Sicherheitsaspekte in mobilen Bluetooth-Anwendungen

Dipl.-Ing.(FH) Alexander Grimm; Matsushita Electronic

Marcel Holtmann; BlueZ-Projekt

Dipl.-Ing.(FH) Andreas Vedral; FH Bochum

Bluetooth-Sicherheit

Verschlüsselung und Schlüssel

Symmetrische Verschlüsselung

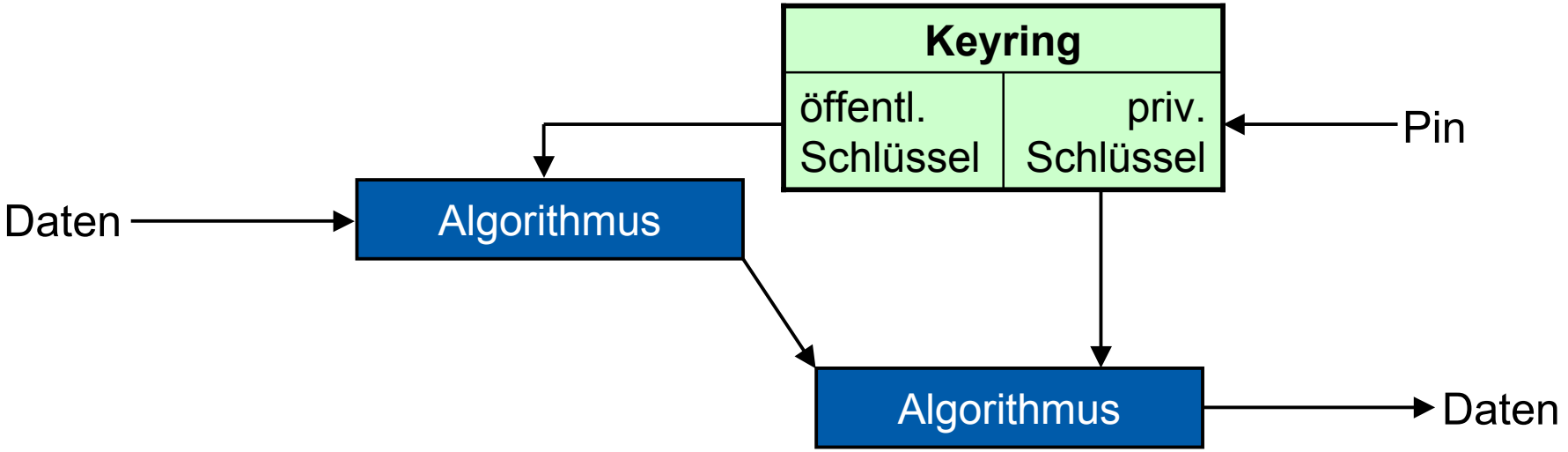
Symmetrische Verschlüsselung setzt ein sog. „geteiltes Geheimnis“ (shared secret) voraus.

$$X \oplus X = 0 \qquad Y \oplus 0 = Y$$

$$\textit{Daten} \oplus \textit{Schlüssel} \oplus \textit{Schlüssel} = \textit{Daten}$$

Vorteil	Nachteil
• einfache Implementierung • geringer Rechenaufwand	• hoher Aufwand bei der Distribution des Schlüssels

Asymmetrische Verschlüsselung



Vorteil	Nachteil
• hohe Sicherheit	• Schlüsselmanagment nötig • hoher Rechenaufwand • hoher Implementierungsaufwand

Initialisierungs- und Kombinationsschlüssel

Initialisierungsschlüssel (lokal)	**Kombinationsschlüssel** (global)
• Algorithmus E_{22} • Parameter - PIN-Code - Länge des PIN-Code - BT-Adresse des Initiators - Zufallszahl	• Algorithmus E_{21} • Parameter - zwei lokale Zufallszahlen - zwei BT-Adressen - vorhandener Schlüssel (K_{Init} oder K_{AB})

Erzeugung der Schlüssel

Erzeugung von **Initialization Key K_{Init}** und **Combination Key K_{AB}**

LMP	T	TID	Opcode	random number
24	M	M	in_rand	35 61 90 18 C9 9B 1F 54 90 71 0A 49 3D EC A0 BB

