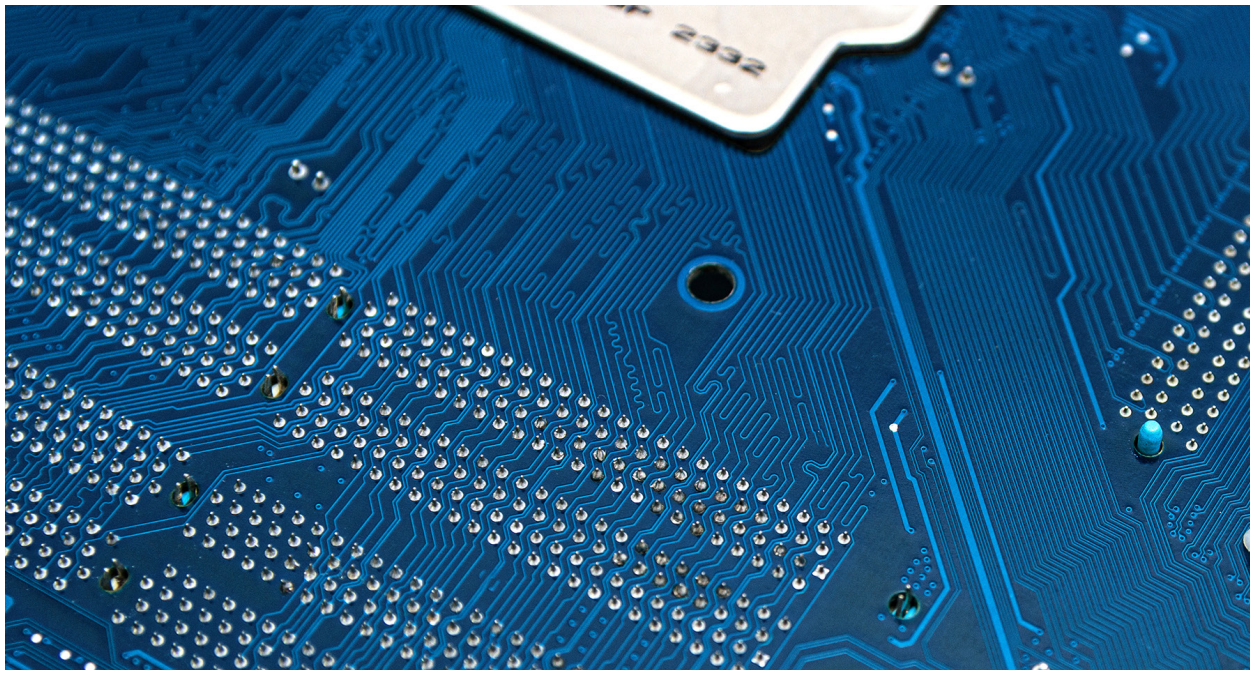
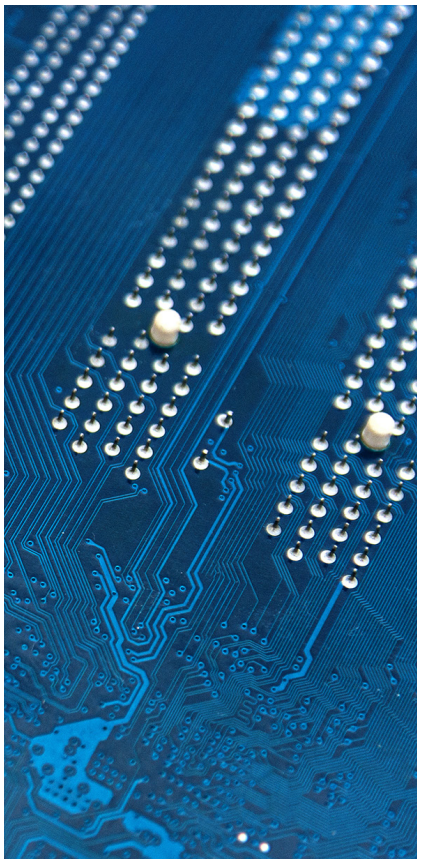




