White Paper, sponsored by DigiCert

IDC

Digital Trust: The Foundation for Digital Freedom

RESEARCH BY:

Jennifer Glenn
Research Director,
Security and Trust Group, IDC

November 2022 | IDC Doc. #US49795922

Table of Contents

Click on titles or page numbers to navigate to each section.

Defining Digital Trust

The digital world has put a vast amount of information and tools at our fingertips. Devices and applications connect business data and users for improved collaboration, more efficient operations, and greater innovation. Personal devices and programs integrate our personal information for everything from managing finances and monitoring health data to controlling appliances and online shopping. All tools rely on the infrastructure of connections and continuous communication of data over the internet. Given the significance of and reliance on these tools for working and day-to-day life, these connections cannot be disrupted, terminated, or altered without consequence. This requires a high degree of protection and validation of the entities and data that make up our digital infrastructure. It requires digital trust.

Digital trust is achieved by strategically implementing technology, processes, and policies that enable users to engage fearlessly with their digital world. It is a measure of confidence and assurance that the digital products and services the world relies on every day are safe to use because they are genuine and secure. It is freedom to work, play, and connect with the digital world without worrying about being compromised by bad actors.

Understanding the Building Blocks That Make Digital Trust a Reality

Despite the importance of digital trust, the mechanics of it are often taken for granted. The average consumer or business user doesn't typically consider the process of how information or services are delivered to them when navigating online (though brand trust can take a hit when the desired information or service is compromised or not available). The *how* of our digital underpinnings has traditionally been created and managed by IT professionals who have dedicated themselves to understanding the technical complexities of key technologies such as public key infrastructure (PKI).

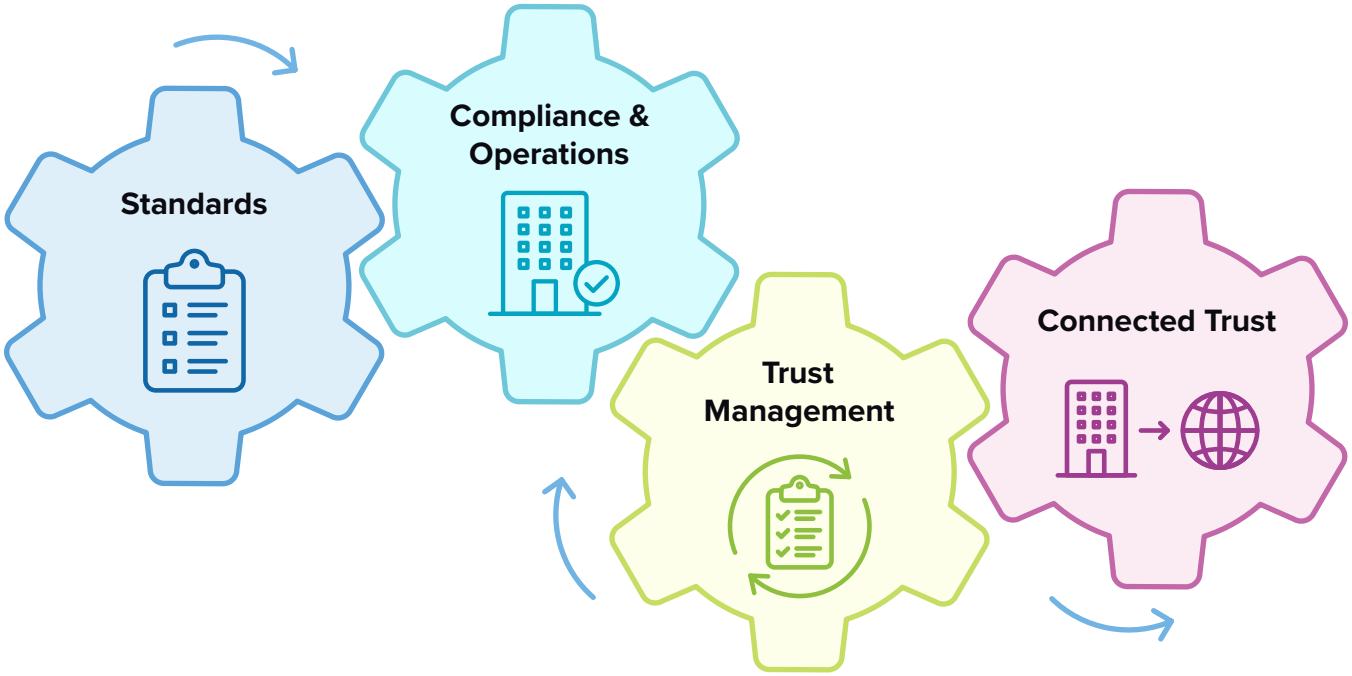
A PKI consists of the infrastructure (including the rules, processes, and technology) used to exchange cryptographic key information between users or devices. These keys are necessary for encrypting and decrypting data while it's stored, as it gets transmitted to different locations across the internet, and/or while it's being used for applications.

