

# Good for Enterprise

Präsentation

**keyon**

**René Eberhard**  
Dipl. Ing. HTL  
Betriebswirtschafts-Ing. FH NDS  
CEO, Partner

keyon AG  
Schlüsselstrasse 6  
8845 Jona  
Switzerland  
www.keyon.ch

Tel. +41 55 220 64 03  
Mobile +41 79 458 05 45  
Fax +41 55 220 64 01  
eberhard@keyon.ch

eberhard@keyon.ch



## Über Keyon

Experten im Bereich IT-Sicherheit und Software Engineering

Als Value added Reseller von Good Technology unterstützen wir Sie bei der Integration der Lösung.

information security?  
just relax.

- Corporate PKI
- Software Engineering
- IT- and Mobile Security
- Digital Signature Services
- Identity & Access Management
- Security- and Business Consulting

**keyon**  
www.keyon.ch / info@keyon.ch



## Sichere Smartphones im Unternehmen

- ▶ Good trennt private und geschäftliche Daten und Applikationen auf Ihrem Smartphone
- ▶ Sichere Speicherung und Übermittlung aller Geschäftsdaten
- ▶ Zentrale Administration und Überwachung
- ▶ Unterstützt iPhone, iPad, Android und Windows Mobile



keyon AG  
Schlüsselstrasse 6  
8645 Jona  
Switzerland

Tel: +41 55 220 64 00  
Fax: +41 55 220 64 01

www.keyon.ch  
info@keyon.ch

Software Engineering • IT & Mobile Security • Digital Signature Services • Corporate PIV • Identity & Access Management • Security & Business Consulting



# Warum Mobile Security?

Vergleichbare Pressemeldungen PC - Smartphones

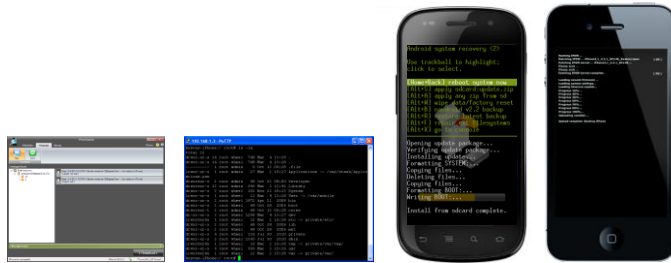
Unterschätzte Gefahren für Unternehmen

- Der Mitarbeiter möchte neben den geschäftlichen Apps auch private Apps nutzen (Spasfaktor)
  - Verschiedene Apps kopieren Kontaktdaten (oder andere Informationen) zu einem Server des Anbieters
  - Die Weitergabe von persönlichen Daten kann gewollt sein, um beispielsweise an einer Community teilnehmen zu können
- Keine sichere Übermittlung der Daten
  - SSL oder VPN gesicherte Verbindungen können aufgebaut werden. Hierzu ist aber eine zentrale Management Konsole sowie eine PKI notwendig, um die Smartphone zu konfigurieren.



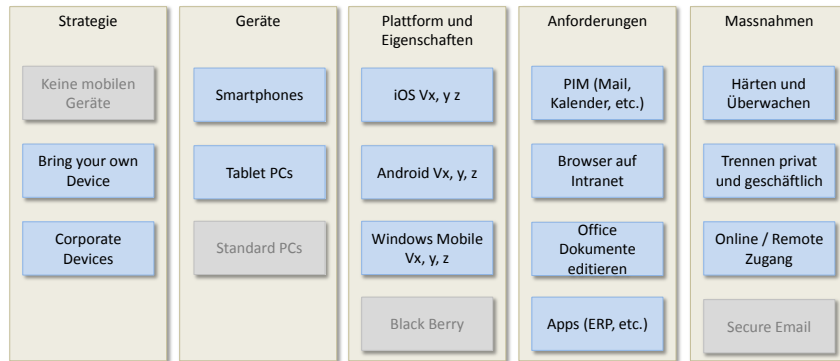
### ■ Unterschätzte Gefahren für Unternehmen

- Die Daten auf dem Smartphone sind generell nicht sicher abgespeichert. Ohne zusätzlichen Schutz können die Daten bei Verlust oder Diebstahl rel. einfach ausgelesen werden.



