Choosing a PKI infrastructure for digital business

CONTENTS

Executive summary p3
Introduction p3
The challenge p4
A range of choices p4
Use of PKI systems p5
Planning for the future p6
Concerns about cost p7
Problems and solutions p7
Reluctance to engage p8
Making the right choice p8
Conclusion p10
About the sponsor, Entrust Datacard p10
Executive summary
The last decade has seen an exponential rise in connectivity, which has led to new challenges for those tasked with securing data, networks and transactions.

At the same time, competitive pressures mean that companies are keen to explore new digital initiatives, in which an emphasis on security is seen by some as a brake on progress.

However, this concern is misplaced. Good security equates to trusted systems, which in turn leads to greater confidence in expanding the sort of collaboration that digital entails. Increasingly, organisations are looking toward PKI technology to establish trusted communications between devices, data and applications that is essential to protect from an evolving threat landscape. Already widely used in cloud and mobile environments, public key infrastructures (PKIs) allow users to securely exchange data across networks and over the internet. Just as importantly, PKI systems can be modified to protect smart device users.

Introduction
There is a lot of talk at the moment about the challenges posed by the IoT, but taking the long view it is really just an extension of everyday connectivity that started with client server, peer-to-peer, desktops, laptops, tablets and smart phones. With each generation technology becomes more connected, more mobile and more flexible.

This is not to make light of the challenge in the here and now. The number of connected ‘things’ is rising exponentially. By 2020, it is expected to top 20 billion (Source: Gartner). This, together with the growing popularity of mobile and cloud technology, is likely to have far-reaching effects on the way in which we live and work – just as other step changes have before.

The early signs of what is to come can already be seen in smart homes and mobile services, orchestrated through cloud platforms and connected to any number of information sources. Large, static applications are giving way to microservices, containers and distributed databases with an emphasis on moving data to where it is needed in real-time.

While we can only hazard a guess as to what the full effects of these trends will be, we can say with certainty that they will have a huge impact on privacy and security.
The challenge

We are fast approaching an era of ubiquitous connectivity. According to recent research, by 2020 there will be 6.1 billion smart phones worldwide, more than the current number of basic fixed phone subscribers (Source: Ericsson). Over the next few years, data volumes are also expected to explode – by 2020 the amount of digital data in circulation will exceed 40 trillion gigabytes, the equivalent of 5,200 gigabytes for every man, woman and child on the planet. While the majority of this data will be maintained offline, 15 per cent of it will be stored in the cloud (Source: IDC).

In addition to the increasing number of endpoints, new digital business models will demand further interconnectivity between companies, partners and their customers.

The consequence of these changes will be immense. With communications being carried out over the public internet, organisations will come under increased pressure to ensure that only authorised users gain access to their resources.

To prepare for these challenges, an increasing number of businesses are deploying public key infrastructures (PKIs). Put simply, a PKI supports the distribution and identification of public encryption keys, enabling users and computers to securely exchange data over networks such as the internet.

PKIs are made up of a number of different components. One of the most important components to any PKI is the certification authority (CA). A CA is a trusted entity that issues electronic documents, known as digital certificates, which verify a digital entity’s identity on the internet. Certificates typically include the owner’s public key, the expiry date of the certificate, the owner’s name and other information about the public key owner.

The trusted technology behind VPNs and secure mobile communications, PKI is now having to move up a gear: as the number of connected ‘things’ increases, a consistent means of managing issues of trust becomes more urgent. How far can each of these millions of connected entities be trusted as secure? This is the security challenge of today.

A range of choices

Organisations looking to use a PKI today can choose from a range of alternatives. They can deploy and manage their own PKI or use a hosted PKI operated by a managed service provider, for example, which will itself offer a number of options. They may feel that the PKI tools bundled free with their operating systems is sufficient, or they may choose to pay for solutions that offer more functionality.

Concerns about cost, security and accessibility figured extensively in an exclusive survey that Computing published in August 2016. More than 100 senior IT managers across a wide range of industries – from those with less than 50 employees to those with more than 1,000 – were questioned at length about their use of PKIs.
Use of PKI systems

To set a baseline, we wanted to establish whether our respondents had a PKI system in place. Almost one third (28%) said that they did not have a PKI solution. Just under two fifths (38%) said that they used an on-premise bundled PKI. Smaller numbers reported using on-premise proprietary PKI systems (12%), managed service PKIs (17%) and open source PKIs (5%).