ST マイクロエレクトロニクス 社のケーススタディ

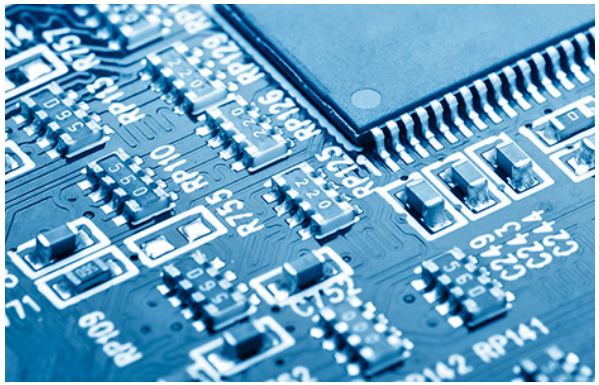
life.augmented

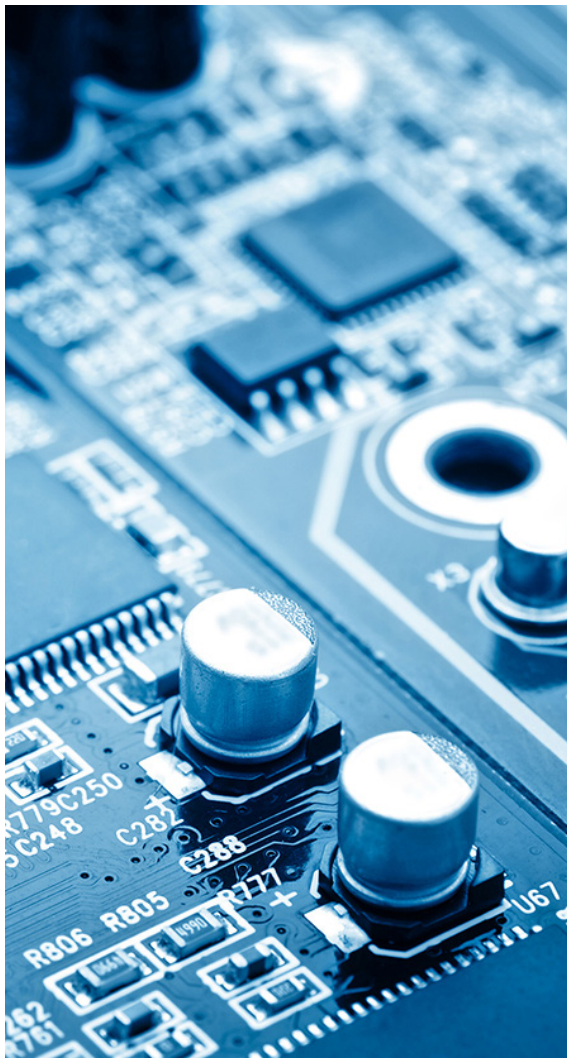
ハードウェアの世界的リーダーがソフトウェア署名により信頼を付与

digicert®

チップとプロセッサのリーディングカンパニー

ST マイクロエレクトロニクス 社（以下、ST 社）は電子機器および半導体の製造を行う多国籍企業で、人々の生活をよくする製品のパフォーマンス、インテリジェンス、効率性の最新の進化を注ぎ込んだチップを開発しています。30 年以上にわたり、同社はチップの設計と製造において評価の高いリーディングカンパニーの一社として知られています。現在、ST 社は欧州最大の半導体チップメーカーであり、その製品は数十億台のデバイスに搭載され、世界中の人々によって毎日使用されています。また、設計と製造をすべてインハウスで手掛けている数少ない半導体会社の 1 つでもあります。

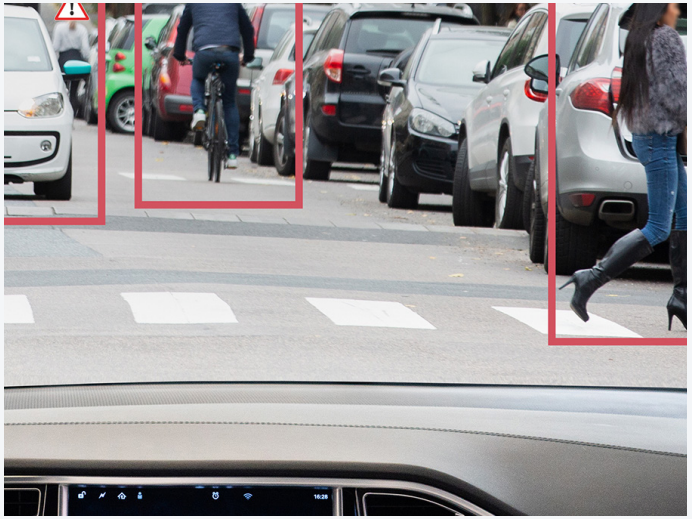




信頼できるハードウェアとソフトウェアを融合

ハードウェアで有名な ST 社ですが、近年、同社のマイクロプロセッサはソフトウェアへの依存度を高めています。パートナーと顧客がテクノロジーとデジタルコネクティビティを新しい製品や分野に融合する中で、信頼性の高いソフトウェアの開発はハードウェアの開発と同じくらい重要になりました。これにより、ST 社の業務は劇的に変化することになりました。

