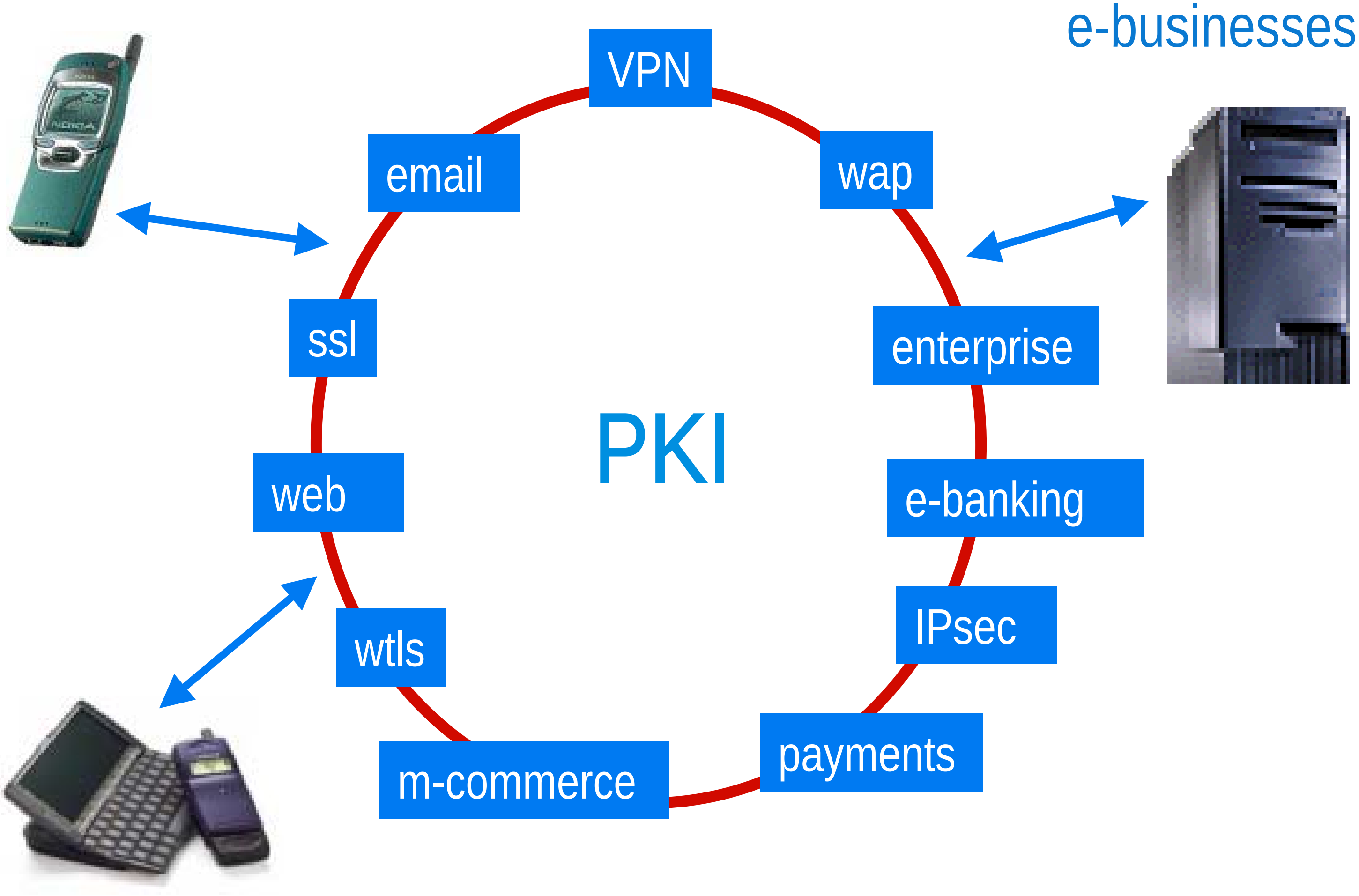
# Wireless PKI - Overview

**Massimo Nardone, Chief Security Architect, R&D Services, Comptel Corporation**

# Security in Wireless World



# Why PKI?

- Information over the Internet is Free, Available, Unencrypted, and Untrusted.

- A big problem for many Applications:
  - Electronic Commerce
  - Software Products
  - Financial Services
  - Corporate Data
  - Healthcare
  - Subscriptions
  - Legal Information

# Electronic trust provided by PKI

- Confidentiality
  - **Cryptography:** to keep information private
- Authentication
  - **Digital Certificates:** to prove the identity of an individual or an application
- Integrity
  - **Digital signatures:** to prove that information has not been manipulated
- Non-repudiation
  - **Digital signatures and certificates:** to ensure that information cannot be disowned

# The Components of a PKI

- Certificate Authority (CA): to issues and verifies digital certificate
- Registration Authority (RA): acts as verifier for the certificate authority
- Certificate Distribution System: One or more directories where the certificates (with their public keys) are held
- PKI-enabled Applications: Communications between web servers and browsers, E-mail, Electronic Data Interchange (EDI), Credit card transactions over the Internet, Virtual Private Networks (VPNs)

# PKI requirements

Main design requirements of a PKI, from legal and technical points of view included the following:

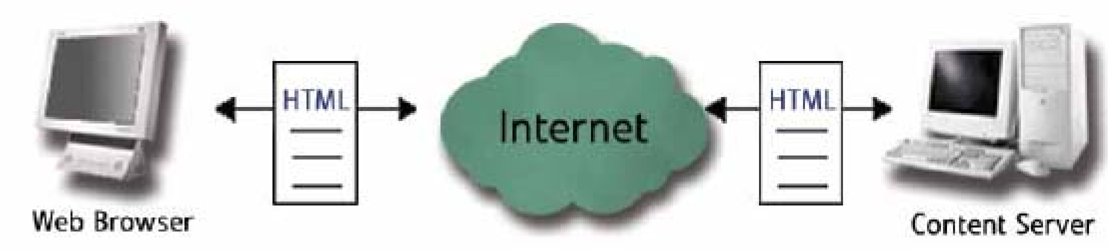
- **scalability**
- **support for multiple applications**
- **interoperability of separately-administered infrastructures**
- **support for multiple policies**
- **simple risk management**
- **limitation of the CA’s liability**
- **standards**

# The Web environment

The best analogy for the WAP environment is the *World Wide Web (Web)* environment.

The Web environment consists of three primary components: a *Web Client*, an *Internet Protocol (IP)* network, and a *Web Server*.

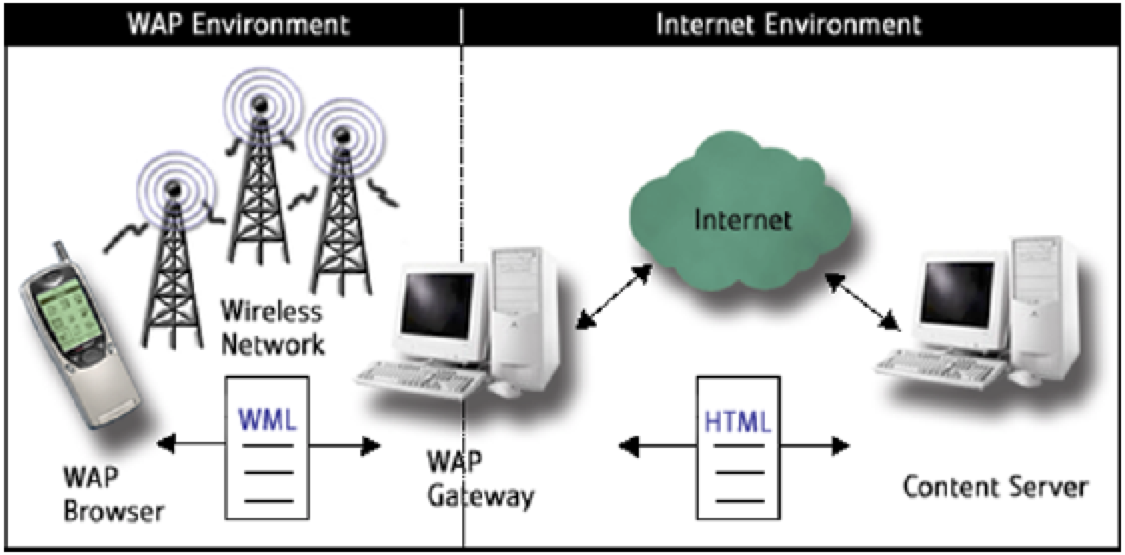
Web components communicate over IP networks like the Internet using HyperText Markup Language (HTML) data.



# The WAP environment

The WAP environment consists of three primary components: *WAP Client*, a *Wireless Network*, a *WAP Gateway*, an *IP network* and a *Content (Web) Server*.

The WAP Client communicates with the WAP Gateway using Wireless Markup Language (WML) data transmitted over a wireless network. The WAP Gateway translates WML data to/from HTML data and also relays the data between the wireless and wired network and communicates with the Web Server.



# The WAP Security

WAP encompasses four standards that apply security at the application, transport and management levels in the wireless environment. These standards are known as

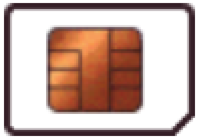
- the *WAP Identity Module (WIM)*
- the *WML Script Crypto API (WMLSCrypt)*
- the *Wireless Transport Layer Security (WTLS)*
- the *Wireless Application Protocol PKI (WPKI)*

# WIM/SWIM: what is a SWIM card?

WIM (Wireless Identity Module): WAP Identity Module is a tamper proof computer chip that resides in the WAP device (cellular phone, PDA, etc.), which contains a digital certificate that authenticates a WAP customer and enables him/her to electronically sign transactions, based on wireless public key infrastructure (PKI)

**The WIM stores the following data:**

- Information on properties of the module.
- Two key pairs: the first for authentication and key establishment, the second one for digital signature.
- A certificate or a “certificateURL” for each key pair.
- The certificate of each trusted CA.
- Data related to WTLS sessions.
- Information on protection of the data with PIN numbers.



SWIM Card: is the SIM card where the WIM is implemented.

# What is WMLSCrypt?

**WML Script Crypto API (WMLSCrypt) is an application programming interface that allows access to basic security functions in the WML Script Crypto Library (WMLSCLib), such as key pair generation, digital signatures and the functions that process objects commonly found in the PKI (e.g., keys and public-key certificates).**

**The basic functions in the WMLSCrypt and WMLSCLib include:**

- **generate key pairs**
- **store keys and other personal data**
- **control access to stored keys and data**
- **generate and verifying digital signatures**
- **encrypt and decrypt data**

# What is WTLS?

Wireless Transport Layer Security is a transport-level security protocol based on the Internet security protocol known as Transport Layer Security (TLS). WTLS can authenticate communicating parties and encrypt and check the integrity of the WML data when it is in transit. WTLS has been optimized for use in wireless devices that rely on narrow bandwidth wireless networks.

