An Introduction to SEAcurIT-e®

SEAcurIT-e® fortifies security and augments security management capabilities for software applications, giving solution providers and developers a clear differentiation in terms of security and control. Its scope is applications and services using cryptographic processes such as encryption, authentication and data integrity. It is applicable to applications ranging from user banking applications to Cloud-resident applications.

SEAcurIT-e® provides core security and control functions. It solves crucial and long-standing issues that are particularly relevant to application and system software, such as properly protecting cryptographic keys and other security values in software environments, efficiently managing security values across multiple devices, and providing effective control of the security functions themselves. It does not rely on single repositories of trust but maintains the benefits of centralised management capabilities.

SEAcurIT-e® can buttress and enhance PKI and other schemes for the management of cryptographic keys, adding distinct benefits and capabilities in security and control. Alternatively, it can serve as a robust and practical framework for constructing a wide range of secure applications.

For applications or devices relying on cryptographic secrets such as encryption or authentication keys, and particularly where dedicated security hardware may not be appropriate, security and control can be significantly enhanced by SEAcurIT-e®. More specifically:

- **Applications requiring user authentication, such as banking-type applications resident on endpoint devices**. Strong authentication utilising cryptographic methods relies on the protection and control of authentication keys. SEAcurIT-e is both a tool to strengthen the security of such authentication methods, or it can provide a complete solution itself. It supports multiple approaches, from the background and largely hidden use of authentication keys in applications using usernames and passwords, to where authentication keys must be available on more than one device, to overcoming vulnerabilities with weak passwords. Intrinsic resistance to malware attacks such as key-loggers. Device specific, with multiple devices and accounts efficiently managed and controlled.
    - Browser authentication is supported by a dedicated authentication scheme that counters *real-time* man-in-the-middle (phishing) attacks, or SEAcurIT-e® can provide key security elements of other approaches such as FIDO2.
    - Server-side deployment protects passwords and other user security values.
    - Identity management is facilitated by the association of identities with authentication values and devices, and powered by the centralised management and control capabilities, with different levels of operational control.
- **Applications requiring encryption.** Strengthen and enrich encryption security and control on endpoint devices, particularly where one or more users or devices are accessing shared or common encrypted content such as stored data. Ensure that stored sensitive information such as encryption keys used by, for example, Cloud applications are not accessible to either the Cloud provider or other unauthorised parties in what is an inherently accessible environment. Secure information for distribution, storage and processing by multiple parties.
- **Data integrity.** Verify the integrity of critical device-resident data (software attestation), such as for IoT devices.