Fire & Security

bravida

We Secure The Nordics

Fire & Security

ECCA CONFERENCE 2013-05-27/28

Jonas Ahlgren Systemhuset

bravida

2013-05-27

Agenda

- Bravida Fire & Security

- New IEC-norm concerning requirements for access control systems

- Examples of how RFID & NFC enabled devices can work in such environments

Jonas Ahlgren, Bravida Fire & Security [SE]

Jonas Ahlgren

Info about Jonas Ahlgren
Product Manager Security at Bravida January 2007 – Present

Based on the company's objectives and policy of the company leading the development of product for market access and purchase.

Responsible for the users association ClubIntegra with the largest Security Buyers that ex TeliaSonera, Hospital and Universities in Sweden and more.

Member of IEC/Cenelec/SEK/TC79 (2008- Present)
Chairman of the Swedish part of TC79/AW11 SEK / CENELEC / IEC as working on the revision of EN 50133 Access Control Systems as present as in may 2013 as IEC 60839-11-1

This is Bravida

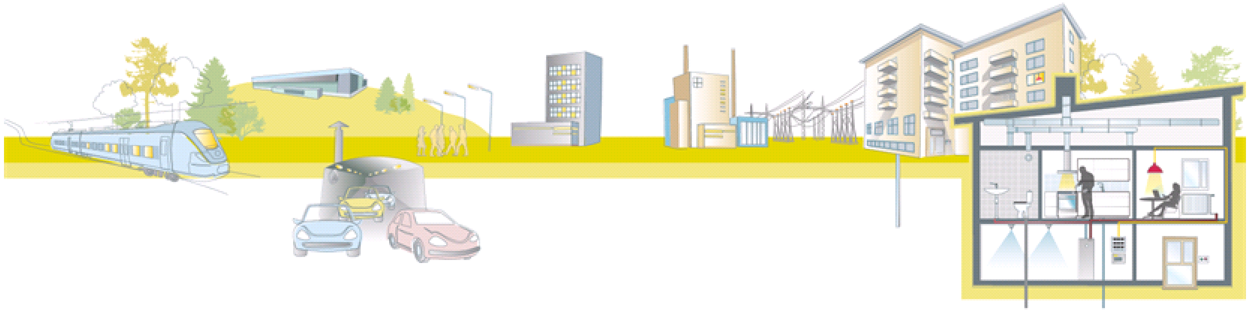
Bravida is Scandinavia's premier integrated supplier of technical installation and service solutions for buildings and plants.

More than 8,000 skilled people in over 150 locations throughout Sweden, Norway and Denmark

In 2011 Bravida’s net sales was SEK 10,8 billion.

Technological solutions for a living society

Bravida's electrical, security, heating & plumbing and HVAC solutions provide buildings, infrastructure and society as a whole with energy, heating, water, air and security – in short, the foundation for a secure life, development and growth.



