

---

*New England ISSA Chapter / HTCIA Joint Meeting*

*January 23, 2001 – Cambridge, MA*

# **Wireless Data**

**An Overview of Technology and Security Issues**

Jim Lilley

Senior Systems Architect, Wireless Data Solutions

Compaq Computer Corporation

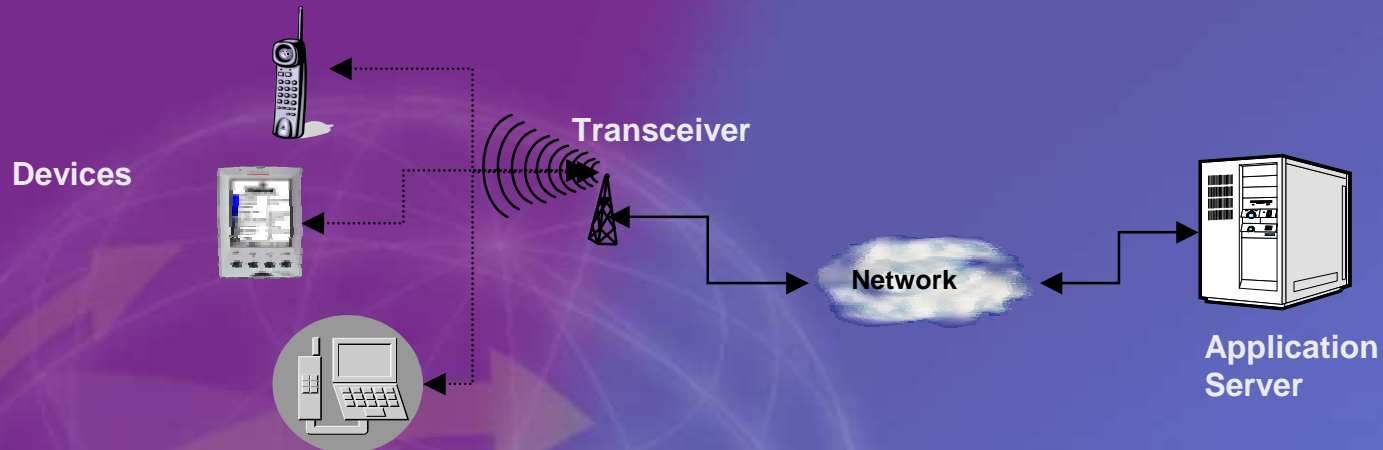
---

# Agenda

---

- ◆ Introduction
- ◆ Technology Overview
- ◆ Cellular Networks
- ◆ Wireless “AN”s
- ◆ Mobile Devices
- ◆ Wireless Applications
- ◆ Security Issues
- ◆ Future Directions

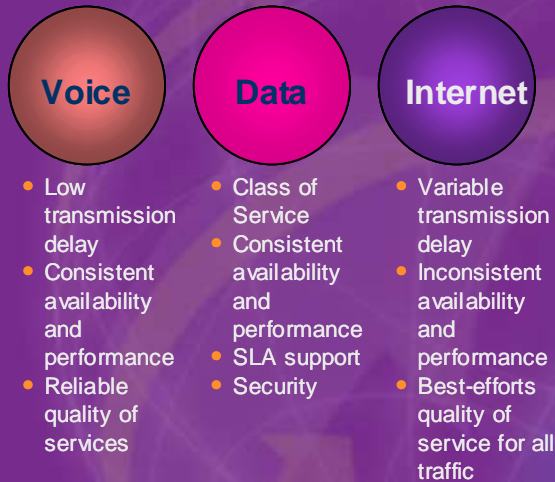
# What is Wireless?



- ◆ What is wireless?
  - Implications
    - Shared transport mechanism (air)
    - No fixed connection points
    - Requires different approach to security
- ◆ Wireless not necessarily same as Mobile
- ◆ Data vs. Voice

# View of the Market

## Separate Networks for Separate Services

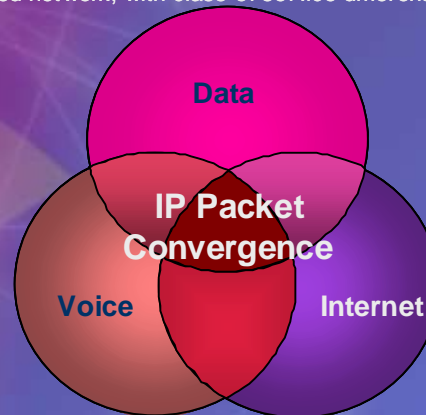


1990

2000

## Next Generation Networks

Next generation networks is one that can combine voice, data and multimedia traffic over a common IP-based network, with class-of-service differentiation.



