



BALTIMORE

www.baltimore.com

Ingo Schubert
Technical Consultant
Central Europe
+49 89 540 523 - 01
ischubert@baltimore.com

Baltimore auf einen Blick

- Weltmarktführer für e|security Produkte, Service, und Lösungen
- Weltweite Niederlassungen mit Headquarters in Dublin, London, Sydney, Tokyo and Boston
- NASDAQ (BALT) & London Stock Exchange (BLM)
- Blue Chip Kunden



FROST & SULLIVAN

Market Engineering
Customer focus award



Global Reach

Über 500 Kunden in über 40 Ländern



BALTIMORE™
www.baltimore.com



Global presence for global market

Zielsetzung von Baltimore

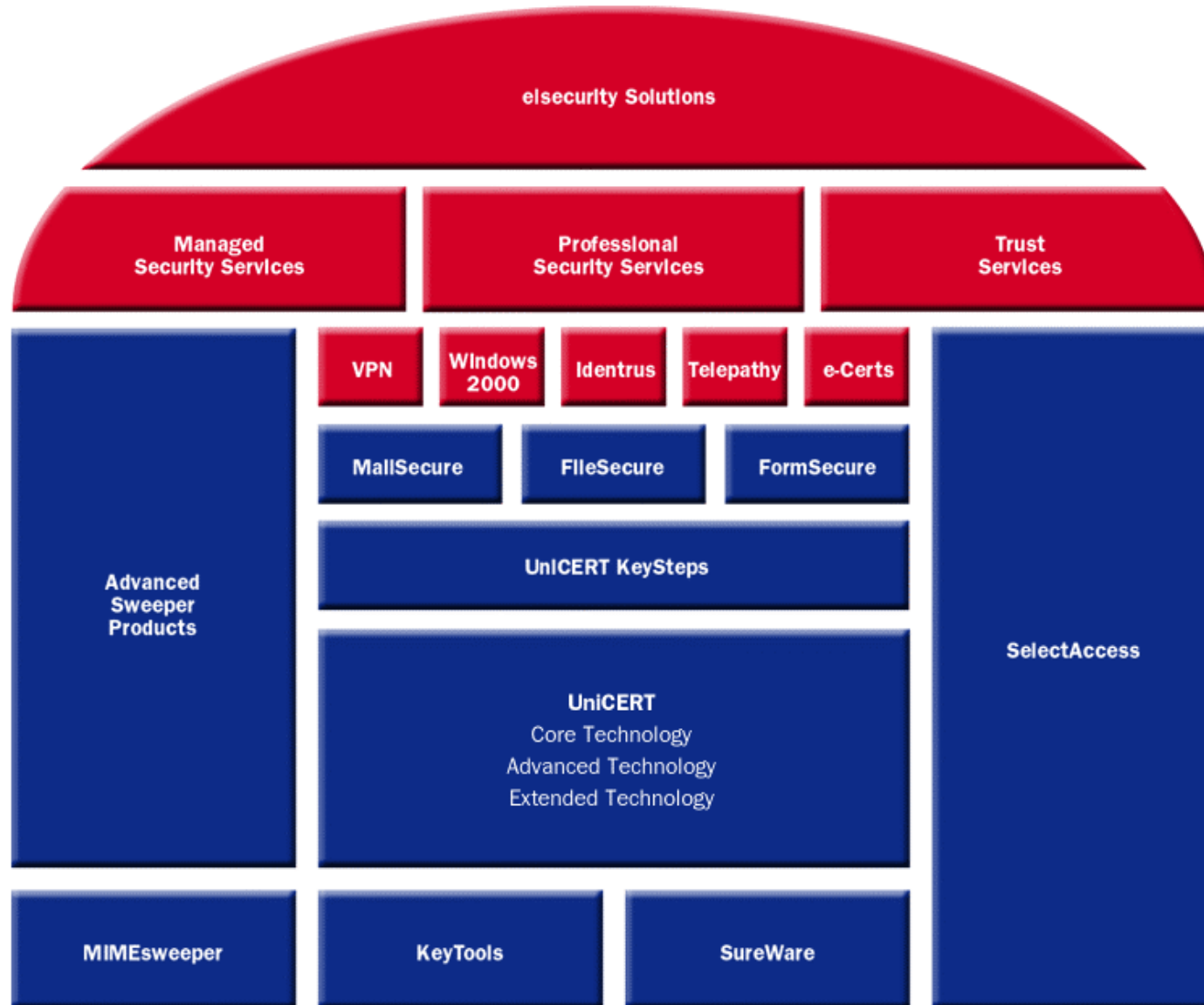
- Baltimore unterstützt seine Kunden bei der Entwicklung ihrer Internet Strategie
 - e-business
 - e-commerce
 - m-commerce
 - Enterprise IT Systems
- Wir bieten Security Infrastruktur und Lösungen an

