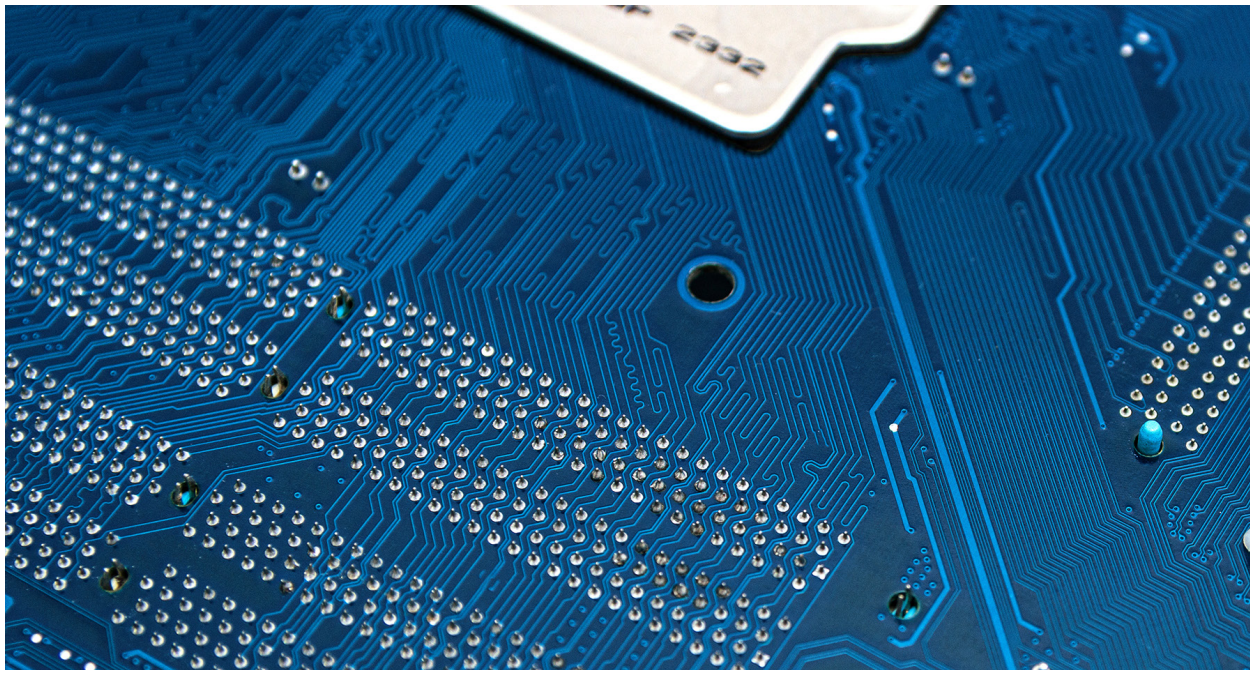
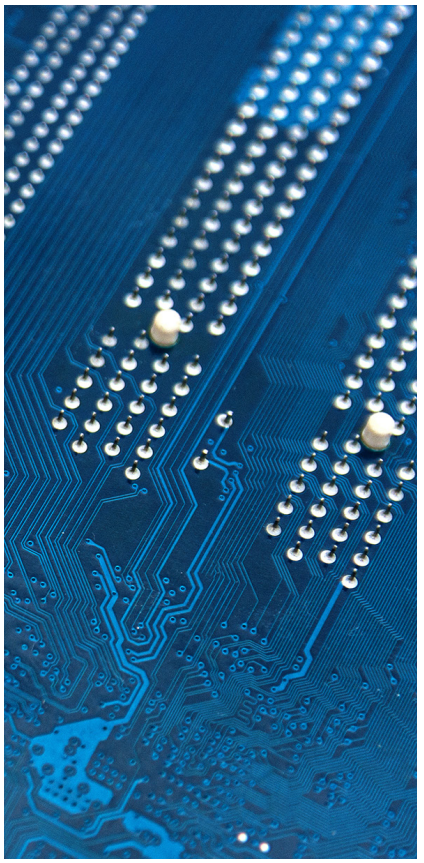