Zufallszahl zur Berechnung von K_{Init}

LMP	T	TID	Opcode	accepted opcode
25	S	M	accept	in_rand

LMP	T	TID	Opcode	random number
26	M	M	comb_key	D5 54 BD 7B 2C DA 57 2F B6 44 E6 8D A0 1B 48 83

$$C_A = LK\_RAND_A \oplus K$$

LMP	T	TID	Opcode	random number
27	S	M	comb_key	D5 85 94 3B 6A 88 68 B5 AA AA FE C6 D5 58 93 03

$$C_B = LK\_RAND_B \oplus K$$

LMP	T	TID	Opcode	random number
28	M	M	au_rand	53 36 AC 83 73 11 FE D0 0C A2 7C C3 C7 8A F3 55

LMP	T	TID	Opcode	authentication response
29	S	M	sres	0F 8D 99 57

LMP	T	TID	Opcode	random number
30	S	M	au_rand	CA 8B 97 3C DA 99 5A 01 E7 B7 2A 63 8E D1 8F 09

LMP	T	TID	Opcode	authentication response
34	M	M	sres	5D 8A 95 EA

Authentifizierung

LMP	T	TID	Opcode	reason
35	M	M	detach	0x13 - user ended connection

vgl. BT-Core Spec. Fig. 14.2

Unit Key und Master Key

Unit Key K_{Unit}

Dieser einmalig generierte Schlüssel wird für ressourcenarme Geräte eingesetzt. Dabei wird K_{Unit} mit K_{Init} verschlüsselt und der Gegenseite mitgeteilt.

Vorteil: Kein Speicherplatz wird benötigt!

Nachteil: Niedrige Sicherheit!

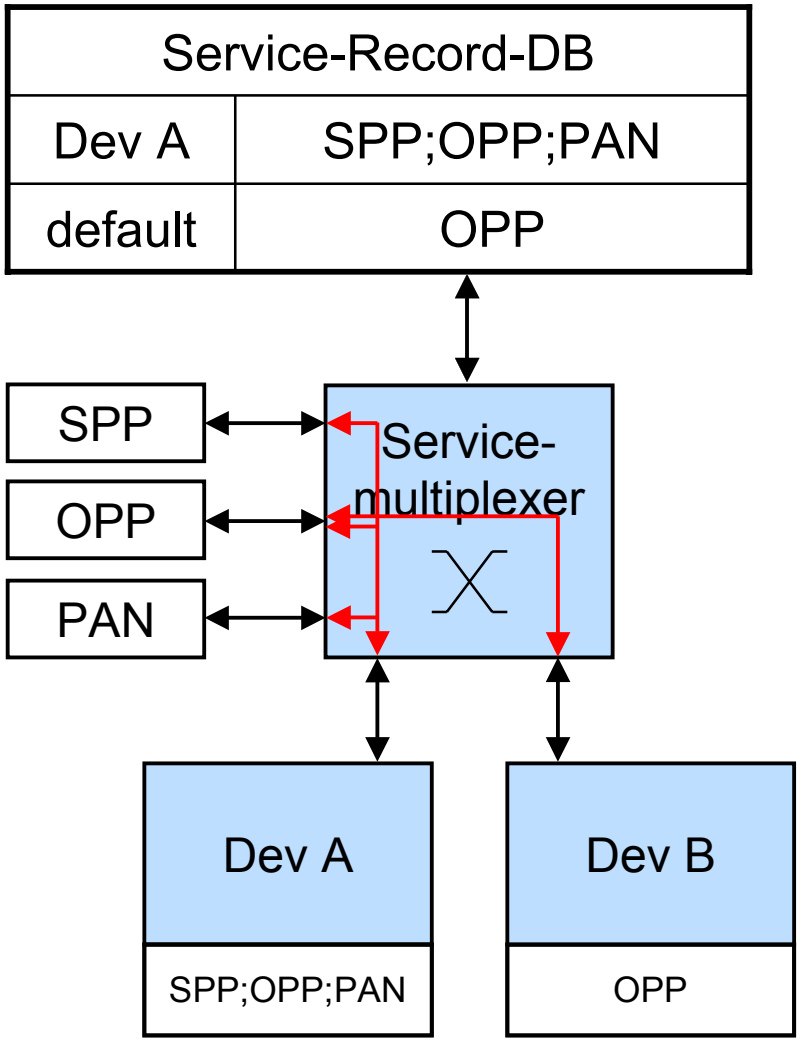
Master Key K_{Master}

Dieser Schlüssel wird in Netzen eingesetzt, in denen Broadcasts verschlüsselt werden sollen. K_{Master} ersetzt dabei temporär den, eventuell verwendeten, Verbindungsschlüssel.