e|security is an e|business enabler

Einige der Kunden von Baltimore Technologies die e|security einsetzen



Baltimore e|security Portfolio



PKI ermöglicht Vertrauen

- Geheimhaltung

Kryptographie



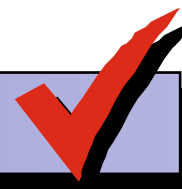
- Authentifikation

Digitale Zertifikate



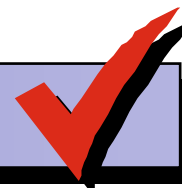
- Integrität

Digitale Unterschriften



- Nicht-Bestreitbarkeit

Digitale Unterschriften und Zertifikate



Zertifikate



- Digitale Zertifikate sind elektronische 'Pässe'
- Digitale Zertifikate beinhalten
 - Information über den Besitzer (Name, Adresse etc.)
 - den Public Key des Besitzers
 - die Unterschrift einer Trusted Third Party
- Trusted Authorities bürgen für die Gültigkeit eines Zertifikates
- Certificate Authorities (CA) wie z.B. UniCERT bilden die Basis einer Trusted Third Party

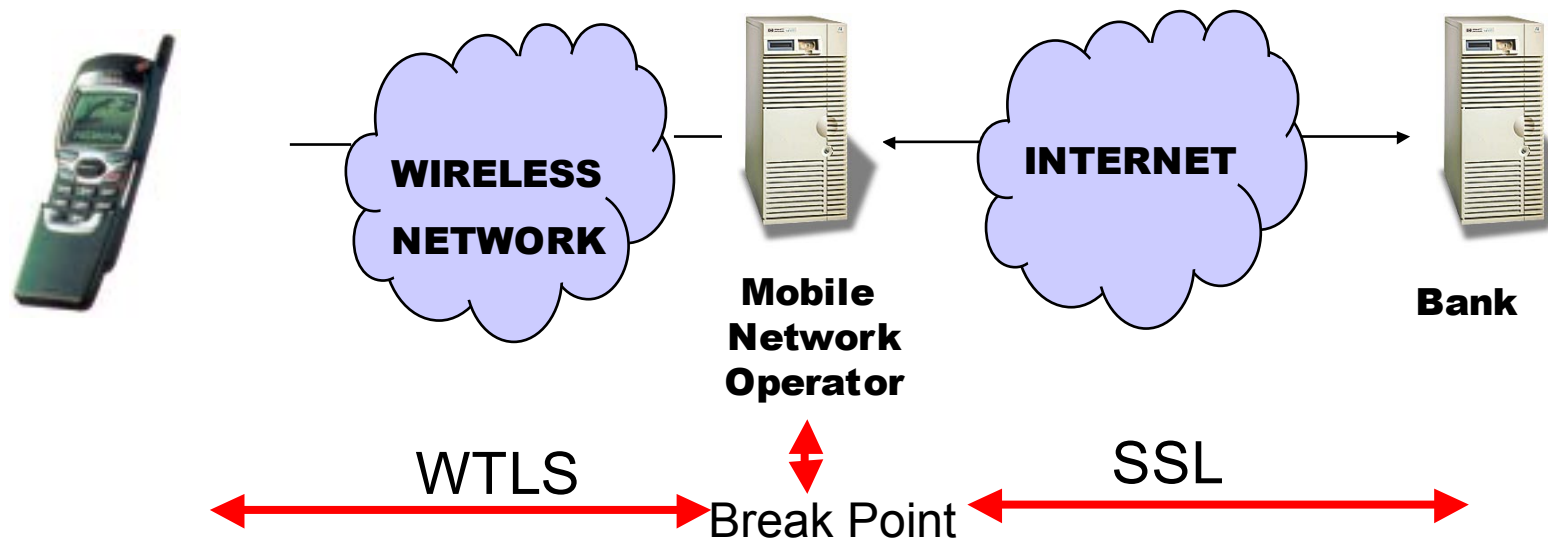
Unterschriften



- Eine digitale Unterschrift erfüllt die selben Aufgaben wie eine physikalische Unterschrift
- Die unterschriebenen Daten werden durch eine Prüfsumme gegen Veränderungen geschützt.
- Wenn die Überprüfung einer digitalen Unterschrift erfolgreich ist steht fest:
 - wer die Daten unterschrieben hat
 - die Daten wurden nicht verändert

Ist WTLS genug?

← End to End Security →



Wege zur End to End Security



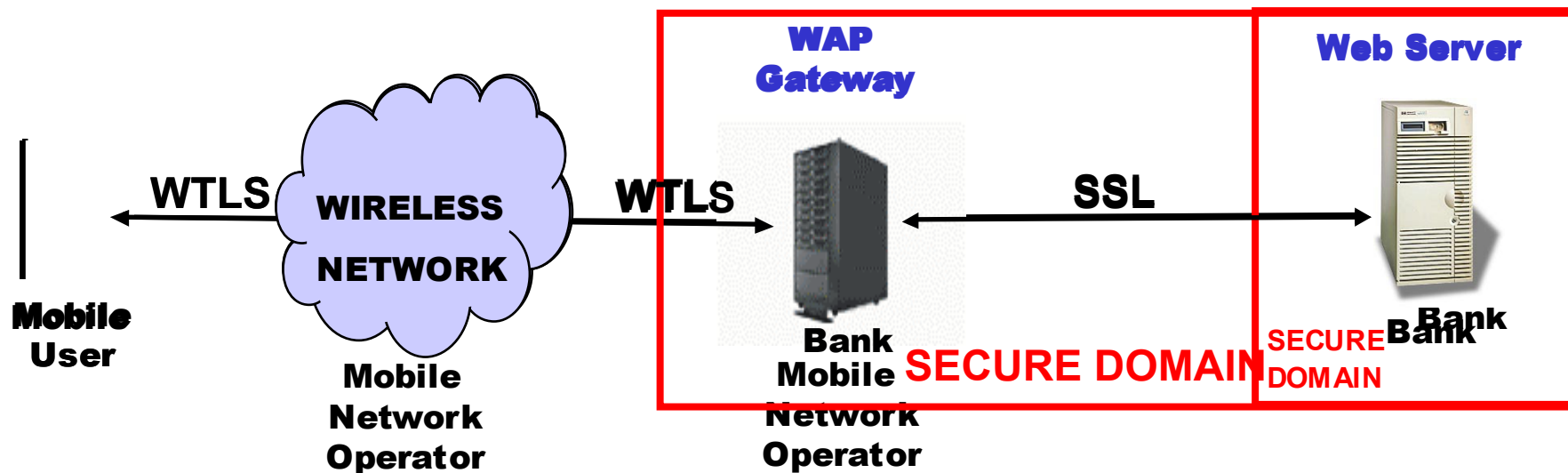
1. Alle Komponenten in einer sicheren Umgebung
2. WAP End to End Security Lösung
3. WAP Application Layer Security

E2E Lösung 1 - Alles in einer sicheren Umgebung



- WAP Gateway und Web Server zusammen in einer gesicherten Umgebung
- Daten werden immer noch ver- und entschlüsselt aber dies passiert in vertrauter Umgebung