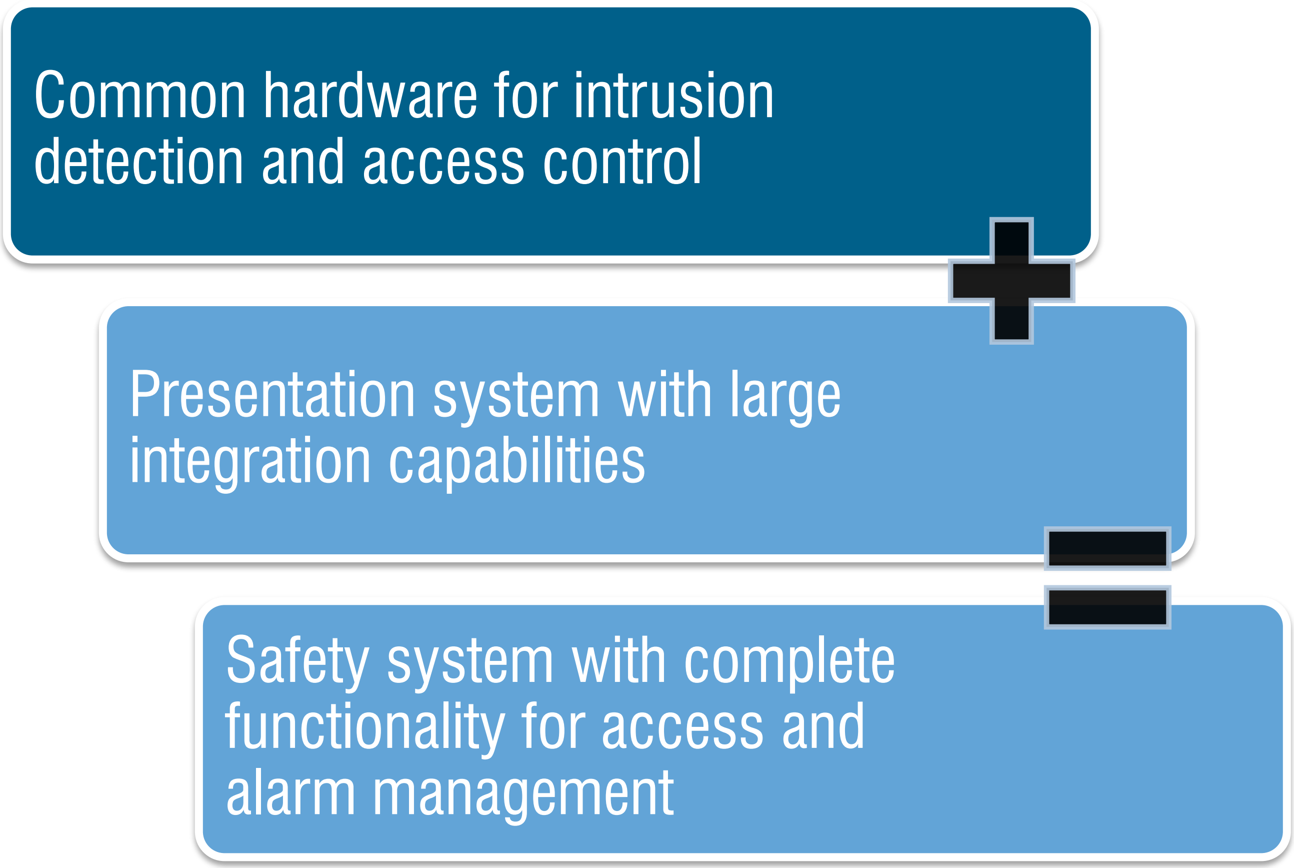
We secure universities

Refernces - Nordic Universities

- Høgskolen Ålesund
- Høyskolen Nesna Nesna
- Handelshøyskolen BI, Oslo
- Handelshøyskolen BI, Lillestrøm
- University for Miljø & Biovitenskap, Ås
- Kalnes Jordbrukshøyskole, Sarpsborg

- Umeå University
- Mälardalens University
- Linköpings University
- KTH, Royal Institute of Technology
- Karlstads University
- Lunds University
- SLU
- Uppsala University
- Malmö University
- Gotlands University
- Luleå University
- Mid Sweden University

What is Bravida Integra



Common hardware for intrusion detection and access control

+

Presentation system with large integration capabilities

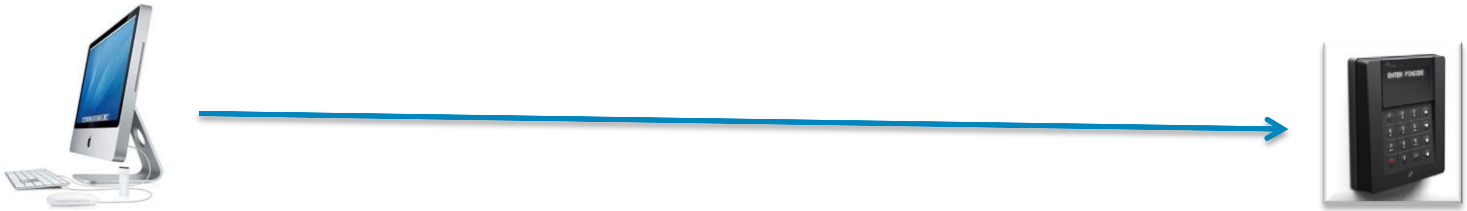
=

Safety system with complete functionality for access and alarm management

Integra SmarCardSolution

- Central units gets the keys from server

- No keys in the readers!



- **Remote Upgrade Service,** Central upgrade of all hardware even cardreader for future new features for low operating costs

IntegraEasyConnect

- Data Services is a program that acts as a data converter between Bravida Integra and one or more management systems or other access control.

Agenda

- Bravida Fire & Security

- New IEC-norm concerning requirements for access control systems

- Examples of how RFID & NFC enabled devices can work in such environments

Jonas Ahlgren, Bravida Fire & Security [SE]

IEC- The International Electrotechnical Commission

•IEC
At the international level is conducted standardization in the electrotechnical field by the IEC (International Electrotechnical Commission).
The basis of IEC consists of national committees.