顧客側では、ST 社のハードウェアテクノロジーの製造に移行するために、スピーディかつシームレスな相互運用性と機能を保証するさまざまなソフトウェアソリューション（組み込みから、SDK のドライバ、デモまで）に対するニーズの高まりが見られました。これらの顧客はソフトウェアに ST 社のハードウェアと同レベルの信頼性を求めています。



信頼は運転手、乗客、そして業界全体のよりどころ

ST 社と同じように、自動車業界でも、部品と組み立てからコンピュータとデジタル接続の統合へのパラダイムシフトが起こっています。そう遠くない未来に、スマートカーが当たり前になり、そのすぐ後には数百万台の自動運転車が道路を走るようになるでしょう。このパラダイムシフトは、ただのテクノロジーの変化ではありません。その成功は、交通量の多い道路で時速 80 km で走りながら、車を自分の手でコントロールすることをやめて、センサーとソフトウェアに数え切れないほどの正しい意思決定を任せてもよいと思うほどに人々がテクノロジーを信頼できるかどうかにかかっています。

車のソフトウェアへの依存度は高まるばかりです。フライバイワイヤのステアリング、ブレーキ、オーディオ、酸素センサはすべてソフトウェアによって監視され、制御され、調整されています。他のあらゆるソフトウェアと同じように、これらのシステムも侵入口が犯罪者に見つかればハッキングされる恐れがあります。このような車が GPS、Bluetooth、WiFi でネットワークに接続されると、車はコンピュータと同じく攻撃の標的となります。車のデータが盗まれ、コードが改ざんされます。車のコントロールが奪われる可能性もあります。

スマートカーや自動運転車が人々の信頼を得るためには、メーカーは不屈の覚悟をもってソフトウェアセキュリティに対処する必要があります。ソフトウェアによって制御される車内のあらゆるデバイスを最強レベルのセキュリティで保護する必要があります。サプライチェーンのつなぎ目がいくら多くなろうとも、このセキュリティは信頼できるものでなければなりません。ST 社が信頼できるソフトウェアセキュリティを内蔵した自動車部品を提供するとき、同社は自動車メーカーのお客様へと引き継がれる信頼を提供しているのです。ST 社のソフトウェアセキュリティは、コードと部品を保護するだけでなく、道路上の運転手や乗客も守っています。

独自のニーズをもつ独自の会社

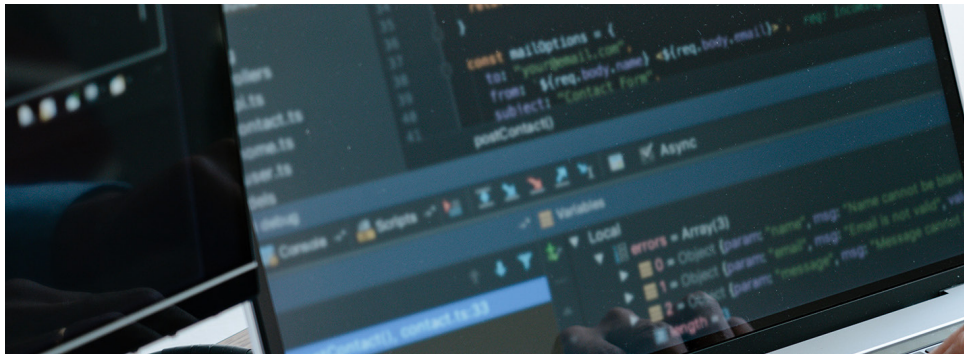
ST 社は顧客が求めるレベルの信頼性を提供可能なソリューションを探し始めたところ、複数の課題が存在することがすぐに明らかになりました。概念設計から納入までの半導体製造プロセスを一手に担う世界でも数少ない企業である ST 社はソフトウェア開発業界で主流の原則やプロセスを基準に動いていません。業界特有の要件、広範囲に分散配置された人材、さまざまな種類のソフトウェア開発プロセスを考えると、ST 社には妥協なしにニーズに適応できる署名ソリューションが必要であることが分かりました。

