SEAcurIT-e®: Introduction and Case study

SEAcurIT-e® gives solution providers a clear differentiation in terms of security and control. It can be integrated into new and existing products and applications to significantly enhance security and control where cryptographic processes such as encryption and data integrity are employed.

It addresses and solves crucial and long-standing security and management issues surrounding the use of such security techniques, such as how to properly protect cryptographic keys in software environments, and provides effective control of the security functions themselves.

It can operate as a robust and reliable system for the management of cryptographic keys, and has several distinct security and management advantages and capabilities over other approaches. Furthermore, it may also be incorporated into other such schemes and applications to give them the same advantages and capabilities irrespective of the type of the cryptographic function being employed.

It is ideally suited to:

- Cloud applications, as a component to support the use of cryptographic functions within Cloud solutions.
- The Internet of Things (IoT), where dedicated security hardware may not be appropriate, where it is necessary to verify the integrity of critical device-resident data, and where information can be secured for onward distribution or storage in the cloud.

SEAcurIT-e® is also beneficial to many other areas of application concerned with the protection of sensitive or critical data and services, such as end-to-end security, medical devices, the association of identities with keys, user authentication, and enhancing password security. It serves as a framework on which to build secure applications, or may be embedded in to existing applications.

The specific application described here is secure Cloud storage and document collaboration or sharing. This highlights some of the principle beneficial and unique features of SEAcurIT-e® that are relevant to both this and to other areas of application.

Prime features of this application

- Security functions such as encryption are applied at endpoints (user devices) prior to being passed to a Cloud provider.
- Organisations can then manage and control their own security, and security is independent of the Cloud provider. This removes the necessity to ‘give’ all your information to a Cloud Provider, which relies on the assurance that it will be protected by the Cloud Provider.
- The framework also readily supports the application of security functions at local gateways allowing a hybrid of local and gateway application.

The Challenge

To have common cryptographic keys (for encryption, integrity, authentication, etc) readily available to endpoints when needed that **effectively solves the difficult issue of how to securely store and protect such security values in software environments** where the use of dedicated security hardware is not appropriate, such as tablets, laptops or IoT devices.

To provide capable, scalable and robust management features that are crucial for **the effective control of security across both large and small organisations**, and deliver secure and reliable monitoring and control of data, devices, users and security values. Features should include the granting of access to information, and ongoing monitoring and control of which devices and users can access information and when it may be accessed.

One approach is to have centralised storage, but this essentially places all trust in a single system element (all eggs in one basket), with the consequence of failure of that element (such as by compromise or breach) being catastrophic. It also creates an ongoing security risk as keys have to be transported to endpoints every time that they are needed.

An alternative approach is to store keys at endpoints, but this leads to the important but problematic question of how to properly protect and manage these keys - a problem magnified by having keys stored at so many locations. Protecting such keys using passwords, for example, essentially reduces the strength of the cryptographic key down to the strength of the password.

SEAcurIT-e® effectively solves these issues. It has distributed security and trust, but with centralised management and control.

Distributed security and trust ensures that:

- There is no single location where all security and trust reside.
- There is no single point of failure.

Centralised management and control provides both *administrators* and *individual users* with the management and control features that they require.

With SEAcurIT-e®

Keys cannot be compromised by the compromise of an endpoint - more specifically, it is not possible (irrespective of computational power) to derive any information about stored cryptographic keys by analysing the contents of the device, thereby ensuring that the long term protection of security values is assured.

Can effectively provide in software the same security benefits as when using dedicated hardware devices such as USB tokens (but without the inconvenience), and bring those advantages to types of devices where the use of such hardware is not suitable or viable.

The SEAcurIT-e® framework is built around the management of cryptographic keys, which ultimately controls access to encrypted information.

- The system associates data with keys, so that controlling keys controls access to data.
- Each key is uniquely identified and tracked throughout the system. This is particularly relevant to when keys are shared, as is typically the case for document collaboration, or when a user has multiple devices.
- For any file, the encryption keys must necessarily be available to all devices and users that need access to the information, and so key distribution is a critical part of the solution. In contrast to PKI-type approaches, the export process allows the strictly enforceable specification of the user and device to which the key may be imported. Furthermore, the distribution process can be fully automated if desired - the exporting user simply specifies the intended recipient(s) using the management component, and the import process can be invisible to the user.
- The SEAcurIT-e® parameters on a device updated (or refreshed) transparently to the user and without requiring any change to the security values being managed or to user passwords.
- Monitoring and control of all security functions calls within a domain.

The SEAcurIT-e® management component:

- Associates individual users and devices with key identification information for those keys they have access to, allowing for the creation of user groups based on key identification information.
- Provides monitoring and control of which keys a user may access from any given device, which in turn controls access to information protected using that key.
- Allows remote removal of access to a key (and therefore any associated data) to specific users and devices, such as when a device is lost or stolen. Furthermore, access to the keys can be reinstated at a later time.

The architecture consists of a number of components, some related specifically to security functions, and some relating to user or device management. It is computationally infeasible to recover any security values from the information held by such components. These components may be managed and maintained internally by an organisation or they may be outsourced, but either way they together enable organisations to take control of the security of their data and devices.