IEC publications serve as a basis for national standardization and as references when drafting international tenders and contracts.

•CENELEC
CENELEC (Comité Européen de Normalisation Electro Technique) is an association of European national committees of the IEC. The aim is to harmonize national standards in the electricity sector and to ensure that technical barriers to trade. The work is based as far as possible on international standards set within IEC

•National committees

IEC 60839 Part 11-1: Electronic access control systems

- **IEC 60839 Alarm systems - Part 11-1: Electronic access control systems - System and components requirements**

- **IEC 60839-11-2 Ed. 1.0**
- Alarm systems - Part 11-2: Electronic access control systems - Application guidelines ACDV
- Draft 2013-05 and date for realise 2014-09
- **IEC 60839-11-3 Ed. 1.0**
- Alarm systems - Part 11-3: Systems for use in security applications - IP Security Device Base Protocol ANW
- Draft 2013-10 and date for realise 2015-01
- **IEC 60839-11-4 Ed. 1.0**
- Alarm systems - Part 11-4: Systems for use in security applications - Physical Access Controller Protocol ANW
- Draft 2013-10 and date for realise 2015-07

IEC 60839-11-1

- **IEC 60839-11-1 System and components requirements**
- Publication date 2013-05-07

This standard specifies the minimum functionality, performance requirements and test methods for electronic access control systems and components used for physical access (entry and exit) in and around buildings and protected areas.

It does not include requirements for access point actuators and sensors.

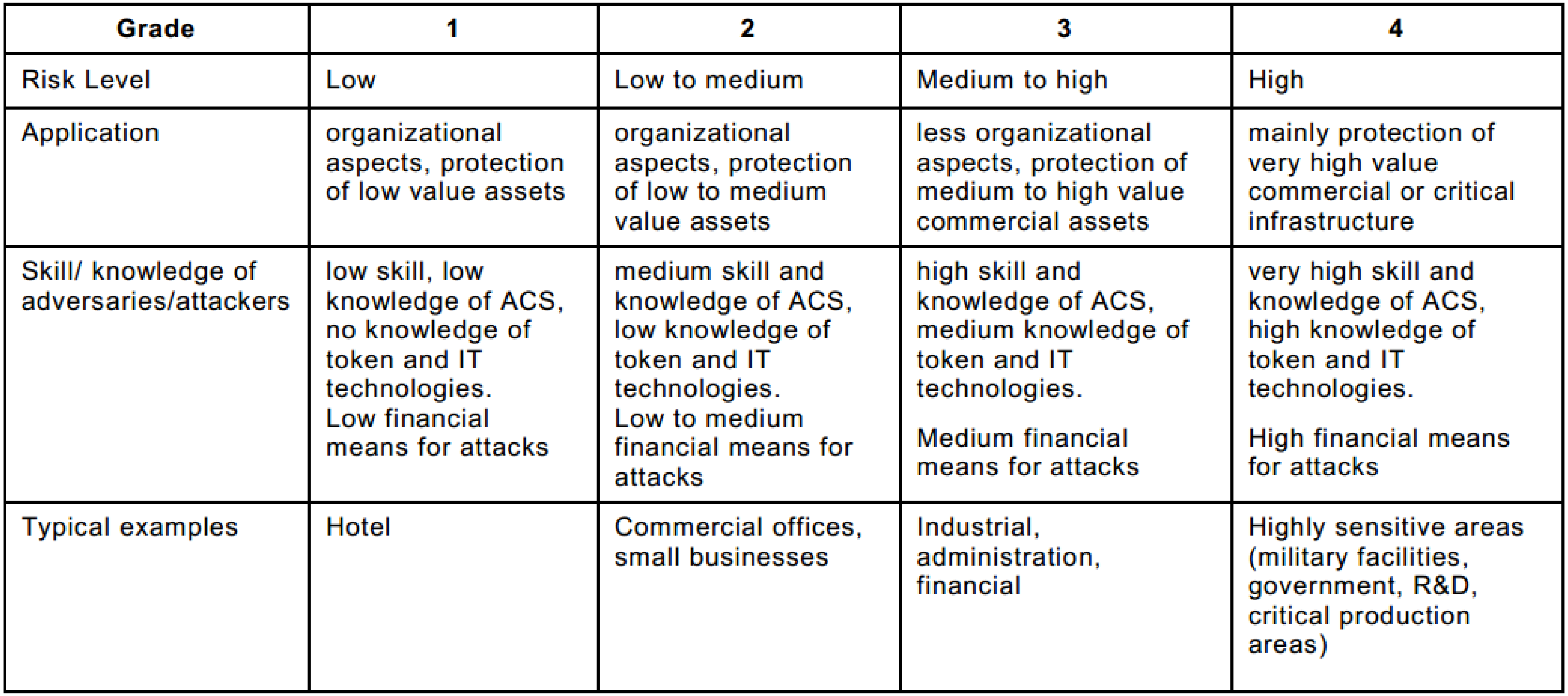
The design, planning, installation, operation, and maintenance are part of the Application Guidelines in IEC60839-11-2.