Among those without a PKI system, some simply felt they had no need for one. However, for others, the issue was a lack of the necessary skills within their organisation.

From here, we narrowed focus down to participants that identified themselves as PKI system users. We wanted to find out more about the functionality of their chosen platforms. Just over three quarters (77%) told us that their solutions had centrally managed policies and controls, while half mentioned that their systems were interoperable with LDAP directories, smart card management systems and hardware security modules (HSMs). A large proportion of respondents told us that their systems had web-based administration and end-user enrolment features (45%) and provided cross-platform support for devices and operating systems (42%). And just over a quarter (26%) told us that their systems had barriers between their operating systems and CA administration functions (Fig. 1).

Fig. 1: Does your chosen PKI platform have the following? (Select all that apply)

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centrally managed policies and controls</td>
<td>77%</td>
</tr>
<tr>
<td>Interoperability with LDAP directories, smart card management systems and HSMs</td>
<td>50%</td>
</tr>
<tr>
<td>Web-based administration and end-user enrolment</td>
<td>45%</td>
</tr>
<tr>
<td>Cross-platform support for devices and operating systems</td>
<td>42%</td>
</tr>
<tr>
<td>Separate operating system / domain administration from Certificate Authority admin functions</td>
<td>26%</td>
</tr>
<tr>
<td>Support for peer-to-peer and hierarchical cross-certification of Certificate Authorities</td>
<td>21%</td>
</tr>
<tr>
<td>Support for large-scale deployments (more than 200,000 users per Certificate Authority)</td>
<td>16%</td>
</tr>
<tr>
<td>None of these</td>
<td>3%</td>
</tr>
</tbody>
</table>

Next, we asked our respondents about their use of PKI certificates. Almost three quarters (70%) told us that they used PKI certificates to secure user, device and application access. A significant proportion mentioned that they used PKI certificates to secure internal web sites (60%) and manage digital signatures (37%).
Planning for the future

In a review last year, entitled *PKI Is Gearing Up for the Internet of Things*, Gartner argued that PKI is seeing a resurgence as a result of the new requirements brought about by the IoT, mobility and cloud.

We were interested in finding out whether or not these factors were having any bearing on our participants. To obtain more information on our respondents' intentions, we asked them to list their reasons for investing in identity management technology.

The answers were revealing (Fig. 2). Almost four fifths (78%) said that remote access was driving their decision making, while just under three quarters (71%) said that they were concerned about securing communications and equipment. Just over three fifths (61%) mentioned increased reliance on mobile devices as a compelling reason for further investment. Only 40% of interviewees mentioned access to cloud applications as a reason for their choice.

**Fig. 2 : Which of the following are driving a need for identity management at your organisation? (Select all that apply)**

- Remote access: 78%
- Securing communications and encryption: 71%
- Authentication of connected devices and systems: 67%
- Increased reliance on mobile devices: 61%
- Collaboration (file sharing, workflow, interaction with third parties): 43%
- Access to cloud applications: 40%
- Transaction signing (workflow approvals, customer interaction): 24%
- None: 3%

We also asked our respondents a number of supplementary questions about their use of cloud and mobile technology. Almost half (47%) told us that they had begun to use services like SaaS and IaaS in a limited way over the previous three years. Just over half (56%) told us that they had increased their use of mobile devices significantly over the same time period. And almost the same percentage (57%) reported an increase in the number of remote workers in their organisations.

1 https://www.gartner.com/doc/3426421/pki-gearing-internet-things
Concerns about cost

Some vendors, such as Microsoft, offer ‘free’ or bundled PKI solutions as part of their enterprise operating systems. While these may be adequate for organisations with simple requirements, for others relying on packaged PKI might turn out to be a false economy, with additional management requirements outweighing any hope for savings and restricting future growth plans.

As the number of mobile workers and devices increases, so does the complexity. The free bundled PKI solutions offer a helpful stop-gap, but may not be capable of properly securing the organisation or offering the flexibility that digital business needs in order to make changes on the fly. Fifty-four per cent of respondents said it is becoming progressively harder to manage their PKI systems, with others worried about ongoing management costs. Clearly, respondents were grappling with supporting a tactical implementation of PKI and the demands of digital business that require a more strategic and holistic approach.