## Strategien im Bereich Mobile Security

Strategien im Bereich Mobile Security



Abhängig von den Anforderungen gib es mehr oder weniger Kombinationsmöglichkeiten

Strategien

- Keine mobilen Geräte  
Das Unternehmen setzt keine Smartphones ein. Die Mitarbeiter haben mobilen Zugang zu Informationen über Laptops und VPN.
- Bring your own Device  
Der Mitarbeiter stellt sein mobiles Gerät für unternehmerische Zwecke zur Verfügung (beispielsweise PIM Synchronisieren, telefonieren, etc.)
- Corporate Devices  
Das Unternehmen stellt dem Mitarbeiter ein mobiles Gerät zur Verfügung

■ Plattformen

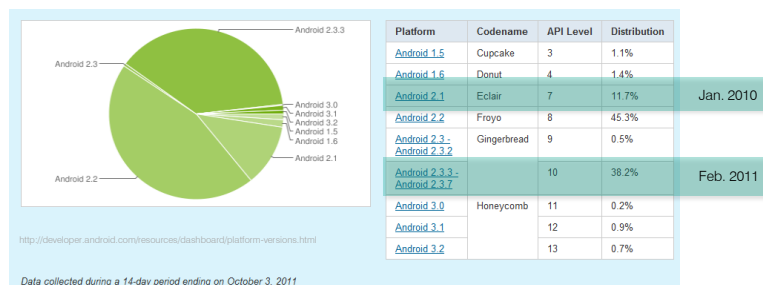
Die aktuellen Plattformen (iOS, Android, Windows Mobile) haben grundsätzlich unterschiedliche Eigenschaften und Schnittstellen hinsichtlich

- Device Management
- Monitoring
- Verteilung und Verwaltung von Zertifikaten (für 802.1x, etc.)
- Sicherheit
- Verhalten im Zusammenhang mit Applikationen (z.B. Datenaustausch)
- Programmiersprachen und native Schnittstellen

■ Plattformen – Fragmentierung

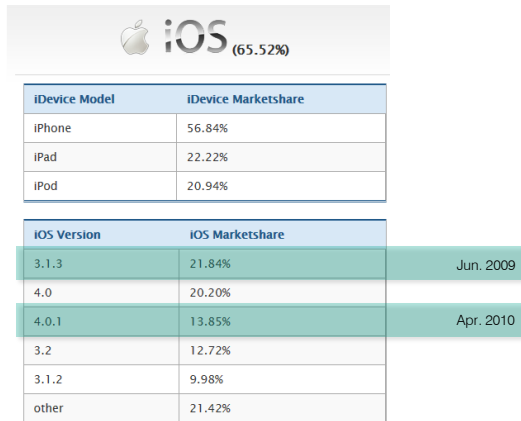
Die einzelnen Plattformen weisen z.T. erhebliche Unterschiede bez. der Funktionalität aus. Bei native Applikationen muss der Code für jede Version einzeln kompiliert werden.

Fragmentierung am Beispiel von Android



■ Plattformen – Fragmentierung

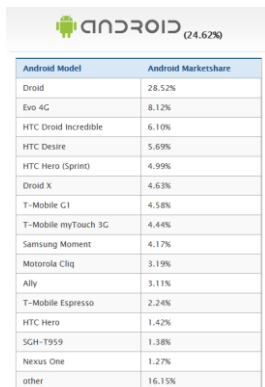
Fragmentierung am Beispiel von iOS



<http://labs.chilika.com/MobileWar/>

■ Plattformen – Fragmentierung – Hardware Fragmentierung

Neben unterschiedlichen OS müssen gegebenenfalls die Eigenschaften der unterschiedlichen Geräte in Betracht gezogen werden (Fragmentierung am Beispiel von Android)



Die einzelnen Anbieter liefern teilweise unterschiedliche Built-in Applikationen mit:

- Office
- Dateiverwaltung
- Etc.

