



E-BOOK

WHERE YOU NEED TRUST, YOU NEED PKI

digicert®





TABLE OF CONTENTS

1	<i>Introduction: From the Alaskan frontier to the edge of space</i>
3	<i>Chapter 1: Trust is a dynamic need</i>
7	<i>Chapter 2: What you may not know about PKI</i>
11	<i>The proof of trust is all around: Case Studies</i>
25	<i>Chapter 3: What you don't know can hurt you.</i>
28	<i>Conclusion</i>

FROM THE ALASKAN FRONTIER TO THE EDGE OF SPACE

On a rainy summer day in 2013, a small, float-equipped plane stalled while flying low over the mountains near Petersburg, Alaska. There were six passengers aboard, headed for a sight-seeing tour of the Le Conte Glacier. While attempting a climb through the pass at Horn Cliffs, the pilot made a miscalculation, lost control of the craft, and the plane spun before pitching at the ground and smashing through the giant evergreens below.

Injured and stranded on steep terrain, the passengers who survived the fall couldn't hope to get off the mountain without help. Night was only a few hours away, and even in June, dark in Alaska would mean freezing temperatures in a place without cell signals or roads. Only an aerial rescue team would be able to get everyone out of the wreckage and take them back to safety.

Five hundred miles above, the Iridium satellite constellation picked up the plane's emergency

beacon signal and transmitted the distress call and location to rescue authorities. More than just GPS or a radio mayday, the Iridium-enabled device had tracked the plane's movements from takeoff to the moment it went down, drawing a real-time digital trail of every moment of the flight. This was possible because each one of the 66 Iridium satellites circumscribes a carefully choreographed orbit around the earth, communicating between the surface and with each other, to provide complete coverage of every inch of the planet every second of every day. On the Iridium constellation network, a functioning device is visible at any time, anywhere in the world—from Antarctica to Alaska.

This particular type of tracker and emergency signal device isn't standard on all planes. But more and more pilots and owners—especially those who fly small craft or traverse remote locations—have installed one.



For most, it's peace of mind, but in some cases, it has meant the difference between life and death.

Knowing exactly where the plane crashed, the United States Coast Guard was able to reach the site of the accident, and within a few hours, helicopters rescued everyone who survived the fall from the sky. After they were safely lifted out of the wreckage and taken for medical care, Alaska Public Media¹ interviewed Coast



Guard spokesman Grant DeVuyst. Talking of the emergency signal device, he said, “That’s the only reason that we knew there was trouble and that’s the only reason we were able to really get on scene and find them.”

In these rare emergencies, when lives are on the line, a pilot needs to know the Iridium satellite network will track the flight and pick up the

distress signal for relay to a rescue team. The signal must be secured against interception, the emergency device authenticated, and the network protected from interruption. If any part of the Iridium constellation fails, lives can be lost. It’s a level of trust with the highest stakes, and there’s no room for error—which is why the Iridium satellite constellation is secured with PKI.

**“PKI IS TRUSTED TO
SECURE EVERYTHING
FROM THE BOTTOM
OF THE OCEAN TO THE
EDGE OF SPACE.”**

*Brian Trzupek
Senior Vice President for Product, DigiCert*

TRUST IS A DYNAMIC NEED

When British cryptologists James Ellis and Clifford Cocks first developed the idea of “non-secret encryption” in the 1970s, they could not have conceived of its use across tens of millions of websites around the world. At that time, the internet was still a DARPA project, used infrequently to connect university researchers looking to share data or findings.

Within a few decades, the world had changed, and Ellis and Cocks’ public key infrastructure stood at the center of the Information Age as the shield against hacking and fraud. To this day, if a website is trusted, that trust is the result of PKI.

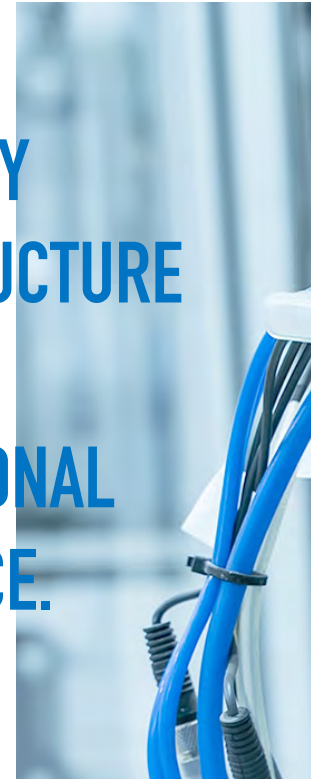
But the invention of the world wide web—which, by itself, would have been enough to define an era of human development—was immediately followed by a second revolution in connected devices. Practically overnight, everything from refrigerators to banking apps became a part of a global ecosystem of networks, devices, applications and users, all communicating across distances.

The speed of growth was, and continues to be, so rapid it can only be measured by orders of magnitude, and as hundreds of thousands of people develop new ideas for connecting millions of people to billions of things, the need for strong security has climbed at an exponential rate.

For all the good created by the Information Age—from cultural exchange to advances in medical care—this massive network of communication has offered up new possibilities for opportunists and criminals to take advantage of our users and an easy willingness to trust in technology.

The solution to this threat is simple. Build the highest assurance into everything that’s connected. Public Key Infrastructure is that foundational assurance. A security and identity solution that’s reliable enough to protect the most sensitive data, but flexible enough to work on the latest-and-greatest things we invent. With PKI, the only thing we need to focus on is enjoying the benefits of a world that can communicate almost instantaneously across the globe—and even into space.

**PUBLIC KEY
INFRASTRUCTURE
IS THAT
FOUNDATIONAL
ASSURANCE.**





The expanding landscape of threats

Every day, we see new, ingenious ideas for using connectivity to build oversight, efficiency and safety into computers, apps and devices. But each new connection represents a new vulnerability, a potential entry point into anything that app or device speaks to.

The financial risks are well known. We've seen for years what happens when cyber criminals exploit a security gap. In 2017, a major consumer finance brand settled a lawsuit for a massive data breach, paying out \$700 million USD in damages². A Ponemon/IBM study, conducted in 2019, found that the average cost of a data breach was just shy of \$4 million³. And the same year, ForgeRock's Consumer Breach Report⁴ documented a \$17.76 billion loss in the healthcare sector. In fact, healthcare was the most targeted sector in 2019, experiencing 45 percent of all breaches.

While the financial cost to the healthcare sector is staggering in itself, the number and nature of the attacks is perhaps even more noteworthy.

These losses were spread across 382 separate breaches, targeting healthcare networks with a variety of methods. Where the norm used to be network and website hacks aimed at banks and consumer transactions, cyber criminals are now exploiting vulnerabilities in devices and under-educated users to extract value from pure information.