WTLS is a cryptograpy-based, PKI-enabled protocol that provides the following security services to WAP applications:

- Specifies a framework for secure connections, using protocol elements from common Internet security protocols like SSL and TLS.
- Provides security facilities for encryption, strong authentication, integrity, and key management
- Compliance with regulations on the use of cryptographic algorithms and key lengths in different countries
- Provides end-to-end security between protocol end points

# Types of authentication with WTLS

**There are three types (or WTLS classes) of authentication:**

- **Class 1: Implies Anonymous Authentication, each party cannot be assured of the identity of the other party.**

- **Class 2: Implies Server Authentication, the client is strongly assured of the server's identity (and thus trusts them to send them confidential data such as credit card numbers).**

- **Class 3: Implies both Client and Server  Authentication, the client is strongly assured of the server's identity as well as the the server is assured of the client's identity.**

| FEATURE | CLASS 1 | CLASS 2 | CLASS 3 |
|---|---|---|---|
| Server certificate | O | M | M |
| Client certificate | O | O | M |

M: Mandatory; O: Optional

**A certificate can be either:**

- X.509v3 certificate
- WTLS certificate
- X9.68 certificate (currently in draft)

The main difference between a  X.509v3 certificate and a WTLS certificate is that the latter is has reduced size and processing required in order to better match the constraints imposed by narrowband radiolink and the processing capacity in mobile equipment.

# What is a *Wireless Application Protocol PKI* ?

The traditional method used to handle PKI service requests relies on:

- ASN.1 Basic Encoding Rules (BER)
- Distinguished Encoding Rules (DER)

BER/DER require more processing resources than a WAP device should effectively have to handle.

WPKI protocols are implemented using WML and the WML Script Crypto API (WMLSCrypt).

WML and the *signText* function in WMLSCrypt provide for significant savings when encoding and submitting PKI service requests as compared to the methods used in traditional PKI.

# WPKI Architecture components 1/2

**WAP Device with WIM** (WAP Identity Module).

**SWIM Card** where WIM is implemented.

**WAP Gateway** with WTLS class 2 and SSL support.

**IP Network** with SSL support.

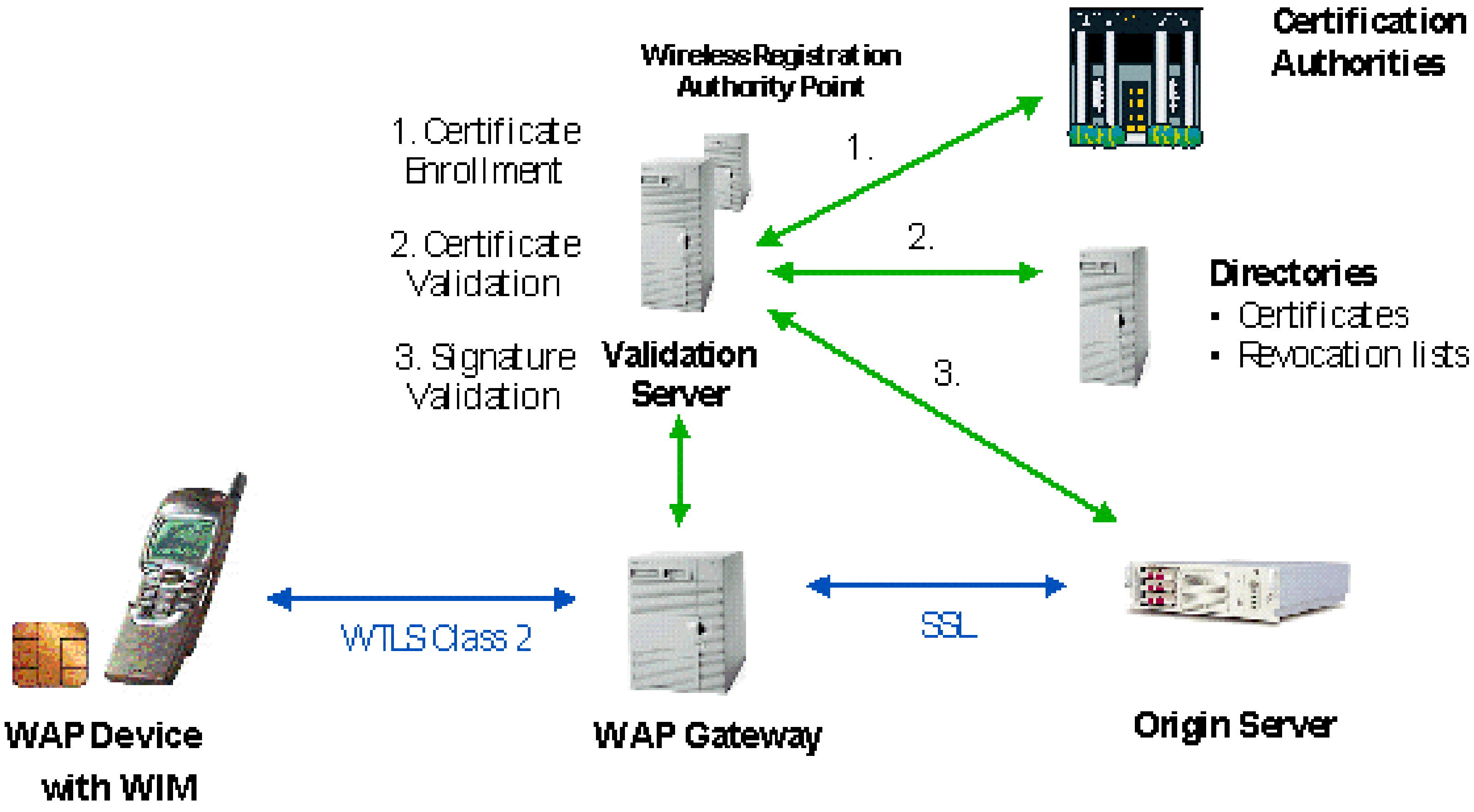
**Origin Server** running secure Service Application.

