.
- **Key Storage and Security** — A lock offers no protection if its key is not secure. Private PKI keys must be protected offline, in ultra-secure, audited facilities.

The Power of PKIaaS Encryption

PKI-as-a-Service (PKIaaS) solutions — hosted in the cloud, managed by external vendors and delivered through a SaaS portal — enable organizations to outsource the complexities of PKI while retaining visibility and control. Best-in-class solutions support the goal of encrypting everything through:

- Scalable certificate issuance and validation
- Automated certificate lifecycle management for every system and device
- Easy-to-use cloud infrastructure that offers a single place to manage all certificates
- Highly secure and audited data centers that generate and store the private root keys for each entity





A New Paradigm in Data Protection

Today's businesses are the custodians of unfathomable amounts of data — data they have a responsibility to keep safe. In this landscape, PKI stands out for its ability to protect against compromises that are increasingly inevitable. Encrypting everything streamlines security and removes the utility of stolen data to a would-be attacker. Doing it through PKI delivers efficiency and trust through a solution that's easier than ever to scale.

Learn more about the power of PKI in our white paper, [The Role of PKI in Protecting Enterprise Networks](#) or [talk to a PKI expert](#).



hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800
Latin America: +52 (55) 9171-1108

For more global phone numbers click here

© 2021 HID Global Corporation/ASSA ABLOY AB.
All rights reserved.

2021-12-09-iams-encrypt-everything-with-pki-eb-en
PLT-06362

Part of ASSA ABLOY