All of this means that organizations must deal with a greater security burden, even though resources have not increased as much as the threats. Digital charts, connected monitors and smart treatment tools are revolutionizing patient care, but the professionals using these devices aren't experts in security vulnerabilities, and IT departments must be nimble in order to negotiate the challenges that come with budget restrictions, new technologies and local or national regulations and laws.

It's an exciting and promising time for the world of information, and everyone from individual consumers to multinational enterprises and nations stands to benefit from technological advances in what we connect. But for the IT professionals behind the scenes, understanding the new threats that come with new technology, and deploying manageable solutions to eliminate risk, can be a daunting task.

To combat this increasing landscape of threat, security professionals need a flexible solution that's quick to deploy, easy to manage, and carries the capability to handle any attack, even while expanding or adapting to evolve as the needs of the organization grow and change. PKI checks every box, and more.



To combat this increasing landscape of threat, security professionals need a flexible solution that's quick to deploy, easy to manage, and carries the capability to handle any attack.

Big fish in a small pond

In July of 2019, news spread around the world of a massive banking data breach affecting 100 million customers⁵. It was another example of huge information theft at a global level.

But at the same time this breach was underway, cyber criminals were testing smaller targets for vulnerabilities, prying here and there to see where they could extract some sort of gain from places where security resources were thin. Increasingly, they found these kinds of vulnerabilities in small governments, where limited resources make it more difficult to secure all systems and users.

Rather than taking on billion-dollar enterprises, where IT departments are large and well-equipped, these criminals sneak into the networks of cities and towns, where they deploy ransomware to hold the local government hostage.

This is just what happened in June 2020, in Florence, Alabama. Situated on the banks of the Tennessee River on the northern border of the state, this town of 40,000 people is known for its annual Renaissance Fair, and for being the birthplace of blues pioneer, musician W. C. Handy.

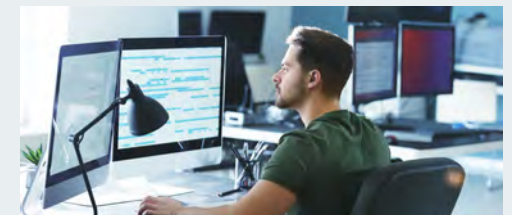
At the end of May, city officials got warning of a potential breach, but by then, it was too late. The criminal who hacked Florence's network appears to have gained access as much as a month earlier and had been working to seize the town's systems. On June 5, the hacker struck, demanding ransom in the form of bitcoin.

After consulting with security experts who were familiar with the habits of this serial criminal, the Florence government decided to pay the \$300,000. But Florence wasn't alone. Just four months before this successful breach, the New York Times reported findings that ransomware attacks rose 41 percent⁶ from 2018 to 2019, and dozens of cities and towns had been compromised.

While much larger data breaches grab the top headlines, a faction of criminals has carved out a lucrative scheme, hunting more vulnerable targets that are more likely to pay. These big fish in a small pond are taking advantage of communities by deploying sophisticated cyber-attacks against those who have the fewest resources for defense.

Unlike other security and identity solutions, PKI is flexible enough to work just as well for networks and email as for the web. PKI solutions uncomplicate security deployments by giving IT and security officers the capability to issue and manage encryption and authentication certificates across a variety of systems, devices and users.

The solution that already works for securing your websites can also secure your networks, devices, email, documents and users—preventing ransomware attacks while also simplifying your security ecosystem.



⁵ <https://www.capitalone.com/facts2019/> ⁶ <https://www.nytimes.com/2020/02/09/technology/ransomware-attacks.html>

WHAT YOU MAY NOT KNOW ABOUT PKI

The challenge in today's connected world is complexity.

If it isn't the challenge of more complex attacks, it's the challenge of securing complex ecosystems where old and new technologies interact. And if it isn't the challenge of more complex ecosystems, it's the challenge of securing a system where users aren't always up to date on more complex, sophisticated threats.

Security consultants and analysts hear the same concerns from IT and security professionals around the world—they need a solution that's simple to set up and manage, and one they can definitively trust.

Enter public key infrastructure.

If you're familiar with internet security, you already know about PKI. You've probably known about it for a long time, because PKI has been the trusted website security solution for two decades—first in the form of SSL and now TLS. It works today with the same proof of trust it had twenty years ago.

But a lot of people are surprised to learn PKI doesn't just protect the web. It also protects applications. It protects code. It protects smart watches, cars, contracts, hospital beds and satellites. The security solution that's been tested and proved reliable for two decades on the web turns out to be just as reliable in the newest and most innovative connected inventions.

PKI is proven

Despite the fact that the connected world is evolving every day, PKI has proven to be just as effective in securing today's latest IoT devices as it was in securing the encrypted world wide web twenty years ago.

The genius of PKI is the simplicity of key pairs using asymmetric encryption. In asymmetric encryption, one party can secure data and transmit it to another party without sharing a common secret. Cracking the code for any one key doesn't solve for encryption on the other key. It takes both keys in the encryption pair to read the data.

The result of this is trust that's proved to be reliable over and over again for decades.

PKI is flexible

In today's ecosystems, professionals need to be able to secure a website alongside an application, or securely sign a document while authenticating an employee's smart phone. One company needs a solution for automated robots on the manufacturing line while another needs to protect its customers' credit card numbers. A solution that works one way but not another, or one day but not the next, not only burdens the IT team responsible for managing security, it also puts the organization at risk.

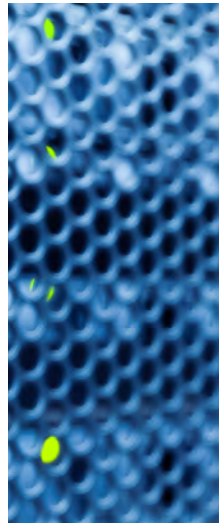
Unlike other types of security solutions, PKI is incredibly flexible. Because it relies on asymmetric key pairs, and the security process can validate just as easily as encrypt, PKI can be deployed in any number of environments to secure a wide range of connections. PKI solutions can scale down or up, run in the Cloud, on-prem or hybrid, secure web and email today, then BYOD and IoT tomorrow. It's one solution for any number of security needs.

PKI delivers public and private trust

More than just simple encryption, PKI binds identity to a key through a signing process. The signature is issued by the root, so anyone with the public key to that root knows the signature bound to the PKI certificate is valid and trusted.

In some cases, that root is public—it's been distributed to a trust store housed by a web browser like Chrome or Firefox or an operating system like Microsoft Windows or Apple macOS. In other cases, the root is private—trusted by whatever systems an organization wants to use internally or within a small group of companies. The cryptography is the same either way, but the ability to deploy both public and private options makes PKI especially versatile.

As a result of this flexibility, PKI bridges the gap between public and private trust. It's powerful and secure enough to be trusted as the private encryption and identity solution for many nations' governments, and equally as the public solution for consumer IoT devices.