Alles in einer sicheren Umgebung



E2E Lösung 1 - Alles in einer sicheren Umgebung



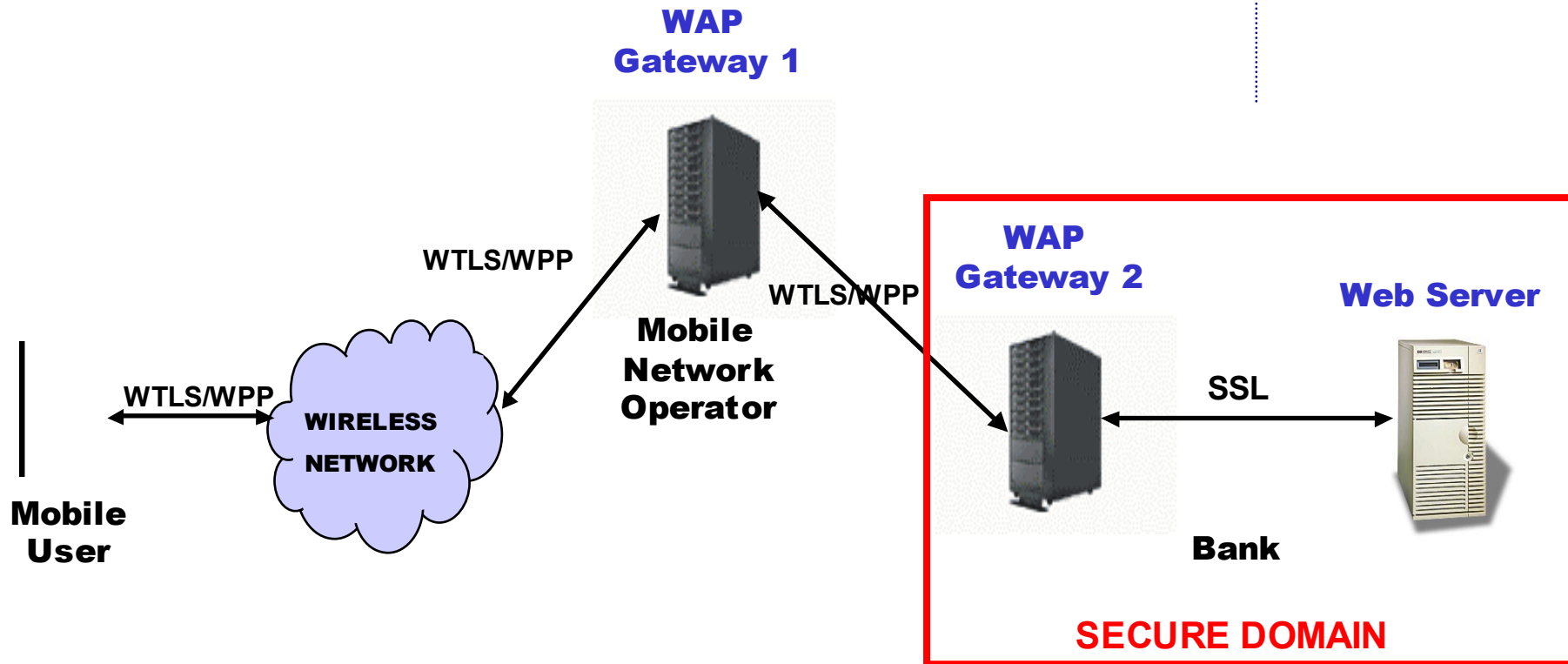
- Vorteile
 - Die einzige Lösung die mit heutigen WAP Endgeräten funktioniert!
- Nachteil
 - Nicht Operator-freundlich
 - Setzt Umkonfigurierung des WAP Endgerätes voraus.

E2E Lösung 2 - WAP End to End Spezifikation



- Erzielt E2E mit WTLS und mehreren WAP Gateways.
- Mehrere WAP Gateways kommunizieren miteinander.
 - Master/Slave Model
 - Client hat die Möglichkeit die Verbindung zu einem anderen WAP GW umzuleiten.

