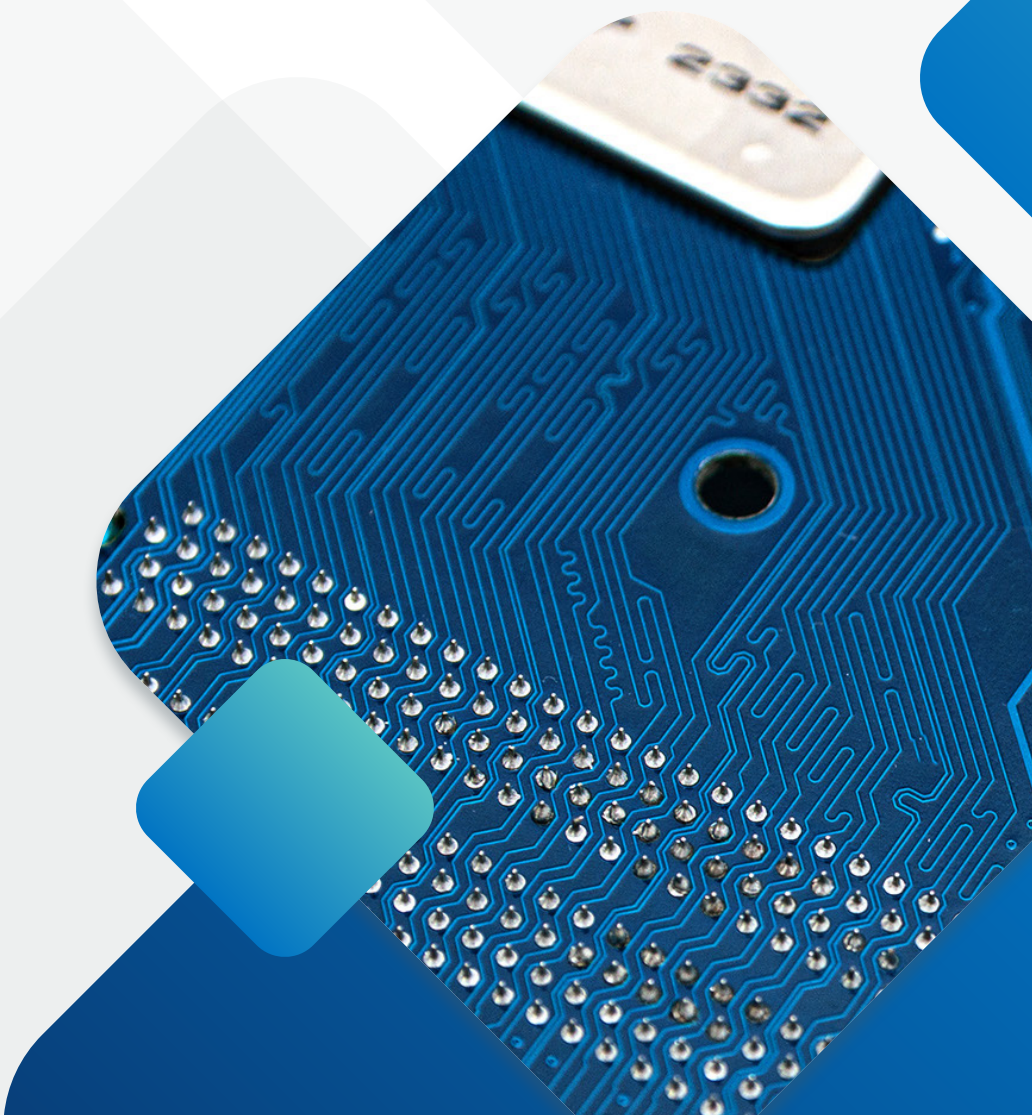
digicert®

ST Case Study

A world leader in hardware provides trust with software signing



WHITE PAPER

A World Leader in Hardware Provides Trust with Software Signing

A leader in chips and processors

STMicroelectronics is a multi-national electronics and semiconductor manufacturer, engineering chips that combine the latest advances in performance, intelligence, and efficiency for products that make a positive contribution to people's lives. For more than three decades, the company has been one of the most respected leaders in chip design and fabrication. Today, ST is Europe's largest semiconductor chip maker, with products in billions of devices people interact with every day around the globe. It is also one of only a few semiconductor companies that integrates design and manufacture, all in-house.

Bringing trusted hardware and software together

Although ST is known for its hardware, their microprocessors have become increasingly reliant on software over recent years. As partners and customers integrate technology and digital connectivity into new products and spaces, the need to build reliable software has become almost as important as the hardware itself. For ST, this represented a significant change in their operation.

On the customer side, ST has seen an increase in the need for a variety of software solutions that guarantee fast and seamless interoperability and functionality—from embedding and drivers to SDKs and demos—in order to move into production with ST's hardware technology. These customers expect the same level of trust in the software as ST's hardware.