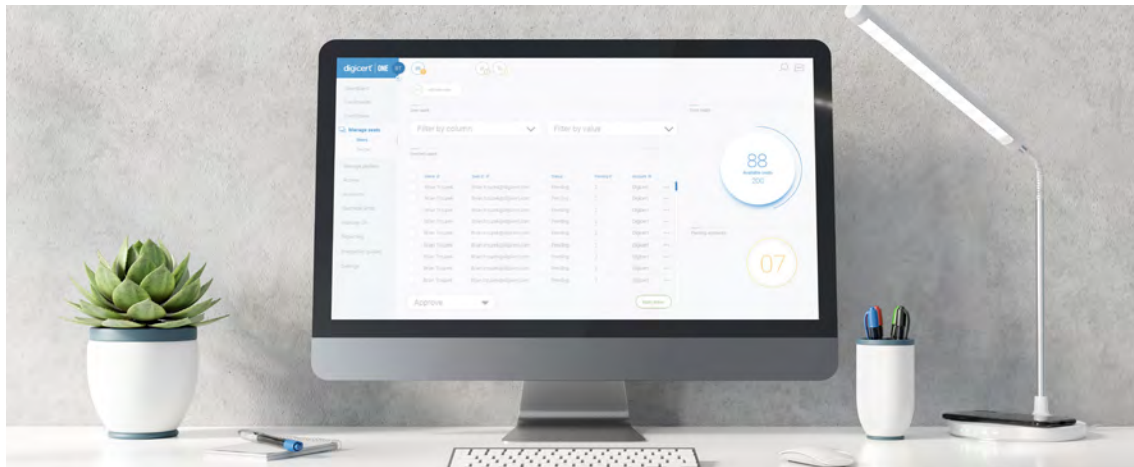


PKI can be easy

In the past, PKI was complicated. Without access to experts and simplified management platforms and tools, individual IT professionals had to take on the risky prospect of developing PKI solutions in-house, without the specialized knowledge required for proper deployment. Its reliability made PKI the ideal solution—once it was running—but getting there used to be challenging and often resulted in more problems than it solved.

Thankfully, those days are long past. Today, PKI can be simple to set up and use, if it's

done properly. Sophisticated tools for deploying and monitoring PKI solutions now run in a single sign-on platform. And because PKI is so versatile, it's easy to run solutions for many different security challenges in one place. Instead of dealing with the complexity of building a PKI solution for one use, now you can deploy and manage multiple security solutions in one place—and you don't need any expertise to stand up and run your PKI environment.



4 misconceptions about PKI

People still use PKI?

What's old is new again. Not only is PKI still in use, it's now in a state of evolutionary growth. The value of PKI is its flexibility, combined with its long history of trust. As engineers find more and more connections where PKI offers the best solution, they can deploy PKI security and identity knowing the technology has a proven history of robust protection.

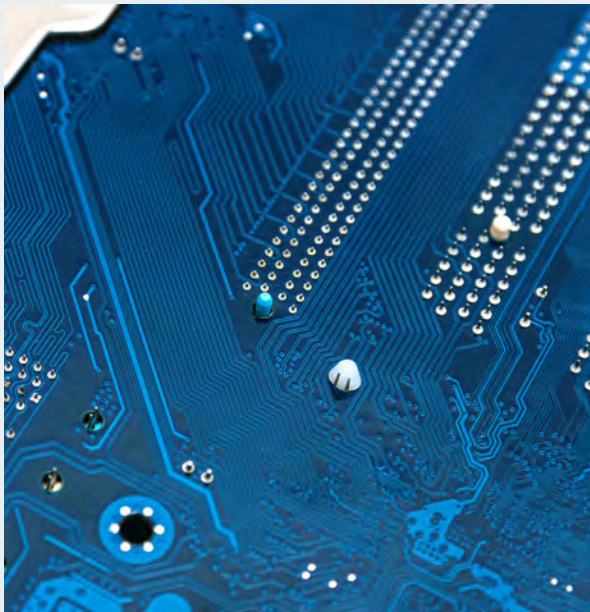
What about that Chrome issue? Isn't PKI broken?

PKI's track record is incredibly strong where security is concerned. How it's deployed, though, depends on the body issuing the certificate. In 2017, Google announced⁷ it would begin to distrust a series of certs issued by Symantec, because those certificates were out of compliance with CA/Browser Forum Baseline Requirements.

It's an unfortunate example of lapsed business practice, and the repercussions were widespread. Reacting to the possibility of a massive gap in worldwide security, Symantec and Google began seeking a Certificate Authority that held the level

of trust and infrastructure needed to manage a massive reissuance. They decided on DigiCert and arranged to move the Symantec certificates over to the trusted DigiCert roots, so Chrome users wouldn't experience any disruption in access to PKI-secured websites.

Today, just as twenty years ago, PKI remains the trusted solution for securing web communication, even on Chrome.



PKI doesn't work on a lot of devices.

It would be more accurate to say that PKI works on any device that has the power to run it. Asymmetric key pairing requires enough processing speed, memory and disk space to perform the action. Of course, PKI has been in use for more than twenty years, so if the processors of the late Nineties could handle key encryption, it would stand to reason that any recently built device should have the power to run PKI. But in some cases, even with the advances in microprocessors, the performance characteristics of IoT devices are so rudimentary, they may not be able to rapidly generate the keys or sign the communications channel.

Fortunately, PKI experts have come up with clever workarounds that don't compromise security. These solutions reduce the contents of the PKI certificates, so they fit into the small bandwidth and simple processing on a number of IoT devices. There are also software vendors who provide key generation or CSR generation systems for low-powered devices.

Moving forward, there will be fewer devices with PKI compatibility issues. New manufacturing

processes allow device makers to inject keys into the silicon, so security is embedded at an early point in the supply chain. Silicon injection not only solves compatibility issues, it also speeds up manufacturing while strengthening security and identity on devices throughout the full lifecycle.

Isn't PKI just SSL for web?

If you've been around the world of connected security for a few years, you probably know PKI as Secure Sockets Layer protection, or SSL. SSL goes back to 1995, when its first functioning version acted as the cryptographic protocol for Netscape. In 1999, SSL was deprecated to its similar successor, Transport Layer Security—TLS. To this day, TLS remains the trusted encryption protocol for the web.

TLS/SSL is PKI's most widely known implementation, but it's only one of dozens of uses. In reality, PKI is everywhere, used reliably in just about every type of connection the world has invented. In fact, PKI now secures all sorts of things that hadn't been imagined when the Netscape team launched SSL a quarter century ago.

THE PROOF OF TRUST IS ALL AROUND

Even the engineers and security experts who build PKI solutions are often amazed by the creative ways people use PKI to secure what they've invented. Like a thread woven through seemingly disparate technologies and unrelated industries, PKI shows up in some of the most surprising places. No matter the use, though, at the heart of each and every case is the need for one thing—uncompromising trust.

