ENCRYPTION USED
BY NATO & THE
DANISH DEFENCE

DENCRYPT

DENCRYPT CORE

OEM Integration Of Dynamic Encryption

Dencrypt Core is a customer-specific package of the crypto components required to integrate Dynamic Encryption into existing or planned products. Dynamic Encryption is applied anywhere that strong end-to-end encryption is required. Dencrypt Core is delivered to both HW and SW platforms with full support for integration, test and release. Dencrypt Core applies to a broad range of applications, such as satellite and mobile communications, backbone networks, IoT devices, sensors and vehicles.

Dynamic Encryption

Based on the customers' product specifications, Dencrypt designs a customised Dencrypt Core, applying the principle of Dynamic Encryption for maximum protection.

HW/SW Platforms

Dencrypt Core is available for both HW and SW platforms. The delivery of Dencrypt Core is a joint integration project, where Dencrypt engineers deliver the customised implementation as well as support and tools for integration, test and release.

Customised For Optimal Performance

Dencrypt tailors the solution for the specific application and ensures optimal performances for security, speed, latency and with the preferred API. Dencrypt provides support for the entire product lifecycle.

Dynamic Encryption Everywhere

Dencrypt Core applies to a broad range of applications, such as satellite and mobile communications, backbone networks, IoT devices, sensors and vehicles.

DENCRYPT Arnold Nielsens Boulevard 72 | DK-2650 Hvidovre | Phone: +45 7211 7911 | info@dencrypt.dk | www.dencrypt.dk

ENCRYPTION USED
BY NATO & THE
DANISH DEFENCE

DENCRYPT

DENCRYPT CORE

Dynamic Encryption

Dynamic Encryption is Dencrypt's patented technology that Vincent Rijmen, coinventor of the AES encryption standard and a world-renowned cryptologist, has called state-of-the-art cryptology.

Dynamic Encryption provides additional security by changing the encryption keys as well as the cryptosystem for each new data transmission.

An outer, dynamic encryption layer wraps a standard, static encryption algorithm – such AES-256 or a national encryption algorithm. The outer layer is selected from a vast pool of re-alisations, ensuring that no two data transmissions are ever encrypted using the same cryptosystem.

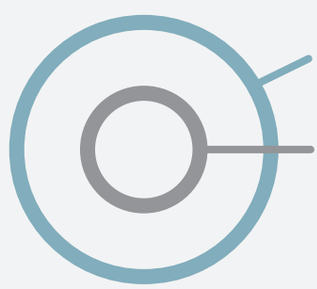
As a minimum, the security of Dynamic Encryption is equal to the security of the inner, static algorithm. In practice it is more secure, as it contains additional encryption components.

Added value

Applying Dynamic Encryption to products and solutions adds value in numerous ways:

- Effective prevention of cryptanalysis attacks that require a vast amount of data encrypted by the same crypto-system
- "Moving target" defence strategy. With an ever-changing cryptosystem, attackers cannot automate their attack, but are forced to change their methodology for each new data transmission
- Lifetime extension. As the dynamic layer shields the inner algorithm from attacks, the Dynamic Encryption principle is used to extend the lifetime of a cryptosystem

Dynamic Encryption



Dynamic Encryption
Mutating algorithm,
changing keys

Eg. AES,
changing keys

The principle of Dynamic Encryption was invented in 2012 by Lars Ramkilde Knudsen.

Lars is a professor of cryptology at the Technical University of Denmark and the designer of several recognised crypto-systems, among others Serpent and DEAL, which reached the final round in the NIST competition in 1997.

Dencrypt has the exclusive right to use the patent for Dynamic Encryption.

Patent: PCT/EP2012/071314

DENCRYPT Arnold Nielsens Boulevard 72 | DK-2650 Hvidovre | Phone: +45 7211 7911 | info@dencrypt.dk | www.dencrypt.dk