RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

#RSAC

SESSION ID: SPO1-T09

Trust in Mobile Enterprise – Have We Lost the Game?

MODERATOR:

Prof. Dr. Norbert Pohlmann

Professor Computer Science Department for Information Security, Director of the Institute for Internet Security – if(is) at the Westphalian University of Applied Sciences Gelsenkirchen, Germany *and* Chairman of the board of the IT Security Association TeleTrusT

PANELISTS:

Ammar Alkassar

CEO of Sirrix AG security technologies, one of Germany's leading security suppliers

Dr. Kim Nguyen

Chief Scientist Security, Bundesdruckerei GmbH *and*
Managing director, D-Trust GmbH

Dr. Hans-Christoph Quelle

Managing Director of Secusmart GmbH, a BlackBerry company

What is the Right Security Solution for Mobile Computing?

Classification in Protection Classes

Share (# of devices out of all)

Class 0 Consumer

- Threat: privacy of personal data, Cybercrime *100%*

Expected costs: adds 5% to personal IT costs | products and vendors: achieve market trust

Core Classes for Enterprises

Class 1 Companies, authorities

- Threat: Cybercrime (higher degree of risk), compliance, **legal privacy protection** *70%*
- Expected costs: adds 10% to IT | products and vendors: certified for effectiveness

Class 2 Companies, authorities, infrastructure

- Threat: Cybercrime, targeted attacks on corporate values, **corporate espionage** *27%*
- Breach of security leads only to individual damage
- Expected costs: adds 20% to IT | products and vendors: certified by internationally approved bodies

Class 3 Companies, authorities, infrastructure

- Threat: Economic espionage (intelligence services) and cyber attacks, **cyberwar (sabotage)** *3%* *+ cost of infrastructure*
- Breach of security leads to collective damage
- Expected costs: adds 50% to IT | products and vendors: certified by nationally approved bodies

Class 4 Classified (beyond Restricted)

- National Security, Protection requirements: according to classification regimes *0,01%*
- Expected costs: adds 400% to IT | products and vendors: approved and certified by national authorities

Appropriate Mechanisms

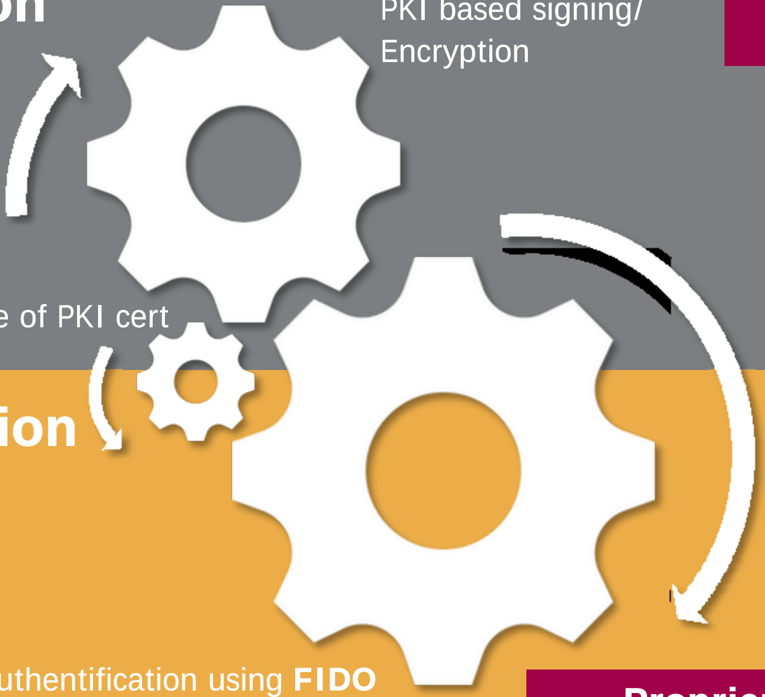
MDM, VPN, Secure Messaging, Voice and Cloud, Container solution

+ Secure Operating System, Mutli-factor authentication, Approved PKI, End2End Encrypted Voice, Messaging and Cloud, E-Mail encryption

+ Hardware-based 2-factor authentication (Smartcard, Token)

