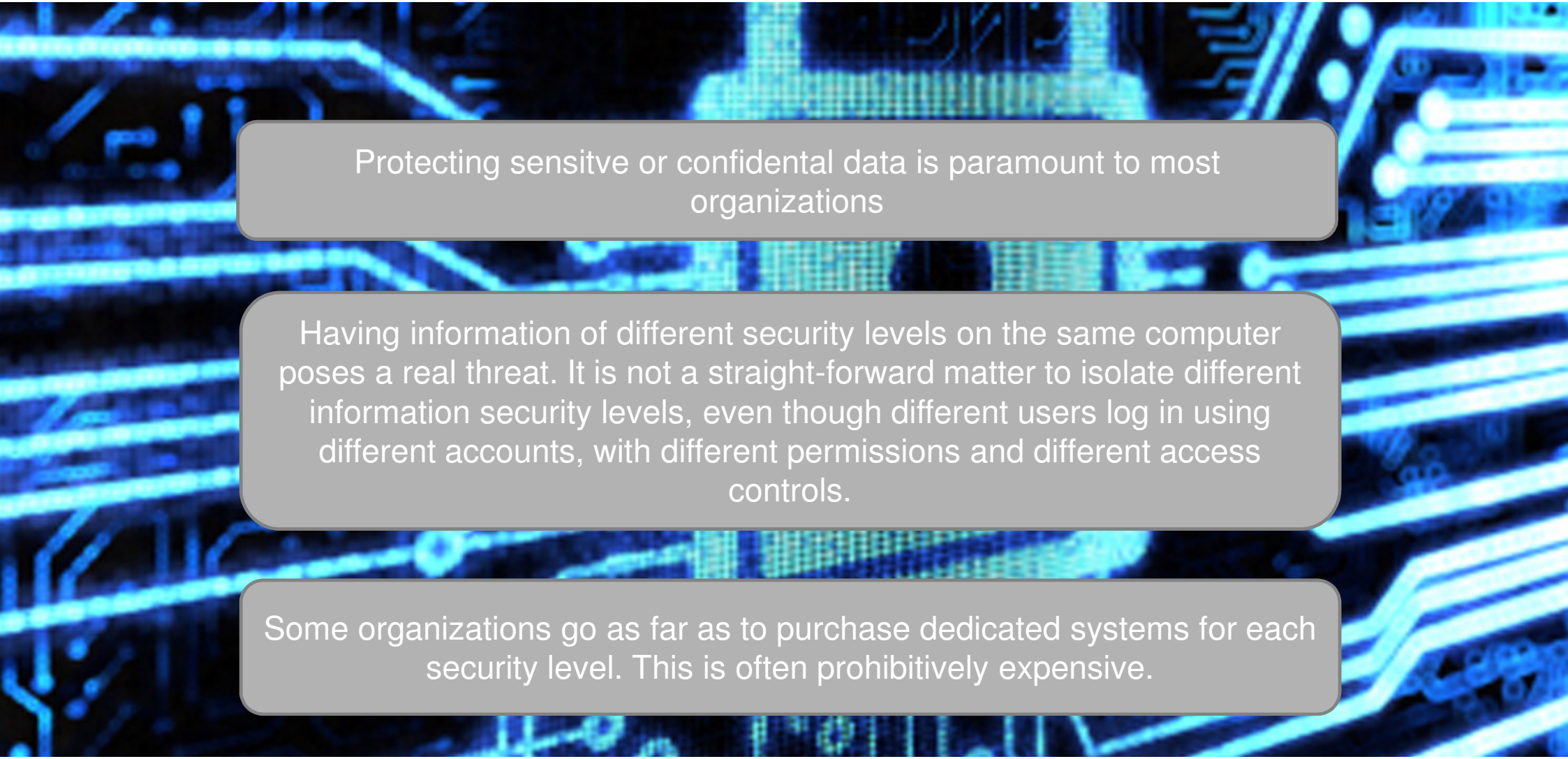
secunet

“FMN / MLS – Lessons learned”

Praha November 12th, 2013

Holger W. Kalnischkies

MLS → a definition



Protecting sensitve or confidental data is paramount to most organizations

Having information of different security levels on the same computer poses a real threat. It is not a straight-forward matter to isolate different information security levels, even though different users log in using different accounts, with different permissions and different access controls.

Some organizations go as far as to purchase dedicated systems for each security level. This is often prohibitively expensive.

