BlueID – Secure offline device authentication for IoT

Florian Schiebl, Chief Sales Officer

Blue ID
by baimos technologies

Use Case „Physical Access“

The challenge - Digitalization of phys. access

baimos technologies
YOUR MOBILE TURNS ME ON!
BlueID DRIVE. THE NEW LINK BETWEEN SMARTPHONE AND CAR.
FROM MARQUARDT AND BAIMOS TECHNOLOGIES
TUT MQ 55
baimos technologies

CONVENIENT SCALABLE HIGHLY SECURE UNIVERSAL

CONVENIENT mobile key

WITH TRUST

EVERYWHERE
WITHIN 0,5 SEC

NO PAIRING

AROUND
THE OBJECT

SCALABLE mobile key

ANY COMMUNICATION

WITH TRUST

EVERYWHERE WITHIN 0,5 SEC

UNLIMITED PERMISSIONS

ON ALL DEVICES

NO PAIRING

AROUND THE OBJECT

HIGHLY SECURE mobile key

WITH TRUST

ANY COMMUNICATION

EVERYWHERE WITHIN 0,5 SEC

UNLIMITED PERMISSIONS

ON ALL DEVICES

SECURE OFFLINE

OPTIONALLY WITH SE

NO PAIRING

AROUND THE OBJECT

WITH IN-REACH DETECTION

UNIVERSAL mobile key

WITH TRUST

ANY COMMUNICATION

EVERYWHERE WITHIN 0,5 SEC

UNLIMITED PERMISSIONS

ON ALL DEVICES

SECURE OFFLINE

OPTIONALLY WITH SE

ON ALL OBJECTS