E2E Lösung 2 - WAP End to End Spezifikation



E2E Lösung 2 - WAP End to End Spezifikation



- Vorteile
 - Transport Layer Secure Channel, Applikation muss nicht verändert werden
 - Operator-freundliche Lösung
- Nachteile
 - Browser und GW müssen modifiziert werden
 - Weitere Schnittstelle (Gateway->Gateway)

E2E Solution 3 – WAP Application Layer Security



- WMLScript Crypto API
 - SignText() - verfügbar WAP 1.2, 1.3
 - Encrypt/EnvelopeText() - in Arbeit WAP 2.0
 - VerifyText() - in Arbeit WAP 2.0
- Wie funktioniert es?
 - Handset beinhaltet einen Browser der WMLScript Funktionen versteht.
 - Content Providers erzeugt WML Seiten die diese Funktionen aufrufen
 - Schlüssel, Zertifikate und ZertifikatID/URLs werden im WIM gespeichert.

Wireless PKI Problemstellung...

- Existierende Internet Standards und Formate sind in der Wireless Welt unhandlich
 - geringe Bandbreite
 - Beschränkte Prozessor und Speicherkapazität beim Client
- Einbinden der heutige PKI Technologie und bereits vorhandener Infrastruktur.
- X.509 ist das standard Zertifikat Format
 - zu gross
 - Benutzer hat ggf. mehrere Zertifikate - Speicherplatz
- Probleme bei neu definierten, schlanken PKIs
 - Inkompatibilität mit vorhandenen PKIs
 - Wired und Wireless Benutzer haben verschiedene PKIs

Wireless PKI Lösung

- Certificate IDs
 - Eine Referenz auf ein Zertifikate, nicht das eigentliche Zertifikat wird übertragen
- Die Certificate ID ist eine URL (String)
- Minimal Bandbreite erforderlich
 - kein Problem bei der Übertragung
- Minimal Speicheranforderungen
 - mehrer Certificate IDs können gespeichert werden

Client PKI Registration

- WAP EE werden ggf. mit Zertifikaten ausgeliefert
 - “device” Zertifikate
- WAP PKI spezifiziert auch OTA Registration
 - Einfacher als vorhandene PKI Registration
 - CMP,CMC,PKCS#10 zu komplex für WAP EE.
- Authentifikation der Benutzer durch vorhandene Device Zertifikate oder z.B. PIN.

Client PKI Registration



- Ein “PKI Portal” verbindet die Wireless Welt mit der vorhandenen PKI
 - Telepathy Registration System von Baltimore
- PKI Portal leitet Registrations Anfragen an eine standard PKI weiter
 - z.B. mit CMP, CMC or PKCS#10

Telepathy PKI Registration System

- Server Anwendung die die Registrierung von Wireless Benutzern bei einer standard PKI ermöglicht
- Schneller, einfache Einbindung von Wireless Benutzern
- Minimal Bandbreiten Anforderung
- Einfach und verständlich für den Benutzer
- Standort unabhängig
 - Network Operator oder e-business
- Verfügbar für verschiedene Architekturen und Technologien
 - WAP 1.3
 - GSM/SIM
 - Internet/Intranet/Extranet

W/PKI Registration



BALTIMORE™
www.baltimore.com

ACME BANK

Register for ACME Bank
Personal Wireless Banking Service

Last Name:

First Name:

Account No:

Branch Code:

PIN No:

BY PRESSING "SIGN & SEND" YOU ARE SIGNING THE FORM
YOU WILL RECEIVE YOUR CERT ID SHORTLY
Good Luck!

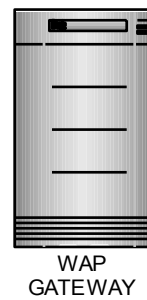
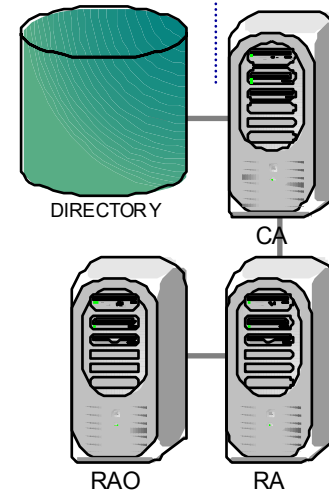
[Sign & Send Details](#) Richard Kinsella



