Dynamic Encryption

Key take away:

Communication infrastructures cannot be assumed secure

→ **Apply security on application level.**

Søren Sennels, COO

Dencrypt A/S

Advanced encryption solutions.

End-to-end encryption across insure networks.

Dynamic Encryption Principle.

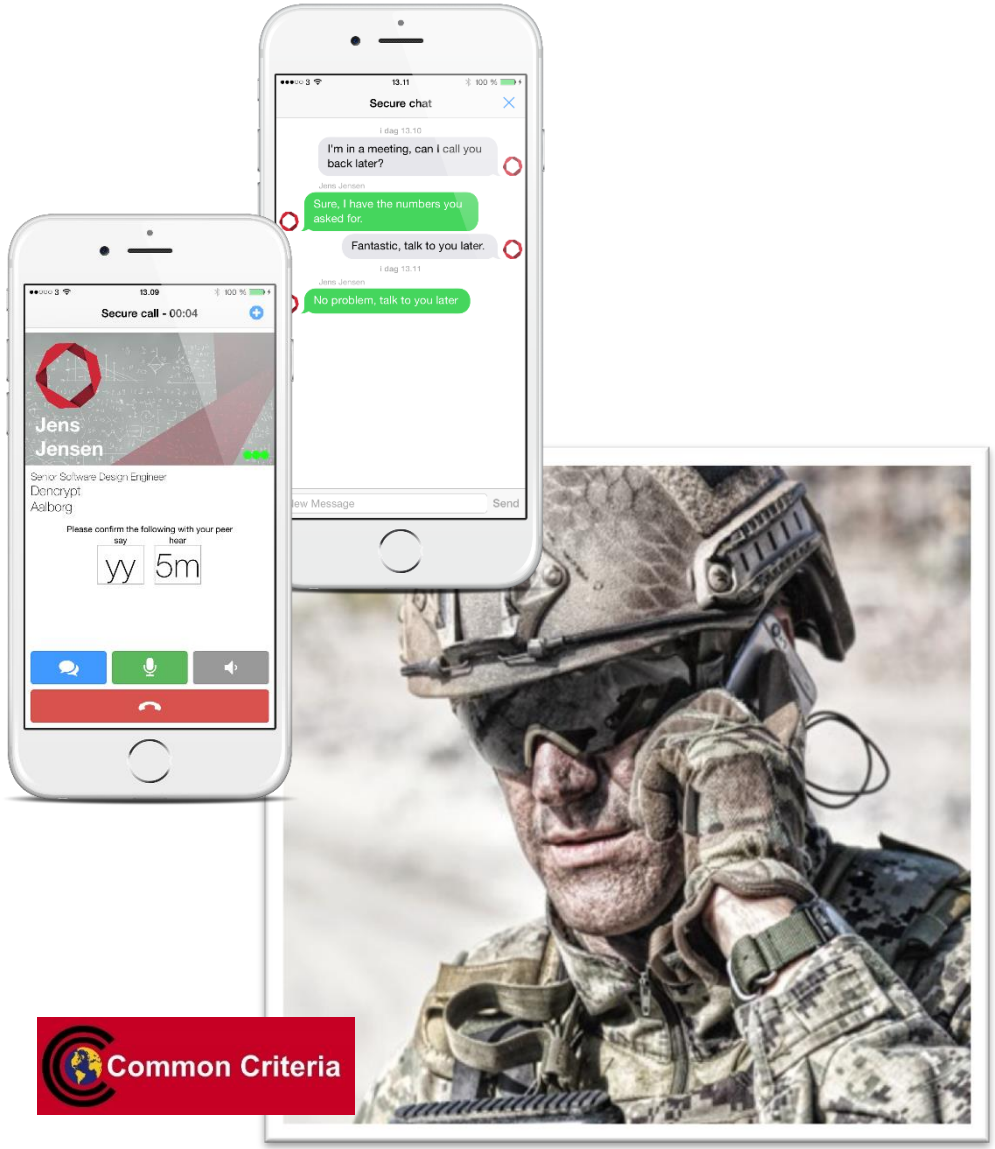
Secure mobile voice calls & messaging

- Common Criteria certified.
- Accredited for classified information.

