

The mCommerce and secure mobile payments in WAP

ECCE-11 & SAFECOMP 2002

Joint Panel on Human-Machine System Dependability

Catania, September 11th, 2002

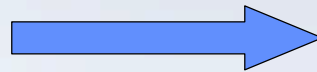
Dino DeLuca, Marcello Salemi

***Nokia, Mobile Software Integration
South Europe hub***

Mobile Commerce

By 2002, one billion consumers globally will have a mobile phone

Mobile Commerce



**buying and paying
using a mobile phone**

digital content (ringing tones, games, cartoons)

physical goods (books, roses, gifts)

tickets (movies, ski lifts), etc. using a mobile terminal

Mobile phones evolve towards **Personal Trusted Devices**

Secure Mobile Payments

Consumer can buy any goods



Consumer and the service must fully trust each other



PKI application needed to secure transactions
(based on RSA or ECC algorithms)

- “mobility” increases **architecture complexity** due to
 - More complex **client authentication**
 - Storing and managing certificates (CA and user certificates) because of PKI

The role of Mobile Devices

- The mobile phone acts as a Personal Trusted Device (PTD)
- PTD contains the security features for accessing information in the network very securely and easily
- Customer certification needed to access the services.
- Solution is based on “Smart Card”, the Wireless Identity Module (WIM)
- Standardized by OMA group (former WAP forum)
 - WAP-260-WIM-20010712-a
 - WAP-217_103-WPKI-20011102-a

Important Features in modern and future mCommerce

- The notion of **Trust** still remains vaguely understood and defined
- **Mobility** and **Locality** are converging to **Global**
- Human Perspective:
 - PDTs are main actors in the mCommerce scenario; Human are associated with PDTs
 - Service-Of-The-Shelf (Related Issues: Integration of different services/devises; Dependencies, Conflicting Services, etc.)
 - Human - PDTs interaction is important to access **remote** services in a **mobile evolving** scenario