**CA, Directory and CRL functionality** consisting of a collection of several different CAs.

**Wireless Registration Authority Point** with Authentication and signing certificate request support.

**Validation Server** for online validation of signatures and certificates which is is capable of accessing the Directory and the CRL of the CA as well as those of third parties.

# WPKI Model architecture 2/2

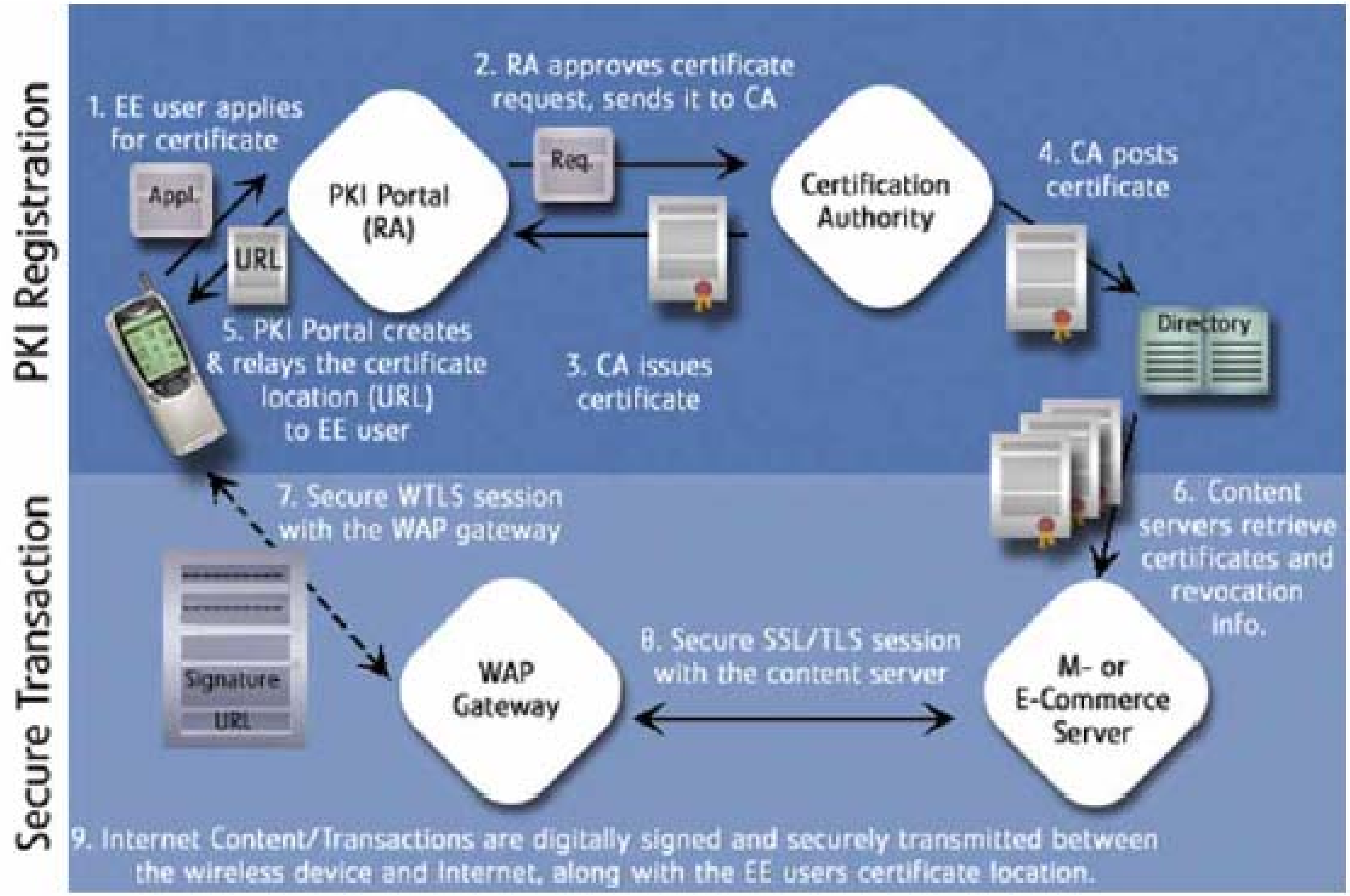


© Comptel Corporation 2001

# WPKI operational flow

**WPKI Components:**

- **End-Entity Application (EE)**
- **Registration Authority (RA)**
- **Certification Authority (CA)**
- **PKI Directory**



PKI Registration
Secure Transaction
1. EE user applies for certificate
Appl.
URL
PKI Portal (RA)
2. RA approves certificate request, sends it to CA
Req.
Certification Authority
4. CA posts certificate
Directory
5. PKI Portal creates & relays the certificate location (URL) to EE user
3. CA issues certificate
7. Secure WTLS session with the WAP gateway
6. Content servers retrieve certificates and revocation info.
Signature
URL
WAP Gateway
8. Secure SSL/TLS session with the content server
M- or E-Commerce Server
9. Internet Content/Transactions are digitally signed and securely transmitted between the wireless device and Internet, along with the EE users certificate location.