<http://labs.chilika.com/MobileWar/>

■ Massnahmen zur Sicherung der Geräte

■ **Härten und Überwachen**

- Einschränken der Eigenschaften der Geräte (z.B. verbieten des öffentlichen App Stores).
- Nutzen der OS spezifischen Eigenschaften zum Härten und Überwachen der Geräte
- Eignet sich im Zusammenhang mit Corporate devices
- Wird im Zusammenhang mit BYOD kaum akzeptiert

■ Massnahmen zur Sicherung der Geräte

■ **Trennen von privatem und geschäftlichem**

- Eignet sich im Zusammenhang mit Corporate devices
- Eignet sich im Zusammenhang mit BYOD



■ Massnahmen zur Sicherung der Geräte

■ **Online – Remote Zugang**

- Eignet sich nur im Zusammenhang mit Tablet PCs
- Erfordert zwingend WLAN Verbindung (Bandbreite)
- Eignet sich um Textbasierte Dokumente zu editieren
- Wenig geeignet für Tabellenkalkulation oder grafische Dokumente (Powerpoint) zu editieren



Good for Enterprises

- Konsequente Trennung der Daten und Applikationen
  - Eigene, in sich geschlossene App ohne Schnittstellen gegenüber anderen Apps
  - Push Email (keine eingehenden Verbindungen in das Unternehmen)
  - Gewohntes look and feel
  - Standard Applikationen, sofortige Synchronisation
    - E-Mail
    - Kontakte
    - Kalender
  - Unterstützt
    - iOS (iPhone, iPad)
    - Android
    - Windows Mobile



19

- Umfassendes Mobile Device Management
  - Corporate App Store (OTA Software Installation)
  - Erweiterte iOS Verwaltung mit User- oder MDM Profiles
  - Document Management Policy (Editieren von Office Dokumenten)
  - Compliance Manager und Compliance Reporting
  - Web clips

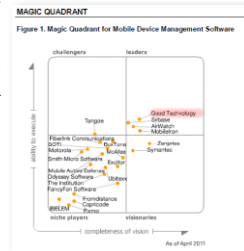


20



Strengths (extract)

- Has the best name recognition in MDM and appears frequently on shortlists, although the company's primary product is secure e-mail.
- Good's mobile security features, particularly platform-independent FIPS 140-2 encryption in the e-mail system, have helped to catalyze entry for Apple devices into organizations bound to stringent data protection requirements
- Good can validate and authorize specific applications before allowing them to connect to a corporate network. This feature is available even on platforms that do not support blacklisting and whitelisting, such as iPhone and iPad.
- Extensive help desk features are included, as well as a user self-service portal.

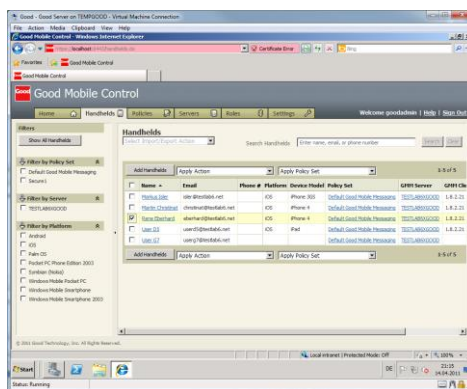


Übersicht - Server



Zentrale Managementkonsole

- Einheitliche, Web-basierte Konsole für alle Clients (iOS, Android, Windows Mobile)
- Zentrale Konfiguration der Smartphones (Profiling)
  - Smartphone Eigenschaften
  - Good Eigenschaften
- Zentrales Monitoring
- Remote Wipe
- Self-Service

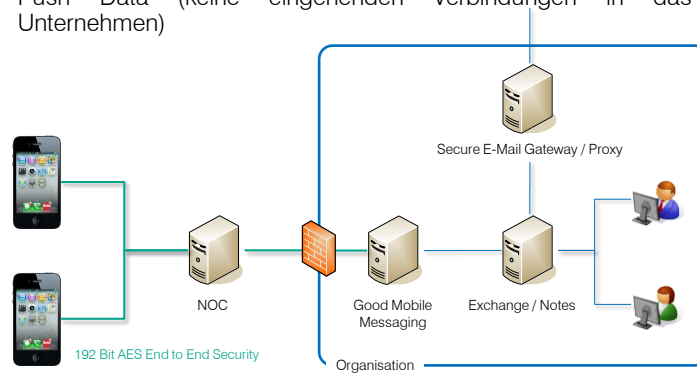


## Übersicht - Netzwerk



### Netzwerktopologie

- Starke End to End verschlüsselte Verbindung (AES 192 Bit) zwischen dem Good Mobile Messaging Server im Unternehmen und dem Smartphone.
- Push Data (keine eingehenden Verbindungen in das Unternehmen)



