intertrust® Building trust for the connected world.

Product Brief

Secure Systems

Secure Keys for Trusted Communications

whiteCryption Secure Key Box (SKB) for TLS

Transport Layer Security (TLS) is the industry standard networking protocol used in web browsers, cloud software and other applications that requires data to be securely exchanged over a network. The security of TLS is enabled by using cryptographic algorithms mutually supported by the client and server. These cryptographic operations, when used in tandem with a cryptographic key, ensures that data remains secure during transmission from end-to-end.

The connection is secure from client to server, but what if an attacker gains access to the keys used to secure either end of the TLS connection? The malicious actor can simply use the key to decrypt the communication and read the data, alter the information in transit, or masquerade as a legitimate device. Without a method for keeping cryptographic keys secure, data integrity and security are at risk.

Importance of having secure TLS keys

If you need a high level of assurance you should protect your TLS keys. In addition to preventing eavesdropping and message manipulation, TLS can also provide mutual authentication for both the client and the server. For machine to machine communications, the ability to perform mutual authentication is very important, as it's not just the client that wants to be able to be sure the server is the one it claims to be, but the server also wants to validate the authenticity of the client device, ensuring it is genuine. Mutual authentication can only be trusted if the key on each end is protected.

What Is whiteCryption SKB?

whiteCryption Secure Key Box (SKB) is a white-box cryptographic library that developers can use to ensure their encryption keys and other secrets are protected. It does this in such a way that the keys are never in the clear in memory of the device, even when in use. That's important as it stops hackers from using open-source tools and techniques to search through memory looking for encryption keys, which is easier than you may think. You can think of SKB as a virtual hardware security module (HSM) running in your application, keeping your keys safe at all times.

What is SKB for TLS?

SKB for TLS is a special implementation of a TLS library that uses white-box cryptography to ensure the keys used to establish the connection, as well as the session keys to secure the transmissions, are always protected. To the developer, it acts and appears much the same as any other TLS stack, in fact it's simpler to use than most other solutions in the market. The difference is that the keys never get loaded into the memory of the device, they always stay encrypted, even when in use.

Storing keys securely, but then loading them into memory when they are needed is no longer sufficient. Let Intertrust deliver proper end-to-end security with whiteCryption Secure Key Box for TLS.

Learn more at: intertrust.com
Contact us at: +1 408 616 1600

Intertrust Technologies Corporation
920 Stewart Drive, Sunnyvale, CA 94085

PB_SS_MH20