A CHOICE OF VENDORS

NO PAIRING

AROUND THE OBJECT

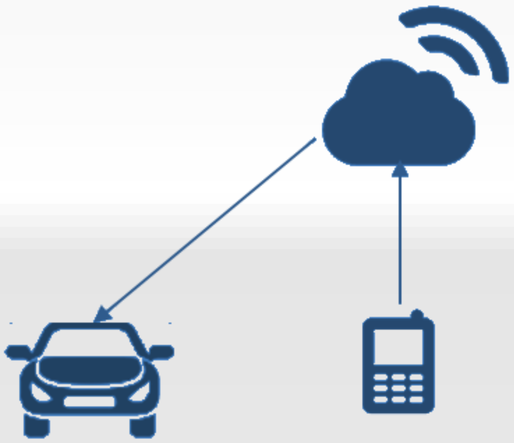
WITH IN-REACH DETECTION

ONE PROCESS FOR ALL

Blue ID
by baimos technologies

The Challenge

Status within the Automotive Sector



B2C
Fleet
Car Rental
Car Sharing

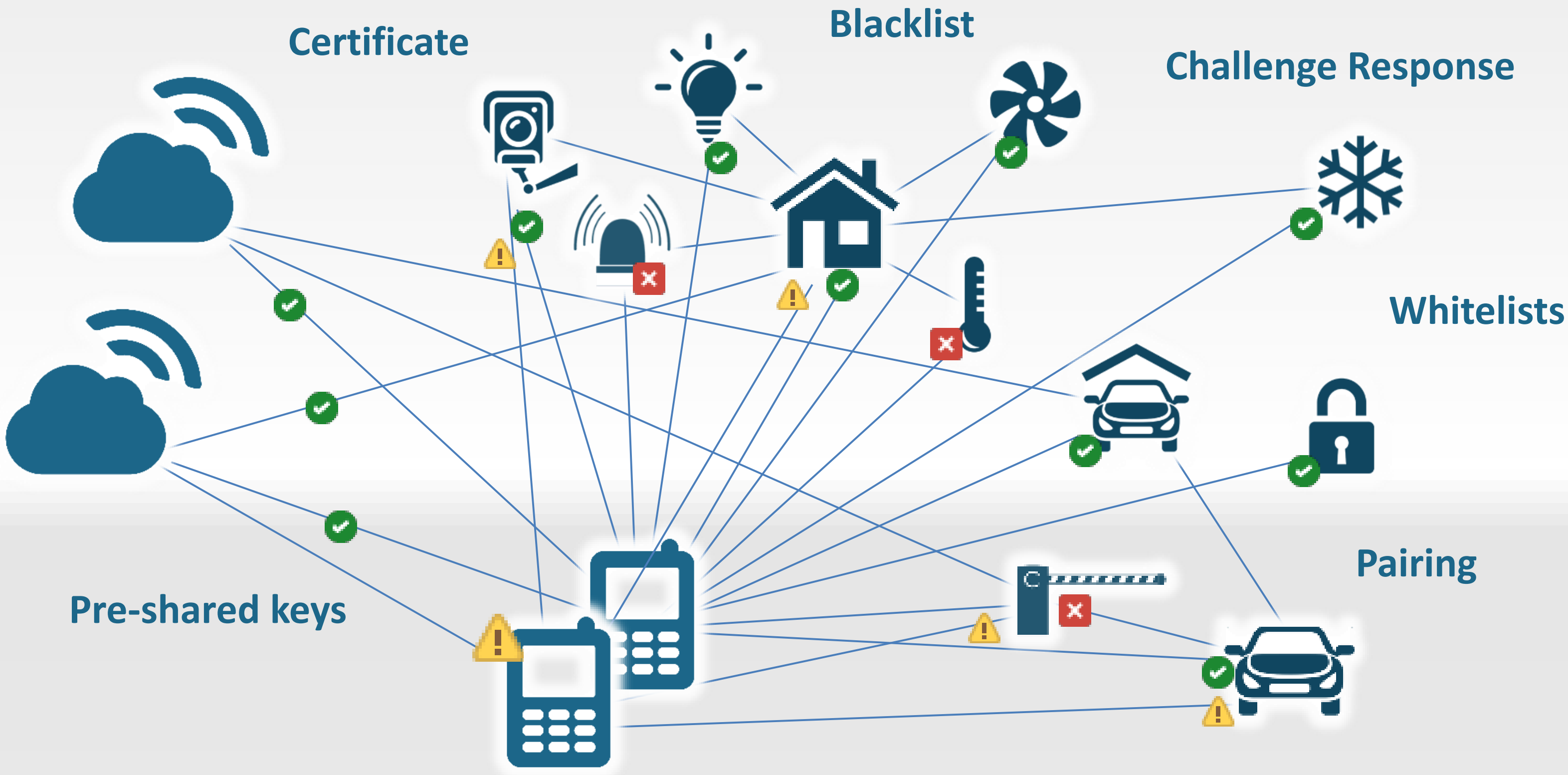
Writing into CAN-bus only empowered for central OEM backend system for a keyless:

- Door, window or trunk opening
- Lights or heating switch
- Engine start

Current OEM set-up challenges:

- ► Only works with online connectivity
- ► With different response time
- ► Using traditional IT network security

The future problem of a connected world



Gartner, Predicts 2014: Identity and Access Management

Fragmented vendor specific key management is the challenge.

Gartner says due to the IoT, Identity and Access Management will change completely by 2020

Blue ID
by baimos technologies

The solution - BlueID

BlueID...

…enables secure - local - immediate communication & interaction of your objects with any smart mobile device