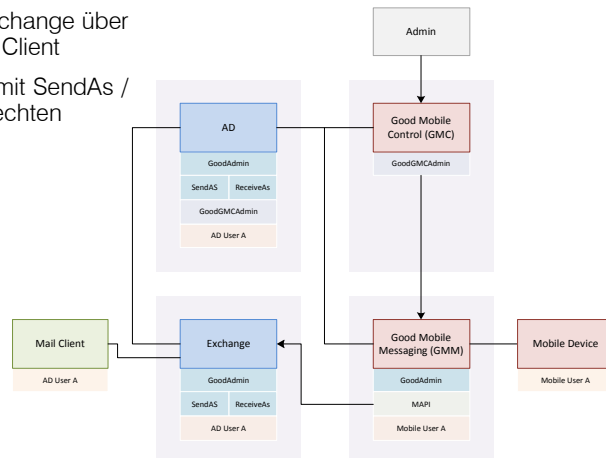
23

## Microsoft Exchange Integration



### Microsoft Exchange Integration

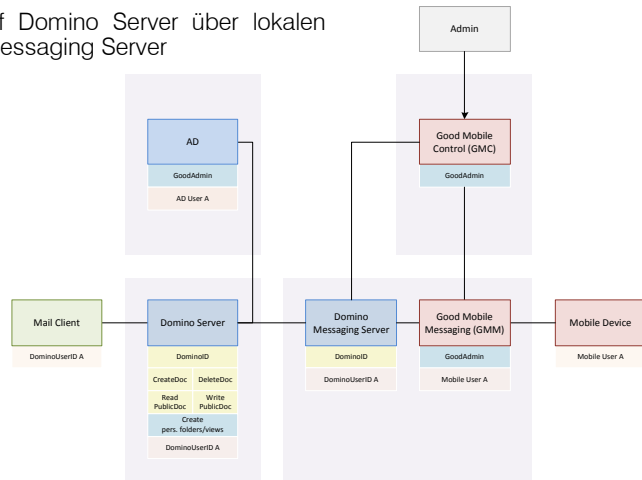
- Zugriff auf Exchange über lokalen MAPI Client
- GoodAdmin mit SendAs / ReceiveAs Rechten



