

Key Production System

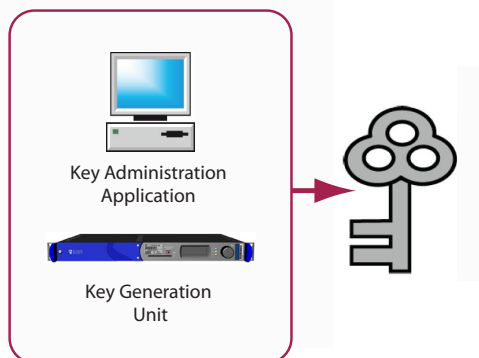
Production of encryption keys in the SecuriVPN system

Key Production System

One of the most critical parts in a security solution is the integrity and confidentiality of the encryption keys used. The production, distribution and storage of these keys are essential parts in the security of such a system. To provide the highest possible quality, the SecuriVPN system consists of a high-grade key production system. Encryption keys are generated with hardware-based mechanisms.

System Overview

The Key Production System (KPS) is a stand-alone system consisting of a Key Generation unit and a Key Administration application.



The Key Generation unit generates the encryption keys. It has a built-in high-class random generator, which guarantees the quality of the key material.

The Key Administration application is used to manage the key production. The application has an easy to use graphical user interface, which guides the user through the process of generating and exporting the encryption keys.

Customization

Customers may prefer to use their own already nationally approved random number generator, in that case interfaces can be implemented on a project basis.

Security features

- Emergency erasure of keys
- Tamper evident chassis
- Configuration & fault-localisation guide
- POST (Power On Self Test)

Good! But, how about the key?

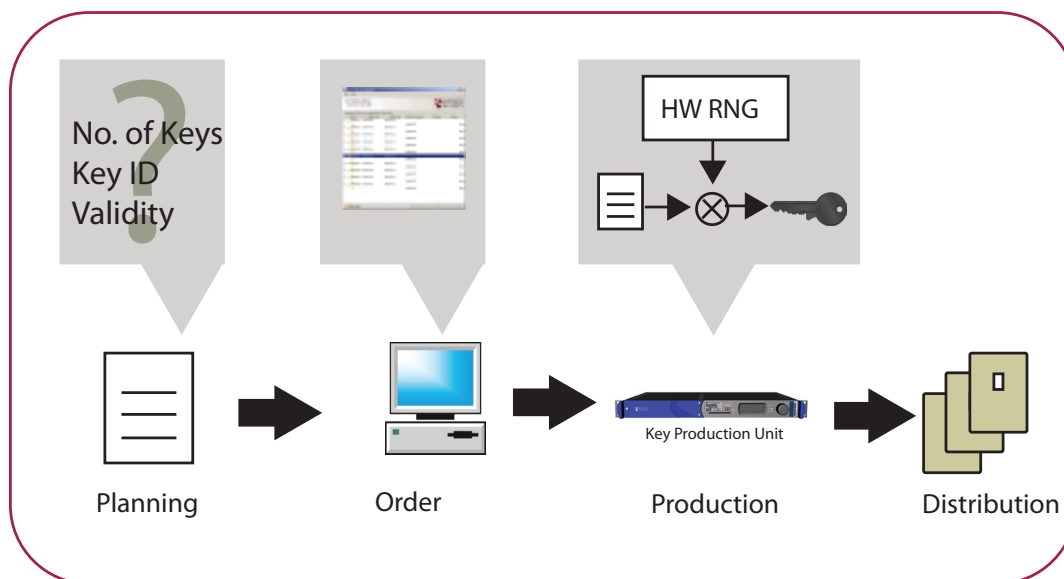
”Encryption itself is simple, it’s just mathematics. The hard bit is controlling the keys - the secret codes that have the power to unlock the data.” ”Once encrypted, information only becomes readable if the encryption key is available to unlock it. Consequently, the key becomes as valuable as the data it is protecting. This situation can be likened to the security of a home - locking the house significantly increases the security of its contents. However, if the key is then left under the mat, then the level of security is compromised.”

Source: *End-to-end encryption is the key to protecting data and reputations* | Tech News on ZDNet http://news.zdnet.com/2100-9595_22-363861.html



Key Production process

The key production process consists of four steps; Planning, Order, Production and Distribution.



Planning involves things like estimation of number of keys required, key sequence planning, key validity decisions, receiving units etc.

In the order phase the information gathered during planning is entered into the Key Administration application and transformed into a Key Order containing all information required by the Key Generation unit to produce the keys.

In the production phase the Key Generation unit generates the encryption keys specified in the Key Order.

In the distribution phase the produced encryption keys are exported to a PIN-protected smart card. Keys are always distributed in wrapped (encrypted) form i.e. as black keys ensuring that plain text keys are never exposed outside of the production system. The keys are not un-wrapped until they are loaded and used by the encryption unit.

In future releases of the SecuriVPN system it will also be possible to distribute encryption keys online using the Central Administration System.

Key Administration application

The configuration application is installed on a PC with the following minimum requirements:

Runtime environment:	Java SE 6 or later
Processor:	Intel Pentium class
Internal memory:	1 GB
Available disk space:	160 MB
Graphics:	1280x1024, 256 colours

Further requirements:	
CD reader:	CD-Rom reader
Smart card reader:	PC/SC

Technical data

The Key Production System has the following technical data:

- Key Generation unit has fibre optic or electrical Ethernet interface
- Height of Key Generation unit is 1U and mountable in a 19" rack system
- 256-bits AES key algorithms
- 256-bits key lengths HMAC using f-cbc integrity protection algorithms
- Hardware based random number generator

Supported key types

- Device Ignition Keys (DIK)
- Master Keys
- Shared Keys

as secure as it gets



Business Security AB

Box 110 65

S-220 11 Lund, Sweden

Tel: +46 46 38 60 50

Fax: +46 46 38 60 55

E-mail: reqinfo@businesssecurity.com

URL: www.businesssecurity.com