Security
Authentification
Connectivity
Identity
Access control
Authorization

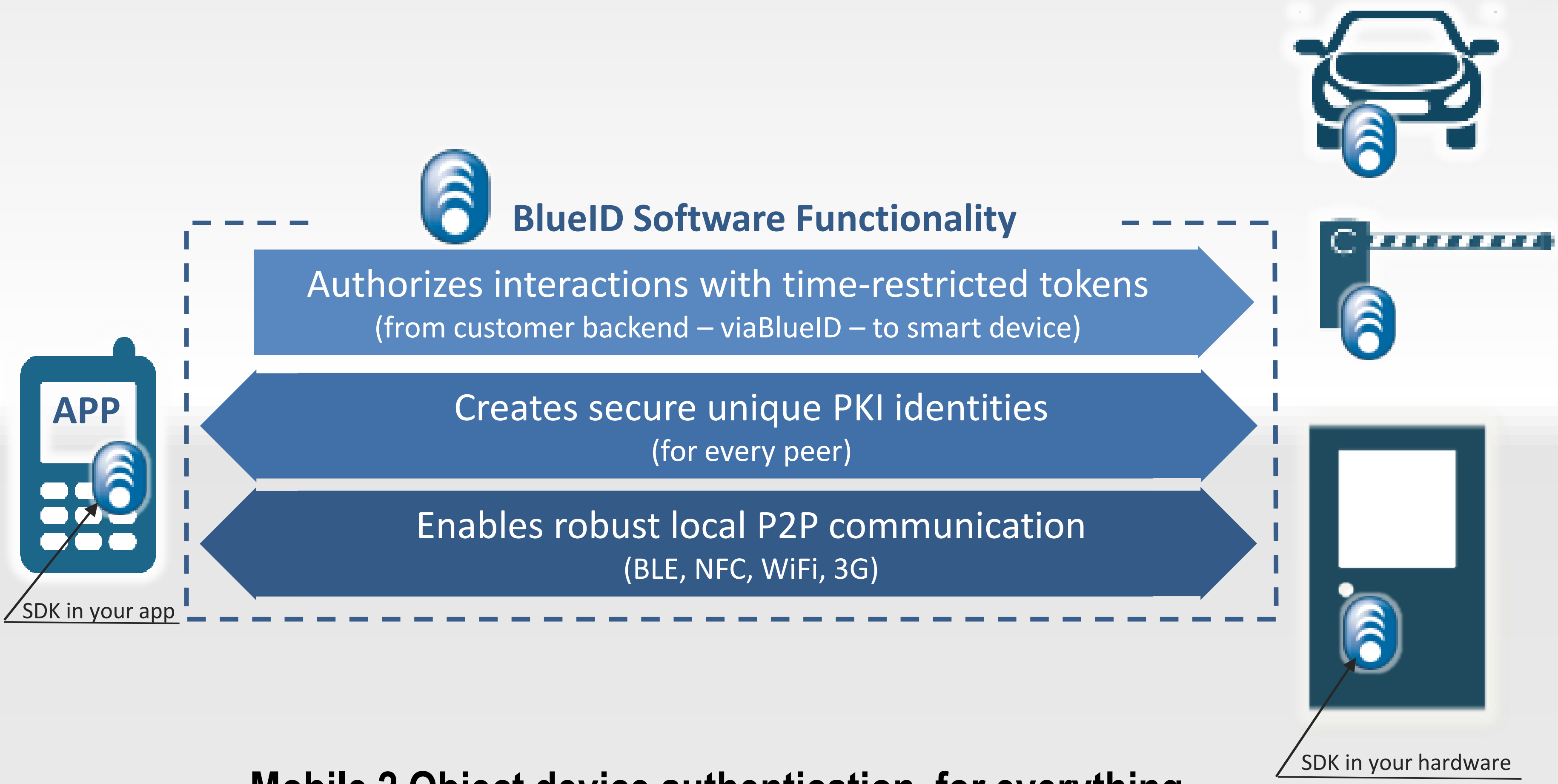
…by controlling which smart mobile device

is allowed
at which point in time
for how long

to interact with
a certain object

…everywhere, at anytime, on any device, for any object & always **in the same way**