- Consistent availability and performance
- Class-of-service differentiation
- Reliable quality of service for each defined traffic type
  - Voice
  - Data
  - Internet access
  - Private data
  - Wireless
  - Wired

2003

20---

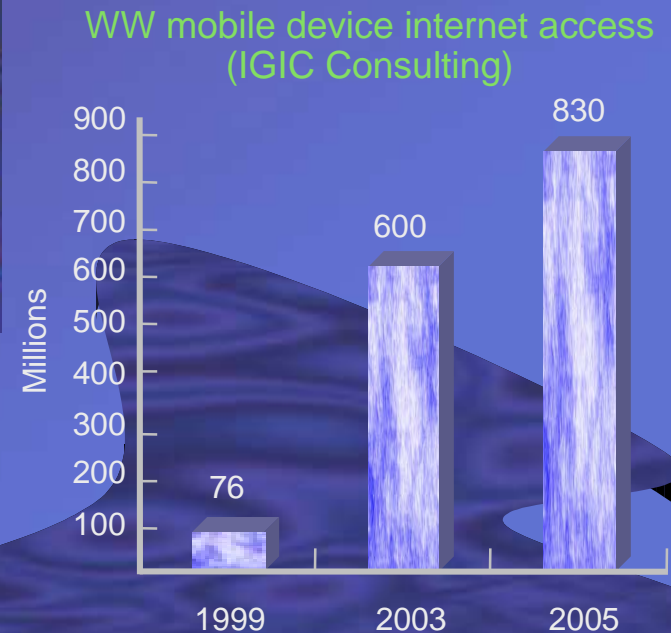
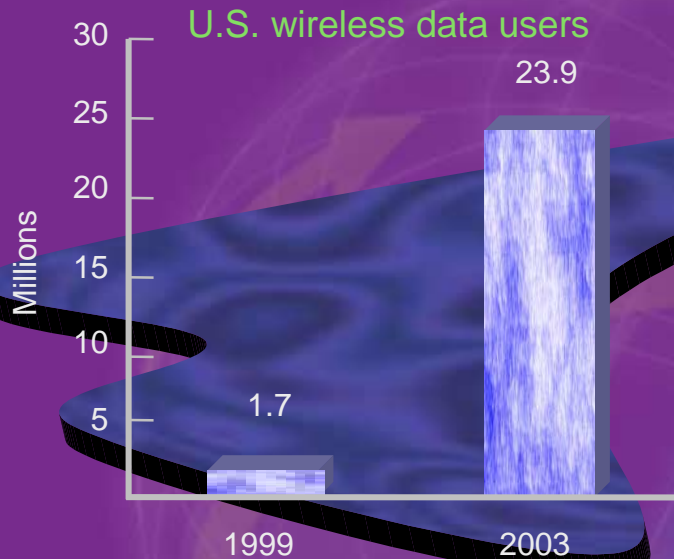


- No separate voice and data networks
- No overlay networks for different services
- All voice, data and multimedia traffic is carried as packets on IP backbone networks, with appropriate quality and class of service for each traffic type
- Services implemented on platforms based on open technology, which are separate from the switching and transport fabric

**Revenue from Worldwide Next-Generation Network Services is expected to grow from \$74 million in year 2000 to \$40 Billion by 2006** *Ovum* <sup>1,2</sup>

