STMicroelectronics statement of interest

Hervé Sibert / Fabio Sozzani

STMicroelectronics is fully engaged in hardware-based security, with related activities ranging from the design and manufacturing of secure microcontrollers for smartcards and discrete TPM chipsets to that of powerful consumer electronics application processors for pay-TV and conditional access in which robust security is crucial. This statement focuses on the latter range of products.

Basing the delivery of value-added services through standards-supporting browsers is one of the most promising ways to achieve scalability and reducing the fragmentation due to the application ecosystems silos. This is an advantage for both consumers and service providers.

However, current browser implementations alone do not meet the security requirements imposed by content owners on content distribution services, therefore limiting the availability of content on browser-based services.

We at ST believe that it is crucial that such services can benefit from all the security available in devices: if browsers are able to access and benefit from the security hardware in devices, then the same browser-based services will run on all devices, and deliver the best experience that is supported by each particular device. Everyone expects a 4G smartphone with HD display to show online videos smoothly with high definition. Similarly, the owner of devices with high-grade security hardware should be able to expect unlimited access to premium content, live events etc…

In order to achieve this goal, while still keeping development complexity at a reasonable level, bridges from standards-based browsers to proprietary interfaces of security components are not scalable. That's the reason why we are engaged with standards such as GlobalPlatform and Linaro to define standard interfaces to security components that applications and browsers in particular, can rely on.

With GlobalPlatform, the association that promotes secure and interoperable deployment and management of multiple applications on secure chip technology, we are standardizing the Trusted Execution Environment that protects the execution of sensitive functions and manipulation of cryptographic data from operating systems that are not trusted enough by content owners to fully rely on them to secure the distribution of content, or by financial service providers to perform transactions without high risk commissions. The TEE provides standard interfaces, ported on chipset hardware such as cryptographic engines, to implement so-called Trusted Applications that deliver security services to applications in the operating system.

TEE implementations may differ in terms of security achieved, depending on how secure the hardware capabilities it relies on are. This stands both for the interfaces the TEE provides to Trusted Applications, and for the isolation of the TEE from the rich operating system. Security certification of the TEE is therefore essential to provide assurance, so that related information can be brought up to applications that use the TEE.

Moreover, with capabilities such as the SE API, which provides access to the highest-grade security components, the TEE is not only capable of leveraging chipset-level security hardware, but can also act as a gateway towards other security components on the device.

Our engagement goes further as, in a joint effort with the Linaro - the collaborative engineering organization developing open source software for the ARM architecture, we have open-sourced our vanilla implementation of the Trusted Execution Environment. The implementation, available on GitHub at https://www.github.com/OP-TEE, is available to anyone and usable with no strings attached, as it is delivered under BSD license. Being engaged with Linaro on this effort is also crucial to foster the ARM community around the implementation and bring trust in its maintenance and evolution. It also enables OP-TEE to be used as the base for reference implementation of advanced security services for specific use cases such as content protection or platform security services.

The other important fact is that the implementation is based on the ST-Ericsson TEE implementation, which passed the GlobalPlatform functional compliance testing and is listed at https://www.globalplatform.org/complianceproducts.asp.

With an open-source TEE supporting standard interfaces and bringing a community around, we believe that the next step is bridging WebCrypto with the TEE as defined by GlobalPlatform. There is also room to extend the scope to the Encrypted Media Extensions. The main advantage of doing this standards-based work is that such efforts will be compatible any implementation that complies with the GlobalPlatform standards.

We are looking forward to the workshop to discuss with more details the merits of the GlobalPlatform TEE standard, and the definite benefits it can bring to browsers-based services. We are also ready to present OP-TEE but we believe that it’s not the purpose of the workshop to promote this or that implementation. We expect that, if several submissions address the same goal and share the same position of promoting TEE technology, a joint session and round table around this topic could make sense.