

TURAYA™ Security Kernel



TURAYA™ Security Kernel

TURAYA is a high-assurance security kernel, developed for fulfilling highest security standards and incorporates Trusted Computing (TC) functionalities at the operating system level. TURAYA offers multilateral security protecting sensitive data, processed on enterprise computing systems, from misuse. Moreover, it uses virtualization and microkernel technology to provide strong isolation of critical tasks, so as to bar such threats as Trojan horses, viruses and worms.

- Enterprises benefit from realizing secure information workflow on their distributed network systems and the central management of all TURAYA-enhanced clients. In contrast to common systems and insecure operating systems in particular, the TURAYA Security Kernel provides an efficient information flow control on commercial of the shelf computing systems.
- Providers of digital content benefit by getting guarantees that their data is only processed according to defined policies as the TURAYA Security Kernel enforces security policies of the originator, even in distributed environments.
- Manufactures benefit from the ability to protect their Intellectual Property. That enables new business models as pay-per-use as well as the protection of valuable firmware in modern production systems.

Thus, TURAYA enables more secure and effective workflows. The TURAYA Security Kernel is available for different platforms, including embedded and mobile systems.



TURAYA™.TrustedDesktop

Comprehensive Endpoint Client-Security

TURAYA™.TrustedDesktop is based on strong isolation of critical applications and the reliable enforcement of security policies. Its innovative technology enables a comprehensive and auditable life-cycle protection of all enterprise data. The overall system guarantees that protected information is only processed by trustworthy components, proving their integrity is the mandatory requirement prior accessing any confidential data. Thus, any data leakage by malicious or accidental errors is prevented efficiently.

The security kernel virtualizes the legacy operating system on the client and enables multiple OS running concurrently and isolated in different compartments. Every compartment can be allocated independently to a Trusted Virtual Domain (TVD), each spanning a closed virtual processing area. Data leaving a compartment is seamless encrypted and can only be accessed in a local or remote compartment that belongs to the same TVD.

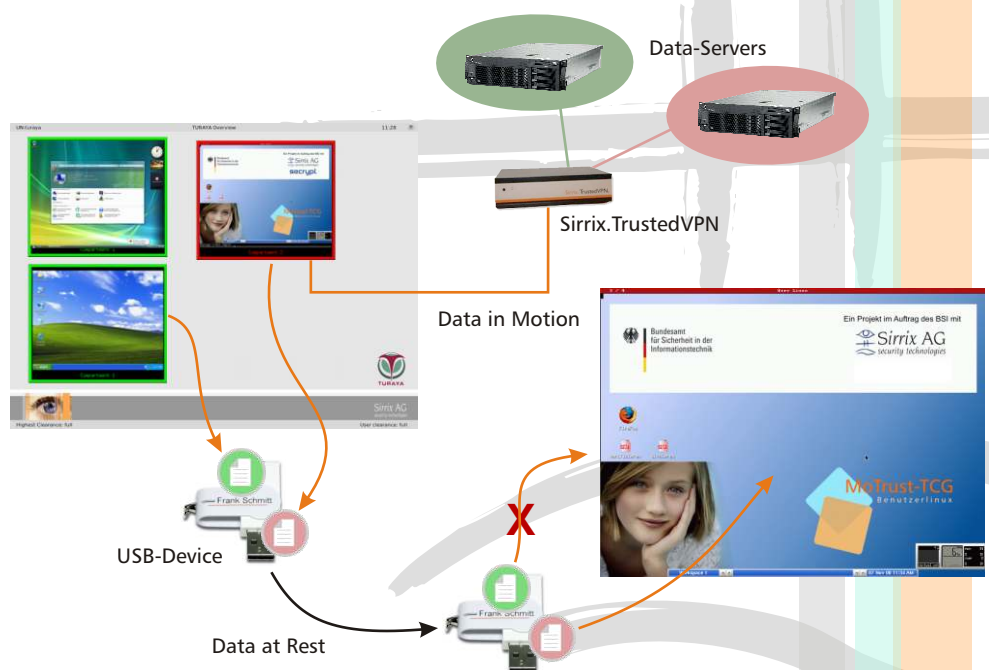
This concept is revolutionary as it enables for the first time efficient information flow control for enterprise systems working with legacy operating systems. This is made possible by security kernel technology along with the full employment of Trusted Computing technology.

TURAYA™.TrustedDesktop provides many security and functional features, enhancing the enterprise security and increasing the efficiency of workflows:

- Full harddisk-encryption, sealed to the TPM security chip. In contrast to other solutions, the encryption key is never seen by the operating system and thus, no viruses, trojan horses or other malware can leak or change sensitive key material.
- Intelligent VPN client enables secure links between compartments and dedicated virtual private networks.

- Comprehensive data leakage prevention with transparent file encryption. Instead of blocking I/O-devices like USB-sticks and external harddisks, the solution transparently encrypts data leaving a secured compartment and restrict the access to other compartments of the same TVD. Thus, it provides offline transport capabilities for exchanged data.

TURAYA saves real money: With a single license, a full-coverage solution is employed, including harddisk encryption, VPN client and data leakage prevention.



Seamless encryption and virtualization makes data leakage prevention being a feature, and no more an obstacle for efficient work.