24

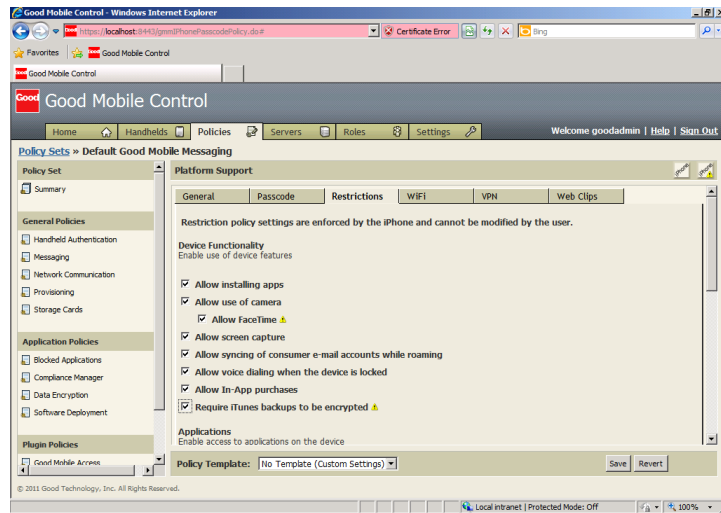
IBM Lotus Domino Integration

- Zugriff auf Domino Server über lokalen Domino Messaging Server

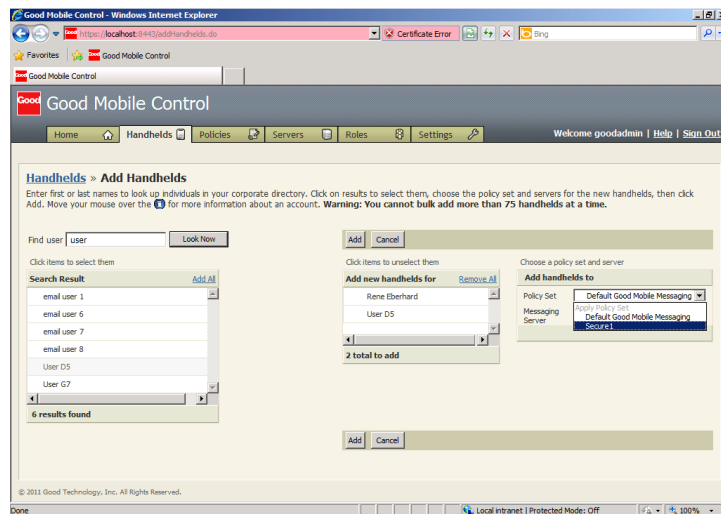


Rollout / look and feel

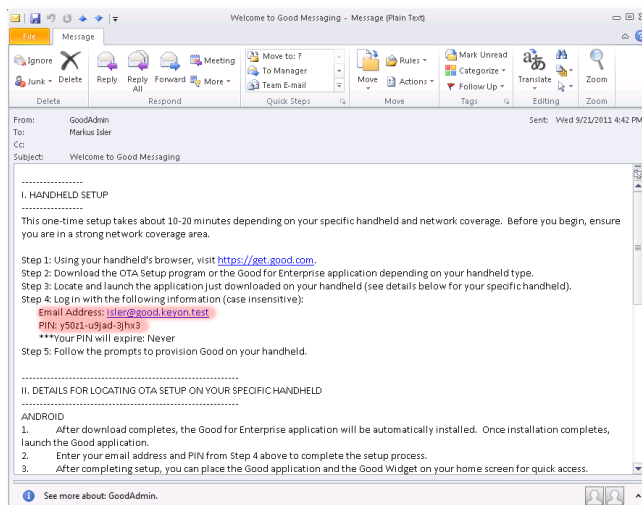
- Definieren der Richtlinien, einmalig (Gerät und Good App, einmalig)



- Registrieren der Benutzer (AD Lookup)



Versand des PIN an den Benutzer per interner E-Mail



Installation

- Kostenloser Download der App
- Installation der App

Alle folgenden Beispiele gelten analog für iPhone, iPad, Android und Windows Mobile Smartphones



## Look and feel



### Setup / Registrierung

- Eingabe der E-Mail Adresse und PIN
  - Der PIN kann dem Mitarbeiter per internem E-Mail oder über andere Kanäle übermittelt werden.
- Ready to use



31

## Look and feel



### Login

- Zentral konfigurierbare Passwortrichtlinien



32

## Look and feel



### Applikationen

- E-Mail
  - Gewohntes look and feel
  - Unterstützt alle bekannten Funktionen



33

## Look and feel



### Applikationen

- Kalender 1/2
  - Gewohntes look and feel
  - Unterstützt alle bekannten Funktionen
  - Erkennt, ob Teilnehmer verfügbar sind oder nicht



34

■ Applikationen

■ Kalender 2/2

- Ereignisanzeigen werden auch über dem locked Screen angezeigt
- Details des Ereignisses werden nur in der Good App angezeigt



35

■ Applikationen

■ Kontakte 1/2

- Gewohntes look and feel
- Unterstützt alle bekannten Funktionen



36

## Look and feel



### Applikationen

- Kontakte 2/2
  - Synchronisieren von konfigurierbaren Benutzerinformationen von der Good App in die Kontaktinformationen vom Smartphone
  - Anzeige von konfigurierbaren Benutzerinformationen bei einem eingehenden Anruf – normales look and feel



37

## Look and feel



### Applikationen

- Secure Browser
  - Zugriff auf definierte Webseiten im Intranet
  - Zugriff auf definierte Webseiten im Internet
  - Sicherer cache innerhalb der sicheren Sandbox von Good



38

## Weitere Eigenschaften



### Policy Check

- Jailbreak detection
- OS Version verification
- Client Version verification
- Hardware Model verification
- Connectivity verification
- Custom rules
  
- Im Falle einer Verletzung
  - Zugriff verweigern
  - Wipe



39

## Weitere Eigenschaften



### Unterstützte Sprachen

Die folgenden Sprachen werden auf der Basis der länderspezifischen Einstellungen unterstützt