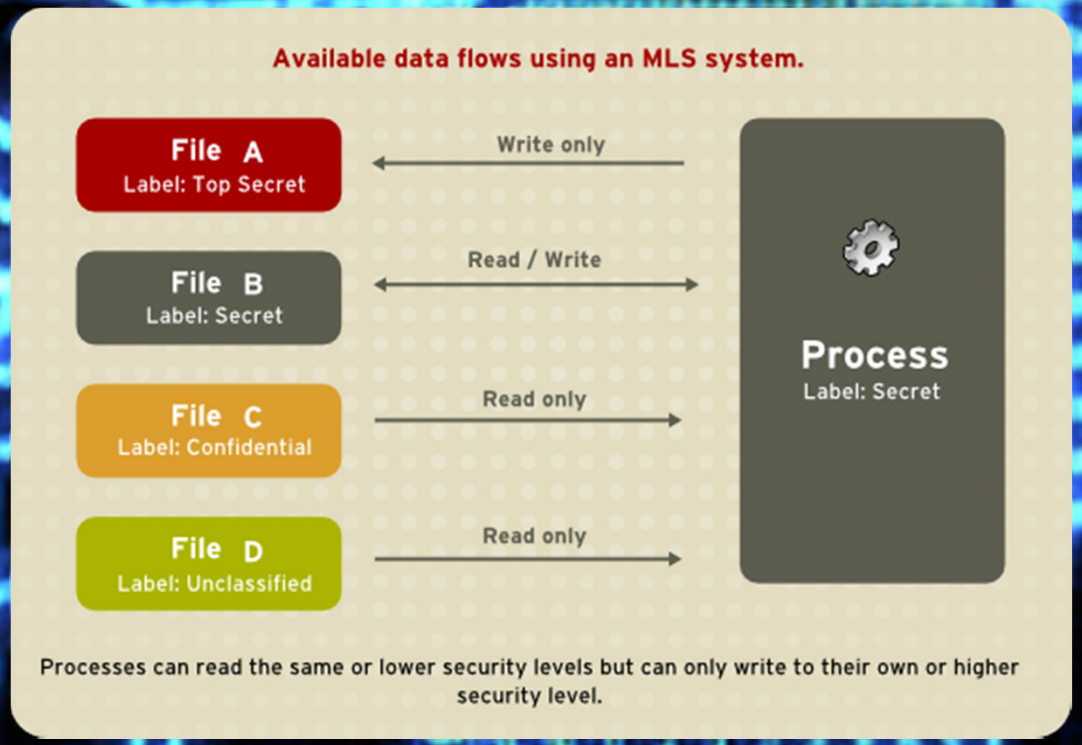
MLS → a definition

The term arises from the defense community´s security classifications: Confidential, Secret, and Top Secret

Individuals must be granted appropiate clearances before they can see classified information

Data flow operates from lower levels to higher, and never revers

Bell-La Padula Model (BLP)



No read up, no write down model

Confidentality

Schutzziel Vertraulichkeit

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

Authenticity

Schutzziel Authentizität

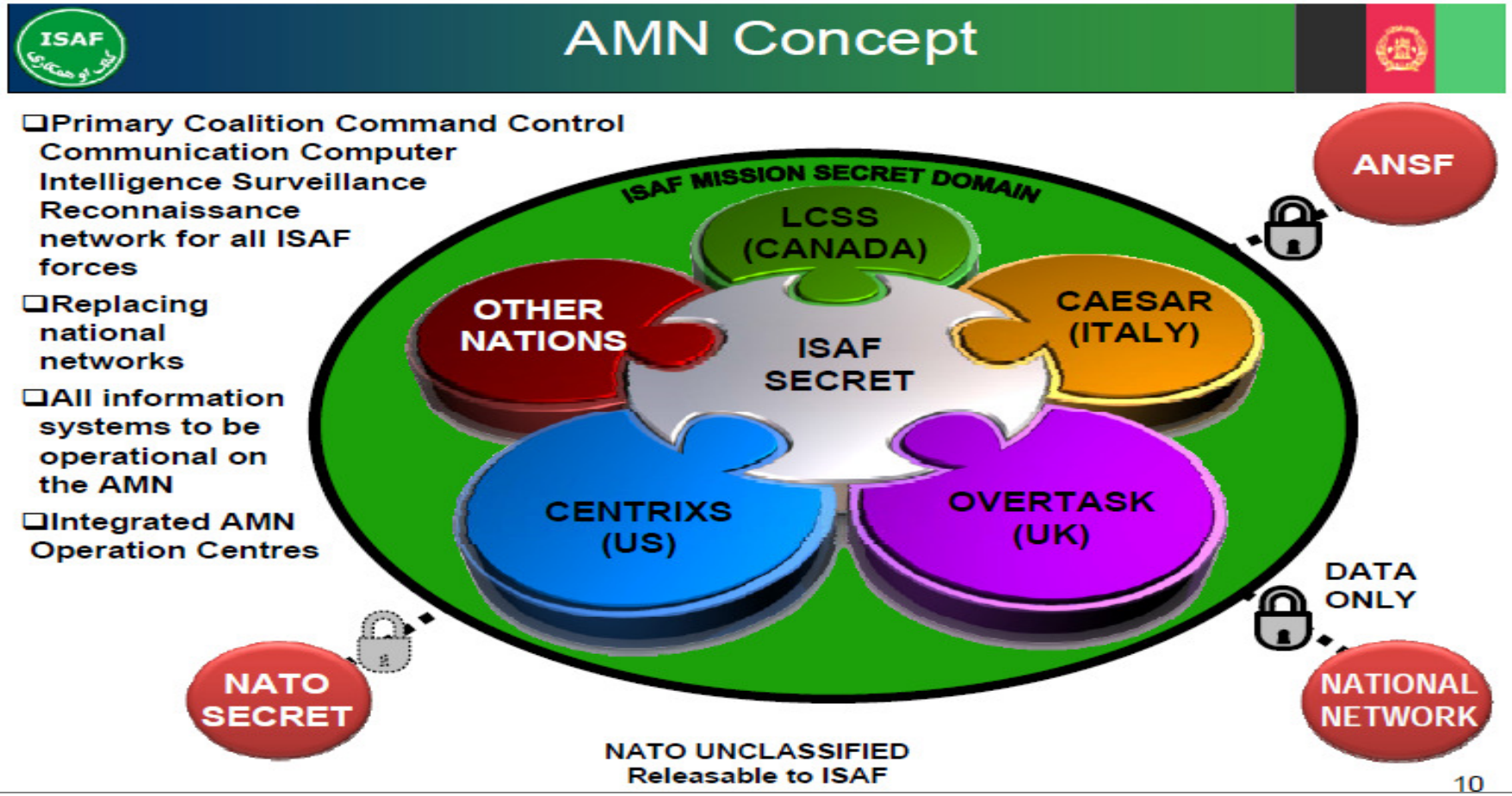
Die Authentizität ist gegeben, wenn Echtheit und Glaubwürdigkeit gewährleistet sind. Informationen sind dann eindeutig ihrem Absender zuordenbar.