Today, this key exchange is uniformly done using digital certificates. Digital certificates are made up of at least a key and a signature. Many certificates also include identity information to accurately identify the entity controlling the key. The use of PKI is essential in facilitating secure online communication and verifying signature integrity and is the foundation for building digital trust.

All strategic initiatives benefit from clear direction and end goals, measurable objectives, strong management, and solid support. Digital trust is no exception. The four building blocks illustrated in **Figure 1** provide the structure and definition to successfully achieve digital trust.

FIGURE 1

The Four Building Blocks of Digital Trust



Source: IDC, 2022

Standards

In any system, the relevant standards define a framework on how participants interoperate and the minimum requirements to create a working project. There are a large number of standards bodies related to digital trust for various use cases, in which digital certificates play a central role, including the certification authority (CA)/Browser Forum, Matter, SAE International, Internet Engineering Task Force (IETF), European Telecommunications Standards Institute (ETSI), and Internet Corporation for Assigned Names and Numbers (ICANN). Keeping up-to-date on changes or adjustments to standards requirements can be a challenge. High-profile attacks and data privacy requirements are driving greater consumer awareness of what data needs to be protected and/or how it can be used. This, in turn, fuels the industry governing bodies to issue updates and changes to standards requirements.

In the case of digital certificates, organizations like the CA/Browser Forum provide clear guidelines about when a certification authority CA can issue a certificate, the contents of that certificate, and when a certificate must be revoked. Standards around PKI vary based on the use case of the certificate and the importance of the information being secured.

To create a strong fabric of digital trust for your business, it's important to keep track of these standards requirements and any changes. While some organizations do their own tracking and managing of standards, most rely on their CAs to keep track of these. Regardless of who is responsible, smart organizations should have a clear process for not only tracking and managing changes to certificate validation standards but also auditing these to stay up-to-date with the latest guidelines.

Compliance and Operations

Knowing and understanding the standards is one thing, but regulating each participant's adherence to these standards can be an initiative all on its own. Compliance has two types of measurement. First, it provides a way to measure and demonstrate how well organizations are meeting the standards set for them by standards bodies. From a business operations perspective, this can look like a checklist of what is required to meet various standards. This leads to the second type of measurement, which is internal. For example, when you have multiple teams purchasing certificates for their servers or devices, these checklists can help get everyone within the organization on the same page. Digital trust is — or should be — a companywide initiative, and this consistency is an important way for every department to measure against those objectives for success.

Further, for suppliers that work with the organization and/or the consumers that rely on the organization for products or services, seeing how the organization tracks and complies with industry standards offers clear proof of its commitment to quality and trust.

Trust Management

On the heels of compliance with industry standards comes the need to unify trust management across multiple use cases, including keys, identities, and certificates. Multiple teams may be purchasing certificates for various purposes. Even with the consistency offered by a good grasp on compliance for the business, each of the components of trust may have a different life cycle. For example, TLS certificates are valid for up to 398 days, whereas some programs require a key rotation every three years. Each component of trust needs to be managed to avoid running afoul of compliance requirements and to optimize security. A failure to manage trust successfully can lead to outages or incidents. While a single outage due to certificate expiration is bad, an outage on a key system might create a domino effect on other systems, causing wider-spread problems for other areas of the business that may rely on that system.

One of the biggest challenges in managing digital certificates is visibility. With multiple departments purchasing certificates (public and private), organizations can have upward of tens of thousands of certificates to manage. If they are not going through some central management system, it is nearly impossible to know what system certificates need to be renewed or whether they meet the compliance standards outlined previously. In addition, the sheer number of certificates in circulation makes it very hard to manage, so tackling the visibility problem can provide a baseline — or at least a justification — for automating the process.

For organizations looking to demonstrate digital trust, centralizing certificate management is essential. As one large technology vendor stated, *"We needed a way to centralize all the certificates across the business — not only to get a handle on upcoming expirations but also to be able to automate the process of renewal. Both things help us reduce the risk of service outage, which would be catastrophic for a business."*

Connected Trust

The final building block required for organizations to create a fabric of digital trust is extending this level of security responsibility and proof out to the increasing number of connected devices that carry their brand name and software — but operate outside of their control. This includes devices like home automation or wearable health monitoring equipment.

There are a number of operational challenges that arise with these types of devices. Like the other building blocks discussed, it can be overwhelming to keep up with the number of certificates required to keep an Internet of Things (IoT) device running optimally. Each device itself may have different certificates, but certificates also run on the web applications, cloud services and gateways that connect to the device. As the device is reliant on these connections, they must all be properly authenticated to ensure the security of the equipment and the protection of transmitted data. Finally, the device needs a way to be updated quickly, without any downtime. This requires secure communication between the device and the organization.

When considering the purpose of these devices, ensuring authenticity and security and maintaining the integrity of the code become significantly more important. Missteps in any of the aforementioned areas could lead to a service outage. This, in turn, not only would reflect negatively on the brand but also could lead to legal action.

Each of these areas represents an essential component of the digital trust fabric. If organizations are deficient in one or more of these areas, digital trust is incomplete.