IEC 60839-11-1

The standard comprises the following chapters:

- A conceptual model and system architecture
- Criteria covering:
- **Classification based on performance functionalities and capabilities**
- Access point interface requirements
- Indication and Annunciation requirements (display, alert, logging)
- Duress signalling and overriding
- Recognition requirements
- System self-protection requirements
- **Communication between the component parts of the electronic access control system and with other systems**
- Requirements for environmental conditions (indoor/outdoor use) and electromagnetic compatibility;
- **Test methods**

IEC 60839-11-1



Grade	1	2	3	4
Risk Level	Low	Low to medium	Medium to high	High
Application	organizational aspects, protection of low value assets	organizational aspects, protection of low to medium value assets	less organizational aspects, protection of medium to high value commercial assets	mainly protection of very high value commercial or critical infrastructure
Skill/ knowledge of adversaries/attackers	low skill, low knowledge of ACS, no knowledge of token and IT technologies. Low financial means for attacks	medium skill and knowledge of ACS, low knowledge of token and IT technologies. Low to medium financial means for attacks	high skill and knowledge of ACS, medium knowledge of token and IT technologies. Medium financial means for attacks	very high skill and knowledge of ACS, high knowledge of token and IT technologies. High financial means for attacks
Typical examples	Hotel	Commercial offices, small businesses	Industrial, administration, financial	Highly sensitive areas (military facilities, government, R&D, critical production areas)

IEC 60839-11-1

Definitions

- Access Control System

  A set of interacting or interdependent components restricting to authorised persons, entry into and/or exit from a security controlled area..

- Electronic Access Control System (EACS)

  A system designed to grant to authorized persons, or entities, entry to and/or exit from a security controlled area and deny such entry and or exit to non-authorized individuals, or entities. The extent of control of entry/exit may include the reporting and recording of related activity.

IEC 60839-11-1

Definitions

- Monitoring Console

  A functional component that consists of devices used for communications between the electronic access control system operator and the access control unit(s)

- Access Control Unit (ACU)/Controller

  A part of an access control system that interfaces to readers, locking devices and sensing devices, making a decision to grant or deny access through a portal.

- Reader

  A device for the input of credentials, e.g. token reader, card reader, biometric reader etc.

- Token

  A portable device containing a readable unique identifier (credential) that can be associated with a user's data and access rights stored within the electronic access control system..

- Credential

  Information either memorized or held within a token, such as a code or biometric image used to identify an individual to an access control system in order to authenticate a user.

IEC 60839-11-1

The following requirements for token and communication between token and user interface unit shall be met in addition to requirements stated in Table 4 and Table 7:

- Grade 1 and 2: no additional requirements

- Grade 3: chip based contact or contactless (RFID) token with access conditions at least for writing/modifying of ID information and for RFID token only session encrypted data communication. This is required only when the token is used as a single method of recognition.

- Grade 4: chip based contact or contactless (RFID) token with mutual authentication and access conditions for reading, writing or modifying information and for RFID token only session encrypted data communication..

IEC 60839-11-1

Communication between readers and access control units

Grade 3:

Communication between readers and access control units shall support encryption with authentication .

Or:

The instruction manual shall contain details of the installation requirements for the mechanical protection limiting access to the communication lines between readers and access control unit.