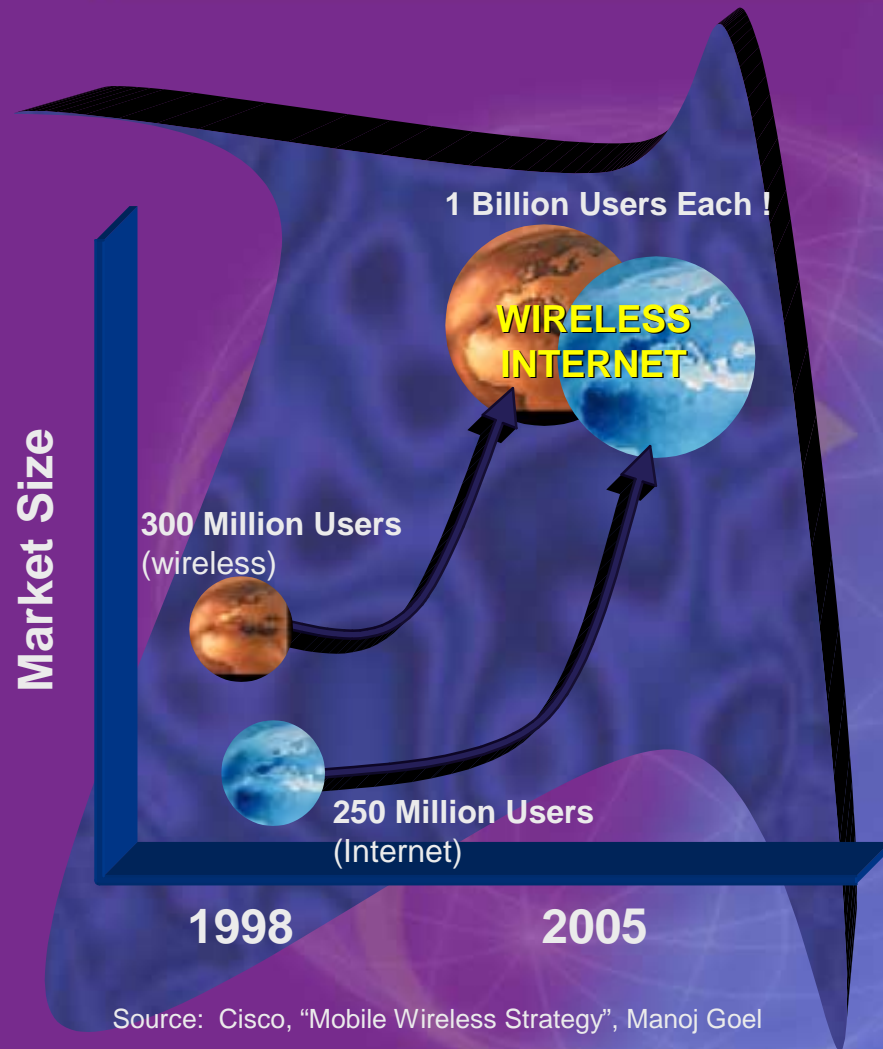
# Trends: Wireless Data Devices

By 2003, more people will access the Internet via Wireless devices than with PCs



By 2005, 830 Million wireless devices will access the internet

# Mega-trend: Wireless Internet




- ◆ 20% World Population is a Mobile User by 2005
- ◆ 60% More M-Commerce Users than E-Commerce Users by 2005
- ◆ CAGR of 226% in Mobile E-Commerce Users between 2000 and 2005
- ◆ The Mobile Services Market is a Regional Play with Europe & Asia in the Lead
- ◆ It took 100 years to create 800 million fixed phone sets, it will take 4 years to double mobile users from 800 to 1600 million users ...

***This is Revolution Not Evolution***

Source: Cisco, "Mobile Wireless Strategy", Manoj Goel

# Technology Overview

- ◆ Wireless characteristics
    - Frequency
    - Analog or Digital modulation
    - Range
    - Mobility (power and size)
- 

# Technology Overview

- ◆ Multiple Access Techniques
  - TDMA
    - Divides channels into time slots
    - Hard ceiling
  - CDMA
    - Code assigned
    - Soft ceiling
    - 4 to 7 times capacity of TDMA
    - Less frequency allocation planning
    - Lower power requirements
- ◆ Circuit vs. Packet data