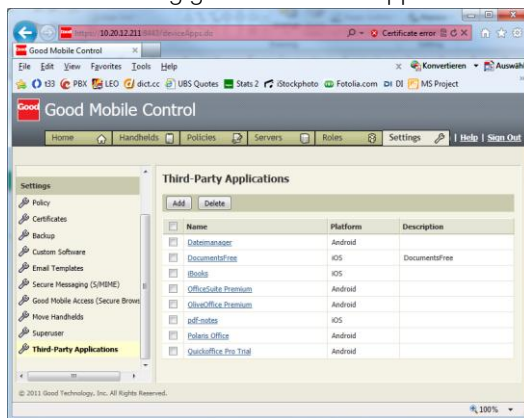
- English
- French
- Italian
- German
- Spanish
- Chinese
- Japanese
- Korean



40

Editieren von Dokumenten aus der Sandbox 1/3

- Austausch von Dokumenten über die «Send to» Funktion mit vertrauenswürdigen gekennzeichneten Applikationen

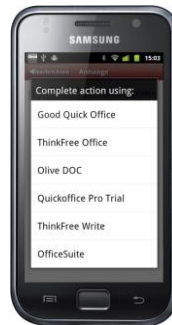


Editieren von Dokumenten aus der Sandbox 2/3

- Austausch von Dokumenten über die «Send to» Funktion mit vertrauenswürdigen gekennzeichneten Applikationen



Attachment



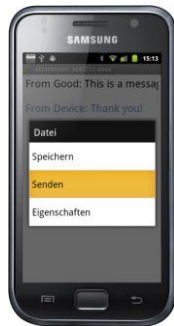
«Send to»  
vertrauenswürdige App  
ausserhalb der Sandbox



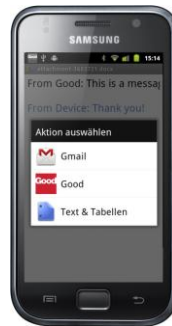
Editieren

### Editieren von Dokumenten aus der Sandbox 3/3

- Austausch von Dokumenten über die «Send to» Funktion mit vertrauenswürdigen gekennzeichneten Applikationen



“Send to”



Good



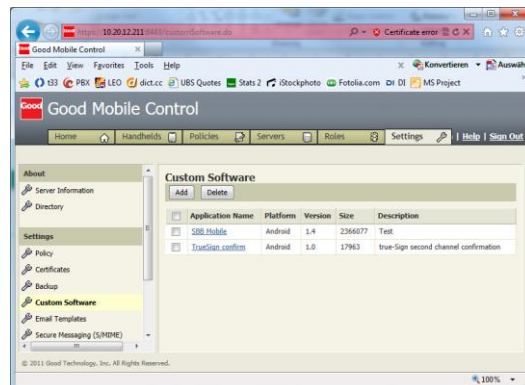
Attachment

Hinweis auf Strategien für das editieren von Dokumenten aus der vorherigen Präsentation.

43

### Corporate App Store 1/3

- Zentrales Bereitstellen von Apps



Vorbereiten der Apps.  
Diese werden verschlüsselt auf den NOC hochgeladen

44

## Corporate App Store



### Corporate App Store 2/3

- Zentraler App Store



Hinweis auf neue App



Neue Anwendung ist verfügbar



Auflisten

45

## Corporate App Store



### Corporate App Store 3/3

- Zentraler App Store



App aus Corporate App Store herunterladen



Installieren



46

Good Dynamics

- Plattform für die Entwicklung und Verwaltung von sicheren mobilen Applikationen

**Good is mobile security and control that allows users to connect and collaborate on the mobile device of choice**

- 5,000+ Enterprise Customers
- Mobility specialists for 12 years
- Largest Customer: US Army 80,000 users - 400 Employees, 300 Mobile Developers.



Good supports iPhone, iPad, Android, Nokia, Windows Mobile, Palm  
Good will continue to support all updated and any new popular OS's



**Good For Enterprise Customers**





## Sichere Smartphones im Unternehmen

- ▶ Good trennt private und geschäftliche Daten und Applikationen auf Ihrem Smartphone
- ▶ Sichere Speicherung und Übermittlung aller Geschäftsdaten
- ▶ Zentrale Administration und Überwachung
- ▶ Unterstützt iPhone, iPad, Android und Windows Mobile



keyon AG  
Schlüsselstrasse 6  
8645 Jona  
Schweiz

Tel: +41 55 220 64 00  
Fax: +41 55 220 64 01

www.keyon.ch  
info@keyon.ch

Software Engineering ■ IT- & Mobile Security ■ Digital Signature Services ■ Corporate PKI ■ Identity- & Access Management ■ Security & Business Consulting