業界特有のニーズ

幅広い業界の数万社のお客様に製品を納める複雑な組織である ST 社では、非常に堅牢な情報セキュリティ運用を発展させてきました。署名ソリューションは、DevOps が求める機能を実行するのに十分な柔軟性を備えるだけでなく、ST 社の情報セキュリティ部門が定める基準全般を満たす必要がありました。

異なる開発プロセス

多くの場合、ST 社の製品は完成されたソフトウェアパッケージとともに出荷される必要があります。そのソフトウェアは従来の CI/CD モデルのメリットを享受することなくライフサイクル全体を通して完全で、安全で、機能可能である必要があります。ST 社にとって、このプロセスは DevOps ループというよりは、一方通行の矢印のようなものです。



分散配置された人材

ST 社では分散型の DevOps 構造を採用しており、大小さまざまの 20 のチームが世界中に配置されています。これらのチームは独自のスコープとペースに従って異なるプロジェクトおよび製品を担当していますが、全チームが情報セキュリティ、ビジネス、および顧客の基準を満たす必要があり、全チームが期日通りに納入する必要があります。

特殊な作業には特殊なセキュリティが必要

当初、ST 社ではすべてのソフトウェアに対して手作業による署名プロセスを採用していました。一般的なビジネス基準と情報セキュリティポリシーを満たすことはできたものの、そのプロセスには非常に多くの時間と手間がかかりました。より多くの製品により多くのソフトウェアを搭載するために需要が増加すると、手作業の署名プロセスが製造とデリバリーの障害になりました。ソフトウェア開発のニーズ拡大に対応できるソリューションを求める中で、ST 社は以下に示す重要な 4 つの要件を特定しました。

シンプルであること

ソリューションを採用することで DevOps プロセスがさらに複雑化してはなりません。また、ソフトウェア開発の進捗を妨げるものであってもなりません。

使いやすいこと

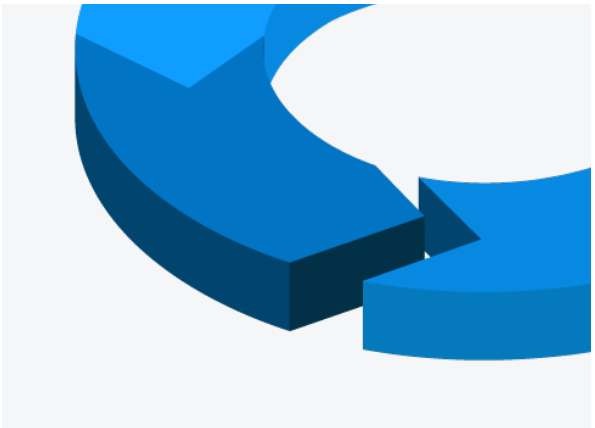
署名者が 1 回限りのタスクや手作業のタスクで手間取ることなくソフトウェアを移動できるよう、署名と鍵管理を可能な限り自動化、効率化する必要があります。