# Cellular Networks

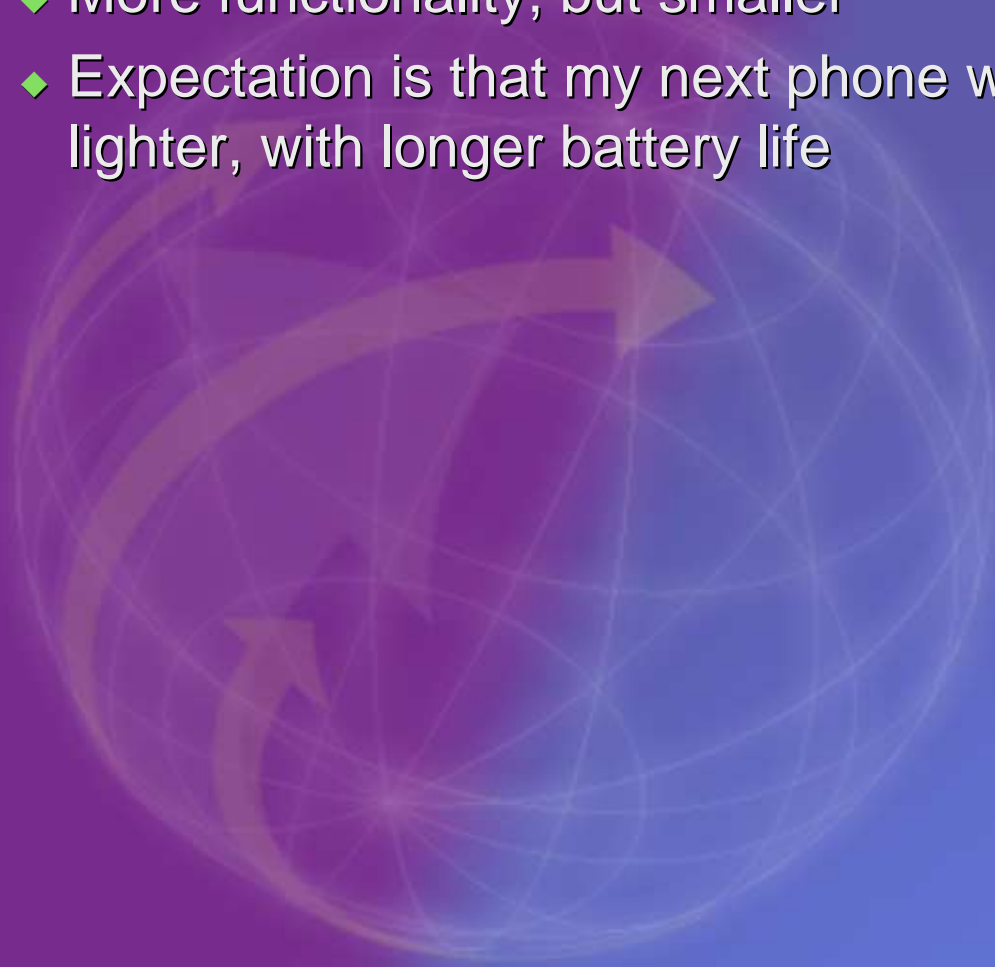


# Wireless “AN”s

- ◆ Wireless LAN and PAN
  - 802.11b
  - Bluetooth
  - HomeRF
  - DECT
  - Infrared
- ◆ Wireless MAN and WAN
  - LMDS and MMDS
  - Broadband to homes, especially rural
  - Current line-of-sight limitations

# Mobile Phone Trends...

- ◆ More functionality, but smaller
- ◆ Expectation is that my next phone will be smaller and lighter, with longer battery life



# .....Then came Messaging & WAP

- ◆ Messaging and Wireless internet access have some demands
  - A screen (color for multimedia)
  - An effective input method
    - iTAP, T9 type technologies help (a little)
    - Voice technology – *emerging*
- ◆ So what are we describing here
  - Is it a handset, or is it a computer?
  - Or is it more than one device?

# Wireless devices – what are they?

- ◆ Mobile phones



- ◆ Personal Digital Assistants (PDAs)



- ◆ Smart Pagers



Motorola Pagerwriter 2000x



# Device Trade Offs

- ◆ Screen size
  - Better power efficiency, good for messaging
- ◆ Black and white
  - Closer to Internet experience, better brand association
  - Multimedia
- ◆ Other needs?



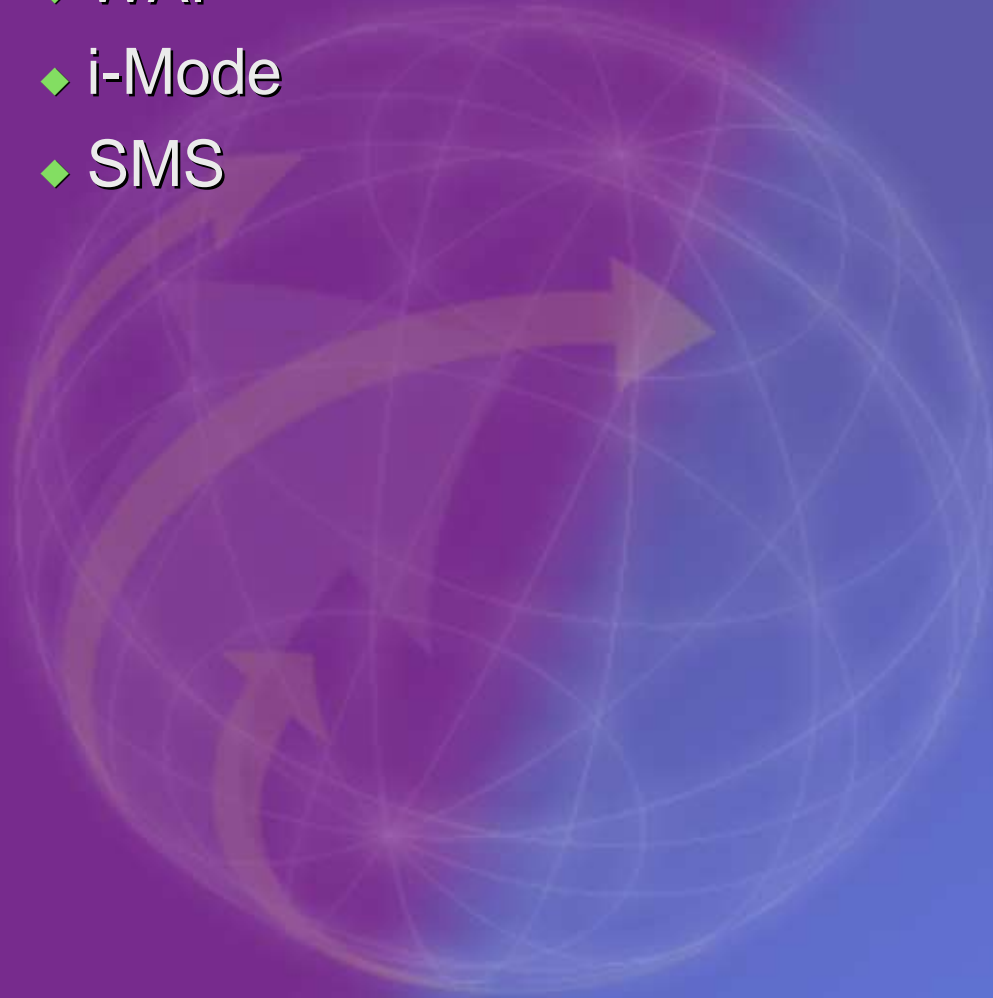
# Flexibility is Key

- ◆ Multiple devices, to suit multiple lifestyle and business needs
- ◆ Maximize effective real estate of increasingly smaller handsets
  - Extend through “seamless” connections to other devices
  - Ir Modems
  - Bluetooth
  - 802.11b
- ◆ Dual or multi device strategy can deliver better value to the consumer in managing his/her voice communications device