Integrety

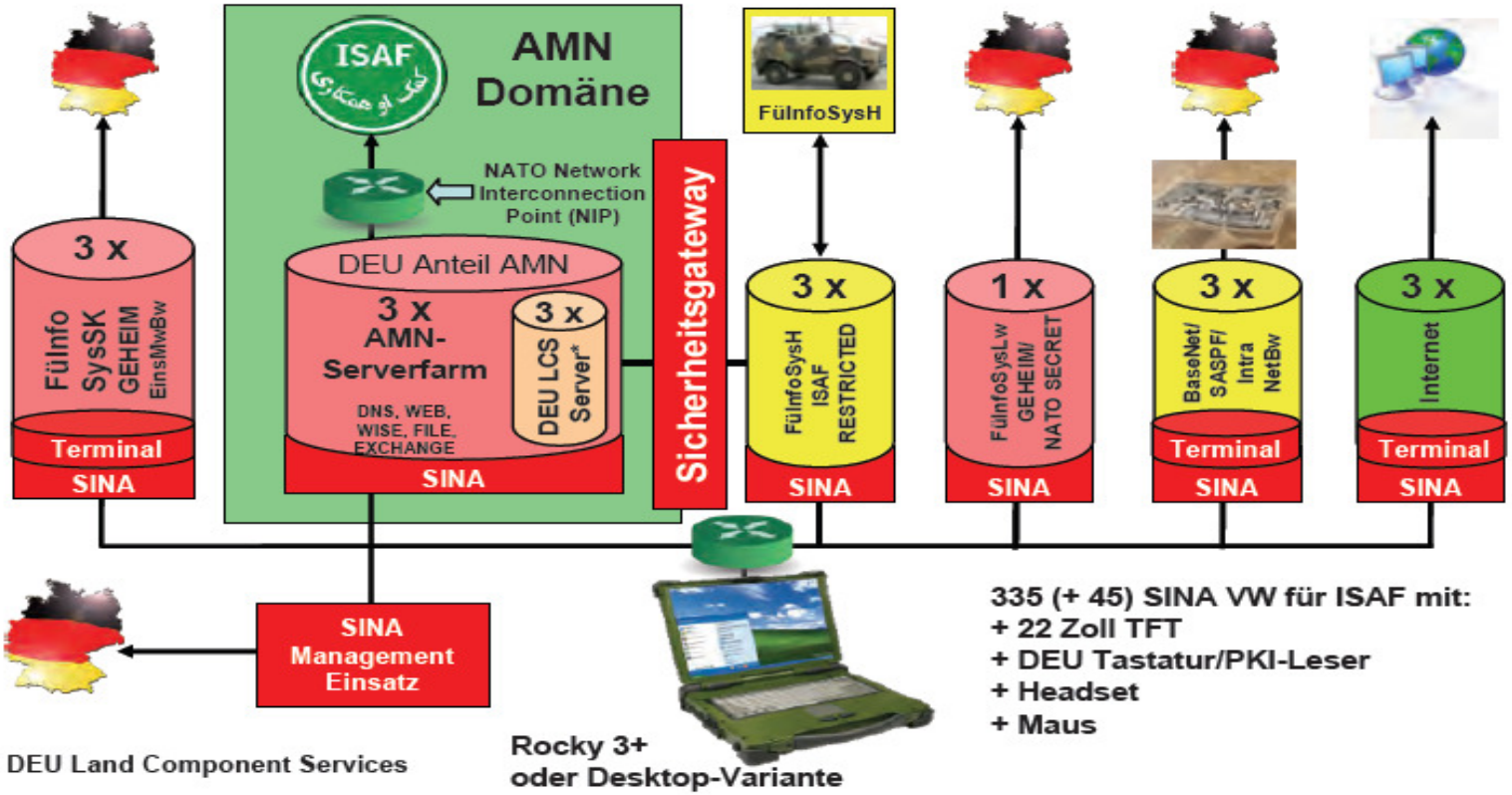
Schutzziel Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und Informationen und der korrekten Funktionsweise von Systemen.

