Trusted Identities in Digital Business: The Benefits of PKI

BLUE HILL RESEARCH

in conjunction with

Entrust Datacard™

Trusted Identities | Secure Transactions

Trusted Identities in Digital Business: The Benefits of PKI

Published: July 2016 **Report Number:** A0246

Analyst: Dr. Alea Fairchild, Entrepreneur-in-Residence

Trust in Digital Business

Strong and long-lasting business relationships have always depended on trust. Trust is a bilateral relationship—one party trusts, and the other is trusted. The backdrop for this has historically been industry rules and governance, allowing some sort of dispute to be decided on the basis of policy and regulation. The responsibility to mitigate these risks is well-understood, and so the required infrastructure (in the forms of legal, financial, and physical controls) has been developed to meet those organizational obligations.

But the fluid and dispersed nature of digital business has made it difficult to scale the trustworthiness of participants, whether they are people, institutions, or things. Cloud, BYOD, and SaaS applications are redefining (and expanding) the network security perimeter and trust boundaries. In a modern cloud environment, data is very fluid, agile, and capable of traversing domains. Next-generation security has to refine how all of this information is privacy-controlled and integrity secured.

Additionally, the ad hoc nature of some of the situations in digital business makes for impromptu situational trust decisions, which need to be guided by mechanisms that are objective and auditable. For instance, if a marketing manager goes to an ecommerce partners' intranet and wants to download a sales report, how can they tell if the file is authentic? And when they send price quotes back to the partner, how does the partner know that the data file has not been tampered with or altered?

In a recent IFS survey of nearly 500 senior decision-makers, 86 percent of the respondents said that digital transformation will play a key role in their market, but 40 percent lacked a strategy for addressing it. To sustain an equivalent level of risk management under new business models that rely on the electronic flow of sensitive information, new infrastructure and trust models must be established.

AT A GLANCE

This report summarizes the important role of PKI and user identity in trust in digital business. Blue Hill believes that to evolve and transform business models based on personalized and individualized relationships, companies must install a structure for trust or accept that relevant participants will never fully trust working with them.

Summary Recommendations for CISOs/CIOs

To develop a trusted organization, CISOs (Chief Information Security Officers) should consider business risk tolerance, strategic executive support, and a deep policy roadmap based on the company's intended future business models.

To build an organization that can support trust, CIOs should effectively manage and control policy definitions, governance, and risk analysis.

The Changing Nature of Trust

Historically, businesses count on third parties to reconcile disputes and ensure trust in the system. But the need for trusted third parties as processors is changing. One example of this is blockchain. What makes blockchain so different is that it is a fully distributed ledger, with no central governing authority responsible for its integrity. Every participant in the blockchain network has a full copy of the ledger and entries in the blockchain ledger are permanent and visible, with cryptographic technology and protocols effectively replacing third-party intermediaries. This is called a "trustless trust," since no *a priori* trust is required between transaction participants. Because transaction histories can be seen but not modified, this shared, visible, immutable ledger enables us to "trust but verify." Eliminating the need for trusted third-party processors can affect everything from business transactions to property ownership records to health and student records.

While the transparency provided by blockchain can be of enormous benefit in many business processes, generally the set of parties privy to any particular transaction is limited, maybe just to the parties directly involved and a third party charged with ensuring regulatory compliance. This requirement is incompatible with a public blockchain. Therefore, many blockchain implementations will contain entries that have been encrypted for just those other parties authorized to review the contents. PKI is the natural choice for managing the required public-private key pairs on the scale demanded by processes involving arms-length business partners.