PUBLIC KEY

PROOF OF IDENTITY

PROOF OF POSSESSION



W/PKI Transaktion

ACME BANK

Secure Funds Transfer
ACME Personal Wireless Banking Service

Account Number:

Payee:

Account No:

Branch Code:

Amount:

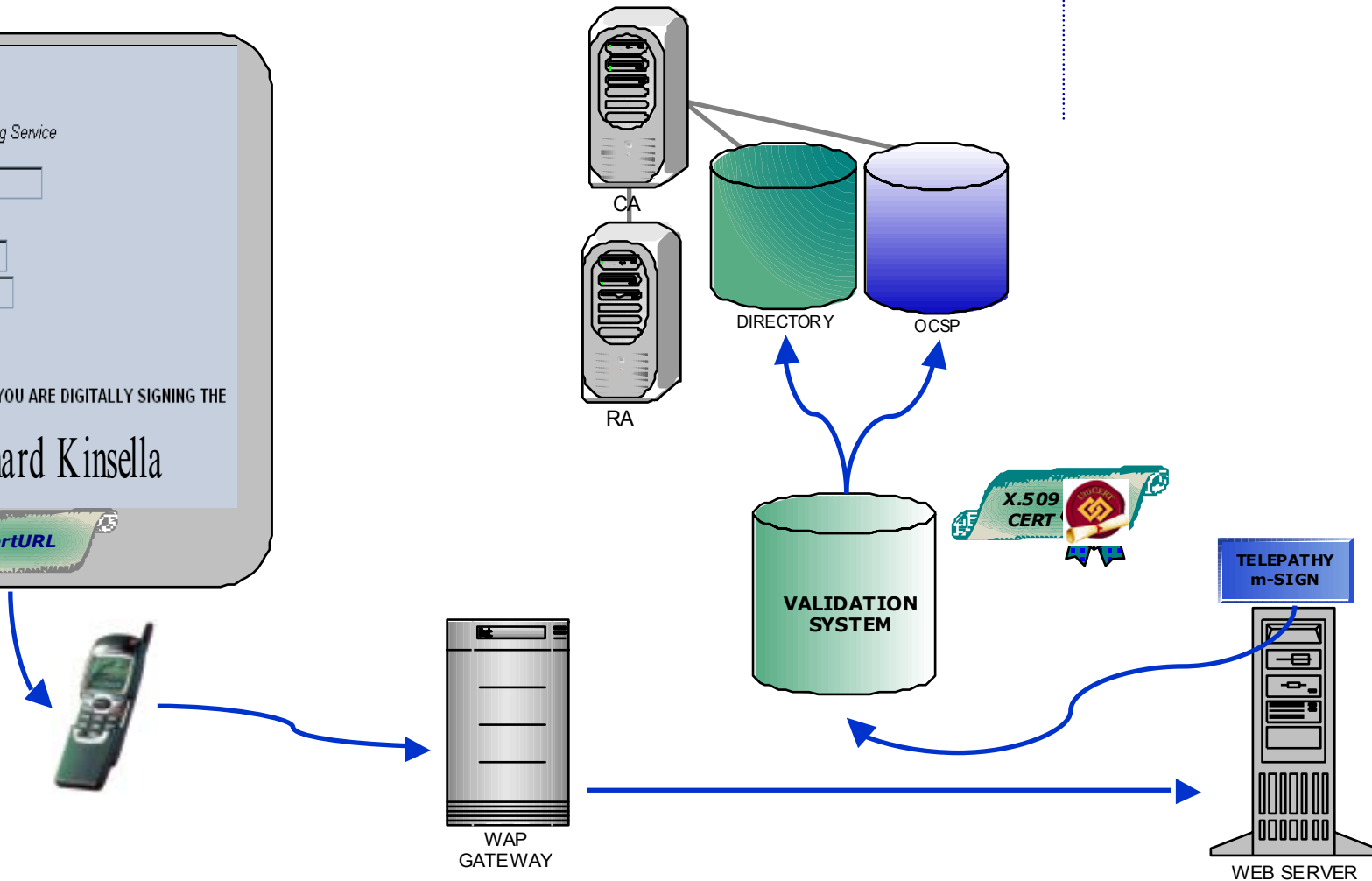

PIN No:

BY PRESSING "SIGN & SEND" YOU ARE DIGITALLY SIGNING THE FORM

Thanks You

Richard Kinsella

[Sign & Send Details](#)



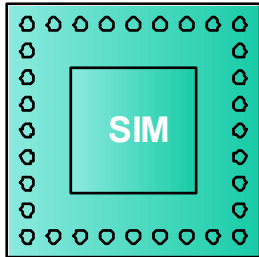
Telepathy PKI Validation System

- PKI Komponente die die Verifikation der Gültigkeit digitaler Zertifikate vornimmt.
- Handling von Certificate IDs
- Optimiert auf geringe Bandbreite
- Zukünftig (> WAP 1.3) nicht nur vom Server sondern auch vom Client genutzt
- Technologien
 - WAP 1.3
 - GSM/SIM
 - Internet/Intranet/Extranet

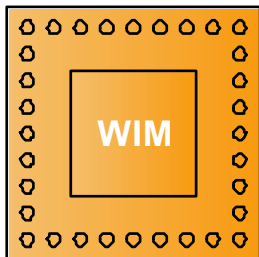
Telepathy m-Sign

- Entwickler API um digitale Unterschriften von WAP EE zu verifizieren.
- Ermöglicht End to End Sicherheitslösungen
- Integration mit PKI
 - Authentifikation des Senders
 - Integrität

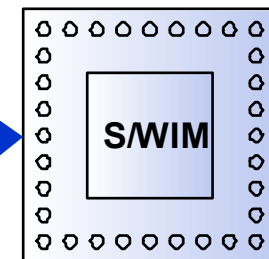
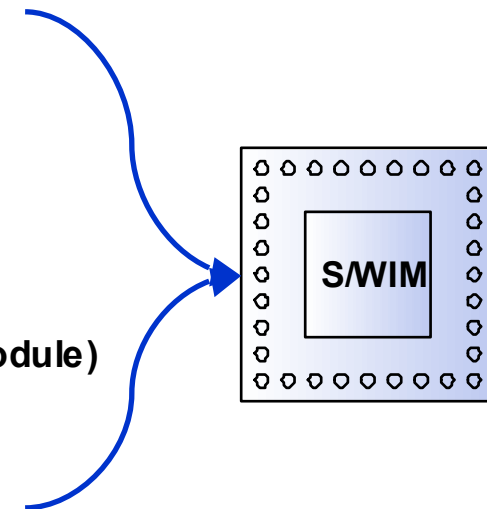
Wireless Identity Module (WIM)



SIM (Subscriber Identity Module)
 SmartCard für GSM Systeme die die Subscriber ID, Security Information und das Telefonbuch des Benutzers enthält.



WAP 1.2
 Nicht zu verwechseln mit der SIM (subscriber identity module)
 Spezifikationen
 user's key pairs
 certificates/certificate ids
 optional cryptographic functions
 Implementation
 Im Handset
 Separater Kartenleser/Karte
 kombinierte SIM and WIM (SWIM)



WPKI Zukunft



- Application Layer Security
 - EE verschlüsseln
 - EE entschlüsseln
 - EE verifizieren mit Validation System
- Download von signiertem, aktivem (?) Content
- Zusammenführung
 - Nutzung der selben Identität im Internet und in der Wireless Welt
 - WTLS ggf. ersetzt durch TLS
 - Bandbreite und Speicher werden unkritisch

WPKI Zukunft

- Entwicklung des *“Personal Trusted Device”*
- Trusted Device zu Authentifikation
 - M-commerce
 - Internet (PKCS#11 Treiber für Telefon)
 - Bankautomat
 - Ggf. Integration mit biometrischen Verfahren
 - ...





BALTIMORETM

www.baltimore.com

baltimore telepathyTM

Making Mobile Commerce Secure

www.baltimore.com/telepathy

Danke!

wireless

wireless e | security