CASE STUDY ONE

AeroMACS

Trusted when the stakes are high

A commercial jet pilot has access to more connected sensor data today than Astronauts Young and Crippen used to de-orbit the *Columbia* during the space shuttle's inaugural mission in 1981.

But just as the human factor was crucial in the shuttle forty years ago, it remains crucial today. The person with their hand on the stick needs to have as much accurate information as possible to safely park that massive machine on the ground.

The majority of air travel accidents occur near takeoff and landing. It's here that the plane is most vulnerable to the forces—human and natural—that affect the complicated act of coaxing 60 tons of metal, fuel, luggage and passengers into the air. A wind shear, a timing miscue, the loss of visibility.

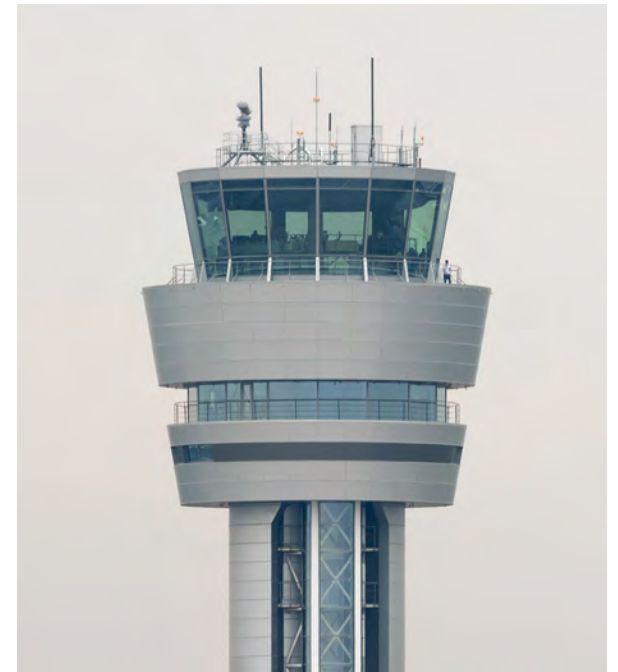
During takeoff and final approach, airline pilots use vital information, gathered from sensors and relayed through cockpit readouts and tower technicians, to make the adjustments needed for safe air travel. Since 2016, that vital information has been transmitted to towers and planes around the world by aircraft IoT sensors secured by PKI.

The majority of air travel accidents occur near takeoff and landing. It's here that the plane is most vulnerable to the forces—human and natural—that affect the complicated act of coaxing 60 tons of metal, fuel, luggage and passengers into the air.





SINCE 2016, VITAL INFORMATION HAS BEEN TRANSMITTED TO TOWERS AND PLANES AROUND THE WORLD BY AIRCRAFT IoT SENSORS SECURED BY PKI.



Doing more with less

The number of planes in the air is expected to double by 2025. More and more planes, more and more flights—in fact, the Beijing Capital International Airport saw a 5% increase in passengers from 2017 to 2018, and Dallas Love Field in the United States experienced a 90% increase in passengers between 2010 and 2020.

AeroMACS IS A BROADBAND, HIGH CAPACITY WIRELESS DATA LINK THAT TRANSMITS IoT SENSOR DATA FROM AIRPORTS TO CONTROL TOWERS AND PLANES.

While new airports are being built around the world, existing destinations dealing with more flights have only one solution—increase the efficiency of their air traffic coordination and ensure the integrity of landings and takeoffs.

What is AeroMACS?

Aeronautical Mobile Aviation Communication System (AeroMACS) is a broadband, high capacity wireless data link that transmits IoT sensor data from airports to control towers and planes. From temperature and wind gauges to flight information display systems—even baggage handling—if it's part of the Airport Surface, the device data is communicated through AeroMACS.

AeroMACS isn't just widgets. It's the eyes and ears on the ground. It's integral to coordinating flight plans and schedules. It's at the heart of airport operations. If compromised, someone could use AeroMACS to feed false information to the plane and pilot. And with so many flights and even more passengers, securing AeroMACS information against tampering is a critical to ensuring planes take off, fly and land safely.

Add PKI to the before takeoff checklist

In industries with complex ecosystems, where there are a lot of connecting parts with limitations on the power of devices and variation amongst the

types of devices, there's a need for an adaptable, reliable security solution. In the case of air travel, all these factors come into play, but there's also a need for data confidentiality. The information transmitted between ground and plane must be secured, just as the device itself must be secured, in order to prevent what could be catastrophic tampering.

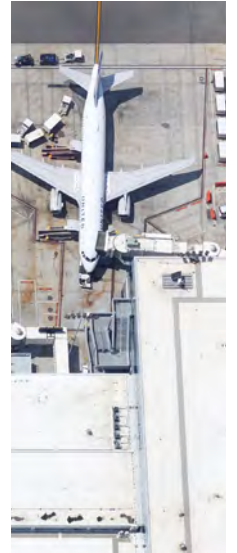
With PKI protecting these devices and the data they transmit, pilots and towers can safely and securely gather, communicate and use a variety of information to ensure planes take off and land safely, regardless of the plane or the airport. If it's on AeroMACS, it works the same—and just as reliably—in a small airport in the United States as it does at a major airport in Australia.

Deployment: worldwide

PKI solutions protect the AeroMACS network, the standard for aeronautical communication that will soon be used by nearly every airport around the world.

Primary need: trust

With thousands of flights in the air, airports, airlines and pilots rely on AeroMACS to guarantee the safe and on-time travel of millions of people every day.



AUSTRALIA GATEKEEPER

Trusted by governments to protect citizens

Most Australians probably aren't aware of the security and identity solution that protects their information and many of the most important transactions they undertake. If you've recently purchased a house in Australia, you've used Gatekeeper. If you've imported goods, you've used Gatekeeper.

Now in its third decade, Gatekeeper Public Key Infrastructure Framework "governs the way the Australian Government uses digital keys and certificates to assure the identity of subscribers to authentication services." From important legal documents to contracts and border protection to banking, many of the most sensitive public areas of trust are encrypted and authenticated with PKI solutions.

Securing an entire country

At the end of the last century, the Australian government began looking for a mechanism that could reliably protect the information filling up more and more digital documents and transactions. At first, individual agencies deployed home-grown solutions, but they quickly discovered that internally managing security to a high standard was difficult, time-consuming and risky.

As a result, the framework commission defined a solution that could keep up with the need to secure an entire nation while minimizing the time and resources needed to manage the ecosystem. Today, the Gatekeeper framework "delivers integrity, interoperability, authenticity and trust between government agencies and their customers."