Grade 4:

Communication between readers and access control units shall support encryption with authentication

Agenda

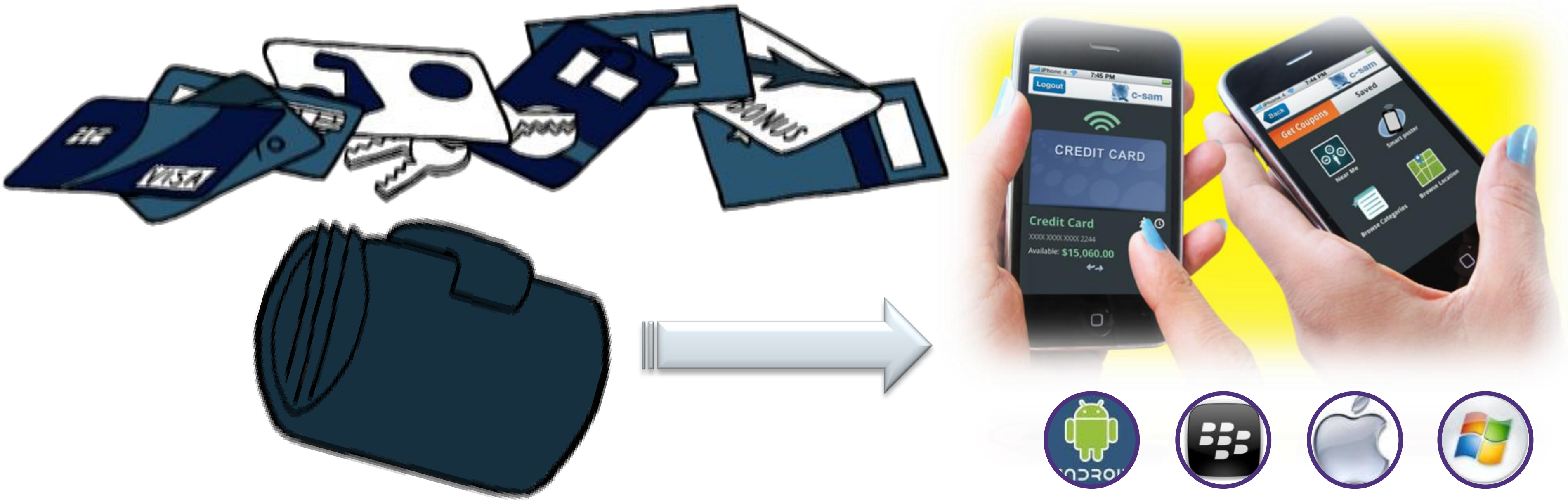
- Bravida Fire & Security

- New IEC-norm concerning requirements for access control systems

- Examples of how RFID & NFC enabled devices can work in such environments

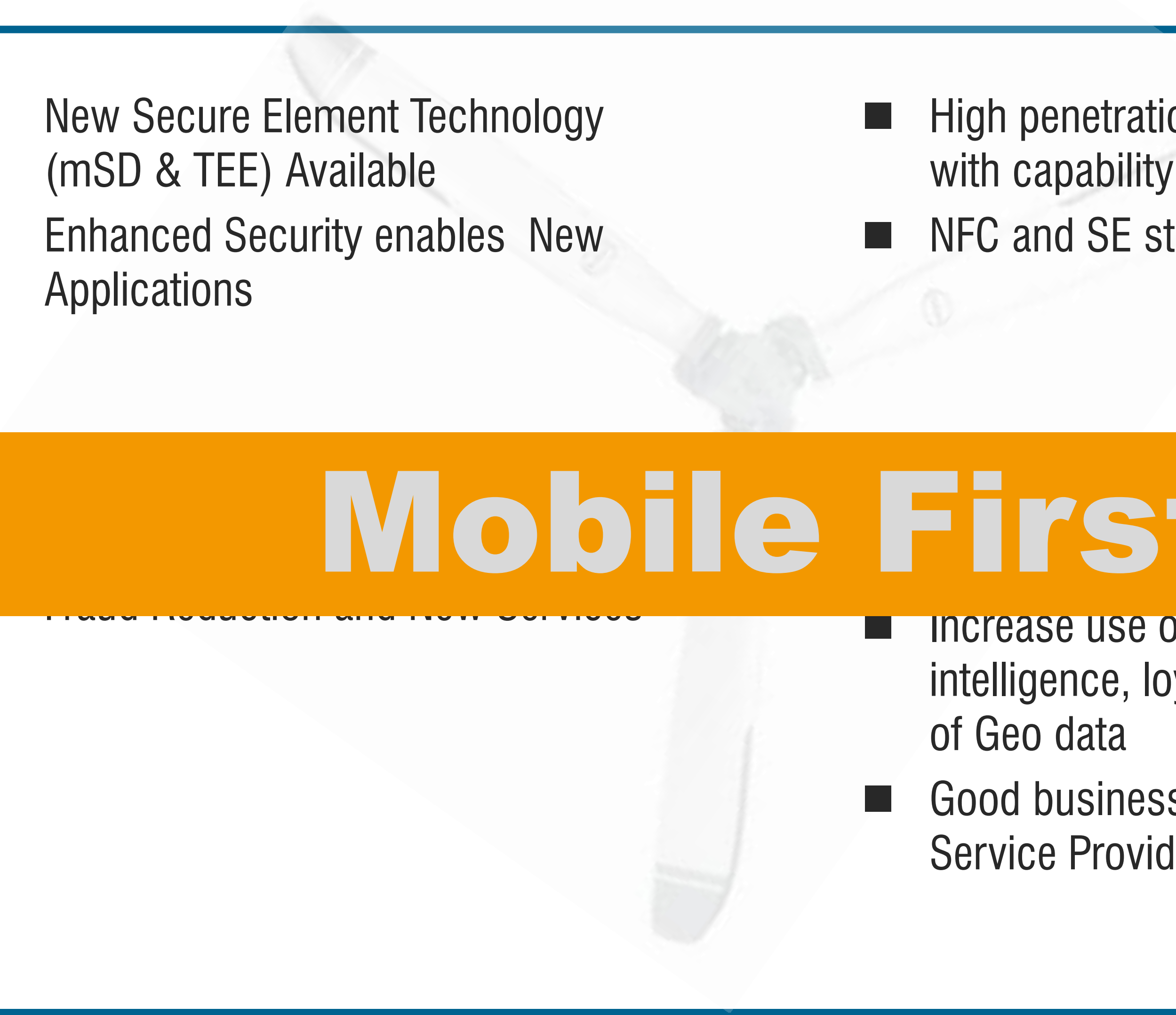
Jonas Ahlgren, Bravida Fire & Security [SE]