# Application Methods

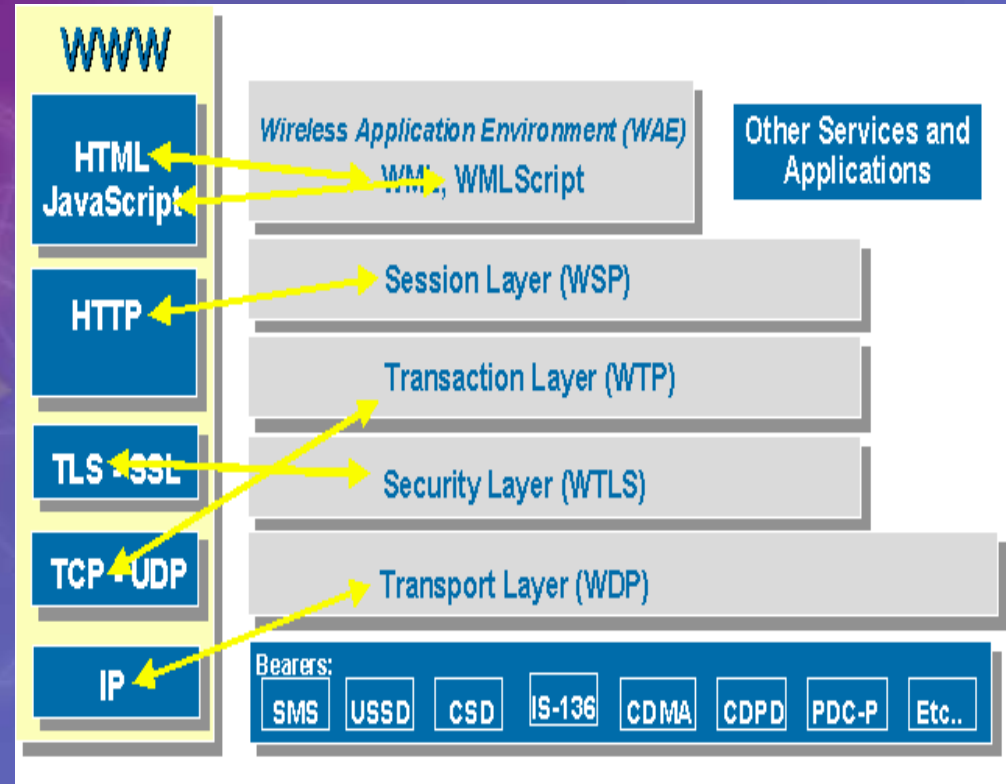
- ◆ WAP
- ◆ i-Mode
- ◆ SMS





# Wireless Application Protocol

- ◆ Similar but incompatible with wired Internet protocols
- ◆ Presentation Layer
  - WML or HDML
- ◆ Security Layer
  - WTLS
- ◆ Most WAP gateways support standard security mechanisms
  - RSA
  - Diffie-Hellman
  - X.509 Certificates (server side)



# i-Mode

- ◆ Launched by NTT DoCoMo in 2/99
  - 40,000 subscribers per day
  - Approaching 17M total subscribers
- ◆ Rapidly expanding
  - N. America (AOL, AT&T Wireless)
  - Europe (KPN Mobile, Telecom Italia)
  - Asia (Taiwan, Hong Kong)
- ◆ cHTML
- ◆ Payment model based on data transferred
- ◆ Just announced
  - SSL
  - Java