Cost savings may be illusory too. Respondents’ PKI costs included investing in staff on a regular basis (mentioned by a quarter), ongoing software costs (26%); infrastructure (22%) and maintenance (15%). The range of answers given shows that the cost of the PKI solution itself is just one part of the total – most likely a minor one – and organisations should consider all the options over the medium and long term before recommending the one with the lowest up-front cost.

Given the level of expertise needed to manage a PKI system, we were interested in finding out if our respondents had the right skills in-house. Just under two fifths (39%) said that they had security specialists with the required knowledge and expertise to manage their PKI systems. A third said that they dispersed responsibility for managing their PKI systems across their IT departments. And just under a quarter (23%) said that they brought in specialist help from third parties.

Problems and solutions

The coming increase in connectivity and acceleration of digital business initiatives will see PKI rising steadily up the list of essentials for organisations of all types, not just those who consider themselves to be digitally oriented today.

Within the enterprise, digital transformation will continue to drive the need for agile trust management frameworks that meet the needs of an evolving technological landscape. The strategic use of PKI will continue to secure trusted communications and data exchange across mobile, cloud and digital workplace initiatives and will increasingly need to accommodate the commercialisation of bleeding-edge technologies like blockchain.

There is also the issue of trust management. As devices proliferate and applications and services move to the cloud, PKI systems will need to become more dynamic in their application of rules. New continuous delivery models for services are pushing applications and databases to containers and distributed file systems, and code is streamlined into microservices that are more agile and efficient to scale. Event-driven standalone functions assigning trustworthiness ratings to the different components becomes ever more challenging, requiring PKI systems to become more dynamic in their application of rules. The challenge many organisations are facing today is determining how to support new distributed architectures with legacy PKI solutions that were not designed to manage and scale trust policies across a diverse ecosystem of interconnected devices, applications and services.
Reluctance to engage

Judging by the responses of our interviewees, many are aware of these trends. When questioned about their rationale for investing in PKI systems, a large proportion of respondents mentioned mobile and cloud technology. Many interviewees told us that they were also worried about keeping up with the evolving threat landscape that was compounded by the fragmentation across new devices and communication systems.

However, many of them had reservations about PKI technology and were tentative about fully embracing it. Some interviewees told us that they did not have the in-house skills and expertise to deploy PKIs. Others expressed concerns about the performance, cost and maintenance of PKI solutions.

A quarter of the respondents had reservations about PKI technology and were looking for guidance on the best ways to embrace the technology to enable their business outcomes while respecting their requirements for administration, performance, scalability and cost. Among these respondents, a typical concern was the lack of in-house skills and expertise to deploy PKI across their organisation, which is increasingly magnified by the acceleration of digital business initiatives and the need to manage risk.

For some respondents, deploying and managing a PKI system proved to be a complex and burdensome undertaking. Besides implementing the software, organisations also have to take into account data centre security and certificate management. It is easy for the expenses associated with a PKI implementation – even a supposedly ‘free’ one – to spiral, which may explain why so many of our respondents expressed concerns about cost. The findings are not altogether surprising when you consider that PKI was traditionally implemented as a tactical solution in IT rather than considered a strategic technology that could enable digital business.

To that end, what should businesses do to avoid these pitfalls and get the most out of an investment in PKI technology?

Making the right choice

Before answering that question it is worth looking briefly at the options that are available to businesses today. Organisations can deploy and manage their own PKI (free or paid for) or use a hosted PKI operated by a managed service provider.

There are a number of advantages to having an in-house PKI solution. It allows organisations to have total control over a very sensitive commercial area. In-house solutions can also be customised to fit a specific set of business needs, something that isn’t always possible with third-party offerings. And if a company is using a PKI to manage confidentiality, integrity and authenticity services for its own employees, it may make more sense to keep the solution in-house.

That said, the market is changing. Not too long ago, firms were reluctant to put any sensitive data in the cloud whereas now most recognise that in general cloud providers can provide levels of security and control that are equal to or better than those in-house. Similarly with PKI, as the environment grows more complex customers will increasingly prefer to leave PKI management to specialist providers, leaving staff to focus on core competencies of their business.
Choosing a PKI infrastructure for digital business

Already, many companies simply do not have the skills and expertise to deploy an in-house PKI system. Before a business can roll out a PKI system, it has to acquire all of the hardware and software components needed to generate digital certificates. It then needs to integrate digital signatures and authentication mechanisms into its internal applications. Assuming that this process is carried out smoothly, the company will then have to commit itself to carrying out regular audits of its own infrastructure. On top of this, unless it has an exceptionally talented IT team, it will have to bring in external support to help employees install and use digital certificates.