ST Fallstudie

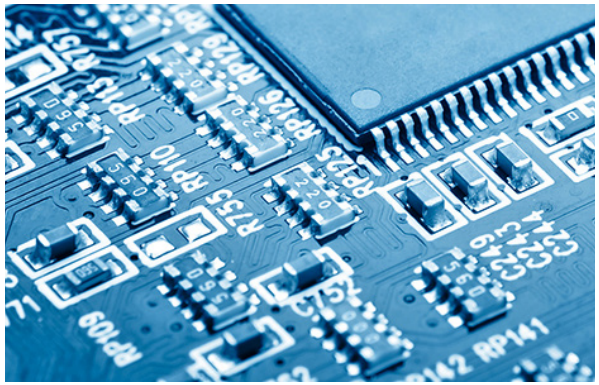
life.augmented

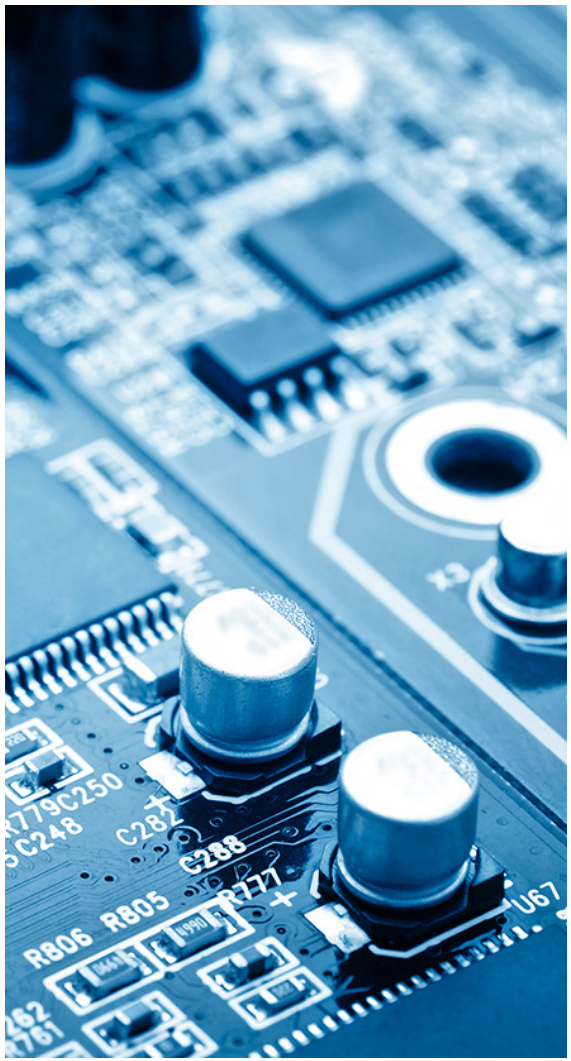
Weltweit führender Hardware-Anbieter vermittelt Vertrauen mit Softwaresignierung

digicert®

Führend bei Mikrochips und Prozessoren

STMicroelectronics ist ein multinationaler Hersteller von elektronischen Bauteilen und Halbleitern, dessen Mikrochips die neusten Fortschritte in puncto Leistung, Intelligenz und Effizienz für Produkte, die positiv zum Leben der Menschen beitragen, vereinen. Seit über 30 Jahren gehört das Unternehmen zu den angesehensten führenden Entwicklern und Herstellern von Mikrochips. Heute ist ST der größte Hersteller von Halbleiterchips Europas, dessen Produkte sich in Milliarden Geräten finden, die Menschen auf der ganzen Welt jeden Tag nutzen. Das Unternehmen ist auch einer der wenigen Halbleiterhersteller, die Entwicklung und Fertigung aus einer Hand bieten.





Neuland: Renommierte Hardware trifft auf Software

Der Ruf von ST gründet zwar auf seiner Hardware, doch wurden die Mikroprozessoren in den letzten Jahren zunehmend von Software abhängig. Da Partner und Kunden Technologie und digitale Konnektivität in neue Produkte und Räume integrieren, ist die Zuverlässigkeit der Software inzwischen fast ebenso wichtig wie die Hardware selbst. Für ST bedeutete dies eine erheblich Veränderung seiner Abläufe.

Seitens der Kunden hat ST eine Zunahme des Bedarfs an verschiedenen Softwarelösungen festgestellt, die von der Einbettung und den Treibern bis hin zu SDK und Demos schnelle und nahtlose Interoperabilität und Funktionalität sicherstellen, um in die Produktion mit der Hardware von ST übergehen zu können. Diese Kunden erwarten von der Software die gleiche Vertrauenswürdigkeit wie von der Hardware.

Fahrer, Mitfahrer und eine ganze Branche in Abhängigkeit von Vertrauen

Wie ST erlebt auch die Autobranche gerade einen Paradigmenwechsel weg von Teilen und Montage hin zu integrierten Computern und digitalen Verknüpfungen. Es wird nicht mehr lange dauern, bis das Smart Car der Standard auf den Straßen sein wird, und kurz danach Millionen autonomer Fahrzeuge. Dieser Paradigmenwechsel ist nicht nur eine technische Frage. Sein Erfolg hängt davon ab, ob Menschen der Technik ausreichend Vertrauen entgegenbringen, um die Kontrolle über ihre Fahrzeuge abzugeben und Sensoren und Software zahllose Entscheidungen bei starkem Verkehr und 80 km/h zu überlassen.