# Short Message Service

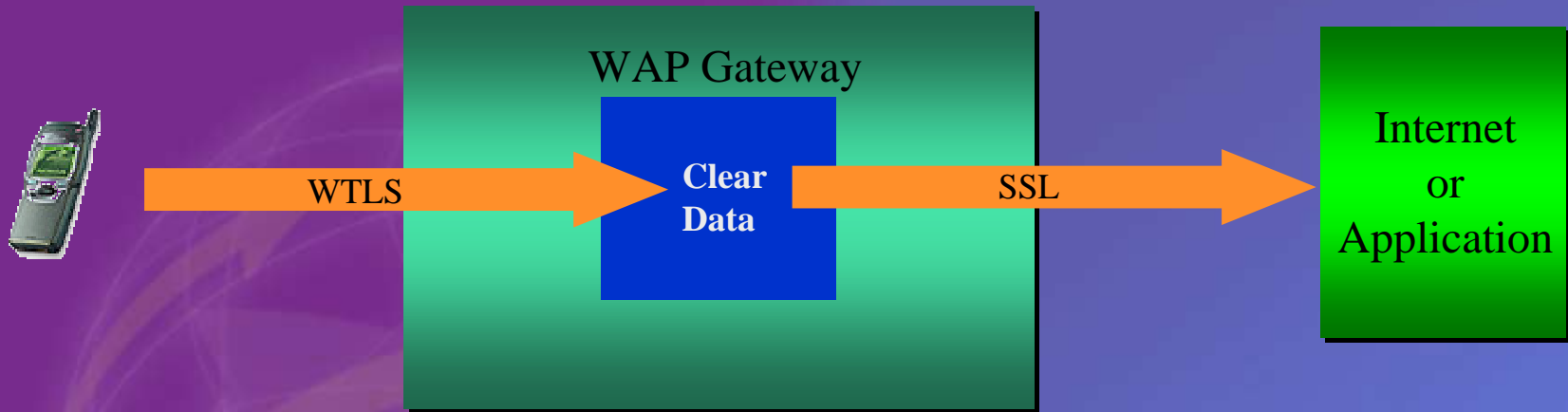
- ◆ Short text messages (160 characters)
- ◆ Typically associated with, but not limited to, GSM networks
- ◆ Popular in Europe, especially younger users
- ◆ Universal mechanism that lends itself to delivery of other information
- ◆ Advantages
  - Push-oriented
  - More SMS phones
- ◆ Potential other uses

# Where are these being used?

- ◆ Europe
  - GSM
  - SMS
  - Prepay
- ◆ Japan
  - CDMA
  - 17M i-Mode users, 5M WAP
- ◆ North America
  - CDMA/TDMA/GSM – too many
  - PDA's more popular
  - Wants WWW-like experience
- ◆ South America
  - TDMA
  - Prepay

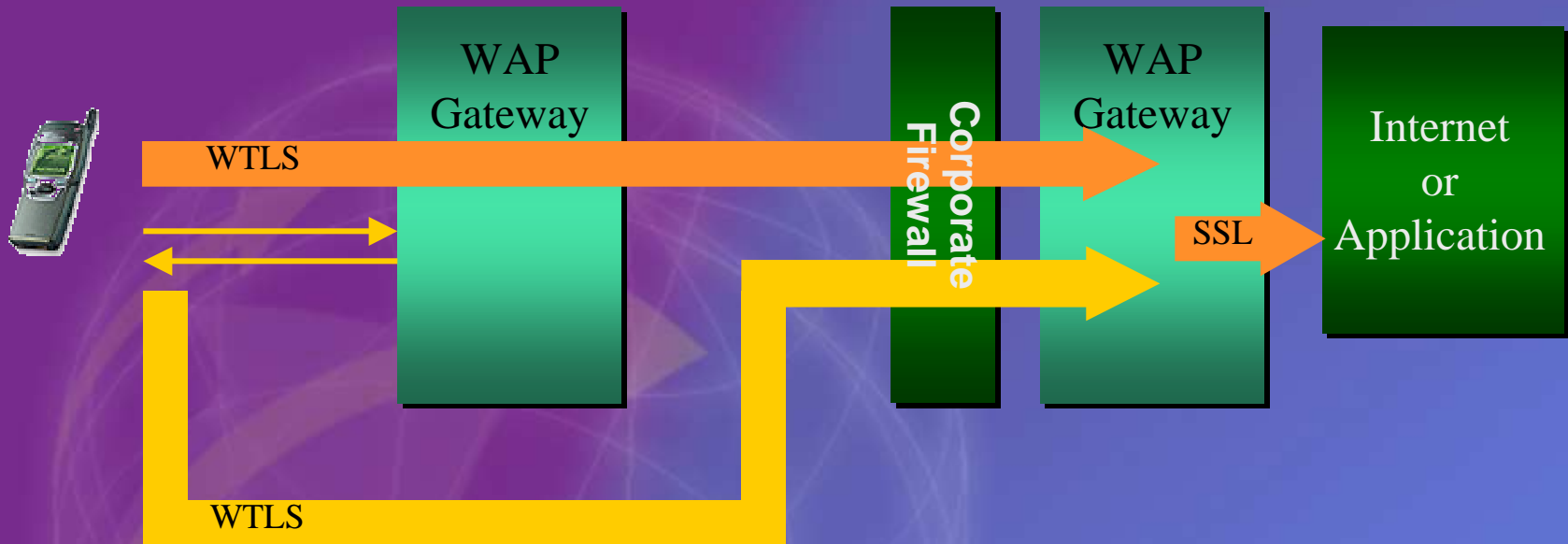


# WAP Gap



- ◆ Conversion from WTLS to SSL at the carrier
- ◆ Data momentarily in the clear

# WAP Forum Proposed Approach



## ◆ Drawbacks

- Data in clear behind behind firewall
- Requires gateway at the enterprise
- How will operator provide services