Authentication and Identification Worlds

Identification



PKI based signing/ Encryption

Post issuance of PKI cert

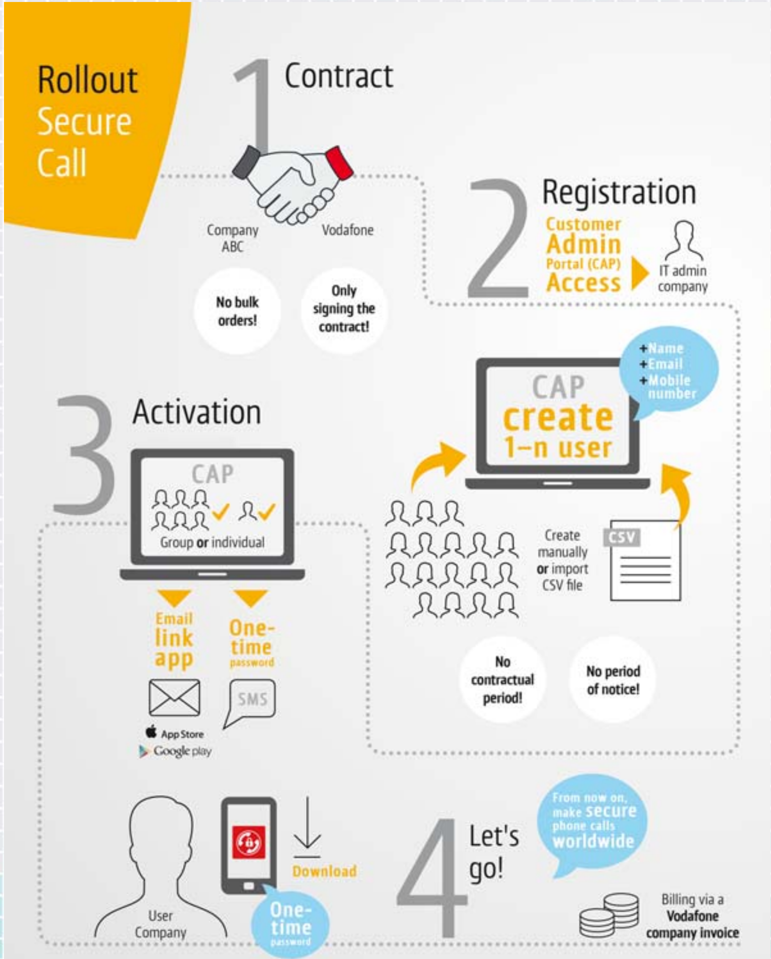
Authentification using **FIDO**

Governmental eID Solutions
with officially verified ID

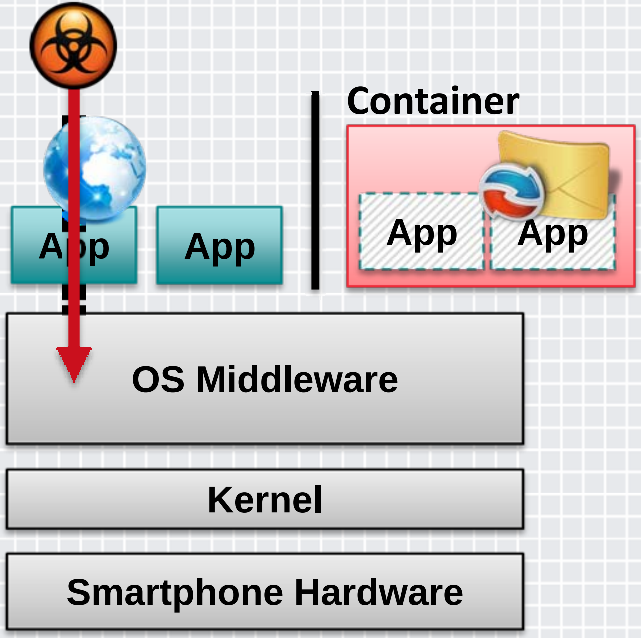
Authentication

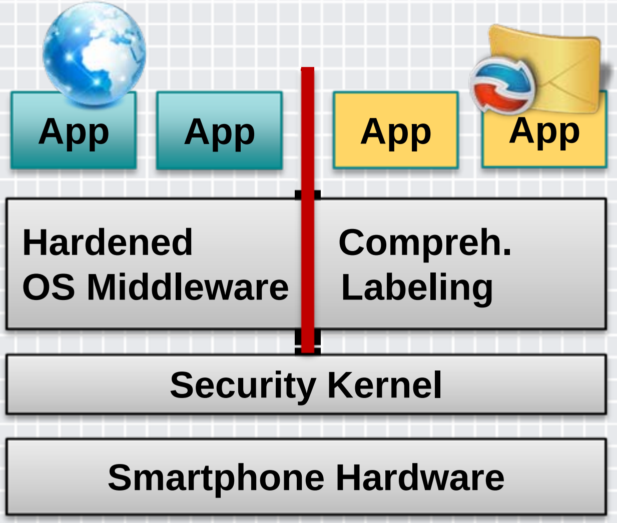
„Proprietary“ authentication systems
e.g. usernames/passwords, AppleID, token…