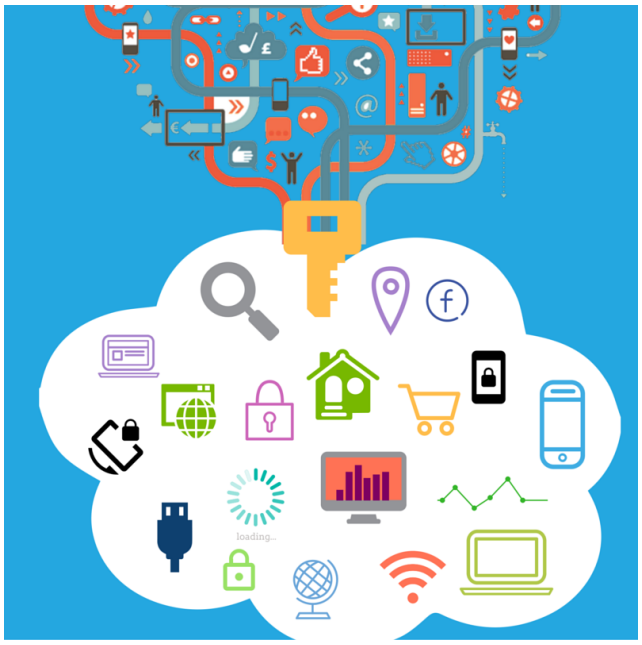
Creating Business Value Using Identity

Establishing verifiable digital identities helps organizations to recognize users and deliver customized, unique experiences. Innovative firms are using identity to create trusted digital relationships that improve and personalize the customer experience, thereby driving greater value and revenue, as shown in the two examples below:

- By using identity authentication, news media content providers deliver opt-in, value-added, personalized services to subscribers by verifying who the subscriber is and then providing more customized services, such as in a paywall scenario. Customers who pay for online news services, for example, expect simple, seamless, and personalized experiences across their own news portal, and the use of identity authentication provides a path for creating the new digital front office for efficiency.
- Food retailers use identity to make their food and grocery items available using third-party affiliates via a mobile app, where customers can create recipes, build shopping lists, and order ingredients. The mobile app can remember user preferences and previous purchases, which has become an essential part of subscription-based and service-based offerings, based on relationship and proactive service.

These firms are succeeding by stretching their boundaries by using data from other digital businesses, digital customers, and even digital devices at the edge of their networks.

Architectural Considerations



CIOs bear the cost of maintaining legacy systems while trying to develop innovative solutions using a more modular approach. One of the challenges in this balancing act is the lack of visibility into those applications that will require PKI. The IT team may not have a clear view of all application deployments, as some departments may go for the "cloud in the corner" approach of shadow IT. But PKI has become a core component of the IT backbone for digital business, which is cloud- and mobile-enabled. Digital certificates have become a ubiquitous component of the system – no longer an exotic add-on – so resources need to be organized to take advantage of an established ecosystem.

One implementation option is to use a managed PKI. This gives access to Digital Certificates without the need to buy, establish, operate and protect an in-house CA, resulting in reduced project costs and perhaps a faster time to market as certificate lifecycle, billing, and user management are all contained within one easy-to-use, cloud-based platform.

Encryption as an Enabler

PKI lends itself, through its intrinsic design, to a systematic approach to information security. Rather than addressing the security needs of disparate services individually, PKI provides an infrastructure that cohesively satisfies these needs. One of the long-term returns on investment in such a system is that future applications can be added without modifying the basic structure. Encryption makes it possible to leverage the benefits of infrastructure "as-a-Service" while ensuring the privacy of data.

In a world that's increasingly built around mobile and cloud, encryption can be an enabler to achieve the flexibility, compliance, and data privacy that is required in today's business environments. Digital business forces enterprises not only to build and develop customer intimacy, but also to ensure that security requirements are part of the strategy. PKI allows them to be satisfied in a cost-effective and frictionless manner. PKI can be seen as a foundational shared service for establishing business trust.

Developing New Trust Models

A trust model can be described as a collection of rules that informs applications how to decide the legitimacy of a digital certificate. PKI is well-suited to a multi-platform, peer-to-peer distributed computing environment that fosters an open, federated network identity model for digital business. The PKI can also support

cross-certification, which is key to creating a truly federated identity, enabling seamless integration among trusted networks.

There are several types of trust models used for controlling the flow of trust in a network, and the choice of model is dependent on the needs of the application. Table 1 summarizes some primary characteristics of the alternative trust models.

