DIGITAL TRUST FOR THE REAL WORLD

digicert®

TABLE OF CONTENTS

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 on board, headed for a sightseeing 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 roads. An aerial rescue team was needed to get everyone out of the wreckage and take them back to safety, but in this remote area, there was no cellular service and radio range was severely limited.

Fortunately, the plane was connected to the Iridium satellite constellation, orbiting five hundred miles overhead. An emergency beacon transmitted a distress call and the plane's location to rescue authorities using a secured digital signal. 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 trail of every moment of the flight. This was possible because each one of the 66 Iridium satellites maintains a digital link between devices and each other, ensuring device visibility and communication at any time, anywhere in the world—from Antarctica to Alaska.

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 Media 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."

We tend to think of digital interactions in terms of things we do on a computer or a smart phone, like shopping, email, or applications. But in today's world, the line between digital and real has become blurred. Connections are everywhere, monitoring and powering vast amounts of data and countless numbers of devices all over the planet.

In these kinds of emergencies, when lives are on the line, a pilot needs to know the Iridium satellite network will track their flight and pick up the emergency signal for relay to a rescue team. It's a need that goes beyond website traffic and email communication, beyond typical definitions of connections and data encryption. These beacons must reliably connect and communicate all around the globe, functioning at a moment's notice under the direst of circumstances to save lives in the real world—which is why the Iridium satellite constellation is built on digital trust.

"DIGITAL TRUST IS CENTRAL TO THE SECURITY OF EVERY CONNECTED THING FROM THE BOTTOM OF THE OCEAN TO THE EDGE OF SPACE."

Brian Trzupek
Senior Vice President for Product, DigiCert

CHAPTER 1

THE REAL IS DIGITAL AND THE DIGITAL IS REAL

Today, everything is connected. From remote workforces to refrigerators, more and more of what we use and interact with connects to everything else. Devices are the internet, the internet is mobile apps, cars are computers, doctor visits are virtual, and entertainment is streaming content. In other words, the line between digital and real no longer exists.

In this landscape of ubiquitous connection, trust is the foundation that enables digital communication. Interactions between systems, devices, and users take on many forms and exist simultaneously in real and virtual spaces, woven throughout an increasingly complex global network. Traditional digital security is still important, but encryption alone isn't enough. For the real connected world to communicate and function, we need a much more flexible and reliable architecture, one which incorporates technology, standards, and practices into a comprehensive system of digital trust.

What is digital trust?

Digital trust is the framework, software, and practices that enable confidence between the digital world and businesses, governments, consortia, and individuals. At its core, digital trust responds to the needs of the connected landscape, defends against threats, and anticipates the growth and evolution of digital technologies. To do this, digital trust operates on four pillars:

A Body of standards

Leading experts and organizations that define the protocols, technologies, and identity requirements for digital trust. For example, the CA/Browser Forum defines standards for TLS/SSL certificates and a common framework to certify identities and encryption across the web.

Compliance and operations

Compliance is the set of policies and continuous audits that verify that operations are being conducted according to the exacting standards set by a governing body. Operations, with datacenters at their core, verify certificate status through OCSP or other protocols.

Certificate Lifecycle Management

Software that provides centralized visibility and control over digital certificate lifecycles for public and/or private trust within an organization.

Delivery across all ecosystems

Extension of trust into complex supply chains, across device lifecycles, into a content community's digital rights provenance, and any other space where an object connects.

REAL TRUST FOR THE REAL WORLD

The notion of trust between two points in a digital connection is as old as digital communication itself. But too often, there's been a disconnect between the technology and the ideal. The principles of trust have lacked harmonious hardware and software solutions, and vice versa. True digital trust is equal parts concept, processes, and tools. It's the point at which digital technology and the ideals of trust meet to deliver value and meaningful impact.

WE NEED AN ARCHITECTURE INCORPORATING TECHNOLOGY, STANDARDS, AND PRACTICES IN A SYSTEM OF DIGITAL TRUST.

CHAPTER 2

THE PROOF OF TRUST IS ALL AROUND

Even the engineers and security experts behind our solutions are often amazed by the creative ways people use digital trust. Like a thread woven through seemingly disparate technologies and unrelated industries, digital trust is at the heart of how we communicate, navigate, and work in the real world.

AVIATION

Smooth takeoff, safe landing

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.

