eKrypto™ SDC (Secure Device Communication) Software Suite

The eKrypto^{TM} SDC (Secure Device Communication) is a complete software suite providing all of the elements necessary for managing secure networked I/O device communication.

eKrypto™ SDC Controls:
- ❖ Software Drivers
- ❖ Secure Key Management
- ❖ Smartlets
- ❖ Remote Maintenance and Programmability
- ❖ J/XFS & XFS Middleware Device Services
- ❖ EMV Level 2 Kernel
- ❖ Secure Logon
- ❖ Digital Signing
- ❖ Communications Port Management
- ❖ SDC VIRCOM - Migration of Legacy Systems

eKrypto™ SDC Software Drivers
The eKrypto™ SDC contains the software drivers and smartlets required for eKrypto™ Chip functionality along with the functionality of all I/O devices RS232 Serial or USB that may be controlled by the eKrypto™ Chip. Such devices may for example include integrated Smart Card Reader/s, Magnetic Card Reader, Check21 Dual Sided Image Reader, Cheque Reader, Scanner, LCD Display, Fingerprint Scanner, Signature Pad, Receipt Printer or Barcode Scanner. All the devices firmware is controlled by the SDC software, allowing In Application Programming of device firmware for ease of maintenance, optimum security and future proofing.

eKrypto™ SDC Secure Key Management
Each eKrypto™ Chip is loaded with a factory PKI certificate, allowing secure remote initial 3DES key load and secure distribution of firmware upgrades. Extension of these services can be provided for customers if required. The eKrypto™ Chip contains three encryption engines, 3DES, SHA-1 and PKI plus a True Random Number Generator.

eKrypto™ SDC Smartlets
eKrypto™ device controllers are loaded with a signed smartlet that dictates the device functionality. A secure transaction is only initiated on receipt and verification of a signed, trusted smartlet by the eKrypto™ device via the connected Host. An individual eKrypto™ device can support in excess of 18 applications as it is not limited to available SAM slots.

eKrypto™ SDC Remote Maintenance and Programmability
Application and firmware changes only require a smartlet revision plus each device is remotely programmable and supports secure remote key loading for greater security, maintenance convenience and cost savings. The upgrade process steps are (1) revision of smartlet (2) replacing the old smartlet file with the revised version on host server (3) automatic download of the new smartlet during next boot operation. A secure operation is only initiated on receipt and verification of a signed, trusted smartlet by the eKrypto™ device via the connected Host negating the threat of rogue updates.

eKrypto™ SDC J/XFS & XFS Middleware Device Services
The eKrypto™ SDC can include J/XFS or XFS Middleware Device Services where a JAVA or Windows middleware platform is being deployed. Device Services for non eKrypto™ devices can be created for clients on request.

eKrypto™ SDC EMV2000 (4.0) Level 2 Kernel

The eKrypto™ SDC can include the optional EMV2000 (4.0) Level 2 Approved Kernel when required by customers seeking a fully EMV compliant solution with EMV2000 (4.0) Level 2 Approved Keyboards and/or PIN Pads. An EMV L2 approved development application can also be provided to assist customer development of EMV compliant applications.

eKrypto™ SDC Digital Signing

The eKrypto™ SDC can be provided with optional Digital Signature application enabling operator / supervisor / customer digital signing and digital signature issuance for secure electronic signing of loan applications, direct debate mandates, secure home banking applications and furthering the move to a paperless environment.

eKrypto™ SDC Secure Logon

The eKrypto™ SDC includes optional Secure Logon application for deployment across the organisation allowing secure network, data and file access management. This functionality allows the provision of greater data access and electronic transaction functionality confident that a secure easily maintained infrastructure is in place that can be used for verifiable audit trailing and fraud prevention.

eKrypto™ SDC Communications Port Management

Coupled with the eKrypto™ Chip the eKrypto™ SDC can provide the engine for USB and RS232 Serial port connectivity by providing and managing the USB ports necessary for integrating peripherals such as PIN Pads and Receipt Printers. Where necessary the SDC can create virtual RS232 Serial and USB Ports for multiple integrated or connected device deployment where limited physical ports are available. The eKrypto™ SDC VIRCOM Solution (see below for more detail) enables organizations with non USB legacy applications but USB workstations to deploy eKrypto™ USB devices via USB ports but communicating in RS232 Serial form. When the organization eventually migrate the legacy application to USB, these devices can switch to full speed plug & play USB communication by simply issuing a revised signed smartlet instruction remotely from the host server.

eKrypto™ SDC VIRCOM - Migration of Legacy Systems

The SDC VIRCOM software enables the eKrypto™ Keyboard and/or PIN Pad to work with legacy serial applications over its USB infrastructure, therefore in the future when an organisation migrates its application to USB the device will continue to work seamlessly, only requiring a remote instruction to turn off the VIRCOM function in the SDC software. This technology combined with best of breed components and full remote programmability contributes to a product life expectancy of 10 to 12 years.

Using the USB based host interface architecture; the SDC VIRCOM driver includes a true virtual communications port for each RS232 serial device. The banking application continues to use the COM ports architecture in the driver for the individual RS232 serial devices interface (maintain actual device interface protocol). There is no application change required for this interface. Only the communications port name changes from the physical port (e.g. comm2) to the Virtual communications port (e.g. comm4).

eKrypto™ SDC VIRCOM Benefits:
- ❖ Huge Savings On Migration Cost And Time
- ❖ Devices Can Be Migrated At Clients Convenience
- ❖ Software Update Switches Device To Pure USB Mode
- ❖ No need for immediate revision of reliable legacy non USB platform