Which Security Level can the IT Security App achieve?

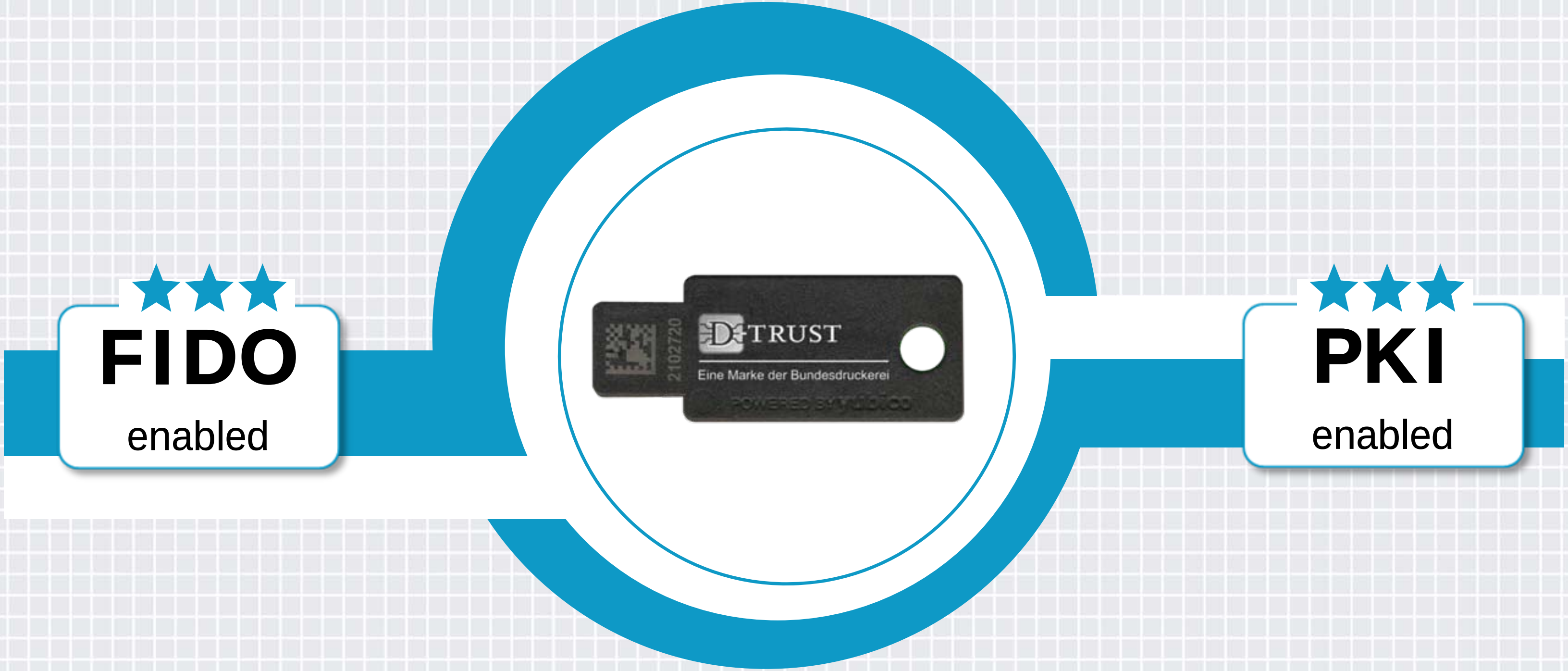


Why are Containers not Sufficient for Enterprise Level Protection?