Idea of Afghanistan Mission Network



Client / Server Architecture – German Extension of AMN

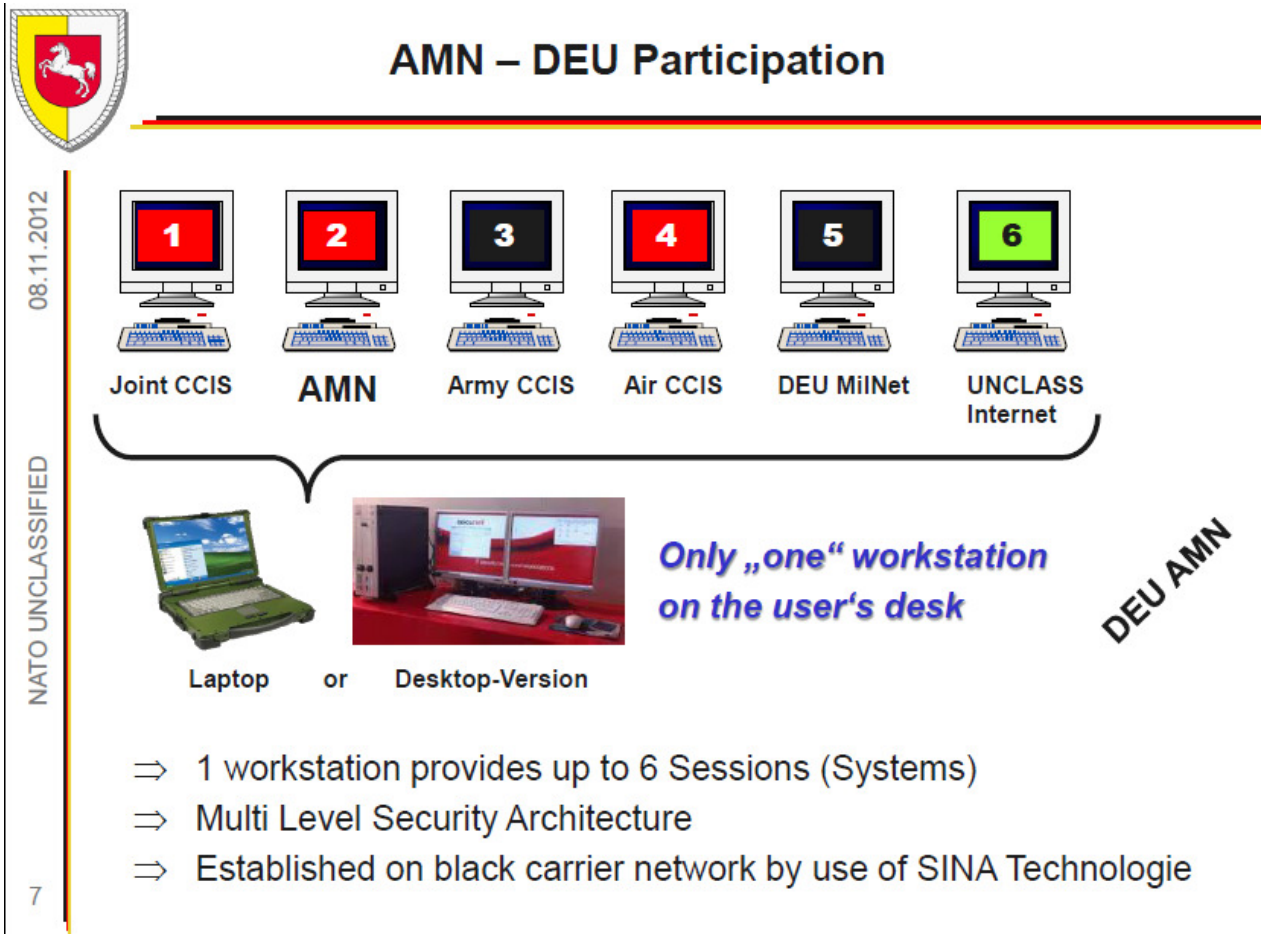


Desktop-based SINA Workstation E (Zone 1) in AMN Configuration

Source: ANTENNE 3/2011

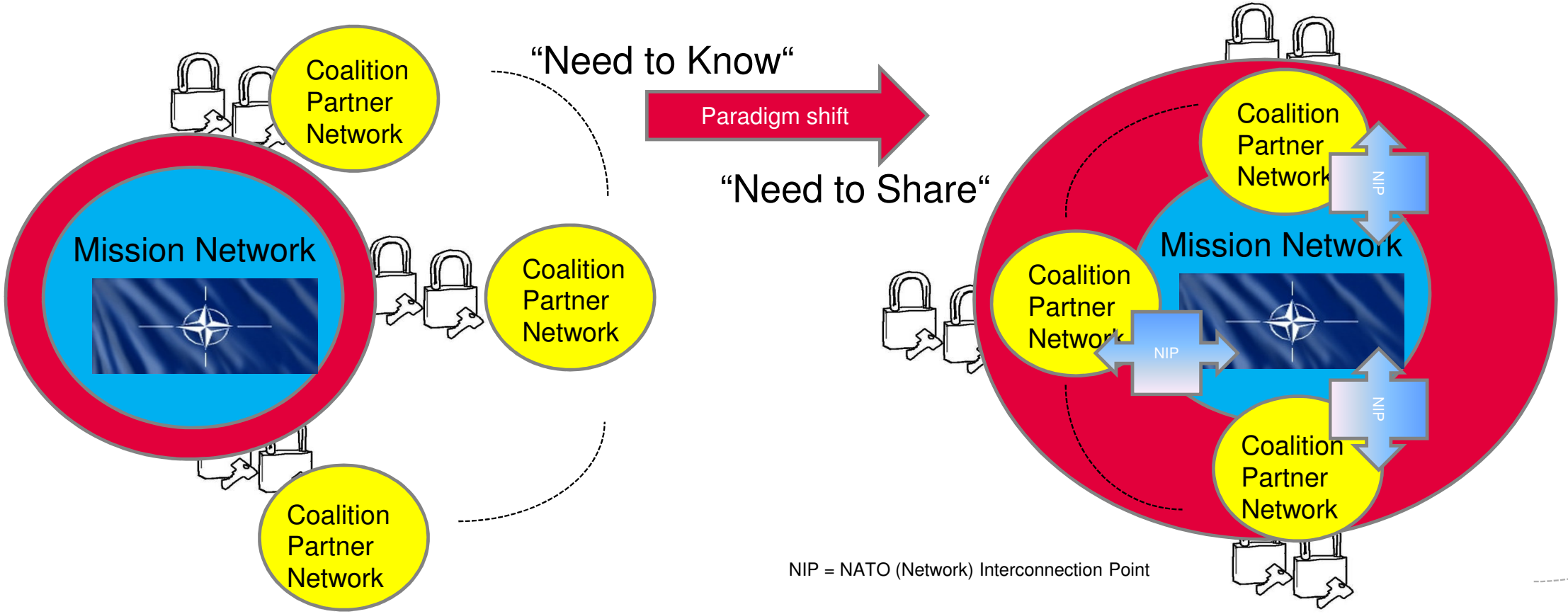
Change from „Need-to-know“ to „Need-to-share“

Afghanistan Mission Network
Afghan Mission Network
Allied Mission Network
Future Mission Network
Federated Mission Network