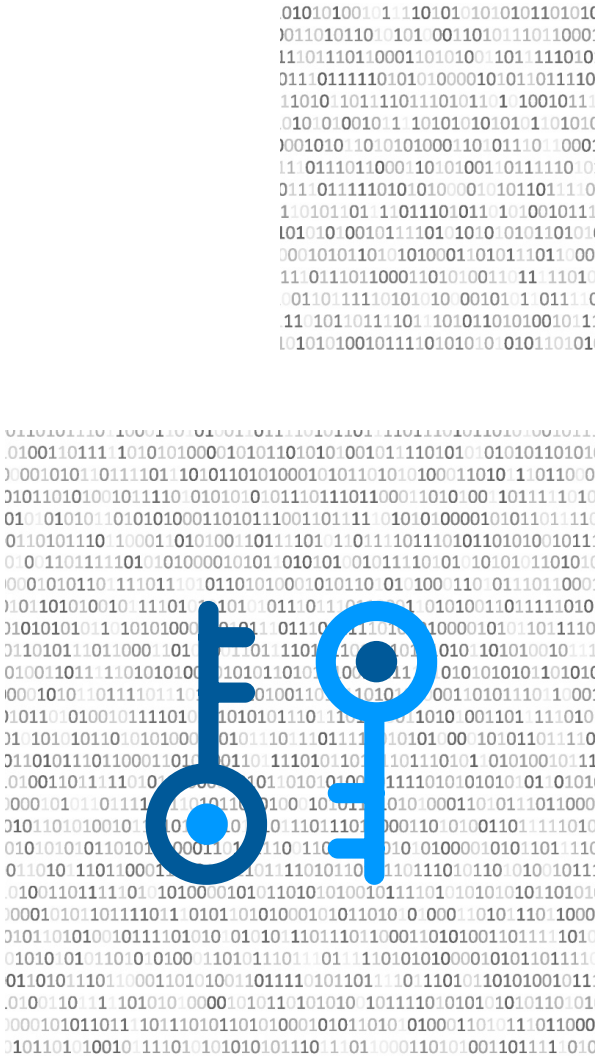
いつでも、どこでも署名が可能であること

チームと開発者が世界中のさまざまな国々、さまざまなタイムゾーンに居住しているため、開発者の場所や時間を問わず、ソフトウェアを署名段階に移行する準備ができた時点でソリューションを利用できる必要があります。

セキュリティ

何より、以上に述べたその他の要因が署名ソリューションのセキュリティを損なうものであってはなりません。ソフトウェアは最高レベルの保証で保護され、ST 社の製品とそのパートナーおよび顧客をマルウェアや侵入などの脅威から守る必要があります。





ST 社のニーズを満たす

柔軟性、スケーラビリティ、制御と自動化を求める ST 社は、DigiCert® Secure Software Manager に注目しました。

管理と制御

ST 社は情報セキュリティやビジネス要件に準拠しながら、容易な鍵および証明書管理ときめ細やかな制御、一元的なアカウント構成を備えています。署名の権限は承認済みの署名者に委任されます。署名権限も鍵のアクセス権も、いつでも調整または失効できます。

自動化と容易な統合

API とワークフローの統合により、ST 社は既存のシステムとの相互運用性を素早く確率できました。Secure Software Manager の自動化により、署名手法の一貫性が促されるともに、手作業によるミスが防止されました。現在、ST 社の署名プロセスは自動化されたため、セキュリティは一貫性があり、開発プロセスは迅速です。

柔軟性

Secure Software Manager は独自のニーズを構成できるように設計されているため、ST 社は有効化/無効化する機能を制御したり、チームまたはグループの階層を制御したりできます。時間の経過とともにニーズが増加または変化した場合でも、ST 社はコンプライアンス違反やセキュリティ侵害を起こすことなく、きめ細かい調整を続け、署名ソリューションをビジネスニーズや個々のチームのニーズに合わせてカスタマイズできます。

拡張性

Secure Software Manager は拡張性に優れているため、ST 社の現在の DevOps チームや製品上のソフトウェアを保護するために使用できるだけでなく、その規模やプロセスや場所に関わらず、将来のチームとプロジェクトのソフトウェアを保護できます。

セキュリティ

Secure Software Manager は、配信中のコードを保護し、コードの改ざんが発生した場合に ST 社と顧客に警告を送信することでサプライチェーン攻撃から守ります。ID も付与されるため、顧客は認証済みの ST 社の担当者がコードを署名したことと署名日時を知ることができます。

デジサートはここが違う

デジサートのルーツは、インターネットのセキュリティをもっと簡単に確保したいと考え、ひたむきに探求したことから始まります。それこそが、デジサートの TLS/SSL サーバ 証明書が世界中で信頼されている理由であり、Fortune 500 企業の 約 90%、世界の上位銀行 100 行のうち 98 行、世界の E コマースの 81% で毎日膨大な数の接続がデジサートの証明書によって保護されています。また、業界のサービスおよびサポートレビューでは、顧客から常に最も高い評価を受けています。デジサートは、企業や政府機関での ID、アクセス、サーバー、ネットワーク、E メール、コード、署名、文書、IoT デバイスの保護を容易にするため、DigiCert ONE プラットフォームと管理ツールを構築することで PKI のモダナイゼーションに取り組んでいます。SSL、IoT、PKI、さらにその先まで、デジサートは一歩先を進み続けます。

大規模に展開される自動化されたソフトウェア署名ソリューションにご興味をお持ちですか？
https://www.digicert.com/jp/signing/secure-software-manager をご覧ください。