Autos stützen sich zunehmend auf Software. Fly-by-Wire-Lenkung, Bremsen, Audio, Sauerstoffsensoren – alles wird von Code überwacht, gesteuert und geregelt. Wie jede andere Software auch können diese Systeme gehackt werden, wenn ein Krimineller einen Ansatzpunkt finden kann. Wenn wir diese Fahrzeuge über GPS, Bluetooth und WiFi vernetzen, werden sie zu Zielen wie alle Computer. Autodaten können gestohlen, Code kann verändert werden. Es könnte sogar jemand von außen die Kontrolle über das Fahrzeug übernehmen.

Um das Vertrauen der Menschen in intelligente, autonome Fahrzeugen zu gewinnen, dürfen die Hersteller in puncto Softwaresicherheit keine Kompromisse eingehen. Jedes von Software gesteuerte Gerät in einem Fahrzeug muss mit den wirkungsvollsten Sicherheitsmaßnahmen geschützt werden und diese Sicherheitsmaßnahmen müssen vertrauenswürdig sein, ganz gleich aus wie vielen Gliedern die Lieferkette besteht. Wenn ST Autoteile mit vertrauenswürdiger Softwaresicherheit ausliefert, dann liefert das Unternehmen Vertrauen für die Kunden der Autobauer. Die Softwaresicherheit von ST schützt nicht nur Code und Teile, sondern vor allem die Fahrer und Mitfahrer auf den Straßen.

Ein besonderes Unternehmen mit besonderen Anforderungen

Als ST begann, sich nach einer Lösung umzuschauen, die das notwendige Kundenvertrauen schaffen würde, sah man sich bald mehreren Herausforderungen gegenüber. Als eines der wenigen Unternehmen weltweit, die den gesamten Prozess der Halbleiterfertigung von der Konzipierung bis zu Auslieferung abwickeln, liegen den Abläufen von ST nicht die gleichen Prinzipien und Prozesse zugrunde wie einem großen Teil der Welt der Softwareentwicklung. Spezielle Branchenanforderungen, eine global verteilte Arbeitnehmerschaft und ein unterschiedlicher Softwareentwicklungsprozess bedeuten, dass ST eine Signierlösung benötigt, die sich uneingeschränkt seinen Anforderungen anpassen kann.

Spezielle Branchenanforderungen

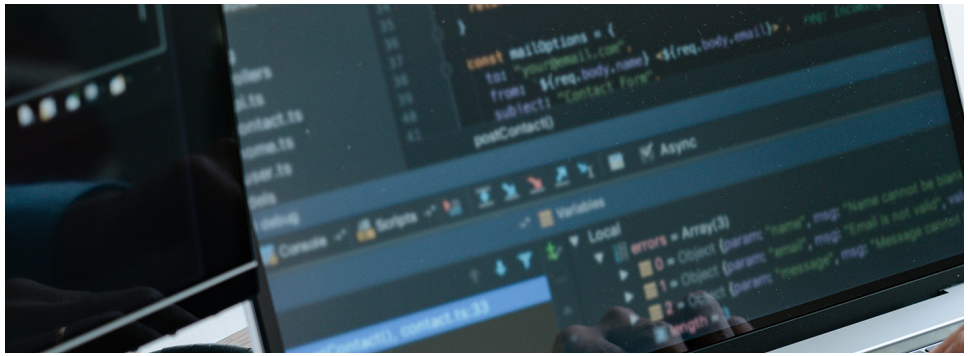
Als ein komplexes Unternehmen, das seine Produkte an Zehntausende Kunden in den unterschiedlichsten Branchen liefert, hat ST sehr robuste InfoSec-Abläufe entwickelt. Jede Signierlösung müsste ausreichend flexibel sein, um die von DevOps geforderten Funktionen ausführen zu können und zugleich die allgemeinen InfoSec-Standards bei ST einzuhalten.

Ein unterschiedlicher Entwicklungsprozess

In vielen Fällen muss ST seine Produkte mit abgeschlossenen Softwarepaketen ausliefern, die vollständig entwickelt, geschützt und über einen gesamten Lebenszyklus funktionstüchtig sind – und das ohne die Vorteile herkömmlicher CI/CD-Modelle. Bei ST gleicht der Prozess eher einem Pfeil als einer DevOps-Schleife.