ONE TOKEN

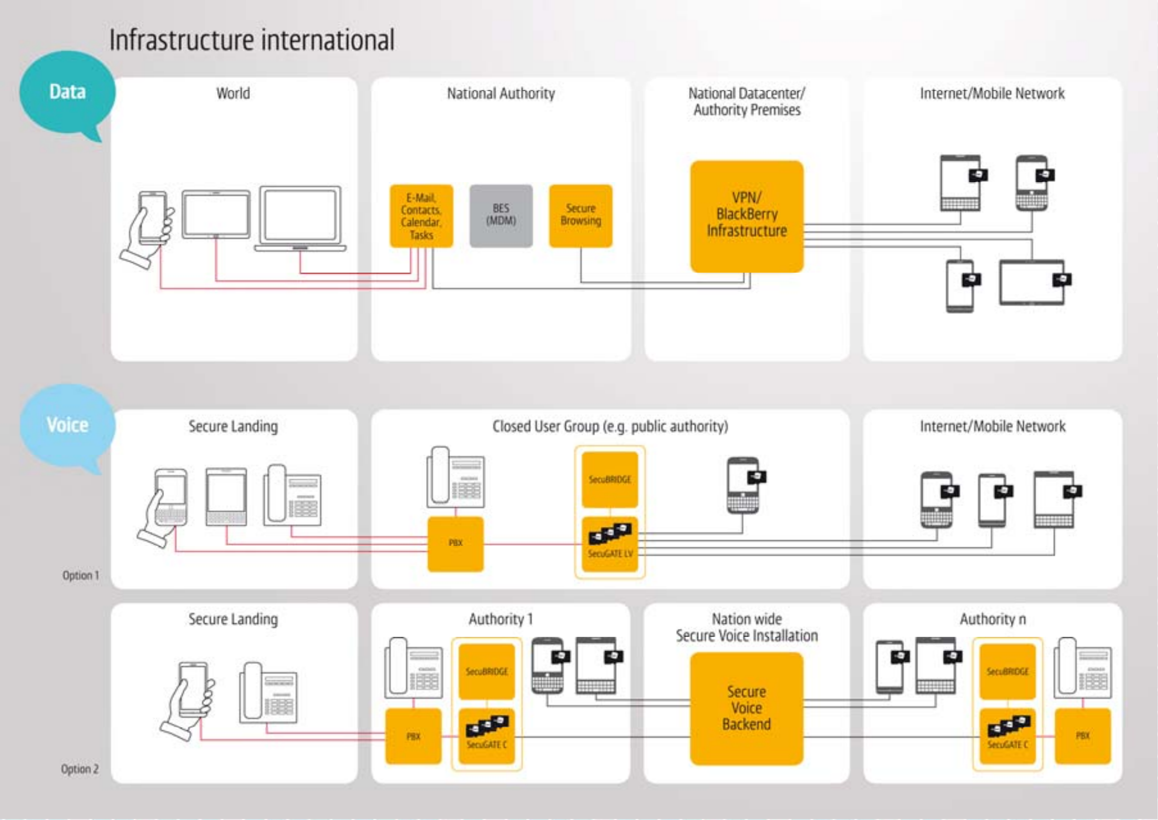


★★★ **FIDO** enabled

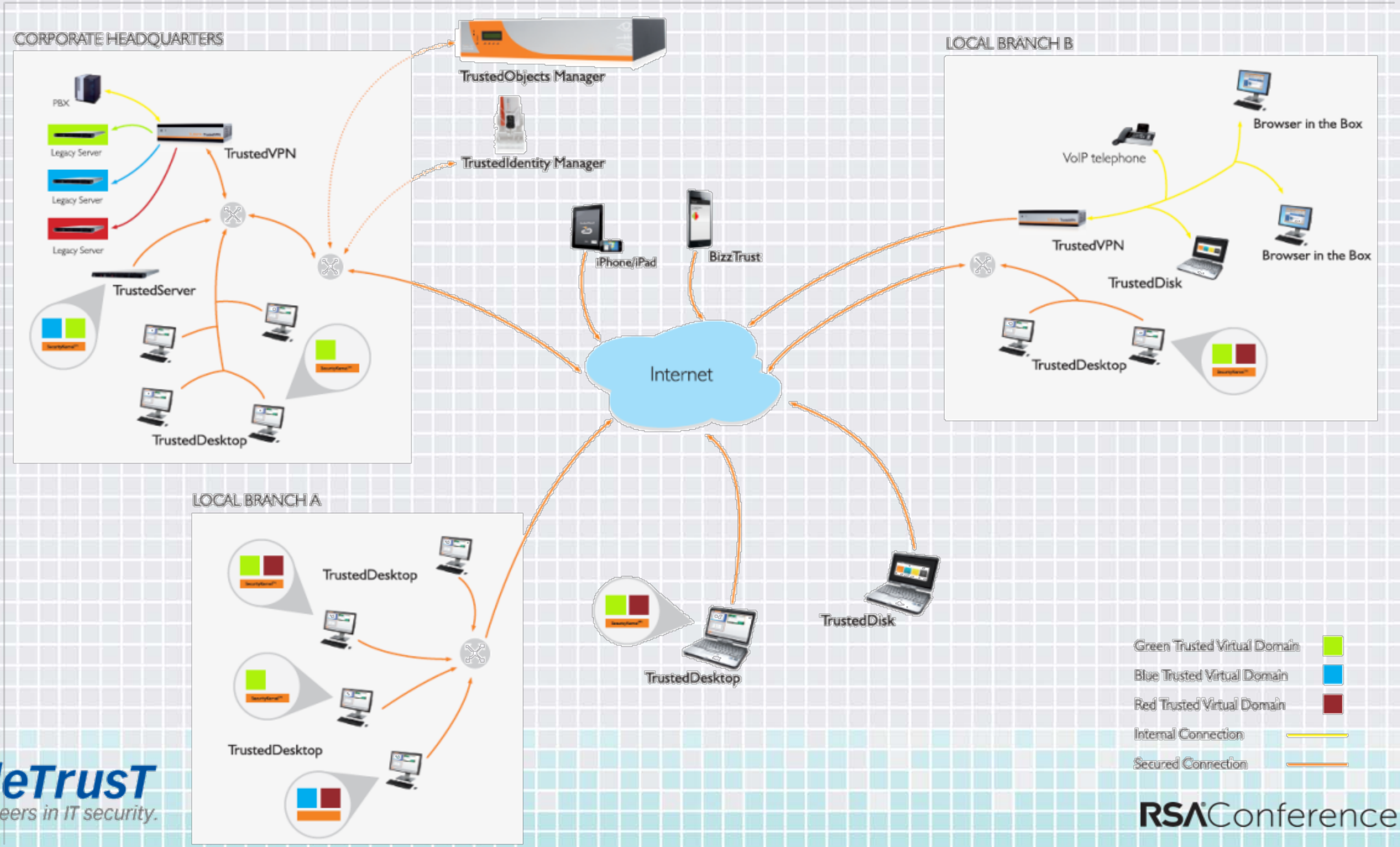
★★★ **PKI** enabled

TWO WORLDS

Which Security Level can a full IT Security Smartphone achieve?



Why Mobile Enterprise Security needs Enterprise-Wide Information Flow Control?