Bluetooth-Sicherheit

Dienstesicherheit

Dienstsicherheit



Um bestimmten Geräten Zugriff auf spezielle Dienste verbieten oder gewähren zu können, muss die Service-Record-Datenbank um Einträge zur BD_ADDR erweitert werden.

Voraussetzung ist ein BT-Stack, der entsprechende Programmierschnittstellen (APIs) anbietet.

Bluetooth-Sicherheit

Anwendungssicherheit

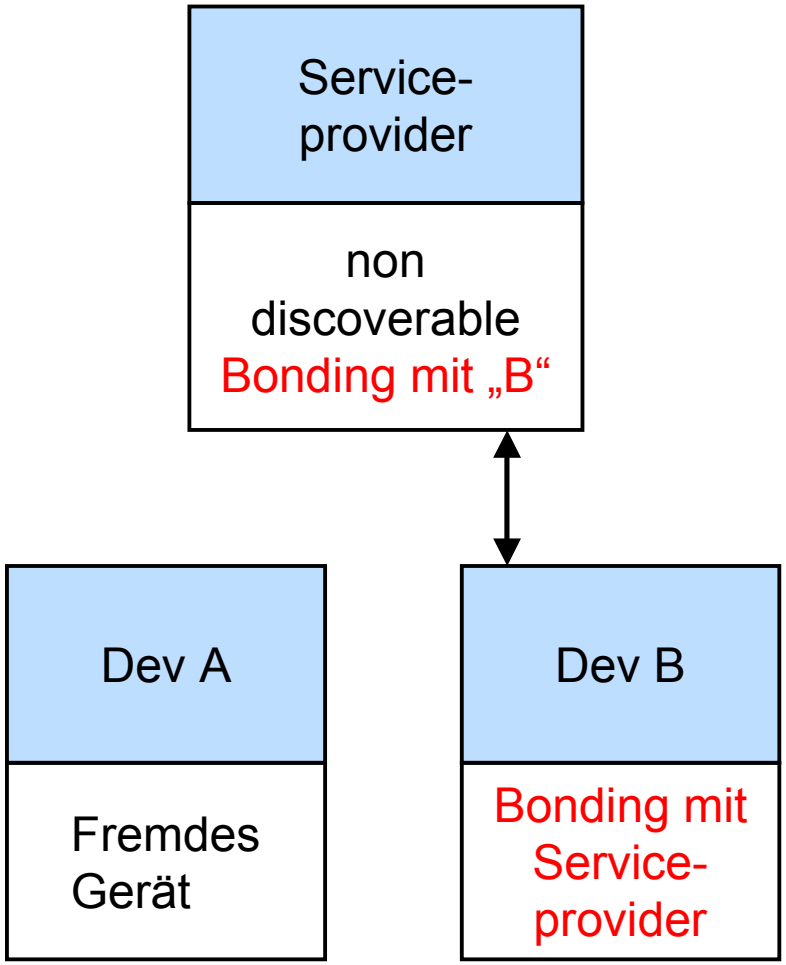
Anwendungssicherheit

Klassifikation der Sicherheitsrelevanz verschiedener Funktionen!

Wirksamer Schutz durch Interaktion mit dem Benutzer!

Funktion	Einstufung
Visitenkarte empfangen	Zulassen
Visitenkarte senden	Abfragen
Telefonbuch empfangen	Verweigern
Telefonbuch senden	Abfragen