# How do I know you're you?

| WTLS Class           | Server Authentication | Client Authentication |
|----------------------|-----------------------|-----------------------|
| 1 (now)              | No                    | No                    |
| 2 (now, but limited) | Yes                   | No                    |
| 3 (2002)             | Yes                   | Yes                   |

- ◆ Client-side certificates not available until WAP 1.3
  - How to get the certificate on the device
- ◆ Smart cards
  - SIM
  - WIM
  - SWIM
- ◆ Dual slot phones
  - Prevents authentication duping digital signature

# Encryption Methods

## ◆ Factors

- Processing ability
- Battery life

## ◆ Standards

- RSA
- MultiPrime
- ECC
- Diffie-Hellman
- A3, A5, A8



# Wireless PKI

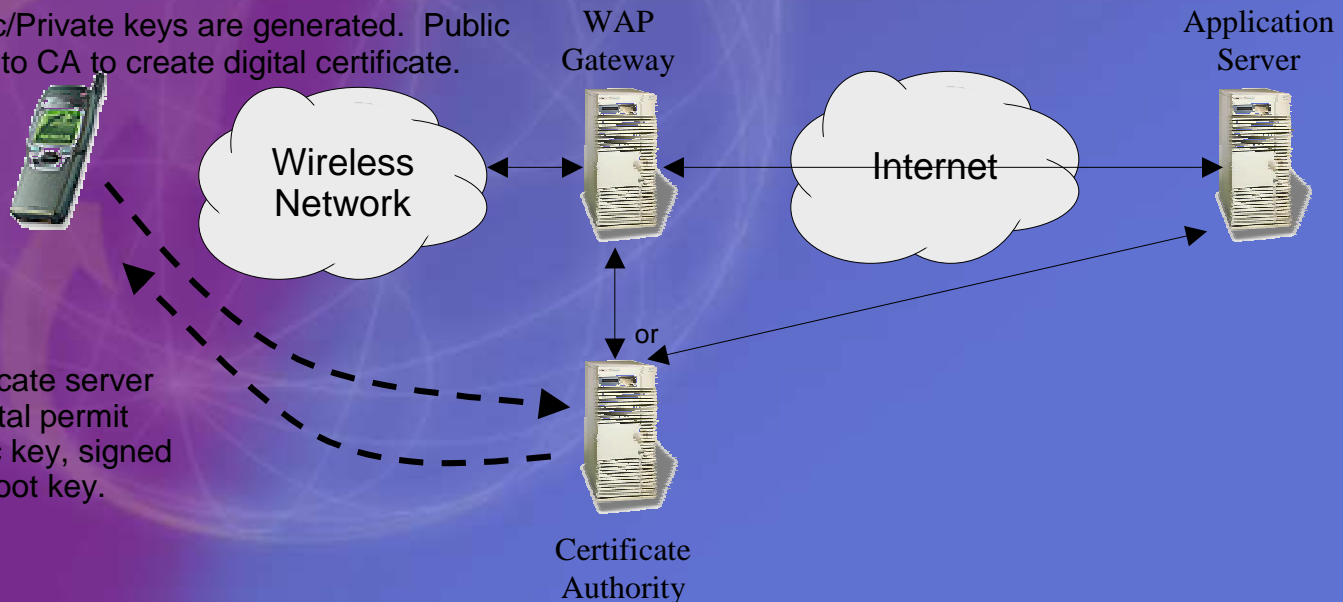
## ◆ Wireless PKI

- WAP 1.3
- Needs to support multiple devices and networks
- Small certificates
- Single pass validation
- Needed for Digital Signatures
  - Need standardized legislation between states/countries