# A European WPKI project

EURESCOM, the European Institute for Research and Strategic Studies in Telecommunications, is the leading institute for collaborative R&D in telecommunications. It works as a virtual company using the resources of its shareholders to perform high-impact research projects.

Project P1001: PKI Implementation and Test Suites for Selected Applications and Services

Project Results:

- Europe-wide PKI model for inter-TelCo applications
- Interoperable PKI test environment for TelCos
- Implementation of PKI for different services and environments:
  - Vol 1 - PKI for selected services
  - **Vol 2 - PKI in a GSM environment (Team leader)**
  - Vol 3 - PKI services for UMTS
  - Vol 4 - PKI for mobile IP security

# WAP Services

## Information:

- news
- stock quotes
- applet downloading

## Communications:

- email
- wireless remote access
- chat

## Transactions:

- remote banking
- **e-commerce**
- stock exchange

## Entertainment:

- games
- date arrangement

# Security services for WAP applications

| Category | Mandatory services | Optional services |
|---|---|---|
| Information | Authentication of origin<br>Integrity of contents | Authentication of recipient<br>Encryption of contents |
| Communications | Authentication of sender and recipient<br>Encryption of contents<br>Integrity of contents | Non-repudiation |
| Transactions | Authentication of sender and recipient<br>Non-repudiation<br>Encryption of contents<br>Integrity of contents | |

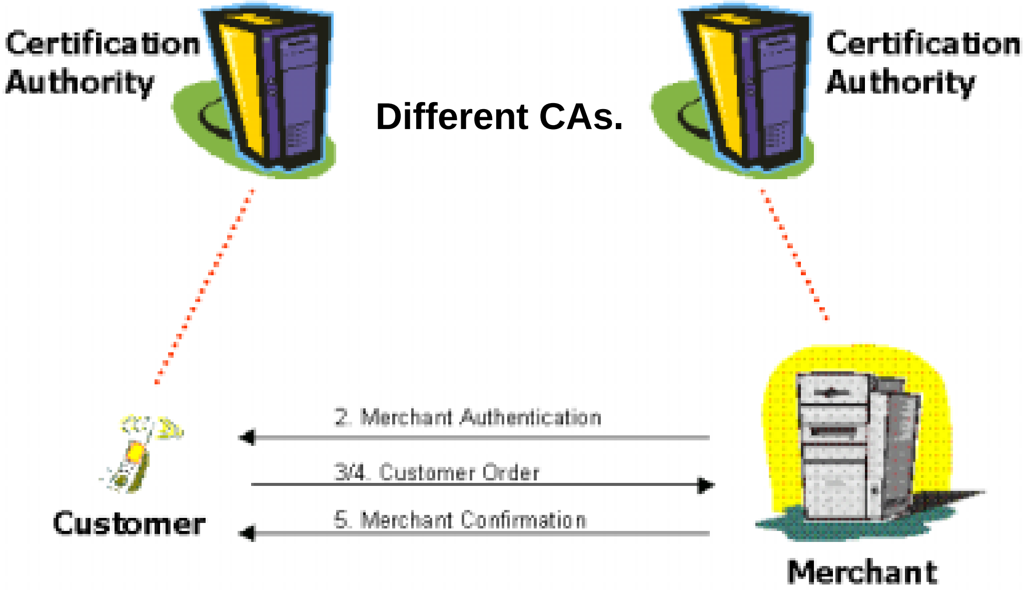
Non-repudiation: **Digital signatures and certificates** to ensure that information cannot be disowned

# WAP Service: Mobile e-commerce

Mobile e-commerce = wireless e-commerce.

- mobile phone
- PDA connected to a mobile phone
- portable PC connected to a mobile phone.