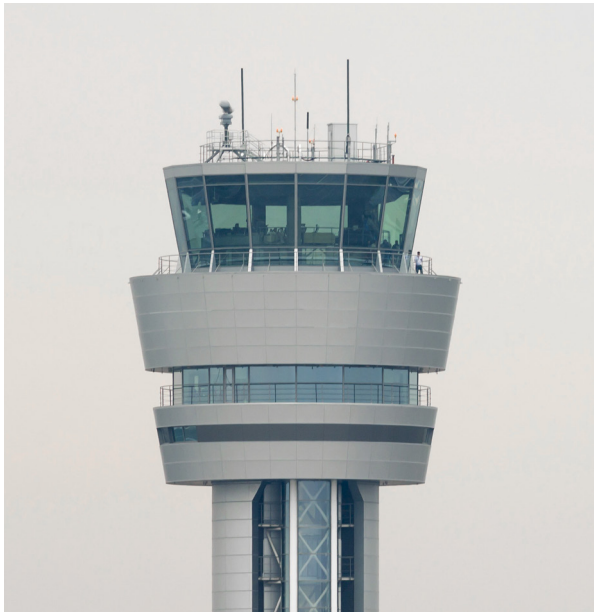
With digital trust solutions protecting these devices and the data they transmit, pilots and towers can safely and securely gather, communicate and use a variety of information to ensure planes take off and land safely, regardless of the plane or the airport. If it's on AeroMACS standard, it works the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

Deployment: worldwide

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

Primary need: authentication

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.



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

SUPPLY CHAIN

Identity for every link

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.

Digital line of sight

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 monumental undertaking.

The challenge with shipping at this scale is in mutually authenticating 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 digital trust, shipping containers can be securely tracked throughout the length of their journey from launch to the port of destination, no matter the number of shipments or 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.

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, DigiCert solutions deliver real-time, secured authentication so the company can locate and identify the device attached to each shipping container.

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

GLOBAL WORKFORCE

Any user, anywhere, any time

In some cases, managing the size of a company is as much a challenge as managing what that company produces. 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 IBM, this wasn't just an intellectual exercise. It was a real problem, one that they had to solve long before the COVID-19 pandemic forced countless more organizations into remote workforce solutions.

Bring your own anything

The task: 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 digital trust 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 present 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.

In this case, flexibility and scalability are crucial, and these attributes are fundamental parts of digital trust. Here, IBM was able to use digital trust solutions to authenticate any number of devices, regardless of who owns them or what they're running, while also simultaneously authenticating 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.

