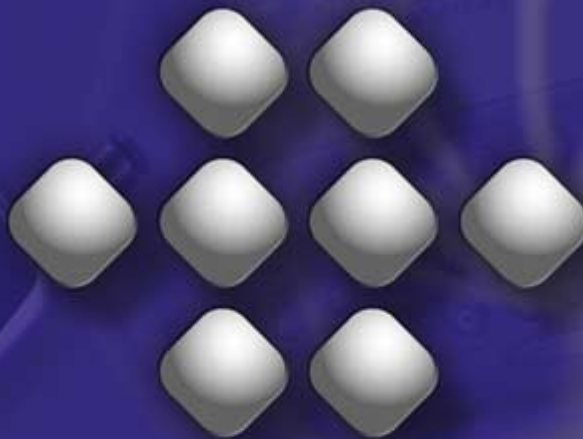


**certicom**  
encryption



**certicom**

**AB mCommerce Symposium**

**March 5, 2001**

**Jim Cowing**

**Senior Director – Professional Services**

# Certicom Profile

- ◆ “Enabling the New Wireless Economy”
- ◆ Industry leading Products and Services for Wireless Internet Security
- ◆ Publicly Traded NASDAQ: “CERT” and TSE: “CIC”
- ◆ 400 employees in Hayward, CA and Toronto, Canada
- ◆ Commercialized “Elliptic Curve Cryptography” or “ECC”
- ◆ Services – provide Security-focused PKI and Wireless Security Consulting to the Financial Services Industry

# Industry Leading Customers



certicom  
encryption

# “Certicom Inside” leading edge wireless products like the Palm VII



  
certicom™

# *The Security Problem*

Transaction Security

**Security**

On-line Fraud

Data Security

**Privacy**

Unauthorized data sharing

Improper use of data

Identity Theft

Fraudulent Transactions = Lost \$ \$ \$

# *The Security Dilemma*



# Privacy Concerns

- ◆ The systematic capture of everyday events
  - credit card purchases, cellphone calls
- ◆ The misuse of private information
  - confidentiality vs. “business need to know”
- ◆ “Runaway” marketing
  - junk mail/e-mail, dinner-time telemarketing
- ◆ Personal information as a commodity
  - selling info databases, “profiling”

# Privacy Concerns

- ◆ 7 Privacy laws proposed on Capitol Hill
- ◆ Although this problem is being caused by, or at least exacerbated by technology
- ◆ Privacy is not a **technological** issue --- it is a **societal** issue
- ◆ We have technology to achieve anonymity or full identity
- ◆ Rules are not yet clearly established.

# Information Security Threats

## Fraud

### ◆ Problem

- Impersonation or identity theft
- Data alteration
- Repudiation

### ◆ Impact

- Financial loss
- Merchants absorb most of the losses
- Reputation Risk to Banks
- Slows adoption (possibly stagnates) of m-Commerce

# The Security Objective



Wireless  
Customer

Web  
Merchant



PKI

101110100010101  
010101010100110



101110100010101  
010101010100110

Digital Signatures

Digital Certificates

Security Protocols

Encryption

Identity = Trust = Low Risk

# *Digital Signature Law (E-Sign)*

- ◆ Digital signatures allowed in e-Commerce
- ◆ Carry same legal weight as wet signatures
- ◆ Effective Oct. 1, 2000
- ◆ Early Applications: Loans, Real Estate, Insurance, Health Care