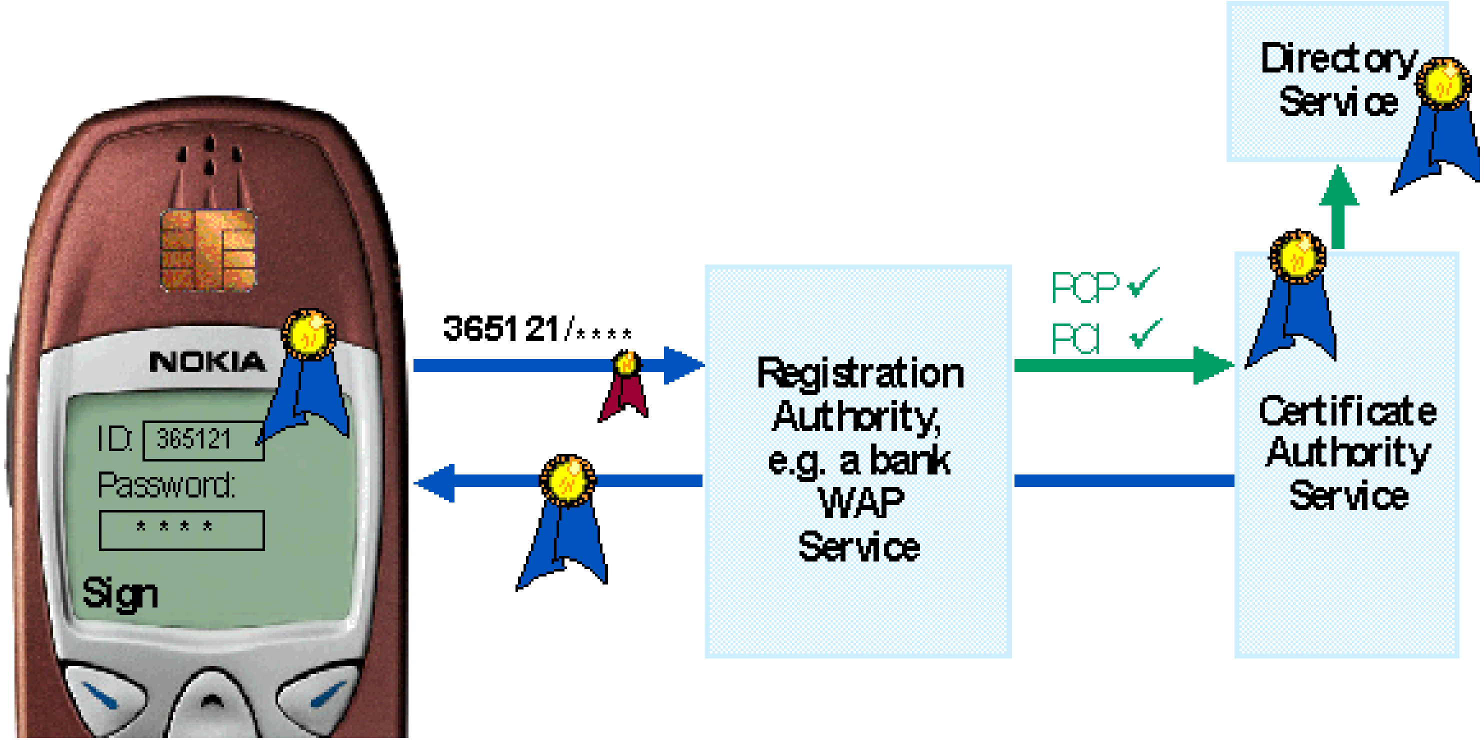
Unlike the traditional communications over Internet,
mobile phones incorporate from the beginning very strong authentication features.



**Phases:**

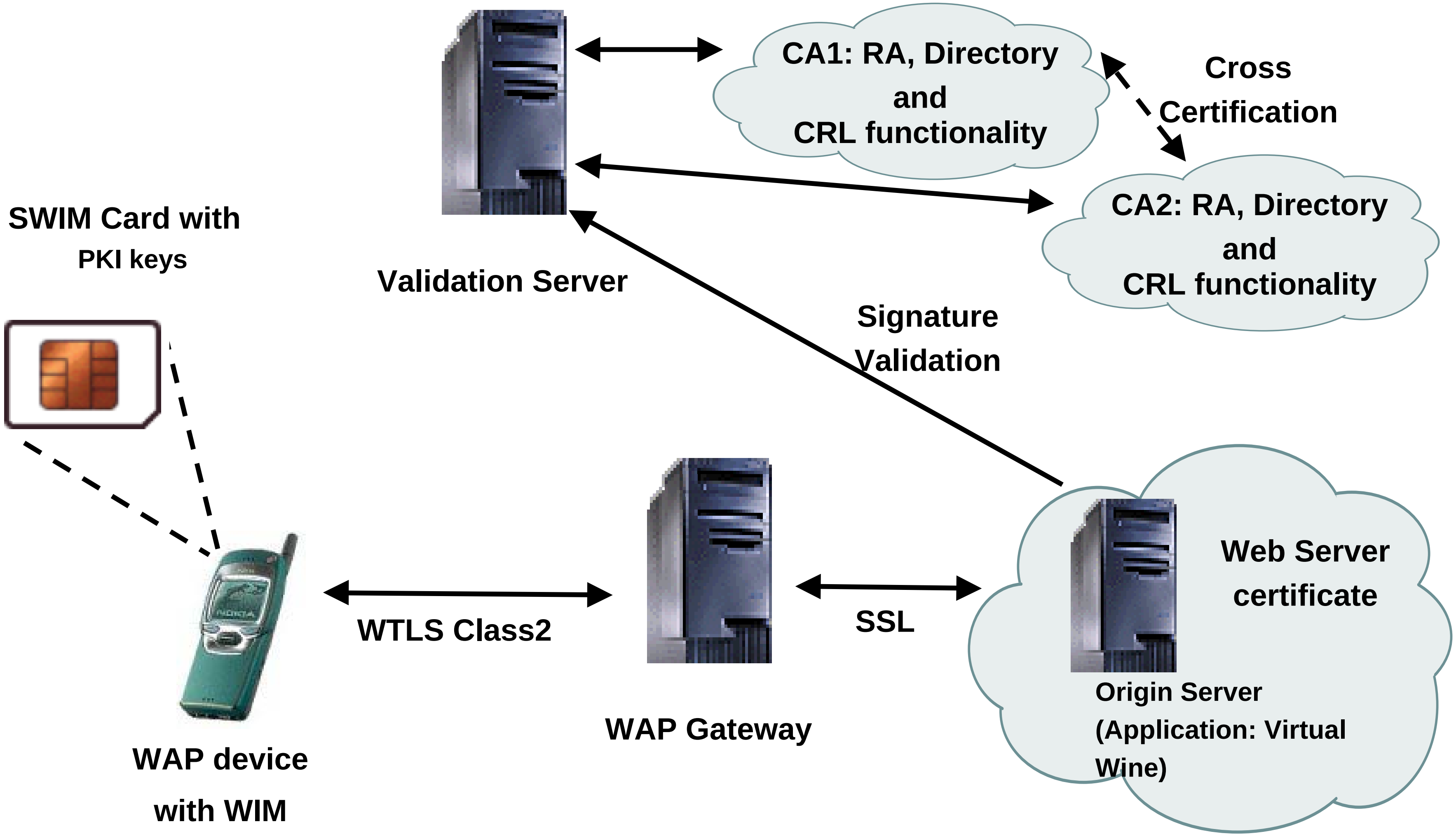
**1. Browsing**
**2. Merchant authentication**
**3. Customer authentication**
**4. Order generation and delivery**
**5. Order confirmation**