Source SPADE 2012

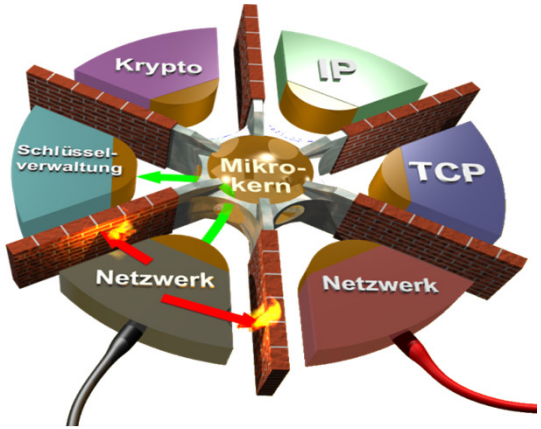
Lesson Learned

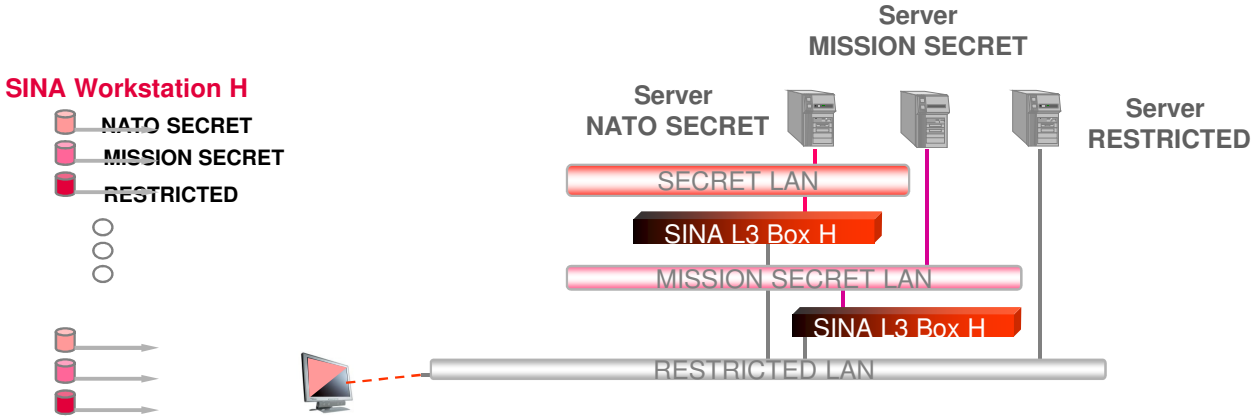


NIP = NATO (Network) Interconnection Point

Deduced Generic Requirements

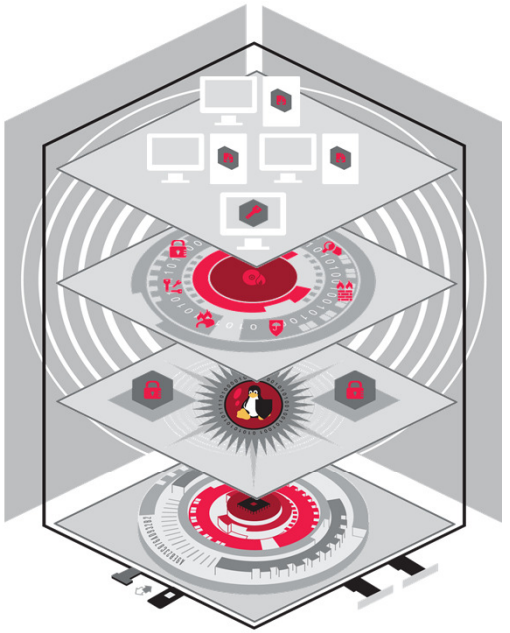
- Virtualisation
- Minimalized and Secured Operating System
- Multi Mission Capable
- Flexible Crypto (Classes, Groups, Parameters)

