INSTITUTE VLATACOM

vKDD

Vlatacom Key Distribution Device

Product Description

Vlatacom Key Distribution Device (vKDD) is a robust terminal with tamper-proof encrypted memory. Its primary function is the distribution of sensitive data, like cryptographic keys. The built-in security access module (SAM) enables device authentication. The smart card reader in combination with the fingerprint scanner and rugged keyboard are used for reliable user authentication. The device has a large variety of connections which allows use with cryptographic equipment that originate from various manufacturers.

Key Features

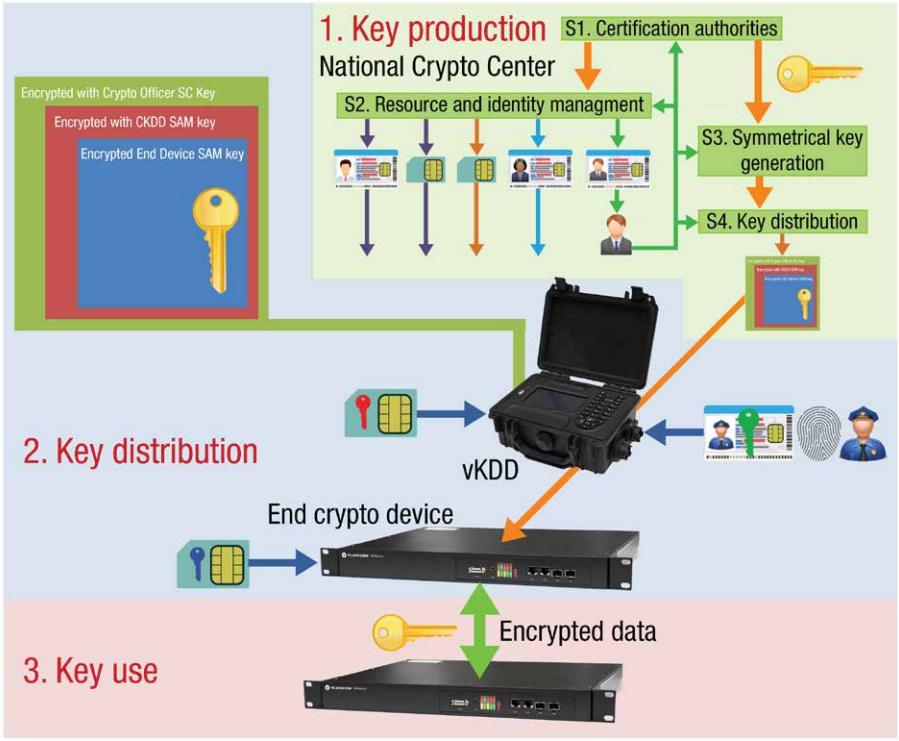
- Distribution of cryptographic sensitive material
- Device authentication by built in secure access module (SAM) contact type (ISO/IEC 7816)
- Contact smart card (ISO/IEC 7816) and contact less smart card (ISO/IEC 14443) interface
- Built in fingerprint scanner
- Multiple encrypted envelopes over transported data
- Digital signing of transactions using both device and user digital signatures
- Tamper proof memory for encryption keys and other sensitive data
- Waterproof case (when cover is closed)
- Dual Ethernet, USB and serial interfaces for connection with cryptographic equipment of different manufacturers
- Built in EMC shield over entire electronics
- Optional encrypted solid state drive for large volume transmission
- Compatible with Vlatacom National Crypto Center - NCC

Market

Reliable transport of sensitive material by dedicated couriers is mandatory at least in bringing cryptographic devices into service prior to the first secure encryption communication tunnels being established. For the highest security level systems, this procedure is also performed in the later operational stage of encryption devices. Thus, vKDD market is: government institutions, police, military, banking systems, telecommunication operators, data centers etc.

Use Case

Typical use case of vKDD is the transport of the initial set of cryptographic keys between the National Crypto Center, where the highest possible quality cryptographic keys are produced, to the cryptographic devices installed worldwide. The cryptographic keys, or other sensitive material, is first encrypted by the end device key, then by the particular kDD, and finally by the courier crypto officer key. When the crypto officer reaches the location where the encryption device is installed, decryption of the sensitive material is possible only after his successful multi-factor authentication and if all the keys from the crypto officer, end device, and vkDD match.



Benefits

- Strong device authentication and multi factor user authentication prevents device misuse
- Large variety of interfaces makes device customizable to cryptographic equipment of various manufacturers
- Tamper-proof memory, EMC shielding and multiple level encryptions along with strict operation procedure ensures data protection

INSTITUTE VLATACOM

Address:
Vlatacom institute d.o.o.
Milutina Milankovića 5
11070 Belgrade, Serbia

tel: +381 11 377 11 00
fax: +381 11 377 11 99
info@vlatacom.com
www.vlatacom.com