# Challenges for m-Commerce

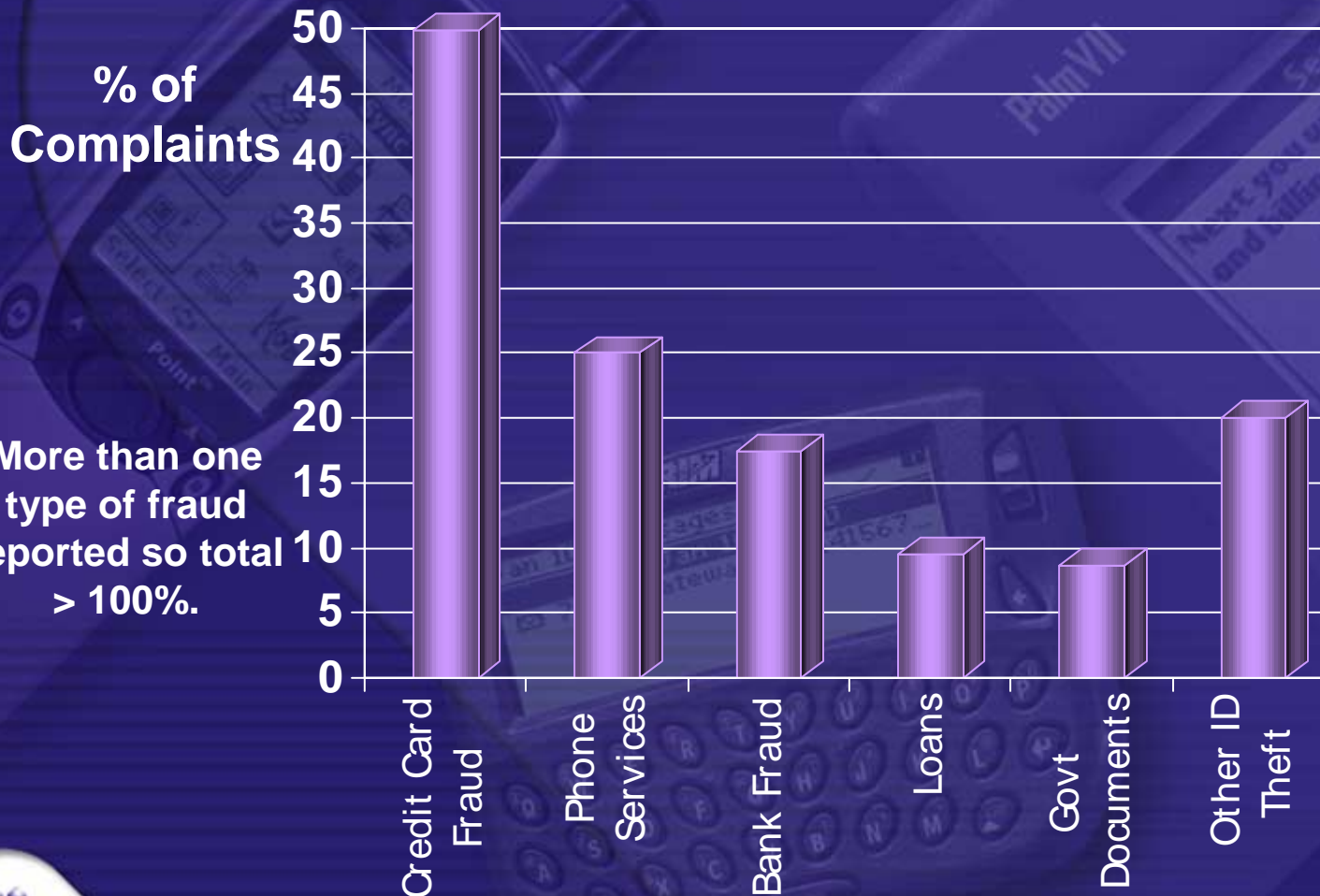
- ◆ Cryptographic functions are computationally intensive – need lighter and faster.
  - Traditional crypto needs hardware accelerator
- ◆ Wireless devices are resource constrained
  - low cost
  - small processor, memory
  - long battery life
  - efficient use of wireless bandwidth
- ◆ Certicom's Solution ... **Elliptic Curve Cryptography**

# Challenges for m-Commerce

- ◆ End-to-end Security Solutions Required
- ◆ Telecoms do not understand security yet !
- ◆ User Experience needs to be enhanced
  - Voice and other Creative Solutions
- ◆ Wireless Standards – WAP, I-mode, GSM, TDMA, etc.
- ◆ Better understanding of Security and more Security Solutions – eg. Openwave server software
- ◆ Solution ...

# Identity Theft

## ◆ Leads List of U.S. Fraud Complaints



Source: Federal Trade Commission Identity Theft Data Clearinghouse

# *E-Commerce Security*

- ◆ Non-Repudiation (solves repudiation)
- ◆ Integrity (solves alteration)
- ◆ Authenticity (solves impersonation)

---

- ◆ Privacy (solves eavesdropping)