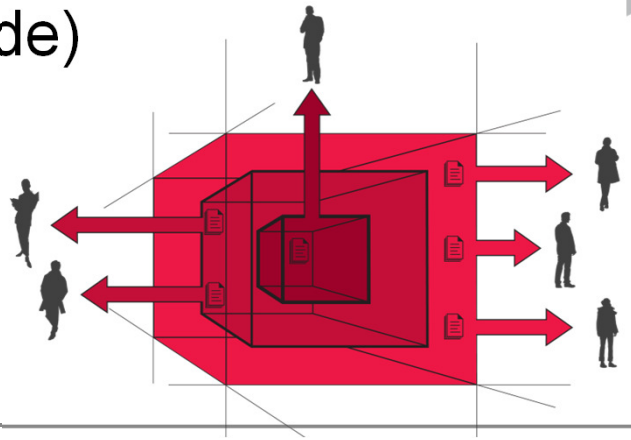




Deduced Generic Requirements

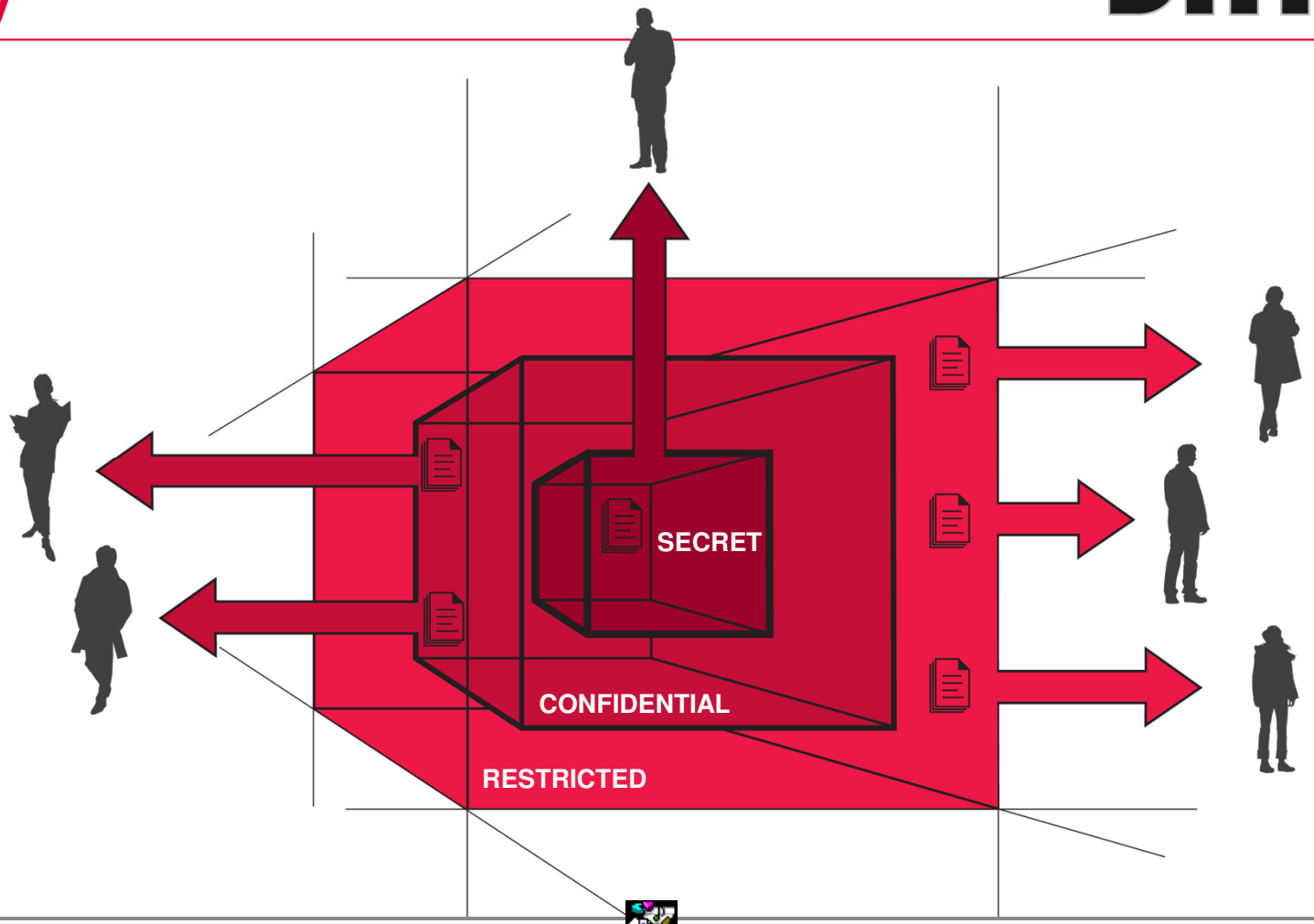
- “Seperation“ by Crypto
  - Multi Domain Support (>= 6 Sessions)
  - Multi Grade Support (up to SECRET)
  - Custom Grades (SECRET_1 to SECRET_X)
  - Multi Level Data Separation
    (at least Compartmented Mode)