While the in-house approach ostensibly gives more control, unless operational staff are properly trained with a brief to track market developments and ensure systems are up-to-date the sense of wellbeing may well be illusory. It is also likely to be the most expensive option and therefore tends to be chosen by those organisations whose security and compliance responsibilities require that control of certificates and identities remain inside the business.

Some organisations will be tempted to limit their deployment to PKI components bundled with their operating system, but as we have seen, this may prove to be a false economy since the real cost drivers of PKI lie in its management, configuration and maintenance. Firms need to consider how their identity and security needs will change as connectivity and digital transformation continue to accelerate.

As an alternative to maintaining an in-house PKI, many organisations are outsourcing their PKI infrastructure to a managed service provider, with the technology managed and hosted by a trusted third party. There are several advantages to this model, including faster time to deployment and lower total cost of ownership.

With advanced security expertise at their disposal, managed services providers can offer a more consistent and ultimately more secure, resilient and flexible proposition that’s not dependent on the need to hire and retain skills that are in short supply. As the environment becomes more complex, regulations more strict and fines significantly larger, firms are better off putting their trust in the expertise of a provider rather than insisting that security and control are better managed in-house. Increasingly, that is a wrong assumption.
Conclusion

According to McAfee, $375bn is lost to cybercrime annually. This figure is likely to increase further as more and more aspects of everyday life move online. By 2020, there will be up to 20 billion devices connected to the internet, massively expanding the opportunities for malicious attack.

Fortunately, businesses already have a series of mechanisms for establishing trust across connected devices on a massive scale – PKI. Aside from providing peace of mind, these certificates also play a critical role in protecting data, employees and businesses.

PKI is a proven technology for protecting connectivity between connected devices for some time. But as more and more devices come on stream, PKI is likely to acquire an increasingly central role in securing data. Organisations continue to be aware of the importance of PKI technology and increasingly appreciate the significant role that identity management solutions play in securing communications, authenticating devices and improving collaboration in the digital workplace.

But as our exclusive survey reveals, many businesses are reticent about embracing the technology beyond using the free solutions bundled with enterprise operating systems, citing concerns about cost, security and accessibility.

A basic one-size-fits all PKI solution is no longer sufficient in a world that has been reshaped by mobile and which will continue to change ever more rapidly, neither will it necessarily save money over the long term. Security must always be the number one priority, and businesses need the flexibility to choose how they secure their data.

So organisations must decide between a bundled PKI or a proprietary one that may tailored to their needs.

They also need to work out how much ongoing support they require in view of ongoing business and technology changes and to decide between an on-premise or hosted PKI deployment.

As well as the familiar benefits of moving budget to opex, a hosted PKI offers advantages of availability, consistency and automated and updates and patching. As hosted services have matured, their ability to offer fine grained controls and tailored solutions has increased.

PKI has evolved to meet the security requirements of the distributed, cloud-based picture that now characterises corporate IT. It is now a strategic investment, enabling digital business practices and allowing organisations to secure data wherever it is located and whatever platforms it moves between.

More than this, it prepares the organisation for the coming IoT age, which will represent another step change in connectivity and, if not thought through properly, an unwelcome jump in cost and complexity too.

PKI needs to be thought of as an overarching solution to enable secure innovation and agility, rather than a point fix for a current issue. Given a trusted framework for data security which can easily accommodate new additions and developments, there’s really no limit to the kind of value that an organisation can drive through imaginative use of technology.
Choosing a PKI infrastructure for digital business

About the sponsor, Entrust Datacard

Single Source for Serious Security & Bold Enablement

Entrust Datacard solutions are used to manage millions of identities and secure millions of transactions every day. Global 2000 enterprises, national governments and the world’s largest banks rely on us for trusted identity solutions. Our sustained investment in cloud-based authentication, PKI, IoT security and SSL certificates makes us a preferred partner for organizations looking to build profitable digital businesses. We support customers with a sales and service network that spans 150+ countries.

www.entrustdatacard.com