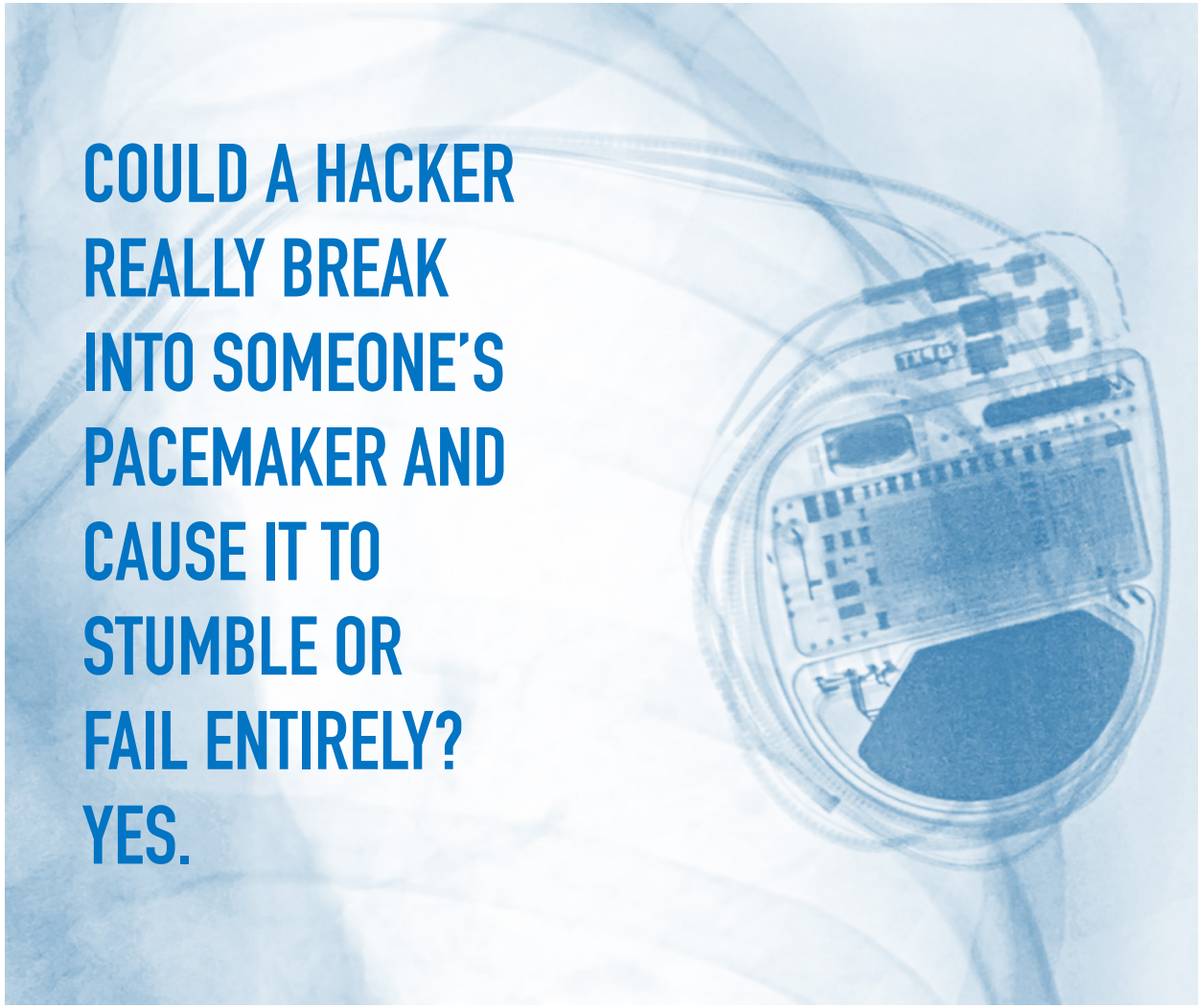
Deployment: worldwide

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

Primary need: flexibility and scalability

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.

AN ENVIRONMENT WITH CONNECTIVITY BETWEEN SYSTEMS, EMPLOYEES, VENDORS, AND CONTRACTORS NEEDS ADAPTIVE AND ROBUST SECURITY.



HEALTHCARE

Trust at the center of medical care

For most of us, digital devices offer convenience. 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. That connection is something we enjoy, but most of the time, it's not something we need. But for some people, that connection means 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. For people with these pacemakers, the need for digital trust is critical and very real.

When "life or death" is literal

In August 2017, an unusual headline 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." 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 medical devices—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 encrypted communication 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 digital trust solutions.

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 digital trust.

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.

CHAPTER 3

BUILT ON PROVEN TECHNOLOGY

Digital trust without underlying technology is simply a mantra. Deploying digital trust in the real world requires software and systems that enable secure connections across this vast and complex landscape. But not just any technology will do. For trust to work in the real world, connections need to possess certain qualities that run on proven security software and protocols.

The three principles of secure connections

Identity

Individuals, businesses, machines, workloads, containers, services, and anything else that connects must be authenticated with a cryptographically unique identity.

Integrity

Objects must be used and transmitted with tamper prevention, as well as tools for verifying that object hasn't been altered.

Encryption

Data must be secured in transit.

FOR TRUST TO WORK IN THE REAL WORLD, CONNECTIONS NEED TO OPERATE ON PROVEN SECURITY SOFTWARE AND PROTOCOLS.

PKI AS A FOUNDATION

Public Key Infrastructure has been proven for decades to secure websites. Over the years, as the connected world evolved, digital security experts realized that the same proven technology used to encrypt websites also verifies digital identity while authenticating data. And these certificates can be issued to nearly any digital object from networks to emails, code to documents, and even users and devices. By its very nature, PKI provides encryption, integrity, and identity to digital connections, which is why it stands as a fundamental component of digital trust—one ready to meet any challenge.

Flexibility

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 encrypt just as easily as validate, 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.

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.

PUT DIGITAL TRUST TO WORK

What's most important about digital trust is often what's overlooked. Digital doesn't mean digital anymore. At the heart of digital trust, we find something that's been the basis of business, agreements, social contracts, and simple human interactions going back millennia. Regardless of the space—physical or virtual—we need to know that our interactions are authentic, our communication is safe, and the information we exchange is legitimate and unchanged.

Digital trust is more than a high-minded idea, and it's more than security software. It's confidence in interactions between anything, or anyone, that connects. In that sense, what's important about digital trust isn't what it is, but what it does.

About DigiCert

DigiCert is a leading provider of digital trust, enabling individuals, businesses, governments and consortia to engage online with the confidence that their footprint in the digital world is secure.

DigiCert® ONE, the platform OS of digital trust, provides organizations with centralized visibility and control over a broad range of digital trust needs, including securing websites, enterprise access and communication, software, identity, content and devices. DigiCert pairs our award-winning software with our industry leadership in standards, support and operations, and is the provider of choice for leading companies around the world who put trust to work.

How will you put digital trust to work for your organization? To find out more, contact sales@digicert.com.