**IN AUSTRALIA,
TRUST IN PKI IS A
MATTER OF NATIONAL
IMPORTANCE, AND
PKI DELIVERS.**



Always on—even when you can't see it

Oftentimes, it's the technology we don't see that makes the biggest impact in our lives. Electrical grids. Water pump systems. Banking networks. We often take for granted the importance of reliability in these behind-the-scenes systems. For Australians, Gatekeeper is one more system that must be reliable. In addition to creating efficiencies and convenience, it rests at the heart of many vital government functions. Without the strong security PKI offers, the personal information of millions of Australians would be exposed to theft, important transactions and legal processes would be slowed or stopped and government agencies that control customs and investments would be open to compromise. In Australia, trust in PKI is a matter of national importance, and PKI delivers.



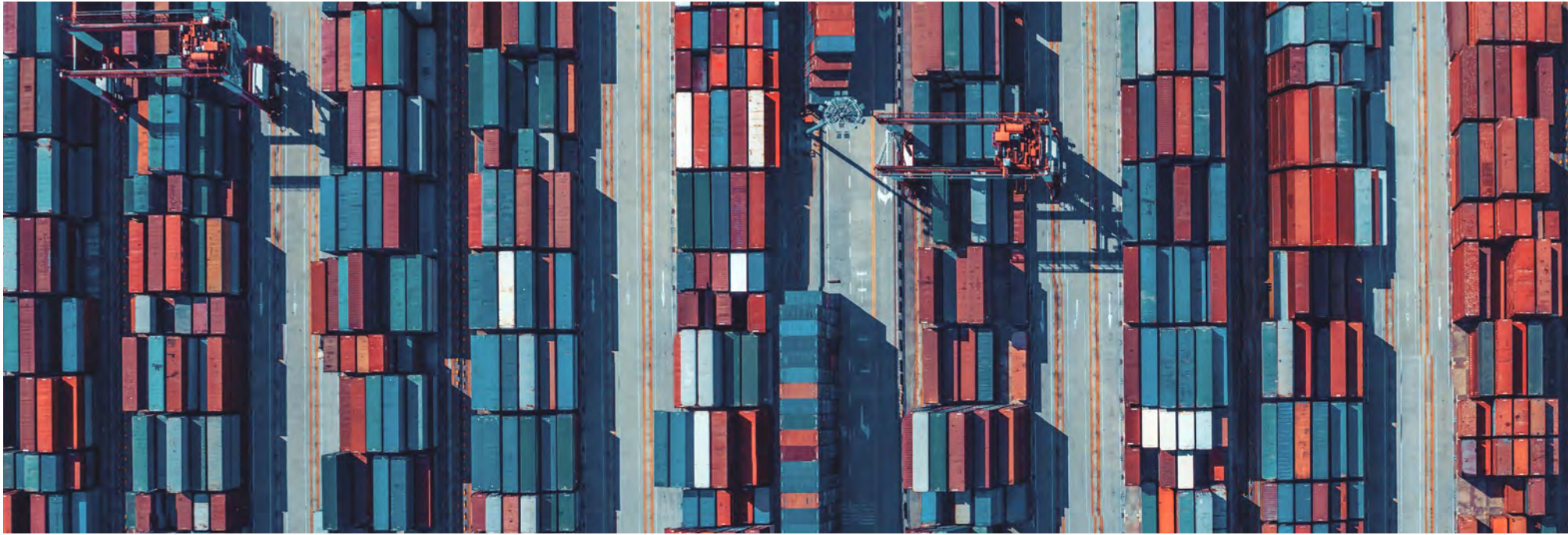
IT NEEDS TO WORK EVERY TIME AND ALL THE TIME.

Deployment: Australia

A nationwide security and identity solution, running across multiple government agencies and protecting many of the most sensitive public trust spaces.

Primary need: integrity

From banking to land ownership to border security, there's no room for lapses or compromises. It needs to work every time and all the time.



CASE STUDY THREE

WORLDWIDE SHIPPING

Trusted at global scale

Imagine trying to locate a single shipping container—one of millions—as it travels from one port to another, between continents and across oceans. Now, imagine trying to locate that single shipping container using databases and cargo logs.

The global supply chain is like a complicated clock—each cog, spring and wheel needs to be in its place, working as designed, for the mechanism to function. Shipping delays slow down the entire chain. Missing shipments can break the chain and cost companies money—both in the loss of materials and the loss of revenue.



More than 11 billion tons of goods move by sea every year.

Today, there are more than 50,000 container ships worldwide.

A digital line-of-site

More than 11 billion tons of goods move by sea every year. Today, there are more than 50,000 container ships in the world. The scale of ocean commerce is massive, but it's also dynamic. The movement is constant, with freighters dotting the globe like a map of a starry night sky.

For as many ships as there are on the water, there are even more containers. Locating and tracking each of these containers in real time—and securely—is a massive undertaking.

The challenge with shipping at this scale is to mutually authenticate devices in the field to the Cloud, where assets are tracked. If compromised, the shipping company can lose sight of the location of the containers, or false information about the containers can be sent to the company. In order to be effective, a security solution must not only secure the device, but also the information in transit. It also needs to be scalable, capable of securing tens of thousands of devices at once without fail.

Any lane, anywhere in the world

With PKI authentication, shipping containers can be securely tracked throughout the length of their journey from launch to the port of destination. And, because there's a need on the shipping side to build more devices and secure more shipments every year, the need for increasing volumes of security increases every year. With PKI's scalability, the supply meets the demand.

As a result, no matter the number of shipments, the data is secured and the containers are tracked, regardless of where they are in the world. This means decreases in the chance of theft or loss, and it helps to ensure efficient movement of goods from port to port. The supply chain is uninterrupted, and businesses and consumers alike enjoy the benefits of higher availability of goods at lower costs.

Deployment: worldwide

At the heart of the global supply chain, connected shipping containers move goods and materials to every continent on the planet.

Primary need: authentication

More than simple tracking, PKI solutions deliver real-time, secured authentication so the company can locate and identify the device attached to each shipping container.

WITH PKI, SHIPPING CONTAINERS CAN BE SECURELY TRACKED THROUGHOUT THE LENGTH OF THEIR JOURNEY.

GLOBAL WORKFORCE

Trusted at global scale

Oftentimes, it's the largest companies that face the biggest challenges. In fact, sometimes the size of the company is the challenge. For instance, how does one organization secure individual users who are not only working in different roles in different offices all around the globe—but also on different devices using different operating systems and applications—many of them BYOD?

For one company, this wasn't just an intellectual exercise. It was a real problem. And that problem affected half a million employees.

Bring your own anything

Authenticate, identify and secure over 500,000 users.