Drivers, passengers, and an entire industry, depending on trust

Like ST, the auto industry is going through a paradigm shift from parts and assembly to integrated computers and digital connections. Before long, the smart car will be the standard on the road, and soon behind it, millions of autonomous vehicles. This paradigm shift is more than a change in technology. Its success depends on people trusting the technology enough to give up control over their cars, to let sensors and software make countless correct decisions in busy streets and at 80 kilometers per hour.

More and more, cars rely on software. Fly-by-wire steering, braking, audio, oxygen sensors—all monitored, controlled, and adjusted by code, and like any other software, these systems can be hacked if a criminal can find an entry point. As we connect these cars to networks via GPS, Bluetooth, and WiFi, cars become targets, just like any computer. Car data can be stolen, code altered. Someone could even potentially take control of the vehicle.

To ensure people trust smart and autonomous cars, manufacturers need to approach software security with uncompromising resolve. In a vehicle, any device controlled by software needs to be protected by the strongest security, and this security needs to be trusted no matter how many links exist in the supply chain. When ST delivers auto parts with trusted software security, they are providing trust that is passed on to the auto maker's customers. ST's software security doesn't just protect code and parts, it protects drivers and passengers on the road.

A unique company with unique needs

When ST began looking for a solution that could deliver the trust required by their customers, they quickly realized they faced several challenges. As one of the few companies in the world that handles the entire semiconductor manufacturing process from concept to delivery, ST doesn't operate on some of the principles and processes that drive much of the software development world. Specialized industry requirements, a widely distributed workforce, and a different kind of software development process means ST needs a signing solution that can adapt to their needs without compromise.

Specialized industry needs

A complex organization with products delivered to tens of thousands of customers in a wide variety of industries, ST evolved a very robust InfoSec operation. Any signing solution would need to be flexible enough to perform the functions required by DevOps while also meeting the standards set by ST's InfoSec at large.

A different dev process

In many cases, ST products must ship with completed software packages, which must be completed, secured, and ready to function throughout an entire lifecycle without the benefits of the traditional CI/CD model. For ST, the process is more an arrow than a DevOps loop.

A decentralized workforce

ST utilizes a distributed DevOps structure, with 20 teams of varying size on multiple continents. These teams work on different projects and products with unique scope and pacing, but all must meet InfoSec, business, and customer standards, and all must deliver on time.

Specialized work requires specialized security

At first, ST utilized a manual signing process for all software. While it met general business standards and InfoSec policies, the process was too slow and cumbersome. As the need grew for more software on more products, the manual signing process became a manufacturing and delivery roadblock. Looking to find a solution that would meet the needs of their growing software development, ST identified four key requirements:

Simplicity

A solution cannot make the DevOps process more complex, and it cannot interfere with software development progress.

Ease of use

Signing and key management must be as automated and streamlined as possible, so signers can move software along without getting mired in one-off or manual tasks.

Anytime/Anywhere signing

With teams and developers in different countries and in different time zones all around the world, a solution must be available when a developer is ready to move the software to the signing phase no matter where they are or what time it is.

Security

Above all, these other factors cannot compromise the security of the signing solution. The software must be secured with the highest level of assurance, so ST's products and its partners and customers are protected against malware, intrusions, and other threats.

Meeting ST's needs

Seeking flexibility, scalability, control and automation, ST turned to DigiCert® Software Trust Manager.

Management and control

In compliance with InfoSec and business requirements, ST has central account configuration as well as granular controls, with easy key and certificate management. Signing permissions are delegated to approved signers, and both signing permissions and key access can be adjusted or revoked at any time.

Automation and easy integration

APIs and workflow integrations allowed ST to quickly establish interoperability with existing systems, and Software Trust Manager automation prevents manual errors while facilitating signing practice consistency. Today, signing processes at ST are automated, so security is uniform, and the development process is expedited.

Flexibility

Because Software Trust Manager is built to configure to unique needs, ST holds control over which features are enabled or disabled, as well as control over team or group profiles and hierarchies. As needs grow or change over time, ST can continue to make fine-tuning adjustments, tailoring signing solutions to the needs of the business, and even individual teams—all without falling out of compliance or compromising security.

Scale

Because Software Trust Manager is highly scalable, ST can not only use it to secure software on current DevOps teams and products, but also on future teams and projects, no matter their size, process, or location.

Security

Software Trust Manager guards against supply chain attacks by securing code in transit and alerting ST and its customers if there's been any code tampering. It also ascribes identity, so customers know that an authorized ST professional signed the code, as well as when they signed.

The DigiCert difference

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.

Want to learn more about automated software signing solutions delivered at scale? Visit https://www.digicert.com/software-trust-manager