Table 1: Trust Models

Trust Model	Hierarchy	Network	Bridge	Hybrid
Trust Anchor Public Key(s)	Hierarchy Root	Local CA	Local CA	CA Hierarchy Root or Local CA
Used for What Business Configuration	Most common implementation in a large organization that wants to extend its certificate-processing capabilities	Less costly way for an organization to provision every user and computing device on its network using certificates	Allows a certification process to be established between organizations or departments. Advantage is additional flexibility and interoperability between organizations.	Combination of a rooted, hierarchical PKI interoperating with a networked PKI. The flexibility of this model also causes challenges due to complexity.
Growth Model	Top-down	Pairwise between CAs	Pairwise with bridge	Top-down or pairwise
Inter-Enterprise Support	Weak beyond common root	Good through moderate numbers of enterprises	Very good through large scale	Good through moderate numbers of enterprises
Path Construction	Simple within local hierarchy; upwards towards the root	May be multiple routes to source, requiring iteration	All non-local paths traverse bridge	Several routes exist, but simple path known

Source: Blue Hill Research, July 2016

Recommendations

We believe that for a PKI deployment to be successful, several factors must be in place:

For the CISO:

- **Understanding of Business Risk Tolerance**: Threat modeling and a proper risk assessment will determine the level of security and investment that should be made in the PKI. For example, an internal PKI supporting wireless LAN authentication will be designed and secured differently from a PKI built for issuing SSL certificates that are trusted by external organizations.
- **Executive Support**: A properly implemented PKI often represents a significant investment, both in capital and human resources. Executive management needs to have a clear vision of the business requirements that using PKI helps to satisfy.
- **Planning and Foresight**: For a PKI to succeed, careful planning must occur to ensure that the policy, procedures, and technical implementation meet the needs of the business, both now and into the future.

For the CIO:

- **Defined Policies**: Prior to implementing any certification authorities or issuing certificates, define and agree upon the policies that govern the use of the PKI, as applications either inside or outside your environment will be dependent on the PKI.
- **Ongoing Governance and Oversight**: Governance plays a significant role in a successful PKI; it ensures that the risk of any changes introduced are well-understood, carefully considered, and are properly communicated to the community of relying parties.

Summary

By using a PKI to issue and manage digital certificates, users benefit from a cost-effective foundation in digital business to:

- Minimize fraud by ***authenticating*** the identities of people who originate digital transactions
- Expand revenue potential to customers who handle ***sensitive or regulated data***
- Protect customer data *against* ***access by unauthorized users***
- Assure the ***integrity*** of electronic communications by minimizing the risk of them being altered or tampered with while in transit without the recipient being notified
- Provide ***non-repudiation*** of transactions so that people cannot deny their involvement in a valid digital transaction.

By selecting the best infrastructural choice, both in terms of trust model and network implementation, PKI can add business value to the foundations of security by using shared services and infrastructure.

Dr. Alea Fairchild

Entrepreneur-in-Residence

Dr. Alea Fairchild is an Entrepreneur-in-Residence at Blue Hill Research. Alea covers the convergence of technology in the cloud, mobile, and social spaces, and helps global enterprises understand the competitive marketplace and to profit from digital process redesign. She has expertise in the following industries: industrial automation, computer/networking, telecom, financial services, media, transport logistics, and manufacturing. Her clients are both commercial, government / public sector, NGO and trade associations. Dr. Fairchild received her Ph.D in Applied Economics from Limburgs Universitair Centrum (now Univ. Hasselt) in Belgium, in banking and technology. She has a Masters degree in International Management from Boston University/Vrije Universiteit Brussel, Brussels, Belgium, and a Bachelors degree in Business Management and Marketing from Cornell University. She is a masters Olympic weightlifter for Belgium, having won many international medals.

CONNECT ON SOCIAL MEDIA

@AFairch

linkedin.com/in/aleafairchild

bluehillresearch.com/author/alea-fairchild

For further information or questions, please contact us:

Phone: +1 (617) 624-3400
Fax: +1 (617) 367-4210

Twitter: @BlueHillBoston
LinkedIn: linkedin.com/company/blue-hill-research
Contact Research: research@bluehillresearch.com

Blue Hill Research offers independent research and advisory services for the enterprise technology market. Our domain expertise helps **end users** procure the right technologies to optimize business outcomes, **technology vendors** design product and marketing strategy to achieve greater client value, and **private investors** to conduct due diligence and make better informed investments.