IDfusion's Secure Runtime Development Environment:
Making Intel® SGX Easy To Use

With the introduction of the Secure Runtime Development Environment (SRDE), IDfusion LLC brings the power of Intel®'s SGX hardware security technology to meet the challenges of secure software development. Understanding the SGX paradigm is one thing. Using the Intel® SDK is another challenge that requires much deeper knowledge. IDfusion's SRDE offers developers a higher level of abstraction that makes realizing the benefits of SGX easier and faster!

Creating applications that take advantage of Intel®'s SGX-based secure enclave technology requires that developers partition security-sensitive functionality into separate code that is compiled and linked against an SGX Software Development Kit (SDK). This SDK provides support for the standalone execution environment that characterizes a SGX *enclave*. A Platform SoftWare (PSW) run-time environment is then required to load, initialize and execute the enclave. In addition, the PSW provides support for the Enhanced Privacy ID (EPID) provisioning process that joins and anonymously identifies a platform to a security group that enables support for remote attestation critical to SGX security guarantees.

IDfusion's SRDE provides an alternative PSW, specifically designed for minimum footprint applications of SGX. Think everything from containers to SCADA to IoT. It enables a toolkit-based approach to all of the functionality that a developer needs to incorporate secure enclave technology. Implemented in the form of a simple to use C-based object library, it has no external OS library dependencies and supports OpenSSL, GLIBC as well as the MUSL C library popular with embedded developers.

The IDfusion *SGXfusion* library extends the Intel® SDK with capabilities that enable seamless source code interoperability between non-SGX and enclave-based software implementations. Applications can be conceived, debugged and tested using standard development tools and techniques and then converted into an enclave-based secure application simply by recompiling. This greatly accelerates developer productivity and time-to-solution.

To these PSW and SDK solutions IDfusion adds a set of pre-built enclaves that provide rich functionality that can be immediately leveraged by platform developers and architects. This functionality includes secured enclave-to-enclave communications featuring IDfusion's Host Specific Enclave Authentication (HSEA). Purpose built to take advantage of SGX-based remote attestation capabilities, HSEA-based network communications enables developers to provide physical processor-based controls over which platforms are allowed to connect and communicate. This provides a compelling solution for organizations reluctant to open network access beyond their internal network.

As an Intel® licensed SGX Independent Software Vendor, IDfusion LLC can provide secured enclave technology in ready-to-be-signed or pre-signed configurations. Contact IDfusion LLC for further details on how to security differentiate your platforms.