Dynamic encryption for OEM integration.

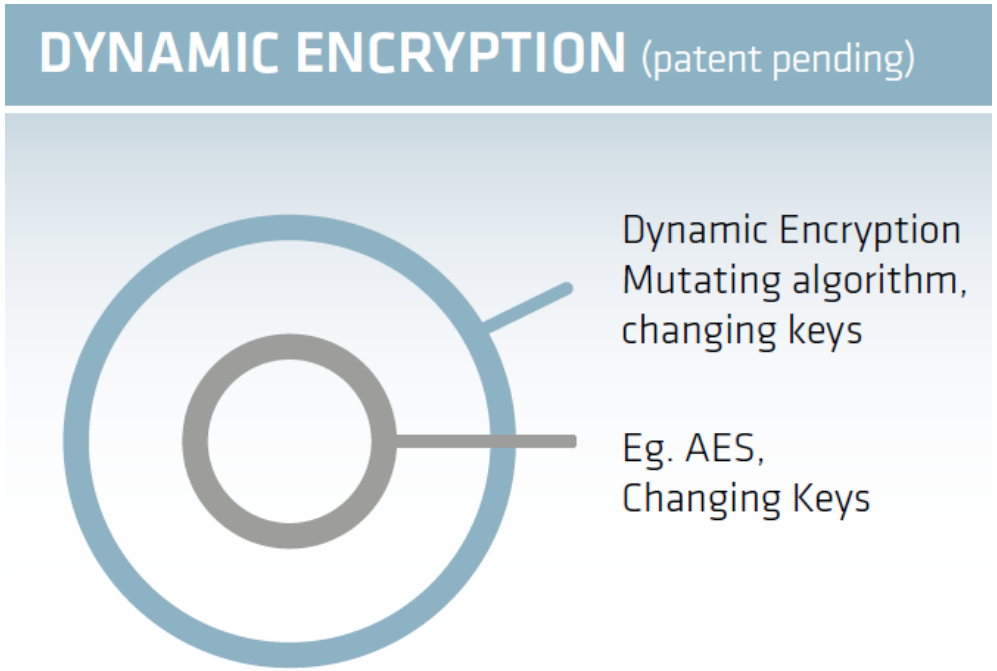
Key references:

Danish Defence, NATO.



DENCRYPT

Dynamic Encryption principle



Novel technology:

Change cryptosystem for each new data transmission.

Proven minimum security.

Today >95% of all data is encrypted using the same standard (Advanced Encryption Standard, AES).

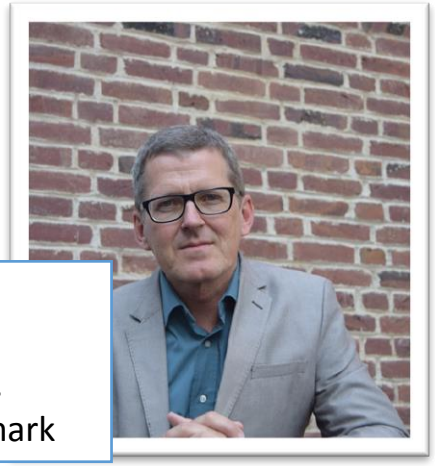
Why:

Extend crypto life time

Moving target defence

Prevent crypt analysis attacks

Enhanced protection

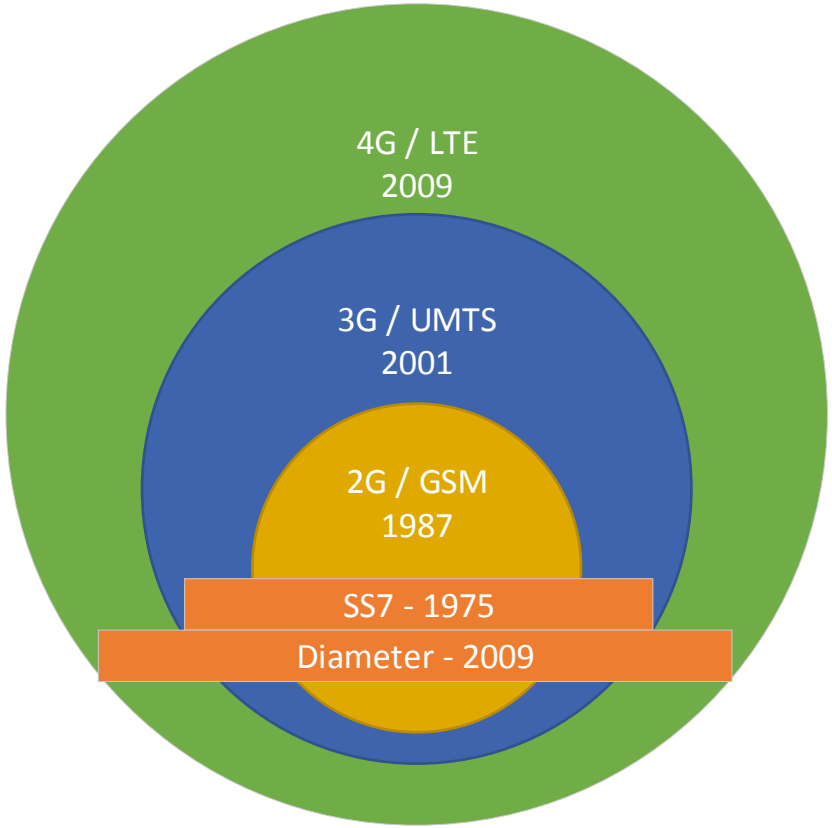


Invented by:
Prof. in Cryptology
Lars Ramkilde Knudsen.
Technical Univ. of Denmark

DENCRYPT

Problem: Mobile infrastructures can not be assumed secure

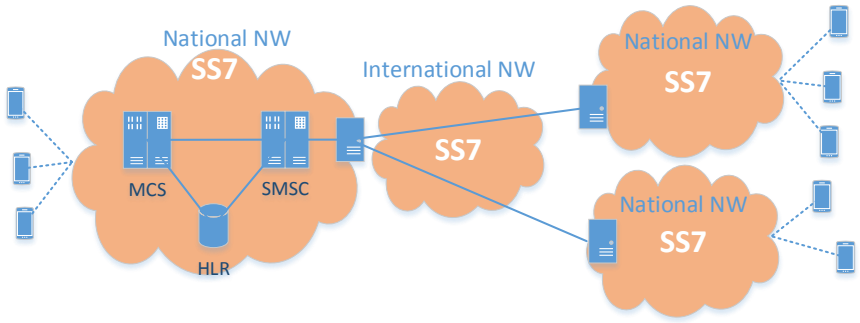
- Today's mobile systems are a result of an evaluation.
- Contain legacy components and protocols
  - Not designed with todays' security implications in mind.
  - Not designed to provide acces for a plethora of 3rd party content providers.
- Attackers force system to use the weak protocols.
- Weaknesses are difficult to mitigate.



Attacks: Signalling System 7 / Diameter

SS7 / Diameter:

Signalling protocal between mobile network core element.



Un-authorized access to core network elements.

- Purchased from 3rd parties
- Misconfigured network elements

Wide range of attacks:

- Location tracking
- Intercept
- Denial of Service
- Spam
- Fraud

60 minutes: Hacking your phone
April 2016

O2, Germany
May 2017

DENCRYPT

Attacks: Signalling System 7 / Diameter

ENISA:

European Union Agency for Network and Information Security

Risk assessment:

"…medium to high level of risk in this area."

Mitigative actions are being implemented be operators, but:

"…, but these measure assure only a basic protection level"

"More effort need to be made so an optimal protection level is achieved."

Future perspectives for 5G:

"…., there is a certain risk of repeating history."

DENCRYPT

Communication infrastructures cannot be assumed secure

→ **Apply security on application level.**