# Validation Server: Certificate Enrolment process

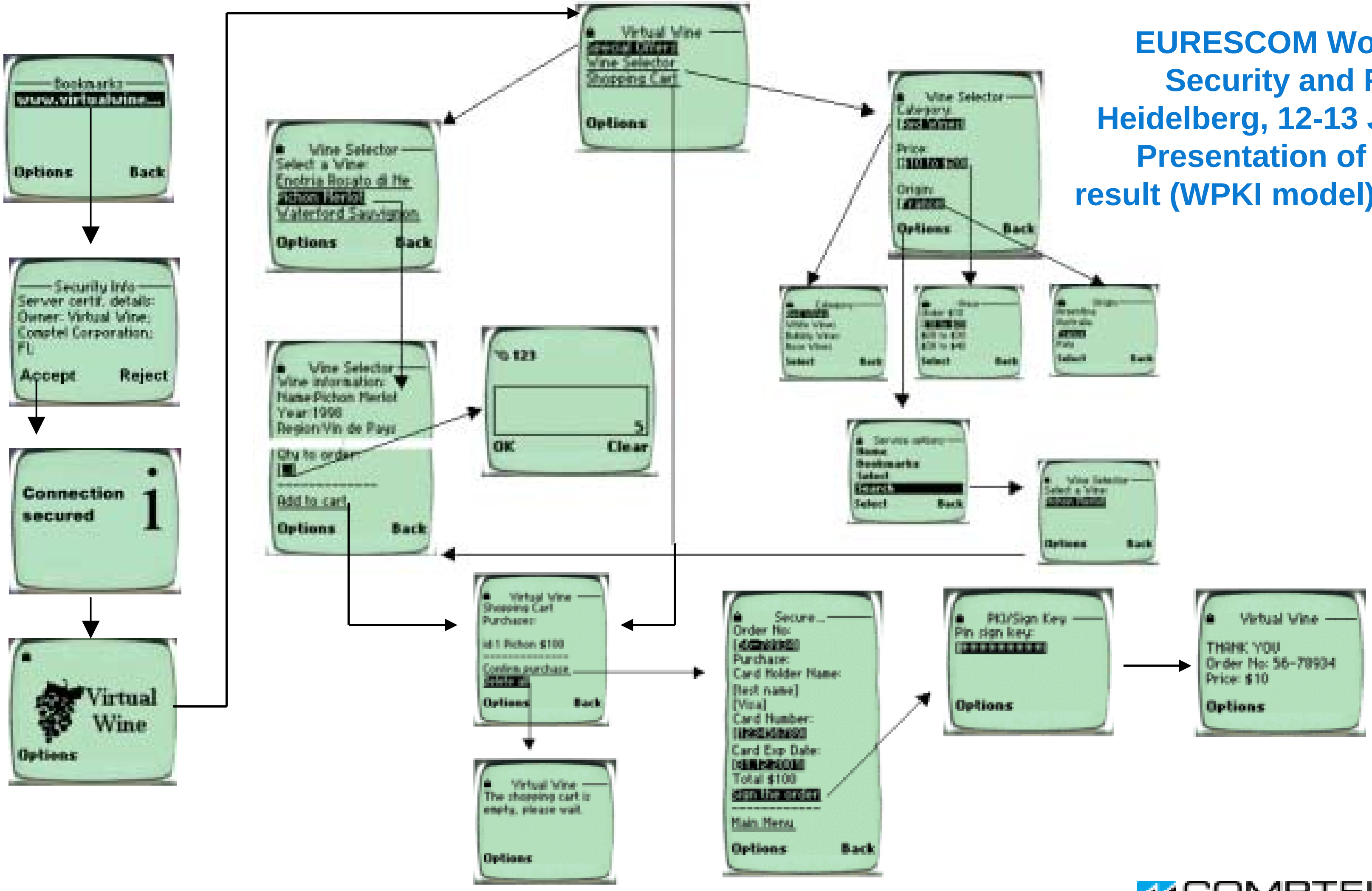

NOKIA
ID: 365121
Password:
* * * *
Sign
365121/****
Registration Authority, e.g. a bank WAP Service
PCP ✓
PCI ✓
Directory Service
Certificate Authority Service

