CASE STUDY

digicert

XEROX ACCELERATES SECURITY AND COMPLIANCE USING DIGICERT TRUSTCORE SDK

Executive Summary

Company name: Xerox
Industry: Technology
Headquarters: Norwalk, CT

Key business requirements:

- Streamline management of MFP (multifunction printer) security
- Provide a secure alternative to OpenSSL that wouldn't impact third-party app development or interoperability
- Ensure compliance with FIPS 140-3 standards to compete for government and other high-security contracts

Solution:

- DigiCert TrustCore SDK

Key benefits:

- SDK library simplifies management and security of embedded TPM chips that are used to protect MFPs from infiltration by bad actors
- Engineers can migrate applications away from insecure OpenSSL libraries on multiple device environments without having to recode them—gaining support, security, compliance, roadmap control, and IP protection
- FIPS 140-2/3 certified libraries streamline and maintain compliance with these security standards on software and hardware

Requirement

Ensure Xerox MFPs have the highest levels of security and functionality in the industry

Xerox, a leading provider of multifunction printers (MFPs), continually must achieve two seemingly opposing objectives: provide the highest levels of security inside their MFPs while at the same time supplying boundless functionality that empowers customers to build a variety of document-centric workflows. However, they needed to do so in a way that would not complicate security management for Xerox engineers, customers, or third-party application developers.

"We have a huge responsibility to our customers to make sure our devices do not lead to an exploit, a loss of data, or something even worse than that," said Marc Rocas, principal engineer at Xerox. "But we don't want to create additional work for our customers or put them in a position to require technical personnel onsite to manage security. It would be like me calling an electrician to change a lightbulb, where the lightbulb costs $10 but the visit costs $200."

“TrustCore SDK provides us with predictable certification milestones and removes vulnerabilities that we might otherwise have to contend with”

To provide the necessary level of security, Xerox MFPs have embedded TPM (Trusted Platform Module) 2.0 chips that serve as Hardware Security Modules (HSMs). However, they are complex to manage without specialized cryptography knowledge. Meanwhile, OpenSSL, which was used to undergird their security stack, was vulnerable to exploits and couldn’t provide Xerox with the latest cryptographic certifications, such as FIPS 140-2/3. “The government will not allow any procurement of devices if they’re not FIPS 140-3 compliant, plain and simple,” said Rocas. “So, if you want to be on their list of approved vendors, you have to meet these requirements.”

But Xerox couldn’t simply junk OpenSSL for another protocol. That would require a great deal of rewritten code, something that would be difficult for the company’s engineers to achieve. Moreover, most third-party applications that interacted with Xerox MFPs used OpenSSL, and Xerox certainly couldn’t count on developers doing the same without risking much of their MFPs’ functionality. Xerox needed something that could seamlessly replace OpenSSL while at the same time provide the highest level of security and support for their devices.

Solution

DigiCert TrustCore SDK provided Xerox with a multifaceted approach to handling these security concerns

Xerox found their solution in DigiCert TrustCore SDK, a comprehensive security suite tailored to meet the company’s exacting standards. TrustCore SDK offered a multifaceted approach to realizing their many requirements and gave their engineers tools for efficient and secure deployments across a wide range of different environments. In addition, TrustCore SDK would enable Xerox to scale their security measures as their IoT infrastructure grew, thanks to its flexible and modular architecture.

“TrustCore SDK provides us with predictable certification milestones and removes vulnerabilities that we might otherwise have to contend with,” Rocas said. “It also means our customers don’t carry the burden of security, which provides cost savings for them and for us. And the technical partnership we have with DigiCert means that we can have discussions about roadmaps and additional say in where we want the technology to go.”

Impersonating OpenSSL to provide a secure environment

One of Xerox’s biggest challenges was figuring out a way to replace OpenSSL without being required to rewrite existing security applications. “We use a large amount of open source to build the software stack, and all the open source software is written against the OpenSSL flavor of things. But OpenSSL isn’t certified, and the ability to be certified is the ticket to the ballgame,” explained Rocas. “So, we asked if TrustCore SDK could ‘impersonate’ OpenSSL so that all third-party applications dependent on it would be none the wiser.”

DigiCert built TrustCore SDK’s OpenSSL Connector as an OpenSSL replacement that worked exactly the way Rocas had hoped. The OpenSSL Connector ensures compliance with the latest regulatory requirements, protects the data on documents transmitted through Xerox’s MFPs, and secures stored data. In addition, the OpenSSL Connector enabled Xerox to maintain and grow its library of OpenSSL-based third-party developer applications without forcing developers to learn a new library.

"It made so much sense because now we have a certified partner in DigiCert to work with, and we no longer have to deal with the ups and downs of the open source community, let alone worry about potential exploits that could impact our products and our customers," Rocas said. "And the migration was pretty painless because things worked as they did before."

Providing APIs to simplify TPM key protection and security

TrustCore SDK also gave Xerox the ability to leverage its pre-integrated APIs to abstract the complexities in managing the TPM 2.0 chips securing their MFPs. Using TrustCore SDK, Xerox engineers could now protect TPM private keys, locally attesting and validating the boot sequence, software versioning, and other protections for data in transit and at rest. This enhancement extended beyond basic protection; it infused each printer with advanced cryptographic capabilities and robust data integrity measures, ensuring that every document processed was under stringent security.

"These APIs work seamlessly with the rest of the security infrastructure that TrustCore SDK provides, which reduces development time and resource needs," said Rocas. "We can keep the private keys in our TPMs secure—and the customer data being stored encrypted—without having to be PhDs in cryptography. Our devices are now equipped to handle the challenges of the modern digital landscape, thanks to TrustCore SDK."

> "It made so much sense because now we have a certified partner in DigiCert to work with, and we no longer have to deal with the ups and downs of the open source community."

> "Our devices are now equipped to handle the challenges of the modern digital landscape, thanks to TrustCore SDK."

Navigating FIPS 140-3 compliance with ease

Additionally, the assurance of certifications and validations, most notably FIPS 140-2/3 enables Xerox to meet the levels of compliance that high-security government agencies demand. "TrustCore SDK has allowed us to turn the complex functions of meeting and staying ahead of compliance standards into a seamless aspect of our operations," Rocas said. "This level of protection and compliance would have been nearly impossible to build in-house, even if we had the time and resources required."

Overall, TrustCore SDK has transformed Xerox's ability to provide security and agility to the full spectrum of their customers. "TrustCore SDK and our partnership with DigiCert has been a cornerstone in reinforcing our market position as a leader in security and innovation," Rocas concluded.

Discover how the DigiCert® TrustCore SDK can revolutionize and expedite your journey towards device security and compliance by reaching out to our sales team at https://www.digicert.com/contact-us.