Here, the term “flexible and scalable” couldn't just be a theoretical description—it needed to be the real-world function of a working PKI solution. But even as the number of users presents a challenge,

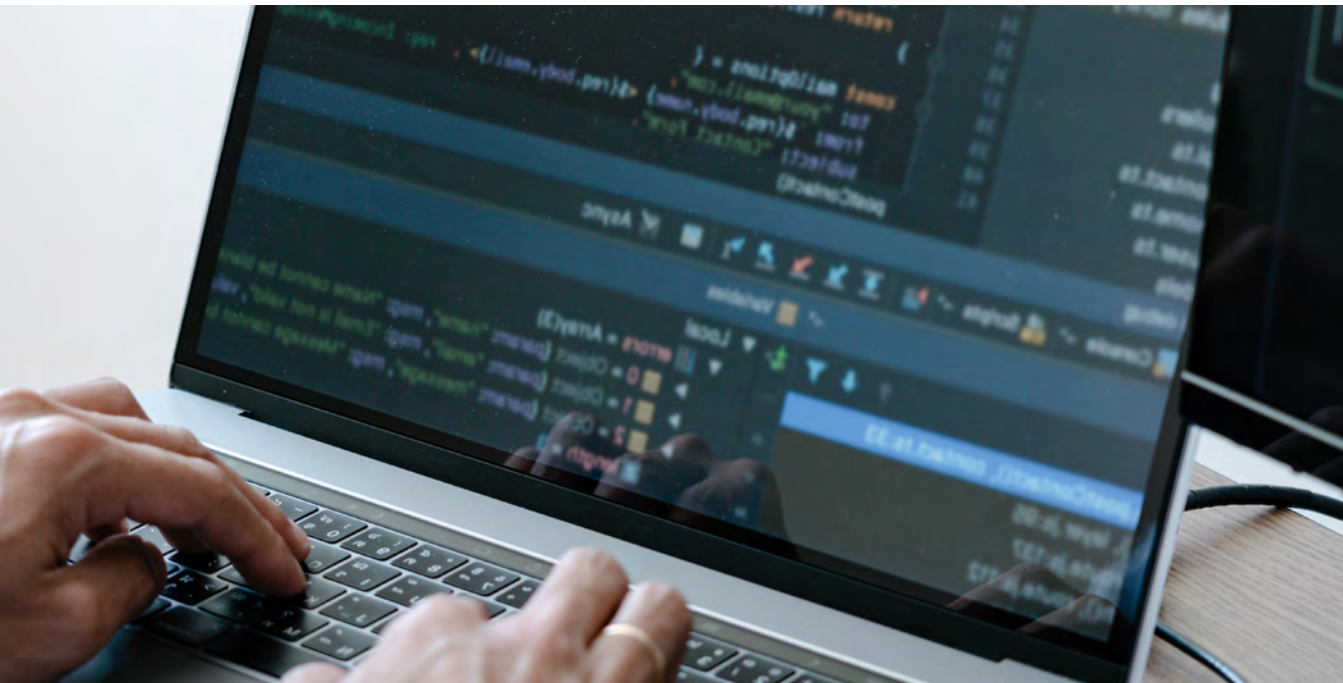
the number of types of devices and applications those users run and bring to work presents an equal—if not greater—challenge. A company-owned laptop. A personal smartphone. An old iPad. If you want to give your employees, vendors and contractors the flexibility to use the devices that make their work easiest, but you don't want to introduce vulnerabilities into your network, you need a security solution that's adaptive but robust.

PKI is not only flexible, it scales. Meaning public key infrastructure can not only authenticate any number of devices, regardless of who owns them or what they're running, it can also simultaneously authenticate multiple devices for hundreds of thousands of users, no matter where they are. To the users—all 500,000 of them—it's entirely seamless.

Trust means reliability

For more than a decade, PKI identity solutions have delivered uninterrupted services in more than 170 countries in one enterprise alone.





PKI IS NOT ONLY FLEXIBLE, IT SCALES.

As much as there is a need for trusted security, there's a need for reliability. At this scale, Software-as-a-Service authentication must be robust enough to work all the time, everywhere. 24 hours a day, 7 days a week, all around the world, hundreds of thousands of users gain secure access to their company network, regardless of the device they're using. It's safe and seamless, so they don't have to think about it, and the company doesn't need to worry about vulnerabilities.

Deployment: worldwide

Thousands of offices located across the globe run the business of a longtime global leader in hardware and software.

Primary need: flexibility

With critical operations on the line, PKI delivers a solution for authenticating, securing and identifying half-a-million employee users spread all around the world.

HEALTHCARE

Trusted when lives are on the line

For most of us, a connected component offers a bonus, a perk. A Bluetooth connection allows us to check the current temperature and humidity on the back patio. A Wi-Fi connection between an iPad in the kitchen and a smart TV in the living room lets us pick up an episode where we left off while getting dinner in the oven. Connected is something we want, but most of the time, it's not something we need. In some cases, though, a connection doesn't just offer a bonus or convenience. For some people, connected is the difference between life and death.

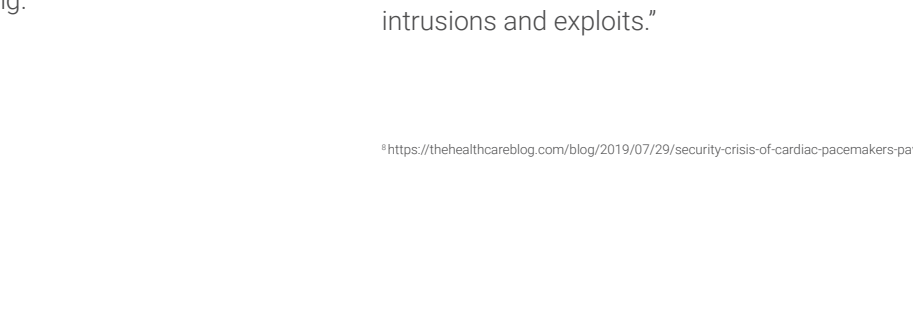
A few years ago, medical engineers unveiled a new form of pacemaker. This particular model was "smart." By connecting via Bluetooth to an external monitor and app on the patient's phone, the pacemaker could not only deliver the electrical signals needed to keep the heart running, it could also tell the patient and the doctor how the pacemaker is functioning.

Is the pacemaker working the way it should? How's the battery life? This data used to require a visit to the hospital, and sometimes surgery to determine or correct. Now, it could all be monitored, recorded and communicated automatically and continuously.

Connected pacemakers are not simply a convenience. Thousands of people rely on their device to keep them alive. But as with any connection, there's the possibility of interference. As with any other IoT device, a connected pacemaker needs secure end-to-end encryption.

When "life or death" is literal

In August 2017, an unusual headline⁸ hit the newswires—unusual, at least, for anyone who doesn't work in the IoT world. The United States Food and Drug Administration was recalling a number of pacemakers due to a cybersecurity threat. In what sounded like another story about internet hacking risks, the FDA warned that certain pacemakers might "be vulnerable to cybersecurity intrusions and exploits."