© Comptel Corporation 2001

# WPKI: Test/Pilot architecture in context



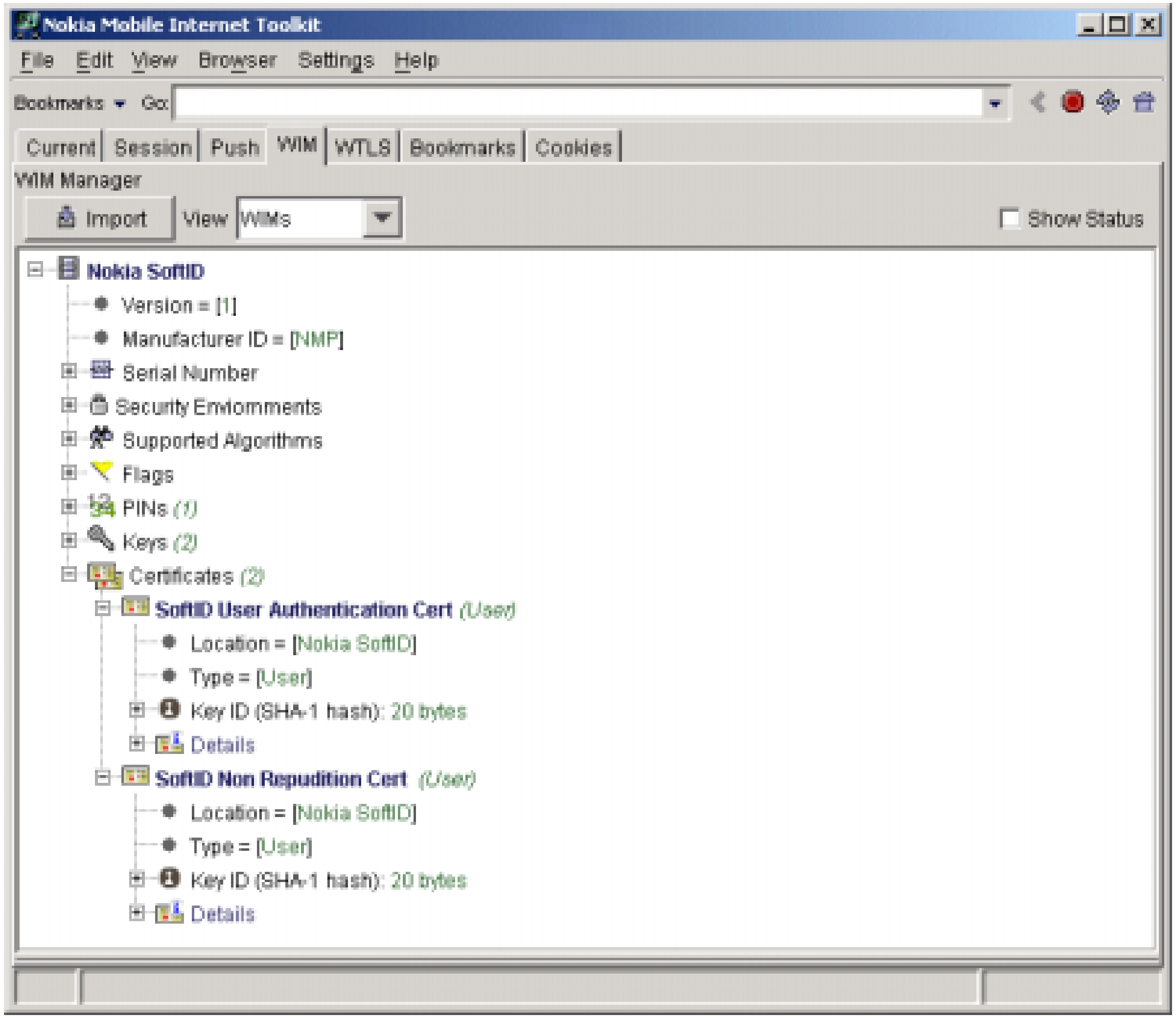
# Describing the implementation: *Virtual* Wine



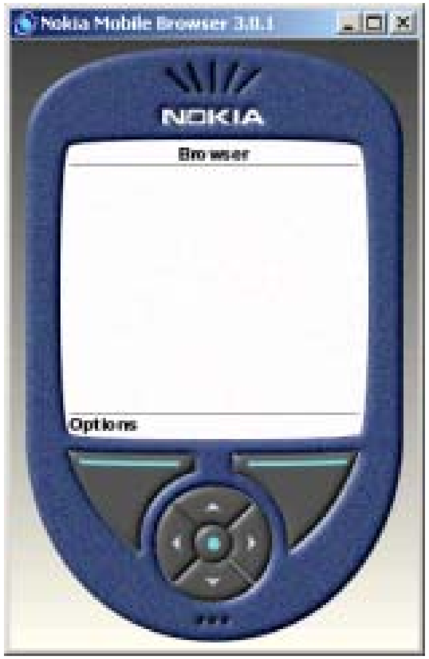
**EURESCOM Workshop Security and Fraud Heidelberg, 12-13 June 2001 Presentation of project result (WPKI model) and demo.**

# WPKI testing tool

### Nokia Mobile Internet Toolkit Version 3.1


Nokia Mobile Internet Toolkit
File Edit View Browser Settings Help
Bookmarks Go:
Current Session Push WIM WTLS Bookmarks Cookies
WIM Manager
Import
View WIMs
□ Show Status

- Nokia SoftID
  - Version = [1]
  - Manufacturer ID = [NMP]
  - Serial Number
  - Security Enviromments
  - Supported Algorithms
  - Flags
  - PINs *(1)*
  - Keys *(2)*
  - Certificates *(2)*
    - SoftID User Authentication Cert *(User)*
      - Location = [Nokia SoftID]
      - Type = [User]
      - Key ID (SHA-1 hash): 20 bytes
      - Details
    - SoftID Non Repudition Cert *(User)*
      - Location = [Nokia SoftID]
      - Type = [User]
      - Key ID (SHA-1 hash): 20 bytes
      - Details



COMPTEL

INTELLIGENT LINK

**Email: massimo.nardone@comptel.com**

Info@comptel.com
www.comptel.com