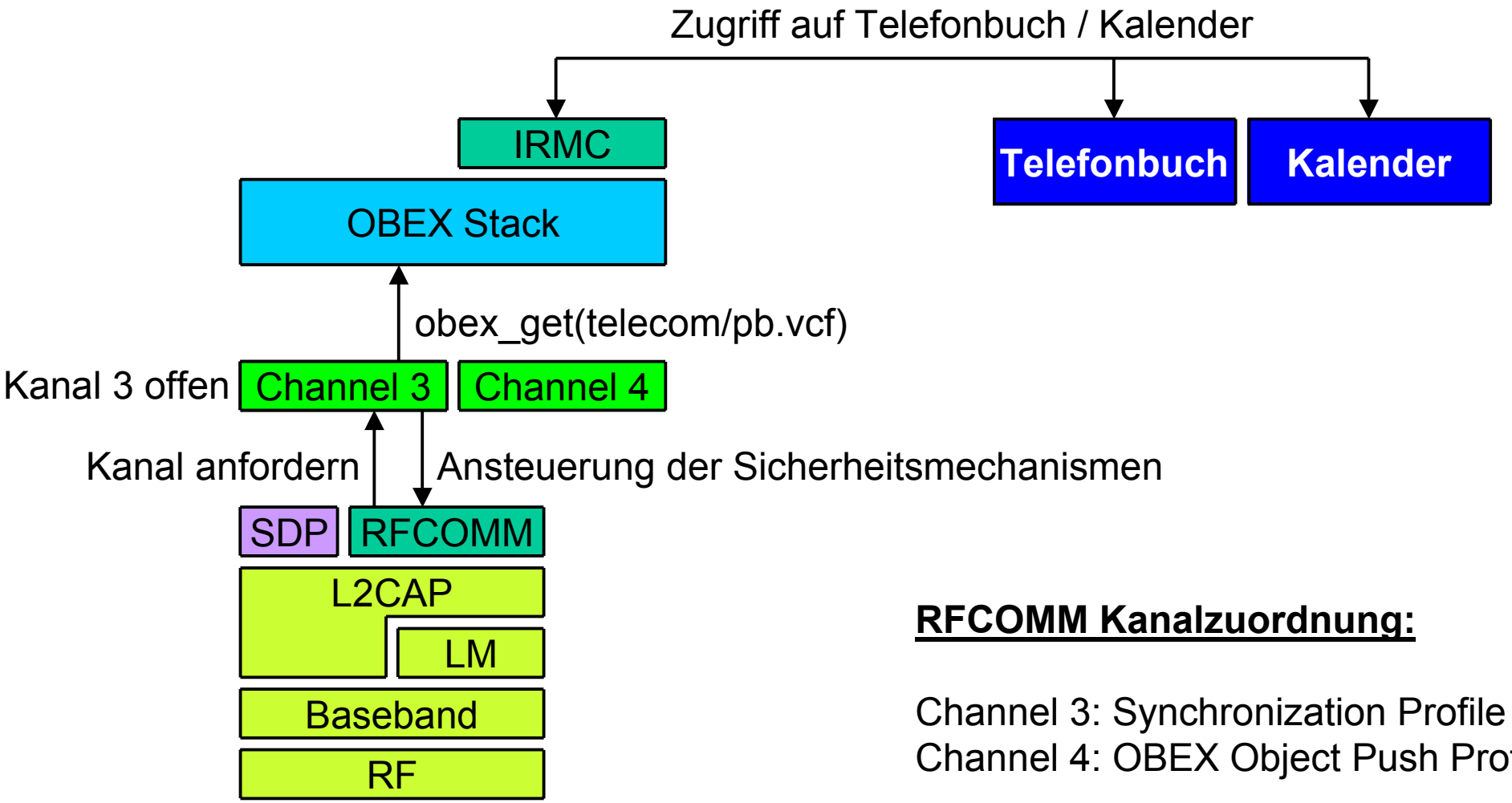
Zugriffssicherheit



Wenn sich der Serviceprovider im „non discoverable mode“ befindet, können fremde Geräte keine Verbindung aufbauen.

An zuzulassenden Geräten muss die Geräteadresse des Serviceproviders zum Bonding explizit angegeben werden.