Dezentrale Belegschaft

ST nutzt eine verteilte DevOps-Struktur mit 20 Teams unterschiedlicher Größe auf mehreren Kontinenten. Diese Teams arbeiten an unterschiedlichen Projekten und Produkten mit jeweils eigenem Ziel und Tempo, aber alle müssen die InfoSec-, Geschäfts- und Kundenstandards erfüllen und fristgerecht liefern.



Spezialisierte Arbeit erfordert spezialisierte Sicherheit

Anfangs nutzte ST für die gesamte Software ein manuelles Signierverfahren. Damit erfüllte das Unternehmen zwar die allgemeinen Geschäftsstandards und InfoSec-Richtlinien, doch das Verfahren war zu langsam und aufwendig. Als die Nachfrage nach mehr Software für mehr Produkte stieg, wurde das manuelle Signierverfahren zu einem Hemmschuh für die Fertigung und Lieferung. Auf der Suche nach einer Lösung für die Anforderungen seiner wachsenden Softwareentwicklung identifizierte ST vier zentrale Anforderungen:

Einfachheit

Eine Lösung darf den DevOps-Prozess nicht komplexer machen und Fortschritte bei der Softwareentwicklung nicht blockieren.

Benutzerfreundlichkeit

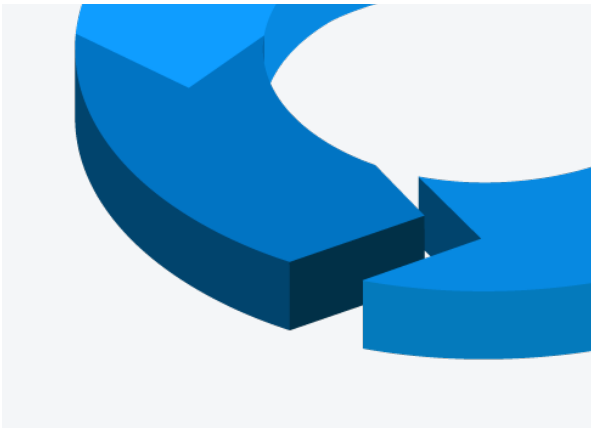
Signierung und Schlüsselverwaltung müssen weitestgehend automatisiert und vereinheitlicht werden, damit Signierer die Software zügig weiterleiten können, ohne sich in einmaligen oder manuellen Aufgaben zu verlieren.

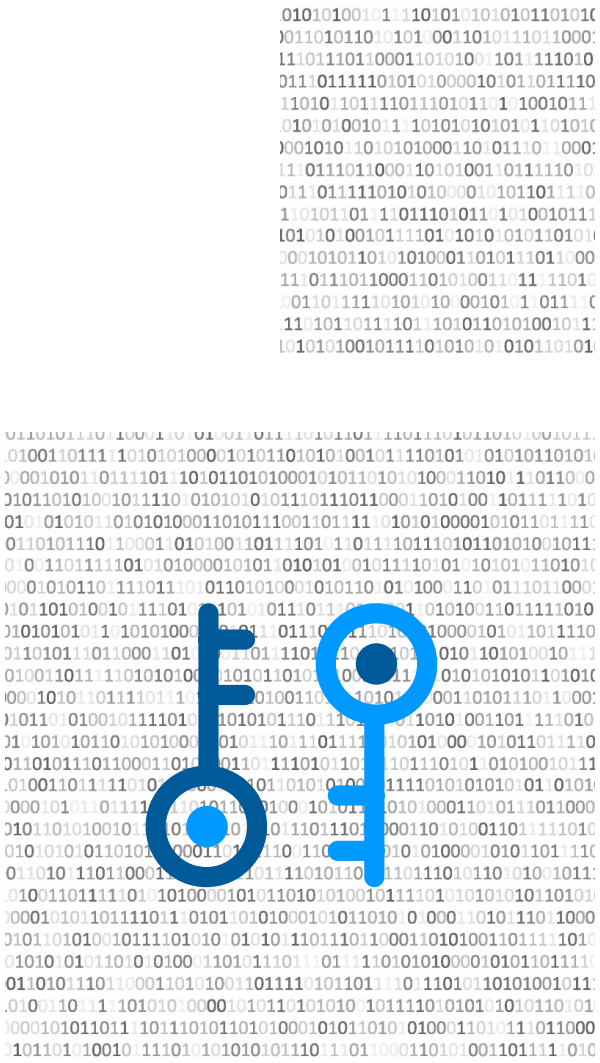
Zeit- und ortsunabhängige Signierung

Da sich Teams und Entwickler in unterschiedlichen Ländern und Zeitzonen auf der ganzen Welt befinden, muss eine Lösung dann zur Verfügung stehen, wenn ein Entwickler so weit ist, die Software in die Signierphase weiterzuleiten – ganz gleich um welche Uhrzeit und an welchem Standort.