Green Trusted Virtual Domain 🟩

Blue Trusted Virtual Domain 🟦

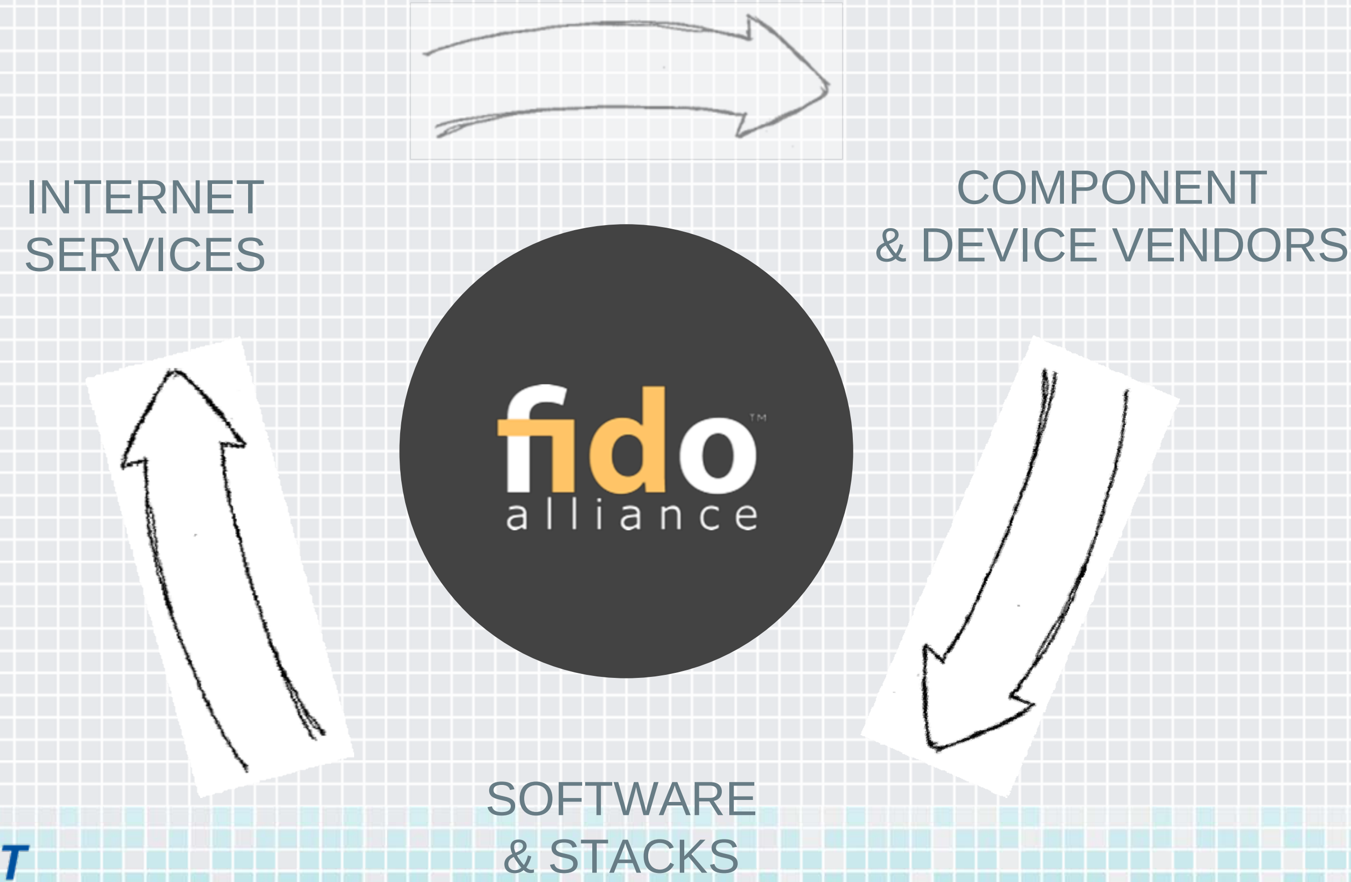
Red Trusted Virtual Domain 🟥

Internal Connection

Secured Connection

TeleTrusT Pioneers in IT security.

Usability: Building an Eco System



INTERNET SERVICES

COMPONENT & DEVICE VENDORS

SOFTWARE & STACKS

SecurITy

made
in
Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig

Lessons learned today?

- Classification in Protection Classes eases the selection of appropriate security solutions for the Mobile Enterprise
- Within the same organization, domains and devices of different Protection Classes can co-exist.
- Consumer-level devices can be enhanced by intelligent integration of smart components for use in the Mobile Enterprise
- Germany deployed public eco-systems provide a good set of best-practice examples

Trust in Mobile Enterprise – have we lost the Game?

We still have an opportunity to win!

Visit the German Pavilion at North Exhibit Hall, Booth 4020

The Partners of the German Pavilion:

- @SEC
- DriveLock
- Intelligent Data Protection
- eperi
- LINK11
- Sirrix AG security technologies
- AUCONET
- OPTISECIO
- glück kanja
- QGROUP GmbH
- TÜViT
- cryptoVision
- infineon
- ROHDE&SCHWARZ
- zertificon
- brainloop
- eco
- inlab
- secucloud.
- BUNDESDRUCKEREI
- EGOSECURE
- secusmart

"Apply" Slide

- CISO (Chief Information Security Officer)
  - Immediate: classification of applications and determine the rules for devices and infrastructure, identification of gaps and risks.
    Medium Term: optimization of the security architecture
- Administrator
  - Immediate: analysis of the state; classification requirements
    selection of security functions like authentication, identification (2-factor method), virtualization, trusted certificates, ...
    Medium Term: adaptation of processes, use of tool's for the control of security requirements in the field.
- User in the field
  - Immediate: recognizing the need for security-related applications and following appropriate rules.
    Medium Term: acceptance of restrictions on the freedom of choice of mobile devices
    Control of security processes for critical applications.