**COULD A HACKER
REALLY BREAK
INTO SOMEONE'S
PACEMAKER AND
CAUSE IT TO
STUMBLE OR
FAIL ENTIRELY?
YES.**



It was a strange idea, something that sounded like the plot of a science fiction movie. Could a hacker really break into someone's pacemaker and cause it to stumble or fail entirely? Yes.

As medical device manufacturers invented novel and valuable ways to connect patient care tools—from smart hospital beds to continuous glucose monitors—the patient benefits were skyrocketing. At the same time, concerns over the protection of patient data collected by connected devices, and eventually, concerns about intrusions leading to device failure, were also mounting.

Indeed, hackers found just such an intrusion point with pacemakers. The manufacturers built symmetric key encryption between the pacemaker and the bedside monitor, but the monitor itself wasn't secured. With access to the monitor, these hackers were able to send repeated commands to the pacemaker, depleting its battery life. Even worse, they could instruct the pacemaker to shock the patient. Searching for an answer to protect not only the device but the safety of the patient, many manufacturers turned to PKI.

The value of PKI in medical devices is not only its long history of strong encryption. It's also the value of built-in identity.



**A SECURITY SOLUTION
THAT PROTECTS THE
INTEGRITY OF THE
DEVICE AND PATIENT
DATA, AND ONE THAT'S
RELIABLE ENOUGH TO
TRUST WHEN LIVES
ARE ON THE LINE.**

Medical devices will get smaller, and smarter, but the security solution that will continue to protect the data—and the life—of the patient will be PKI.

PKI makes it easy to secure device data while at the same time, authenticating those devices with encrypted ID. This means a device can be secured during manufacture, and that security can be handed off to a hospital, and then eventually to the patient, and even though the device itself has moved through different phases in its lifecycle, and the people monitoring the security of the device has changed, that security remains intact and uninterrupted the entire time.

The future of medical devices is even smarter

Recently, there have been new funding and health agency approvals for R&D into smaller, even more sophisticated devices. Leadless pacemakers are now in use in the real world—small enough to be inserted through a femoral catheter and implanted directly in the heart, eliminating the need for more invasive surgery or electrical leads which can wear out as the heart tissue flexes over millions or billions of beats.

The next wave of pacemakers will also be leadless, and they will be smarter. Connected to small defibrillators, they will not only monitor the health of the device, but also the health of

the heart, capable of telling the defibrillator over Bluetooth to deliver a shock if the heart is failing. They will send data to the patient's cardiologist, and they'll be capable of real-time adjustments, without surgery, so the patient's heart health can be perfected without any procedure, while they sit in their living room.

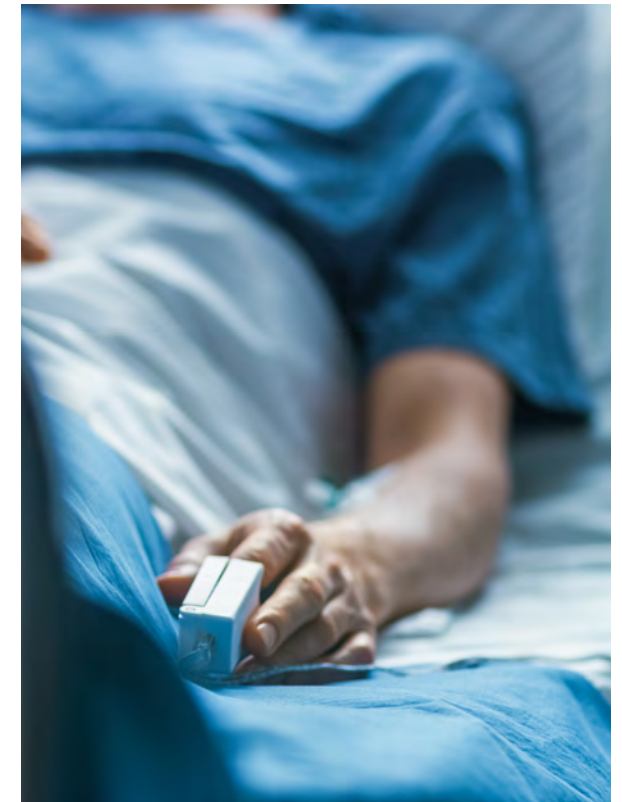
Today, thousands of people enjoy peace of mind knowing there's an effortless, secured monitoring system, working to ensure their pacemaker continues to function, and alerting them of any potential issue. In the near future, the capabilities of cardiac technology will grow, offering more patients and their doctors more options for better data and immediate assistance without surgery or hospital visits. The medical devices will get smaller and smarter, but the security solution that will continue to protect the data—and the life—of the patient will be PKI.

Deployment: multiple countries, worldwide

Thousands of hospitals and care centers, and millions of people, across differing compliance and implementation standards, for use by providers and patients alike.

Primary need: reliability

A security solution that protects the integrity of the device and patient data, and one that's reliable enough to trust when lives are on the line.



WHAT YOU DON'T KNOW CAN HURT YOU.

Yes, PKI is trusted—and it has been for decades. But that trust relies on expertise. After all, if a PKI solution is improperly deployed, the vulnerabilities can pose as big a risk as an unsecured system.

Because PKI has been around for so long, engineers and computer scientists have had a long time to study how it works in the real world. There are examples of smart, innovative deployments, and there are cases of failed attempts, where design mistakes or mismanagement have led to lapses in what is otherwise a nearly perfect system.

Every time PKI is deployed, there's another opportunity to see how it works, especially if that deployment is in a novel environment or attached to a new technology. And every time something goes right, PKI engineers learn more about the smartest and safest way to use the technology.

A few things security experts know today about PKI

Proper key protection

PKI is only as good as the private key used to sign the certificate chain. This is generally a key for the Root Certificate Authority and for the Issuing CA (ICA). If either—or both—of these keys are generated or stored in an insecure manner, the PKI certificates issued are not very trustworthy. This can happen in enterprise, for example, if an IT professional creates keys in clear text on a server they manage using software downloaded from the internet, then transfers those keys to their CA running on the network so there's a backup. In this case, the PKI system is extremely insecure, because the keys—which were never protected—can be easily stolen. Only proper protection ensures the entire PKI hierarchy is trusted.

Certificate status

PKI systems should provide a means for a device or browser to determine if the certificate is still valid and usable. When PKI isn't properly deployed, the hierarchy is often missing the information needed for revocation, or that information is missing altogether. In some cases, the system isn't properly managing the requests when the information is present and correct. Regardless of the cause, the result is an untrusted system.

Improper configuration

In addition to proper systems setup, configurations within the certificate or certificate chain often require specific configurations for PKI to protect software and hardware. In the case of “roll-your-own” deployments, it's not unusual to find workaround configurations that solve a problem for one instance while leaving the certificate open to other risks for bypassing, impersonation or misuse.