What is BlueID? - Pure software that scales



BlueID Software Functionality

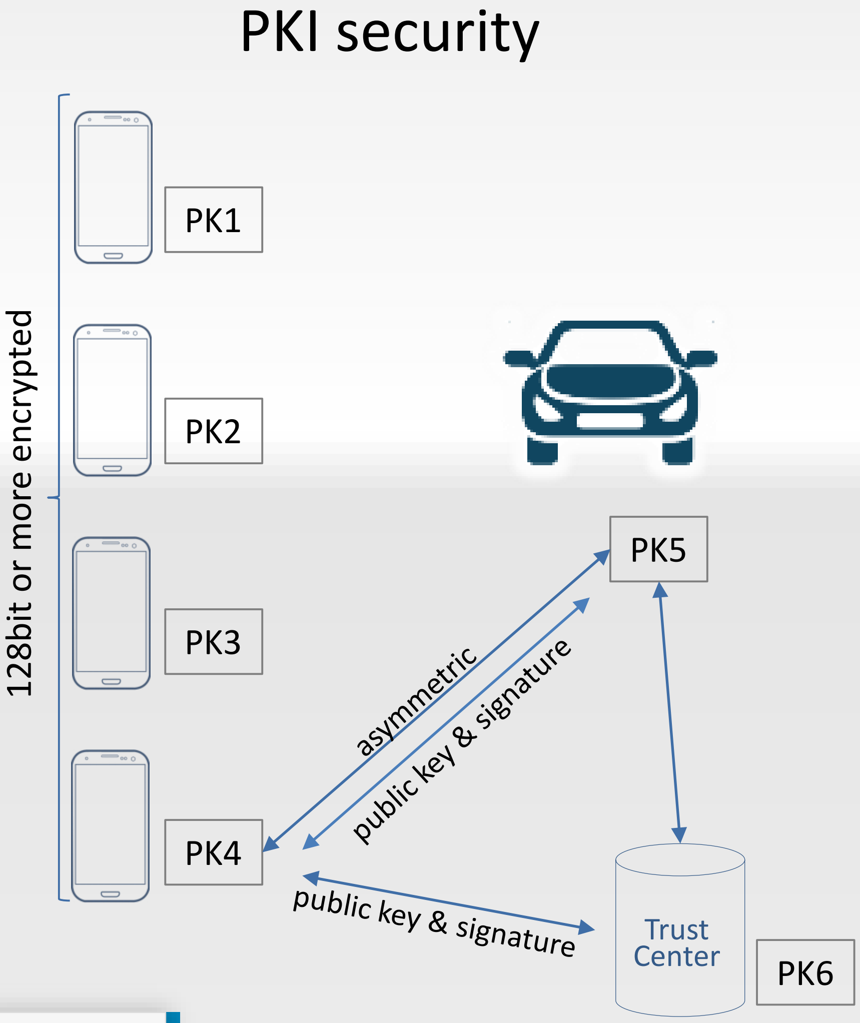
Authorizes interactions with time-restricted tokens
(from customer backend – viaBlueID – to smart device)

Creates secure unique PKI identities
(for every peer)

Enables robust local P2P communication
(BLE, NFC, WiFi, 3G)

Mobile 2 Object device authentication for everything

Asymmetric encryption & identities



- Every member has an unique private key
- Private keys never get shared but public keys only
- Private/public key pair of every member represents an unique identity
- The object stores only its own private key
- There is no master key involved
- A trusted third party (trust center) endorses the authenticity of each member and signs every token sent