Vision



- Replacing todays wallet by transferring all of your plastics into a mobile wallet – EASY AND SECURE
- With and without NFC.

What is Propelling the Market?



- New Secure Element Technology (mSD & TEE) Available
- Enhanced Security enables New Applications

- High penetration of smart phones with capability for SE/NFC
- NFC and SE standards in place

Mobile First

Fraud Reduction and New Services

- Increase use of business intelligence, loyalty cards and use of Geo data
- Good business cases for the Service Providers

Support for any Secure Element (SE)

SIM UICC

Owned by the MNOs

mSD cards

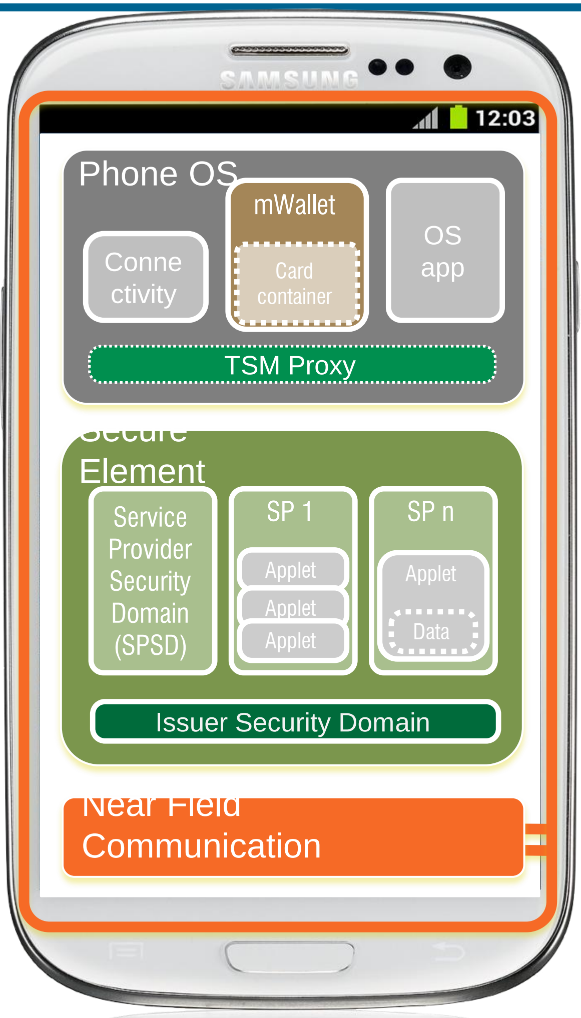
The TSM owns the SE

Embedded SE

The handset manufacture owns the SE

Other SE

- •Cloud based SE
- •Encrypted SW SE



Phone OS

Connectivity

mWallet

Card container

OS app

TSM Proxy

Secure Element

Service Provider Security Domain (SPSD)