Holistic Security

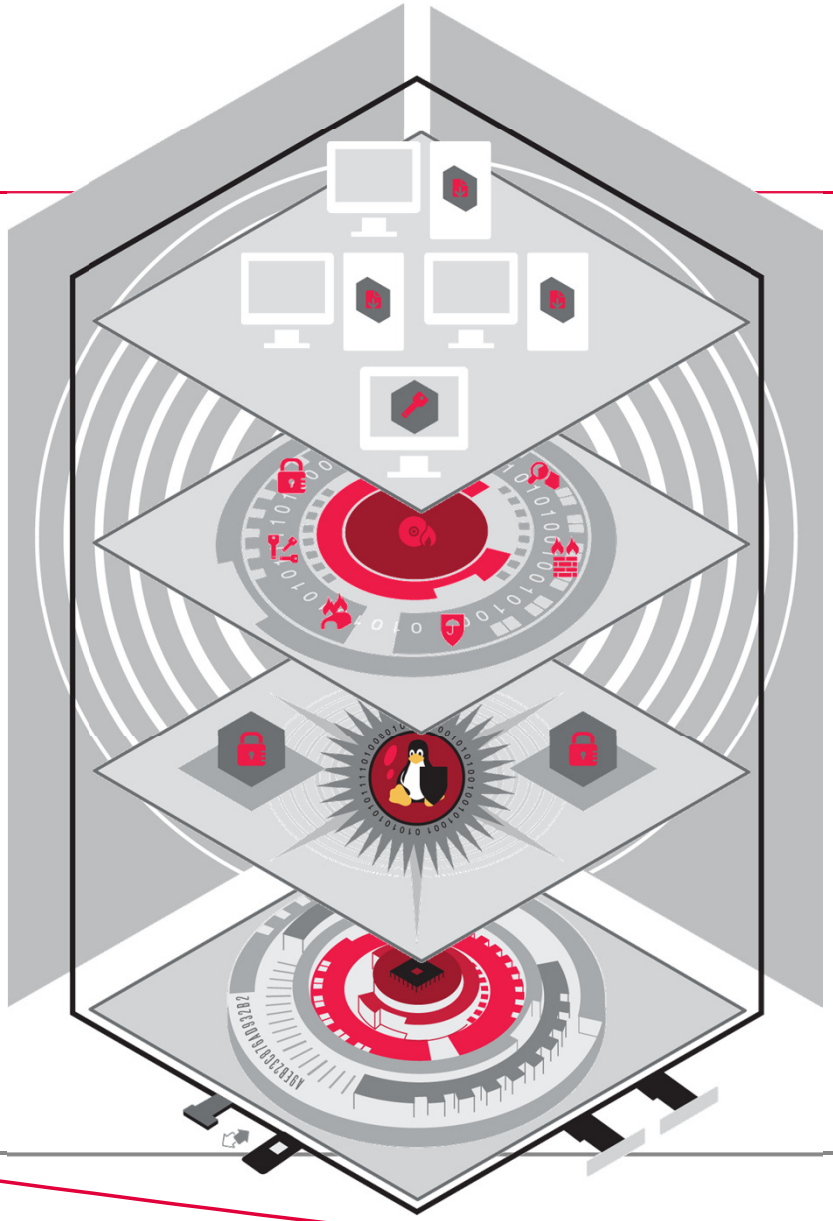
- multi level
- innovative
- flexible
- integrated
- efficient
- compact



Package

Multiple Levels of Security

- **Applications and virtual guest operating systems**
  separated sessions of varied classification
- **IT Security Functions**
  multistate supplementary security features
- **Secure System Platform (SINA Linux)**
  pruned, hardened and intensely evaluated
- **Hardware and Firmware (SINA BIOS)**
  including smartcards and crypto modules
  dimensioned and configured to conform to approval standard