BlueID capabilities for secure mobile keys

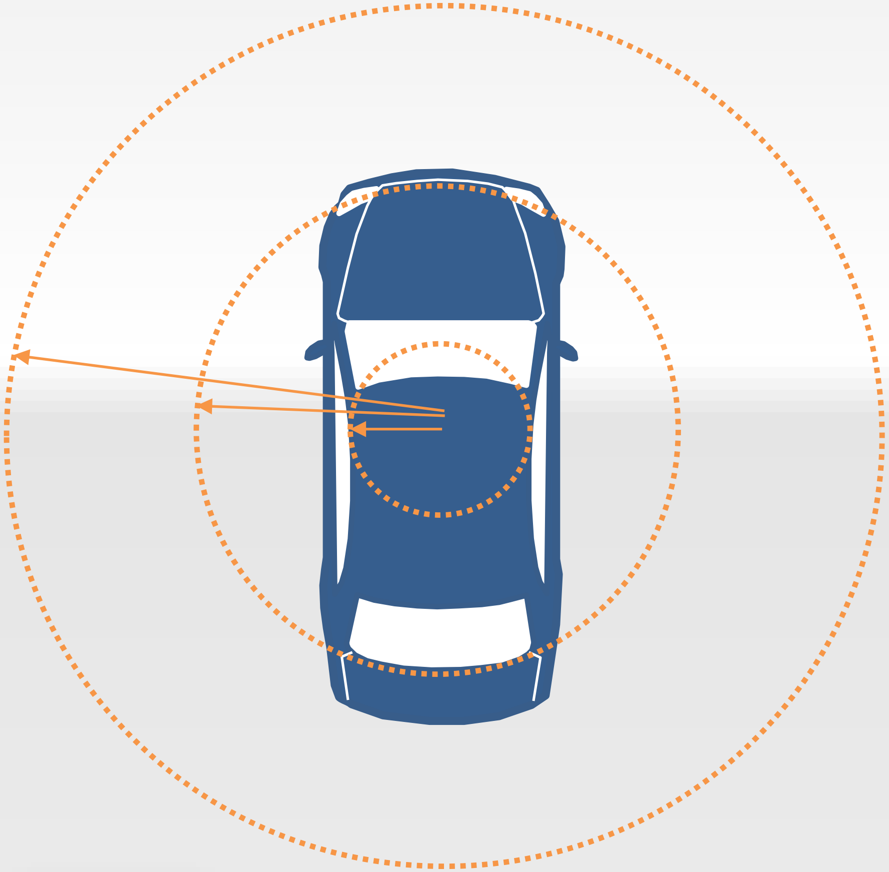
OPEN CAR

- with BLE
- offline enabled

START ENGINE

- combining BLE & NFC
- with thatcham like detection
- using scalable SE concept

Securing Bluetooth 4.0 with BlueID

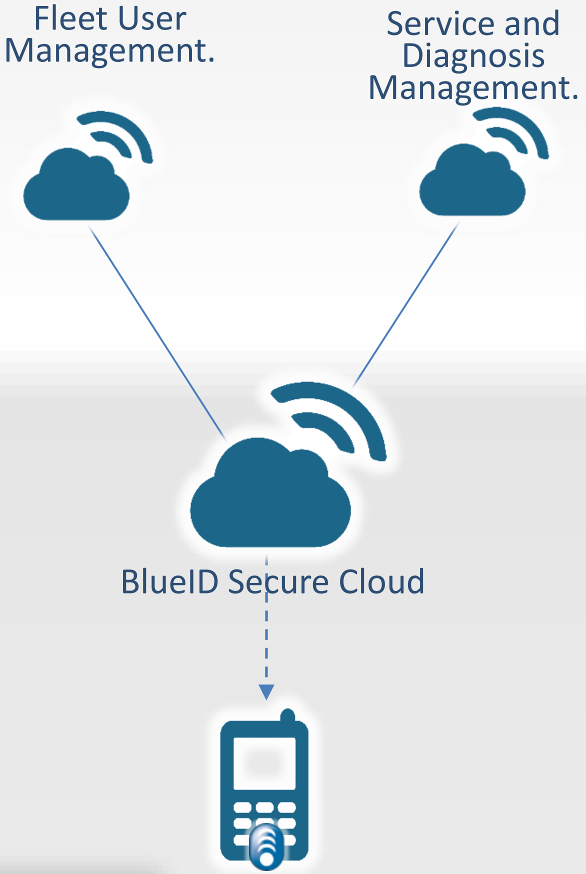


- BlueID enables to robustly restrict BLE reach
  - down to 30 cm
- BlueID utilizes BLE frequency only for transport
  - No use of device based BLE security mechanism
  - No use of BLE authentication & pairing via link keys
  - No security built on adaptive frequency hopping (AFH)
- BlueID secures BLE with trusted service
  - Unique PKI identities to create trusted devices
  - Tokens permitting BLE connectivity between identities
  - Tokens endorsed by trusted third party
  - BLE communication optionally encrypted