SP 1

Applet

Applet

Applet

SP n

Applet

Data

Issuer Security Domain

Near Field Communication

Supported Applications - Examples

Payment

Debit Cards

Credit Cards

VISA MasterCard DISCOVER NETWORK AMERICAN EXPRESS Cards

Prepaid

Invoice/SMS

fakturera mig / klarna

Loyalty

Retail

NorgesGruppen

Gas Stations

Statoil

Airlines

Coffee

END USER

Access

Hospitals

University

OPEN ACCESS

Parking

Skidata

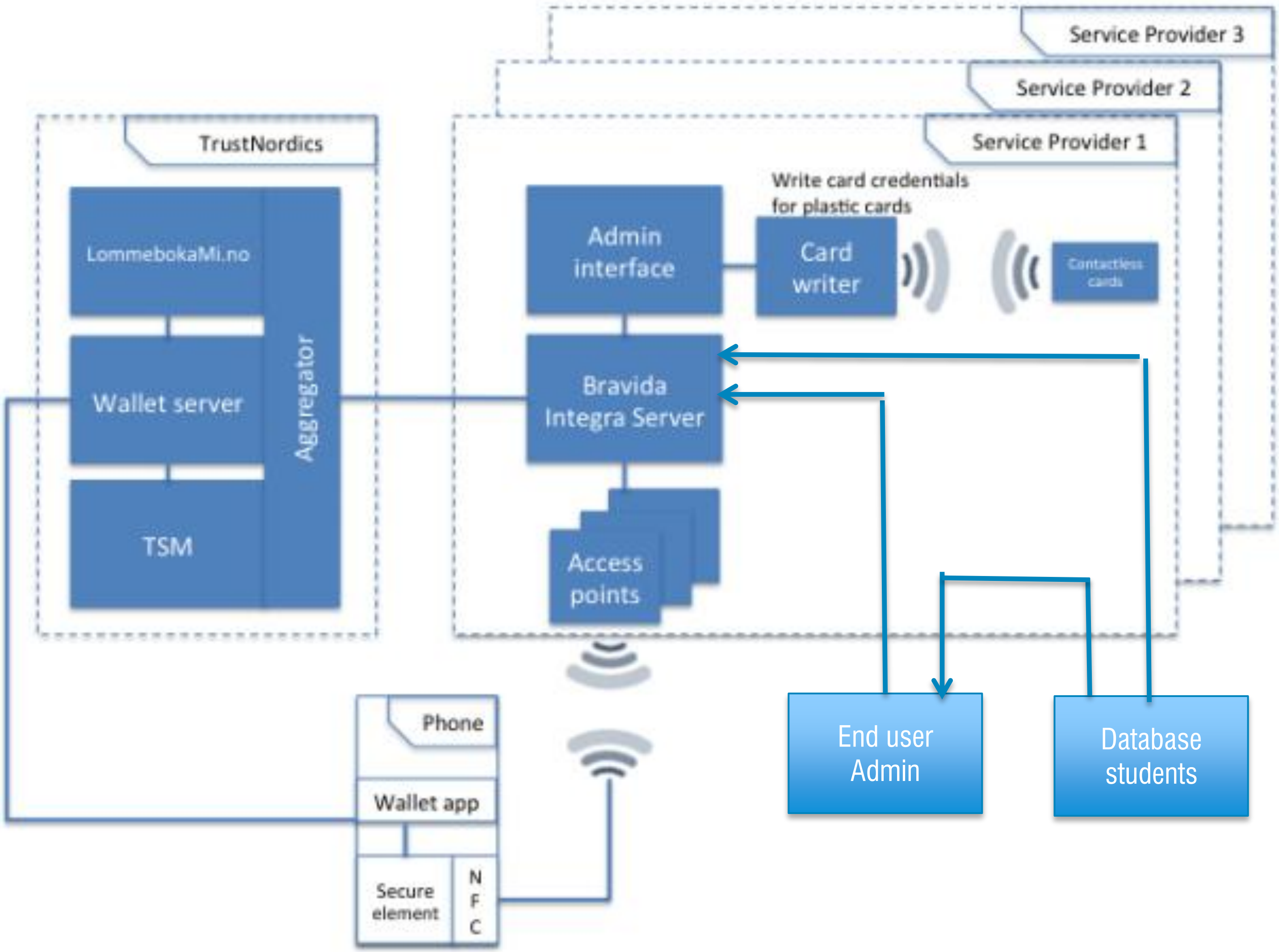
ID-Cards

Passport

Driver license

Health Cards

E-ID Cards

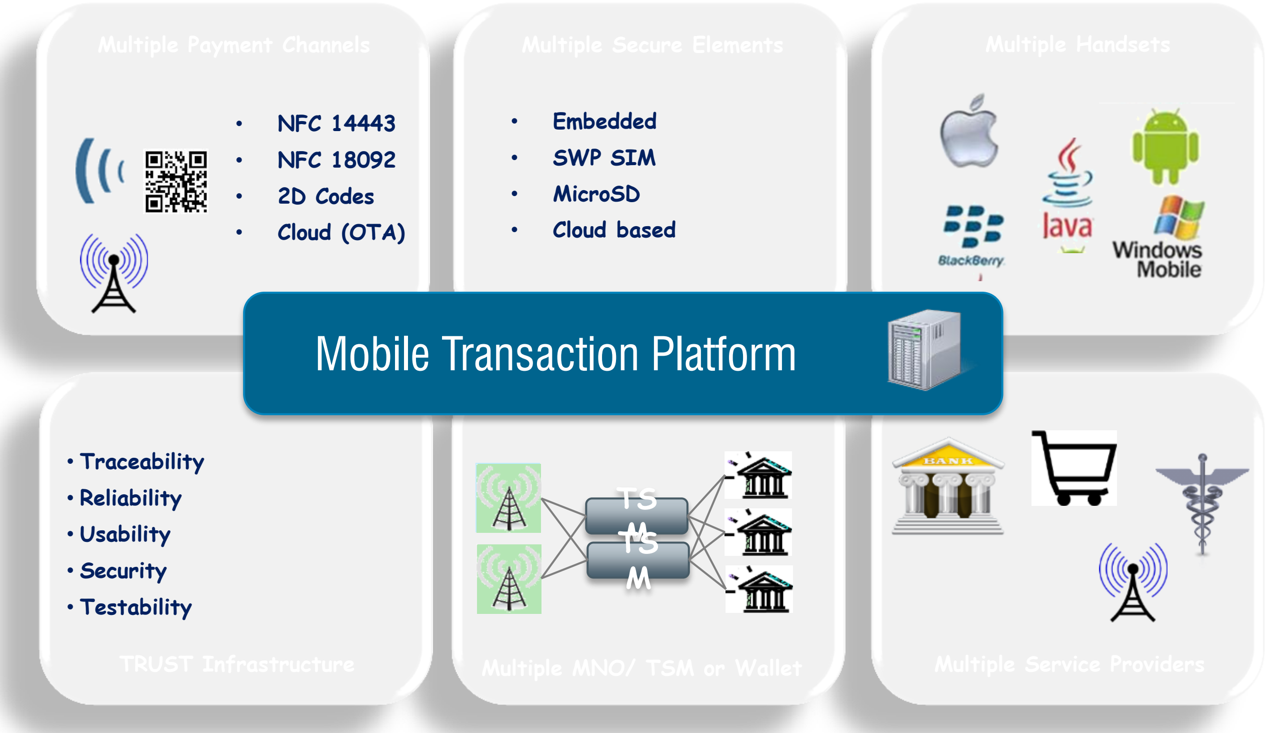

Service Provider 3
Service Provider 2
Service Provider 1
TrustNordics
LommebokaMi.no
Wallet server
TSM
Aggregator
Write card credentials for plastic cards
Admin interface
Card writer
Contactless cards
Bravida Integra Server
Access points
Phone
Wallet app
Secure element
N F C
End user Admin
Database students

Turn-key solution

- Turn-key Mobile Wallet solution
- Mobile Wallet Framework
  - APP (stand alone)
  - TrustNordics Wallet
  - White Label Wallet
  - 3. Party Wallet
  - EMVcertified
  - Support: MS, Android, Apple, BB
- TSM (Turn-key)
  - Hosted solution
  - Secure Element provider
  - PCI and EMV

TrustNordics Wallet V2.00

- Turn-key solution for Banks, MNO and Service providers
- Support 4 Operating systems
- Full TSM integration
- Release June 1st. 2013
- August 1st. PCI and EMV approvals
- 25 standard Widgets or Applications



Multiple Payment Channels

- NFC 14443
- NFC 18092
- 2D Codes
- Cloud (OTA)

Multiple Secure Elements

- Embedded
- SWP SIM
- MicroSD
- Cloud based

Multiple Handsets

Mobile Transaction Platform

- Traceability
- Reliability
- Usability
- Security
- Testability

TRUST Infrastructure

Multiple MNO/ TSM or Wallet

Multiple Service Providers

Questions !