## Registration

**A** – Public/Private keys are generated. Public key is sent to CA to create digital certificate.

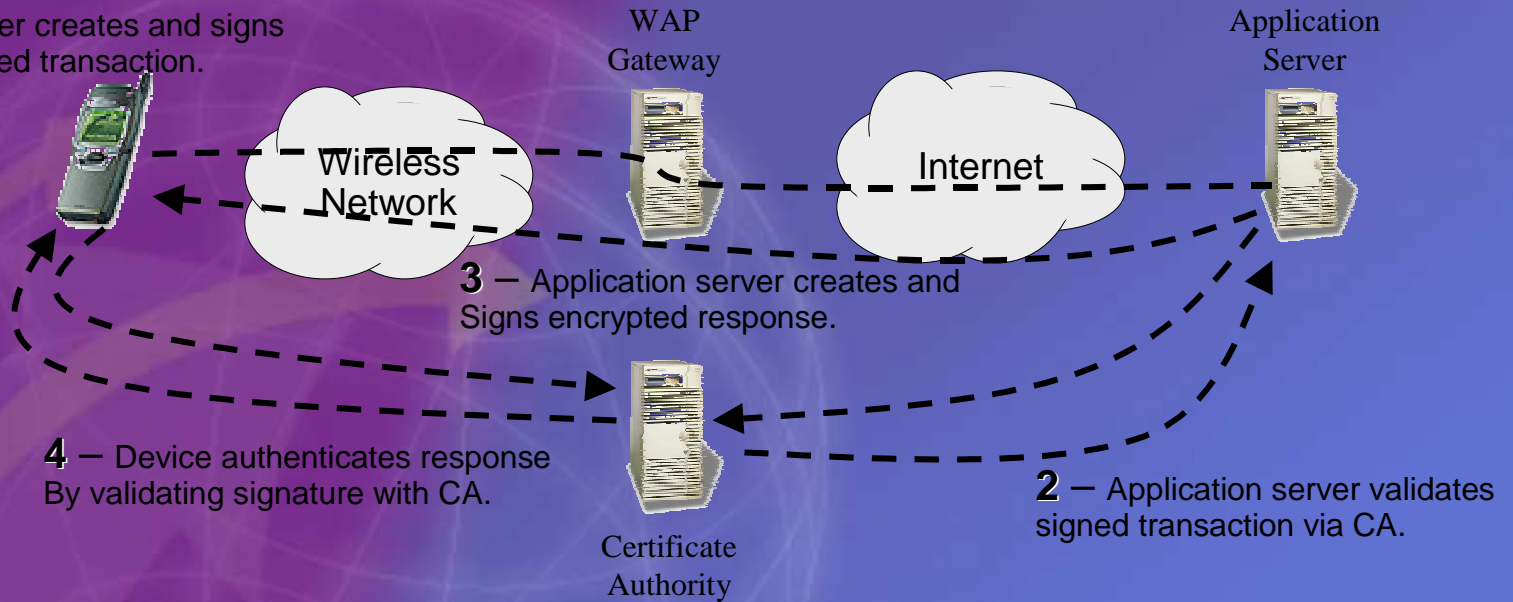
**B** – Certificate server creates digital permit using public key, signed by the CA root key.



# WPKI Transaction

## Transaction

1 – User creates and signs Encrypted transaction.



# Wireless Virtual Private Networks

- ◆ Wireless device access to corporate intranets
- ◆ Wired VPNs typically use IPSec (triple DES)
  - Extremely processor intensive
- ◆ Some solutions becoming available
  - Certicom
    - Supports IPSec to provide secure transmission to devices
  - 3Com
    - Tunneling approach for CDMA networks

# Other Topics of Interest

- ◆ Biometrics
  - Authentication through Voice, Fingerprint, Retina, others
  - Voice holds most promise in near future
  - Potentially can enable card present transactions
- ◆ Location services
  - Very powerful
  - Absolutely crucial that user controls this information
- ◆ Fraud detection
  - Usually involves identity fraud
  - Many techniques already in use today
- ◆ Viruses
  - Not much of an issue yet – but will be major problem
    - Executable code on devices
    - Virus enabling functions in WAP 1.2 (Push, WTA)
    - “Always on” networks
  - Must protect the network and gateways as well as devices

# Consumer Trust

---

- ◆ Sufficient security required – not bulletproof
  - Element of trust

- ◆ From Cahoot Internet Bank

“We will take all reasonable steps to ensure that unauthorised access to the secure zone does not occur. Provided you have followed the requirements set out in this condition (3d), we will accept liability for any loss you suffer as a result of any unauthorised access to the secure zone.”

- ◆ From Direct Debit

“If an error is made by us or your bank, you are entitled to a full refund”

- ◆ From NatWest Credit Card

“Lost or Stolen Card?”

Phone straightaway (0113) 277 8899 – 24 hours

Your maximum liability will be £25, unless the card is misused with your consent or you have acted with gross negligence.”

# Consumer Mistrust

- ◆ From unnamed European network operator

“What to do if your SIM Card is lost, stolen or damaged

12.2 You must inform us immediately if the SIM Card supplied to you is lost, stolen or damaged. You will remain liable for all Charges incurred until you do so. We will send you a replacement SIM Card as soon as reasonably practicable, but we reserve the right to charge you for doing so.”



# Future Directions

---

- ◆ Standards consolidation needed
  - WAP Forum
  - MeT
  - PKI Forum
  - Radicchio
  - SIM Alliance
  - IETF
  - Global Mobile Commerce Forum
  - Mobey Forum
  - Mobile Electronic Signature Consortium
  - ITU
- ◆ No “killer app” - Fragmented market
- ◆ Dynamic content
- ◆ Multimedia
  - Video, music
- ◆ IPv6
  - Virtually unlimited IP addresses
  - Better suited for mobile environment (Mobile IP, VoIP)
  - Will play major role in 3G, but still being defined

# Thank you



[Jim.Lilley@compaq.com](mailto:Jim.Lilley@compaq.com)