Blue ID
by baimos technologies

BlueID Strengths

BlueID technology strengths – control center

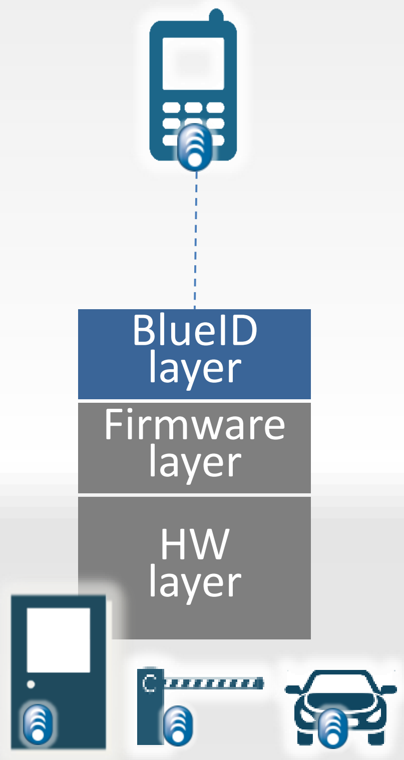


- Enables central secure cloud based access control (global)
  - Less IT infrastructure onsite in single building
  - Supports various country specific lock hardware
  - Large providers can host their own cloud onsite
- Solid data privacy protection
  - No touch on hotel user data
  - No sensitive data in token on smartphone
  - Compliant with EU law
- Creates secure token for every access right (Tokenization)
  - Provides secure time restricted token (who, what, when, how long, where)
  - Enables full flexibility in combining user & object
  - Disables prolongation or hand-over of tokens by user
  - Supports automatic revocation of token with a new token

BlueID technology strengths – smart mobile device

- No storage or transport of pre-shared keys on unknown devices
- No pairing required for BLE, WIFI
- No online connectivity required for command execution (only for provisioning token)
- No SE mandatory (but optionally as add-on)
- Very fast & robust processing within under 1 sec
- Replaces password with unique traceable machine identity based on PKI
- Controlled by time restricted individual tokens
- Works on any smart mobile device & smartcard
- Can turn Android smartphone in card reader

BlueID technology strengths – smart objects



- No extra processor hardware needed
  - BlueID can run in central CPU or directly in BLE chip
- Objects can respond to unlimited number of users
  - No storage of Master Keys
  - No whitelisting and storage of multiple UID's
- Enables full offline control (patent protected)
  - No wiring or extra Wifi routers
  - No extra bridge controller hardware
  - No online readers
- Protected by highly secure mobile device authentication (PKI)
  - Unique traceable machine identity based on PKI
- Customizable regarding power consumption & crypto length

Our mission – solid trust

With our software we deliver solid trust in any kind of smart device and we protect objects at the heart of a connected world

MARQUARDT
baimos technologies
TUT MQ 55
Auto-KLAIBER.de Balgheim-Spaichingen
baimos technologies
BlueID by baimos technologies

Facility references

ISEO Serrature / DORMA GmbH

BlueID opens BLE cylinders and trims with smart devices

Pango Parking Ltd.

Pango parking system | Mobile parking via smartphone app

eQ-3 AG

HomeMatic home automation | Open doors via smartphone app

Emerson Electric Co.

Knürr @Lock BlueID | Unlock server cabinets via smartphone app

Automotive references

Marquardt GmbH

BlueID Drive | Start vehicles via smartphone app

Novero GmbH

Dolphin TCU, empowered by BlueID for Smartphone access

Shared e-Fleet R&D project

Open, start and fuel BMW i3 by smartphone app

LG Vehicle Company

Open car with latest smartwatches and smartphones from LG

BlueID – software technology for IOT

- **BlueID enables universal keys**
  - √ Fits in any hardware and can control any object in the same way
  - √ Supports any Smartphone in the same way
  - √ Provides all kinds of communication: Bluetooth, NFC, WiFi
  - √ Enables hardware supplier independence

- **BlueID grants convenient & secure mobile keys for end-users**
  - √ Opening process within 1 sec
  - √ Supports one-click or automatic access
  - √ Has the patent for offline virtual network access in EU and US
  - √ Allows individual device based monitoring and tracking
  - √ Protects keys against typical hacks

- **BlueID assures business freedom**
  - √ Integrates in any existing or 3rd party app
  - √ Connects to any existing access control system
  - √ Keeps user data in operator hands only
  - √ Provides software lifecycle management for all smartphone versions

Thank You!

Florian Schiebl
Chief Sales Officer

baimos technologies gmbh
Marcel-Breuer-Strasse 15
D-80807 Munich
Germany

Phone:	+49 / 89 / 809 90 26 – 13
Fax:	+49 / 89 / 809 90 26 – 19

Company information

Web:	www.baimos.com
E-mail:	fsi@baimos.com

Product information

Web:	www.BlueID.net
E-mail:	info@BlueID.net