The Benefits of Making Digital Trust a Strategic Initiative

In the past decade, perspectives on cybersecurity have shifted from utilitarian to strategic. This is likely due to highly publicized ransomware attacks and data breaches. Data privacy and compliance regulations have also contributed to this shift and shone a spotlight into the activities of security teams. That being the case, encryption, key management, and certificates — essential foundational elements of digital trust — have largely been relegated to a small team within IT.

For years, PKI administrators and cryptography operations teams have quietly been the glue holding together our digital world. Their jobs, and their successes, are often unseen and/or misunderstood as a security function. As security moves further into the executive purview, this can — and should — change.

Successfully implementing digital trust should not rest simply with that small group of administrators in IT. Like any cybersecurity initiative, digital trust is the responsibility of the entire business. By refocusing desired business outcomes around achieving digital trust, organizations can rally the entire business to deliver the following benefits:

- **Improved customer satisfaction and engagement:** According to IDC's June 2022 *Future Enterprise Resiliency and Spending Survey*, customer satisfaction and operational efficiency rank as the top business priorities worldwide. This means providing an ideal experience for customers where the devices, applications, and services they need are available and functioning optimally.
- **Better operational efficiency:** Digital trust efforts can help organizations run more efficiently. Centralizing certificate management provides a basis for automation as well as improved visibility into the certificate landscape. Both activities are instrumental in helping keep business systems connected and running efficiently.
- **Stronger overall security posture:** Implementing each of the building blocks for digital trust means integrating consistent security controls everywhere it is needed: the tools used to communicate for employee collaboration, the servers that display customer-facing information, and the IoT devices out in the world.

Considering DigiCert for Digital Trust Initiatives

There are numerous vendors and consultants out there to help organizations tackle individual components of this digital trust fabric. Choosing the right partner is critical.

Founded in 2003, DigiCert is a global provider of digital trust, delivering comprehensive solutions that enable both businesses and consumers to have confidence that their digital footprint is secure. DigiCert provides the foundational pillars of identity, authentication, encryption, and integrity. The company provides the building blocks for digital trust: standards, compliance and operations, trust management, and extended trust into digital ecosystems. An industry leader, DigiCert helps develop global standards for digital trust, including leadership within the CA/Browser Forum, Matter, SAE, IETF, and NIST. DigiCert supports multiple industries, helping write and implement standards of digital trust within multivendor collaborative efforts. The company operates in 20 worldwide offices and deploys globally dispersed datacenters to ensure compliance, uptime, and reliability.

The DigiCert ONE platform offers unified trust management that addresses regional and local needs. DigiCert ONE and its Manager modules help organizations unify trust management for the certificate landscape and feature full reporting capabilities, discovery and automation, and deep integrations with partner tools. DigiCert ONE also extends trust into software supply chains, connected device ecosystems, and documents and electronic signatures and is available via on-premises, cloud, DigiCert-hosted, or hybrid deployment models. With its recent acquisition of Mocana, DigiCert added end-to-end device life-cycle security prior to manufacturing, during production, and with devices in the field.

Challenges and Opportunities

Reimagining business outcomes and priorities based on traditionally "technical" concepts like PKI is going to be a challenge. For many business leaders, PKI and the other elements of digital trust are simply part of the cost/process for doing business on the internet. PKI is considered almost like a utility — and a very technical one that they don't need or want to understand, the reigning thought process being, *Why change something if it doesn't appear to be broken?*

For security teams and PKI administrators, this presents an opportunity to share the value of PKI and build a fabric of digital trust, demonstrating not only the risks that can happen due to missteps in the digital trust fabric but also the opportunity for finding efficiencies in the process.

Conclusion

Digital trust is more than just the technologies that make it possible. For organizations to be champions of digital trust, they must understand and actively implement the structure, processes, and activities that make it possible. This includes keeping up with changes to industry standards, maintaining compliance with regulatory requirements in each geography, managing the life cycle of digital trust technologies, and extending trust into digital ecosystems. For many organizations, regardless of size, this is a significant undertaking that requires skilled staff, dedicated time, and budget. Organizations that are committed to digital trust outcomes should consider their capabilities to implement and manage each of the digital trust building blocks outlined previously and, if necessary, look for a partner to help manage one or more of these processes. It's a mindset shift, particularly in the executive ranks. However, for companies that focus their efforts on digital trust — and make it a strategic imperative for the business — the benefits are notable, including reliable uptime, reduced risk of data compromise, and improved user trust.

About the Analyst

Jennifer Glenn
Research Director, Security and Trust Group, IDC

Jennifer Glenn is research director for the IDC Security and Trust Group and is responsible for the information and data security practice. Jennifer's core coverage includes a broad range of technologies including messaging security, sensitive data management, encryption, tokenization, rights management, key management, and certificates. As part of this research, Jennifer will demonstrate the critical role of data security in top enterprise initiatives such as generating customer trust and digital transformation.

More about Jennifer Glenn

Message from the Sponsor

DigiCert is partnering with leading organizations around the world on digital trust initiatives that are driving real world outcomes.

To learn how DigiCert can support your objectives, contact sales@digicert.com.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.