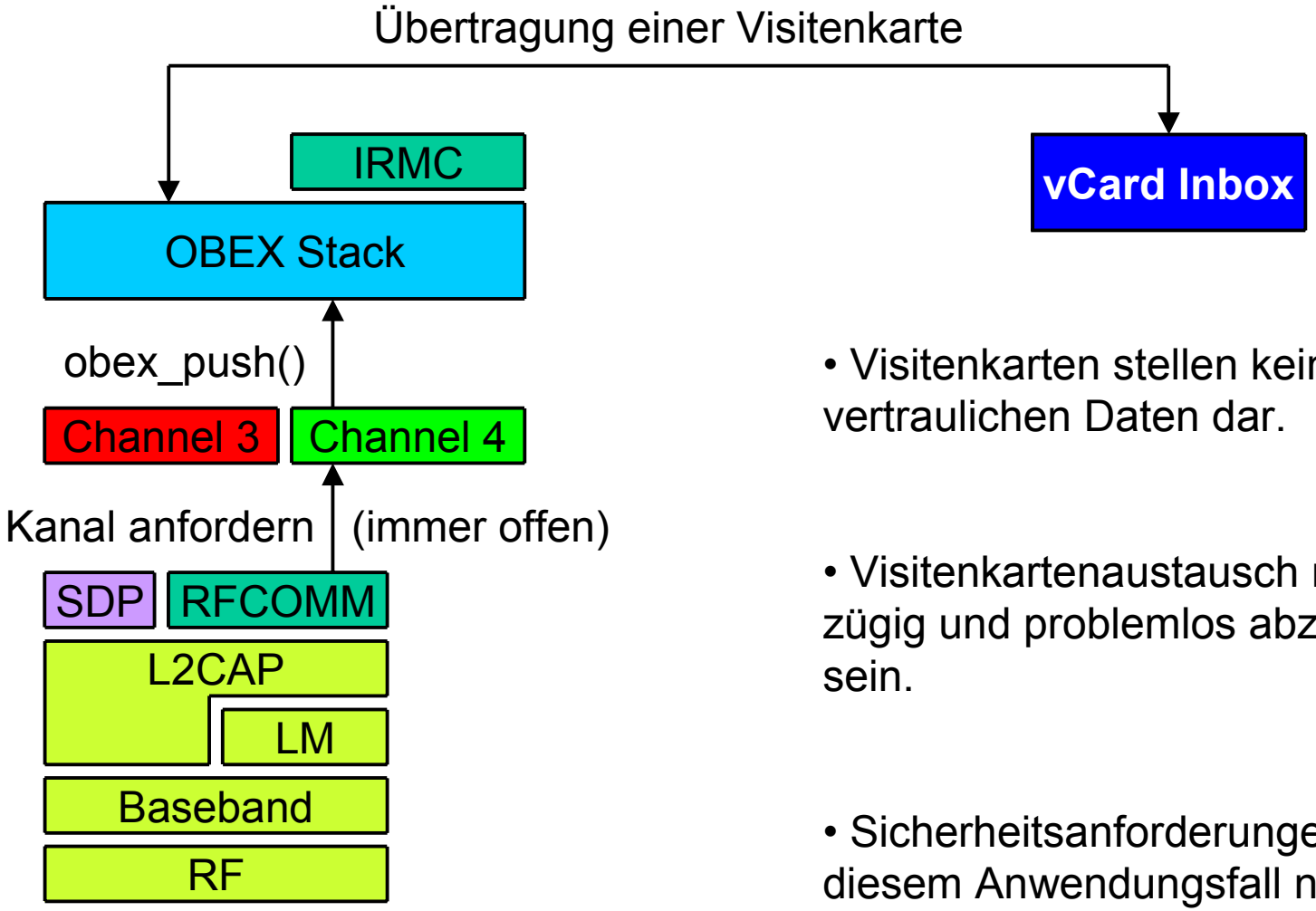
Synchronization Profile



RFCOMM Kanalzuordnung:

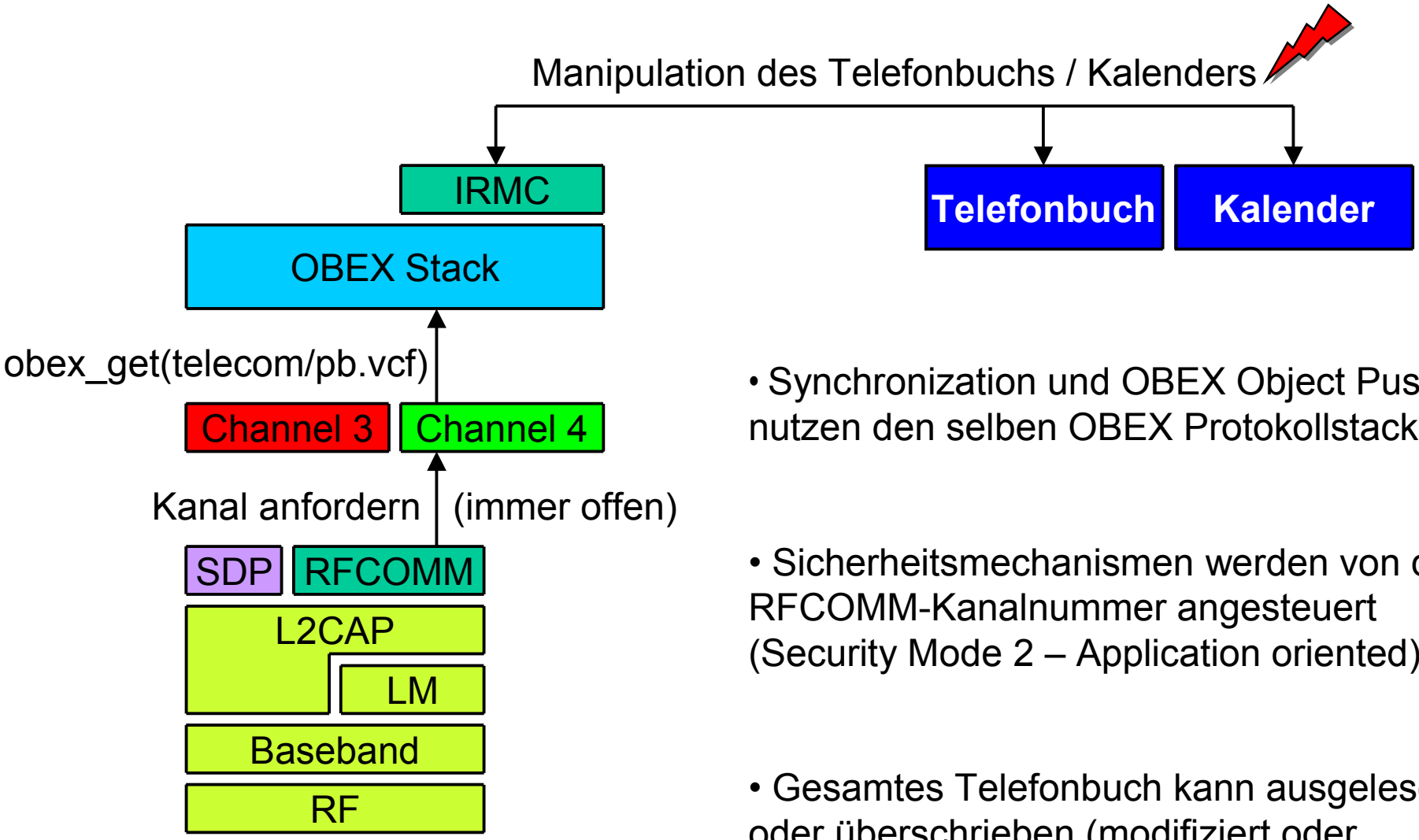
Channel 3: Synchronization Profile
Channel 4: OBEX Object Push Profile

OBEX Object Push Profile



- Visitenkarten stellen keine vertraulichen Daten dar.
- Visitenkartenaustausch muss zügig und problemlos abzuwickeln sein.
- Sicherheitsanforderungen sind in diesem Anwendungsfall nicht erwünscht.

IRMC-Funktionen über OBEX OPP



- Synchronization und OBEX Object Push nutzen den selben OBEX Protokollstack
- Sicherheitsmechanismen werden von der RFCOMM-Kanalnummer angesteuert (Security Mode 2 – Application oriented)
- Gesamtes Telefonbuch kann ausgelesen oder überschrieben (modifiziert oder gelöscht) werden.

Bluetooth-Sicherheit

Sicherheitsrelevante Daten

Datenkonzentrator Mobiltelefon

Das Mobiltelefon hat sich in den letzen Jahren mehr und mehr zum Sammelpunkt aller persönlichen Daten weiterentwickelt.

Beispielsweise können gespeichert werden:

Kontakte
Name, Vorname
Firmenname + Funktion
Telefonnummer (priv., Firma, mobile...)
Adressen (priv., Firma)
Geburtstag

Termine
Datum + Uhrzeit
Ort
Teilnehmende Personen

Datenkonzentrator Mobiltelefon

Ergebnis einer Blitzumfrage:

- auf elf Telefonen fanden sich 1404 Telefonbucheinträge (30 – 250 pro Telefon)
- lediglich zwei Telefone werden regelmäßig und systematisch gesichert
- drei Telefone werden regelmäßig synchronisiert
- sechs Telefone sind „einziger“ Speicher der Informationen

Sensible Daten

Fazit:

Die im Mobiltelefon gespeicherten Daten sind für den Nutzer zum Teil extrem bedeutend.

Bei drahtloser Zugriffsmöglichkeit, wie z.B. Bluetooth, muss sich der Entwickler eines mobilen Gerätes und dessen Produktmanagement der Sensibilität der Daten bewusst werden und besonders stark auf deren Schutz eingehen.

Ende

Vielen Dank für Ihre Aufmerksamkeit!

Kontaktinformationen

Dipl.-Ing. (FH) Alexander Grimm
Matsushita Electronic

04131 xxx xxx
a.grimm@ecom.panasonic.de

Marcel Holtmann
BlueZ Projekt

05223 xxx xxx
marcel@holtmann.org

Dipl.-Ing. (FH) Andreas Vedral
FH – Bochum

0234 xxxx xxx
andreas.vedral@fh-bochum.de