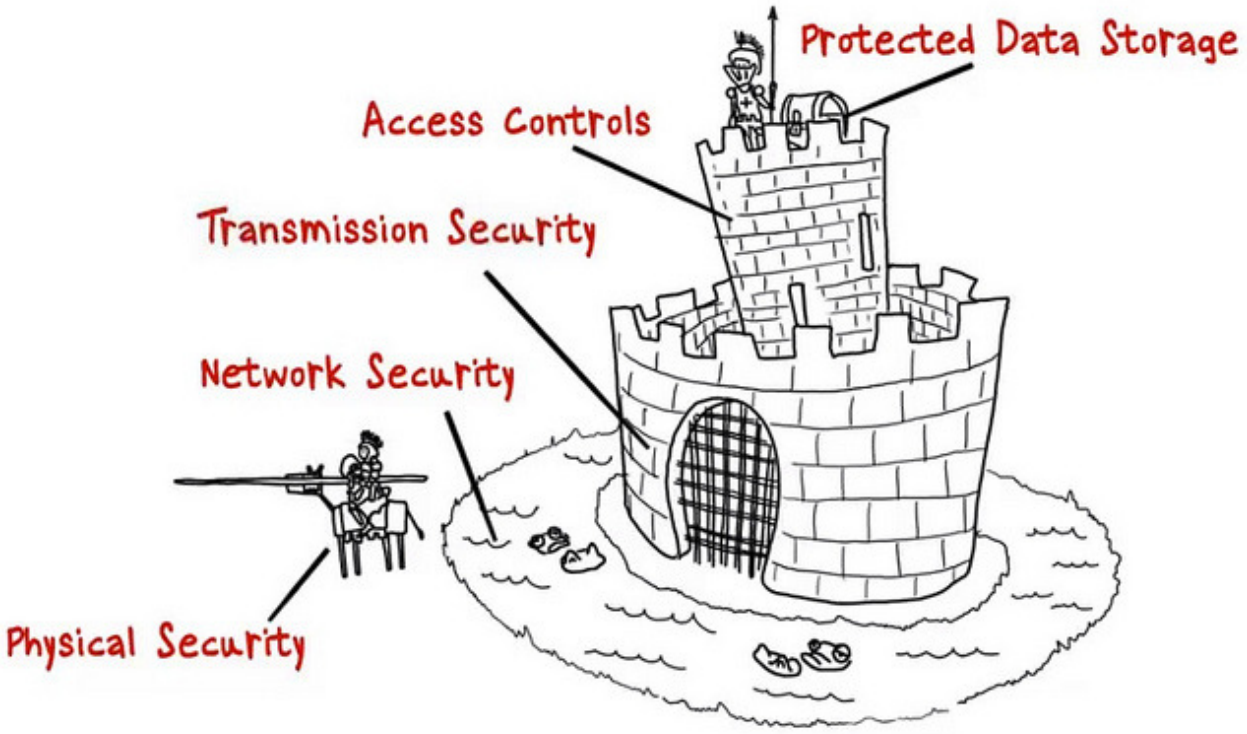


Package

SINA Workstation Functionalities

- SINA Workstation supports “Need to Share“ approach in a classified IT environment
- All relevant data and information can be shared secure between mission / networks
- Usage of secure SINA workstation platform allows reduction of IT-system complexity
- Multiple security domains possible e.g. mission domain, mission national extension, national domains
- Multi-level security possible e.g. open, restricted, confidental, secret
- Reduction of number of end user clients and spare part logistics

Multi-Level Security is the Ideal



Federal Office
for Information Security

Approvals (October 2013)

Product	Germany	NATO	EU
SINA L3 Box	VS-NfD	NATO RESTRICTED	RESTREINT UE
	VS-VERTRAULICH	NATO CONFIDENTIAL	CONFIDENTIEL UE*
	GEHEIM / STRENG GEHEIM	NATO SECRET*	SECRET UE*
SINA One Way	GEHEIM	NATO SECRET	—
SINA L2 Box	VS-NfD	NATO RESTRICTED	RESTREINT UE
SINA Terminal	VS-NfD	NATO RESTRICTED	RESTREINT UE
	VS-VERTRAULICH	NATO CONFIDENTIAL	CONFIDENTIEL UE*
	GEHEIM / STRENG GEHEIM	NATO SECRET*	SECRET UE*
SINA Workstation	VS-NfD	NATO RESTRICTED	RESTREINT UE
	VS-VERTRAULICH	NATO CONFIDENTIAL	*CONFIDENTIEL UE (coming soon)*
	GEHEIM	*NATO SECRET (coming soon)*	*SECRET UE (coming soon)*

For approval-compliant operation, the regulations and security notes specified in the relevant BSI approval certificate have to be observed

* Under 2nd evaluation.

secunet

secunet

secunet Security Networks AG

Holger W. Kalnischkies

holger.kalnischkies@secunet.com
www.secunet.com

Q & A

Sharing of files within sessions of same classification, for example two virtual sessions „restricted“

Due to current certification and best practice sharing of files even within sessions of the same classification is prohibited. This would undermine the security features of seperation kernel.

However, sharing is possible through a USB device in the same classification level (if the security polocy allows usage of storage devices).

For future product development a sharing option for restricted systems, utilizing the the transfer virtualization and crypt-module is considered and under testing.

Q & A

Which classification is used in the Transport-Network AMN-DEU?

The transport network AMN is classified as „restricted“ in layer 2 (payload encryption). The national networks are classified restricted, confidental, secret, national secret and NATO secret. Those networks as well as the „Mission Secret“ network are layer 3 encrypted.

Basically this idea is used in the current plan of NATO protected core network. The whole „NATO cloud“ or NATO transport network will be based on a layer 2 encrypted system. Considering the heavy utilization of routers and the idea of NINE encryption standard the target timeframe 2016-2017 is a development challenge. NINE encryption standard is still not finalized and under discussion.