wolfSSL Enables Saficard to Securely Transmit E-Care Bills Using Cryptography Message Syntax and TLS

Since 1999, Saficard has offered innovative solutions in healthcare billing software for electronic payment terminals in France. The terminals accept France's health insurance card, Vitale, and a medical professional card, CPS. Both cards have an embedded chip that contains sensitive information that needs to be processed and transferred securely.

Key Requirements

Saficard must adhere to an ever-growing list of security requirements set by the French government.

The requirements included securely transferring e-care bills using Cryptography Message Syntax (PKCS#7) through a TLS (Transport Layer Security) connection.

Their software design targeted the iWL250 terminal by Ingenico and was constrained to a 400 MHz ARM CPU, 32 MB RAM (2 MB per application) and 128 MB flash.

Saficard needed a C-languaged-based SSL/TLS library with a small footprint and high configurability that could meet these requirements.

Solution

Saficard faced a challenging embedded platform to develop on. They needed to create their main application and user interface on very constrained hardware. They also needed to ensure the safety of their clients and meet French regulations for secure information transfer. A large cryptography library would take up resources that could be used for features that Saficard customers would pay for.

A cryptography library with well-tested TLS/PKCS#7 functionality and a small-configurable footprint is in short supply.

Saficard surveyed various SSL/TLS cryptography libraries for a possible solution to their needs.

They found many libraries available could not meet their constraints. OpenSSL was too large for the embedded hardware in the iWL250 terminal. They tried using mbed TLS, but it could not implement Cryptography Message Syntax (PKCS#7).

Saficard finally found wolfSSL. After initial testing they chose to use the wolfSSL Embedded SSL Library and wolfCrypt Embedded Cryptography Engine.

Saficard contacted wolfSSL for support during their development cycle. They requested additional features for PKCS#7 to be implemented. wolfSSL was more than happy to create the extra functionality and documentation they needed. wolfSSL also created additional unit tests for the additional functionality to ensure validity and robustness.

"It was a perfect fit! The library is really tiny in code and memory, and easily adaptable to the terminal's proprietary SDK we work with. The library is well maintained, has extensive documentation and really good support."

"The development was fast and they gave us custom documentation of new functionalities and examples of how to use it."

Results

Saficard was able to meet their objective using the wolfSSL Embedded SSL Library and wolfCrypt Embedded Cryptography Engine.

Saficard was able to securely transmit e-Care bills on the embedded platform, iWL250, using Cryptography Message Syntax (PKCS#7) and TLS. This was in accordance to French government regulations regarding transfer of health insurance and billing information with the use of the Vitale and CPS card.

Saficard was pleased with how wolfSSL is highly configurable to allow for a minimum size of 20 – 100 kB, runtime memory of 1 – 36 kB and standards up to TLS 1.3 (RFC 8446).

The PKCS#7 expansion requested by Saficard was created by wolfSSL and was based on RFC 5652. It was placed in the wolfCrypt library. An example for generating a PKCS#7 Signed Data bundle was added to the "wolfssl-examples" GitHub repository.

"We were able to successfully upgrade security on our application and conform to government requirements in our very constrained electronic payment terminals. We can now use the very last TLS versions and cryptographic suites, for securing e-care bills with PKCS#7 and smart cards. wolfSSL is a tremendous solution for us."

"We also greatly appreciated the quality of technical support: they understand our questions
well, even the very technical ones, and the replies were quick and accurate… It's very reassuring for our company to know that a critical component like wolfSSL has very good support."

wolfSSL prides itself on providing a GPLv2-licensed version of wolfSSL in addition to commercially-licensed versions, with the GPLv2 version available direct from wolfssl.com. With the GPLv2 download, companies like Saficard can test and prototype before making a license decision.

For More Information

www.wolfssl.com info@wolfssl.com
www.saficard.com contactweb@saficard.com
PKCS Wikipedia Article: https://en.wikipedia.org/wiki/PKCS