Trusted Computing Consulting

ONBOARD SECURITY CONSULTING SERVICES

When it comes to security, there's no better place to go than to OnBoard Security. With our team of industry-recognized security experts, we don't just follow the security standards - we lead in their creation. As a result, we can help you implement security hardened solutions with trusted computing that deliver real value to you and your customers. As established software security specialists, we understand the challenges our customers face in building industrial strength security solutions for their products. By having OnBoard Security look at your designs, answer questions as they arise, and validate your objectives, you can move confidently to heightened security for your products.

WHY ONBOARD SECURITY

If you are new to implementing security hardened products with trusted computing using a Trusted Platform Module (TPM), you'll find it is a steep learning curve. It can be a difficult journey to start - and continue - without expert advice. In a consulting role, OnBoard Security can help this process go smoothly. Not only do we have a great track record of success, but we also have members of our team who are at the forefront of trusted computing innovation. For instance, the Trusted Computing Group (TCG and its members awarded OnBoard Security's Business Development Engineer Lee Wilson a "2016 Key Contributor Award." This award was presented in recognition of Wilson's longstanding participation in TCG, as well as his ongoing commitment and contributions to the organization.

There are many ways in which our team can help you achieve success. In the past, some of the ways we have been able to do so include but are not limited to
- TPM BIOS/BIG-IP Measured Boot
- Local Attestation for TPM Chain of Custody
- Extend TPM measurement to include SW and provide Remote Attestation
- Measure through to selected SW applications
- Eliminate gray market by tying licensing to TPM
- BIG-IQ remote attestation

CURRENT COLLABORATIONS

"OnBoard Security gave us in-depth insight into the TPM 2.0 specification, helping us navigate through this complex technology"

- Trusted Computing Consultation customer

1.978.905.6796 ■ onboardsecurity.com

KEYFEATURES

OnBoard Security TrustSentinel 2.0

TSS 2.0 is a standard specified by the Trusted Computing Group. But even though it is a standard, not all TSS 2.0 solutions are alike.

WHY ONBOARD SECURITY'S TRUSTSENTINEL 2.0?

- OnBoard Security's TrustSentinel 2.0 supports TCG Specifications

- Comprehensive testing ensures correct, secure TSS 2.0 behavior regardless of the vendor

- Versions for Linux, Windows and other operating systems

- World-class support to properly implement the transitive trust chain

- All code security and safety vulnerabilities addressed

- Leading provider of Industrial-Strength TSS 1.2

TrustSentinel 2.0 provides a simple, consistent API for application developers, allowing them to use the strong security features of the TPM 2.0 without having to learn the intricacies of the hardware.

ONBOARD SECURITY CONSULTING SERVICES

• Ongoing mentorship in trusted computing technologies and trends

• Extension of trusted computing solutions into complex high end and high value solutions

• Onsite and remote collaboration available

• Trusted computing expertise that will point you in the right direction, and keep you on track for success

• Bring about a focus on and understanding of trusted computing that will save you time and money, as well as make you more efficient in your product production

• In working with you, we will be accomplishing a trusted computing skills transfer, so that your organization becomes increasingly self-sufficient

1.978.905.6796 ■ onboardsecurity.com