**YES, PKI IS
TRUSTED—AND
IT HAS BEEN FOR
DECADES. BUT THAT
TRUST RELIES ON
EXPERTISE.**

4 mistakes to avoid when setting up PKI encryption

Failing to plan for future iterations

Oftentimes, when a security officer sets up home-grown PKI solutions for their organization, they fail to account for changes that occur over time. As organizations evolve, as business goals shift, as new products or new teams come online, a PKI solution that isn't adaptable, or one that wasn't constructed to allow for new deployments, becomes obsolete—or worse, a liability.

Trying to manage a PKI ecosystem in house

The simplicity of PKI's reliability can be deceiving. Yes, it's flexible, scalable, fast and reliable—but only if properly integrated and deployed. Internally built solutions often end up being unwieldy, resource-consuming security measures. Without expert installation and powerful oversight, it becomes difficult to track where PKI is implemented, the status of the PKI, and where they might be lapses or gaps. Managed PKI and centralized platforms solve for these issues, eliminating the need to put an unnecessary

amount of time into monitoring, and ending worries about security failures, stray keys, or user mistakes.

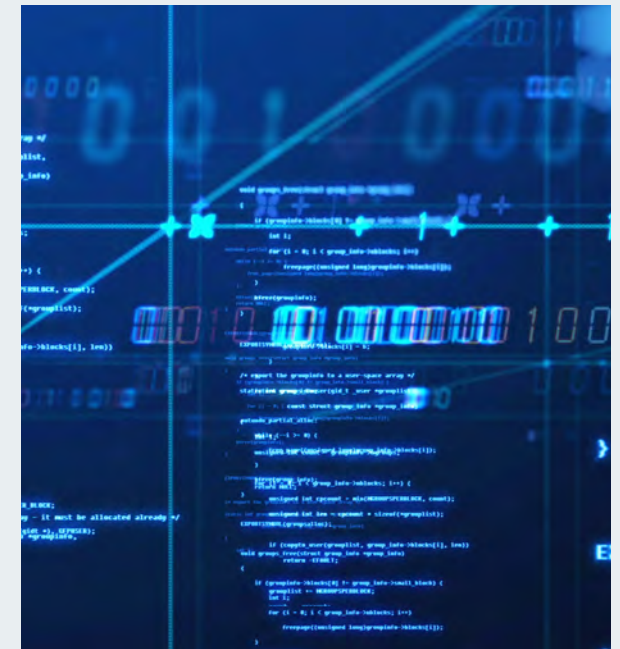
Building PKI without compliance

One the hallmarks of PKI—and one of its greatest benefits—is the power of flexible deployment options. There are a number of models, from on-premises to Cloud. It's not only important to know which option is the best for an organization's business, security and user needs, it's also important to understand which option delivers security in compliance with local, regional or national regulations. It's also important to understand how the PKI solution fits into the larger security strategy for an organization and an industry.

Failing to prepare for the upcoming PQC revolution

Post-quantum computing is quickly moving from science fiction to the new, living reality of technology. Along with the advantages of quantum computing, there are dangers. But the full extent of the power to use quantum computers to break mathematically impossible codes is still unknown. One of the mistakes a

security professional can make is waiting until quantum computing is here before preparing their environment for potential threats. Solutions that lay the foundation for securing systems in the world of Post-Quantum Cryptography already exist, and savvy security officers know it's important to begin learning about and testing systems that will protect assets after quantum computing becomes the new reality in daily life.



CONCLUSION

RETHINK WHAT YOU KNOW. THIS IS MODERN PKI.

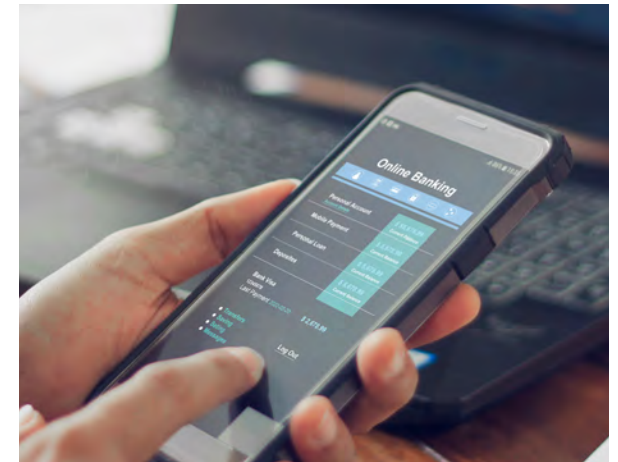
How can a decades-old technology, with a reputation built on reliability, become new again? The answer is not in a change to the technology, but rather a change in the way the world uses the technology.

PKI works. It has proven itself a trusted solution for security and identity going back as far as Netscape and 33.6k modems. While there have been updates to protocols and minor modifications, keeping up with changes to other parts of the computing world, PKI of today is fundamentally no different from PKI of yesteryear.

But in 1996, the people working with PKI were thinking about protecting search results on Excite and making safe purchases on eBay. To a large extent, many people still think along these lines when they think about PKI today. Yet, many don't realize modern PKI is securing trains to prevent crashes and protecting people by stopping

hackers from stealing personal information from their smart watches. And meanwhile, it's still encrypting eBay.

Modern PKI has evolved as technology has evolved, and it has expanded to fill security needs all around the world, in all types of industries and organizations, governments and in the home. In the end, the role of PKI in emergency rescue beacons is perhaps no less powerful than the fact that every day, PKI ensures that millions of people complete online banking transactions and nobody steals their debit card number. In either case, the importance of that trust cannot be understated. PKI is the perfect marriage between tried-and-true technology and a solution that delivers security and identity to the things people are inventing today and dreaming up tomorrow. Regardless of what comes next, PKI will continue to deliver proven, flexible trust.



**MODERN PKI HAS EVOLVED AS
TECHNOLOGY HAS EVOLVED, AND
IT'S EXPANDED TO FILL SECURITY
NEEDS ALL AROUND THE WORLD.**

Know someone who is using PKI in an innovative way? We'd love to showcase them. Interested in learning more about DigiCert PKI solutions? We'd love to help. PKI_Info@digicert.com

About DigiCert

The better way can't become common practice until someone finds it.

At DigiCert, building a better way to secure the internet is the single-minded pursuit that goes all the way back to our roots. That's why our TLS/SSL certificates are trusted everywhere, millions of times every day by 89% of the Fortune 500, 97 of the 100 top global banks, and for 81% of global e-commerce. It's why our customers consistently award us the most five-star service and support reviews in the industry. It's why we're modernizing PKI by building the DigiCert ONE platform and management tools to help enterprises and governments secure identities, access, servers, networks, email, code, signatures, documents and IoT devices. In SSL, IoT, PKI, and beyond—DigiCert is the uncommon denominator.