Sicherheit

Vor allem aber dürfen die zuvor genannten Faktoren die Sicherheit der Signierlösung nicht beeinträchtigen. Die Software muss mit dem höchsten Maß an Sicherheit geschützt werden, sodass die Produkte, Partner und Kunden von ST vor Malware, Infiltration und anderen Bedrohungen geschützt sind.





Erfüllung der Anforderungen von ST

Für seine Anforderungen der Flexibilität, Skalierbarkeit, Steuerung und Automatisierung entschied sich ST für DigiCert® Secure Software Manager.

Verwaltung und Steuerung

Konform mit den InfoSec- und Geschäftsanforderungen verfügt ST über eine zentrale Kontenkonfiguration sowie granulare Steuerungen mit einfacher Schlüssel- und Zertifikatsverwaltung. Signierberechtigungen werden zugelassenen Signierern zugewiesen und sowohl die Signierberechtigungen als auch der Schlüsselzugriff können jederzeit angepasst oder zurückgenommen werden.

Automatisierung und einfache Integration

APIs und Workflow-Integrationen ermöglichten es ST, rasch Interoperabilität mit bestehenden Systemen herzustellen, und die Automatisierung im Secure Software Manager beugt einerseits manuellen Fehlern vor und erleichtert andererseits eine konsistente Signierpraxis. Heute sind die Signierprozesse bei ST automatisiert, sodass ein einheitliches Sicherheitsniveau besteht und der Entwicklungsprozess zügig vorankommen kann.

Flexibilität

Da Secure Software Manager im Hinblick darauf entwickelt wurde, die Konfiguration für besondere Anforderungen zu ermöglichen, besitzt ST volle Kontrolle darüber, welche Funktionen aktiviert bzw. deaktiviert sind, sowie die Kontrolle über Team- und Gruppenprofile und -hierarchien. Wenn die Anforderungen mit der Zeit zunehmen oder sich verändern, kann ST die Feineinstellung anpassen und die Signierlösungen auf die Anforderungen des Unternehmens oder sogar einzelner Teams abstimmen, ganz ohne gegen Vorschriften oder Richtlinien zu verstoßen oder die Sicherheit aufs Spiel zu setzen.

Skalierbarkeit

Da Secure Software Manager hochgradig skalierbar ist, kann ST damit nicht nur die Software der jetzigen DevOps-Teams und Produkte schützen, sondern auch die künftiger Teams und Projekte, unabhängig von deren Größe, Prozess oder Standort.

Sicherheit

Secure Software Manager schützt vor Angriffen auf die Lieferkette, indem er Code während der Übertragung schützt und ST und seine Kunden benachrichtigt, wenn es Versuche gab, Code in irgendeiner Form zu manipulieren. Er weist auch eine Identität zu, sodass Kunden wissen, dass ein autorisierter ST-Mitarbeiter den Code signiert hat und wann die Signierung erfolgt ist.

Der Unterschied mit DigiCert

DigiCert steht für mehr Sicherheit im Internet. Dieses Ziel zieht sich als roter Faden durch unsere gesamte Unternehmensgeschichte. Deshalb genießen unsere TLS/SSL-Zertifikate tagtäglich und millionenfach das Vertrauen von 89 % der Fortune 500-Unternehmen, 97 der 100 größten internationalen Finanzinstitute und 81 % aller weltweit tätigen Online-Händler. Nicht umsonst erhalten wir von unseren Kunden branchenweit die meisten Fünf-Sterne-Bewertungen für Service und Support. Mit der Plattform DigiCert ONE und mit unseren Verwaltungstools modernisieren wir die Public Key Infrastructure und unterstützen Unternehmen und Behörden beim Schutz von Identitäten, Zugriffen, Servern, Netzwerken, E-Mails, Codes, Signaturen, Dokumenten und IoT-Geräten. So stellen wir sicher, dass DigiCert auch in Zukunft eine Vorreiterrolle bei der Entwicklung innovativer SSL-, IoT- und PKI-Lösungen einnehmen wird.

Sie möchten mehr über Lösungen für die automatisierte Softwaresignierung in großem Umfang erfahren? Besuchen Sie https://www.digicert.com/de/signing/secure-software-manager