# The Security Objective = Confidentiality



Wireless  
Customer

Web  
Merchant



101110100010101  
010101010100110



01110100010101  
10101010100110



Security Protocols  
Encryption

Privacy of confidential data

# The Security Objective = Authentication



Wireless  
Customer

Web  
Merchant



PKI

101110100010101  
010101010100110



01110100010101  
010101010100110

Digital Signatures

Digital Certificates

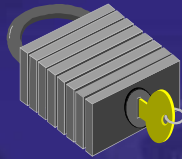
Security Protocols

Encryption

# The Internet - "Open" by Design

## Eavesdropping

- ◆ Intercepting and viewing confidential or sensitive information



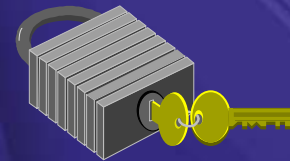
Secret Key Cryptography



Privacy

## Impersonating

- ◆ Using another's identity and doing e-business in their name



Public Key Cryptography

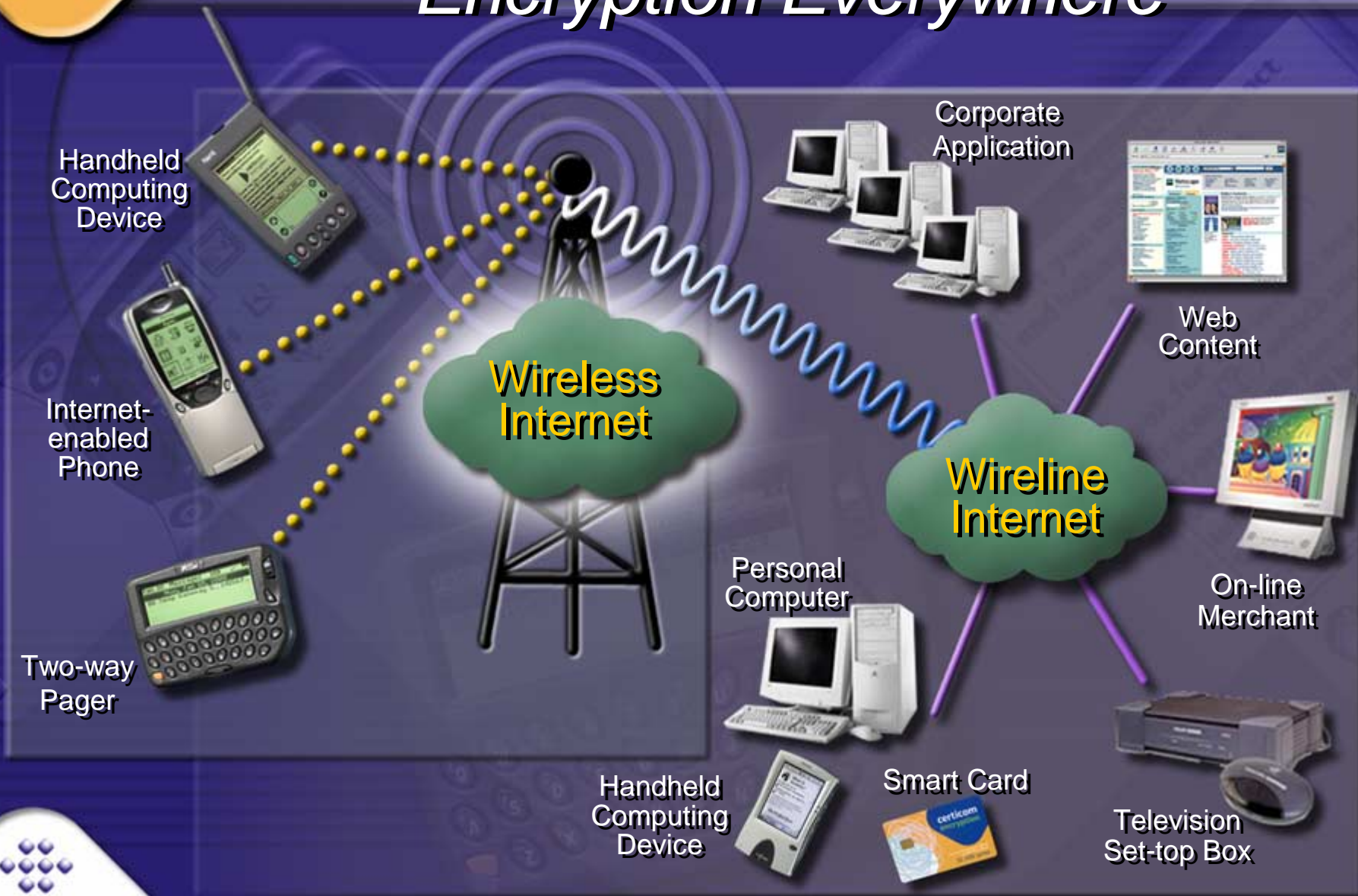


Authenticity

# *Electronic Signature (E-Sign) Law*

- ◆ Electronic “signatures” solves the Non-Repudiation problem.
- ◆ Carry same legal weight as physical signatures.
- ◆ Loans, Real Estate, Insurance, Internet Commerce

# Our Security Goal – “Encryption Everywhere”



# *ECC - Elliptic Curve Cryptography*

ECC Key Size (Bits)	Traditional Key Size (Bits)	Key Size Ratio
163	1,024	1 : 6
283	3,072	1 : 11
409	7,680	1 : 19
571	15,360	1 : 27

*Small, Efficient, Low Power*

# Cryptography's Future

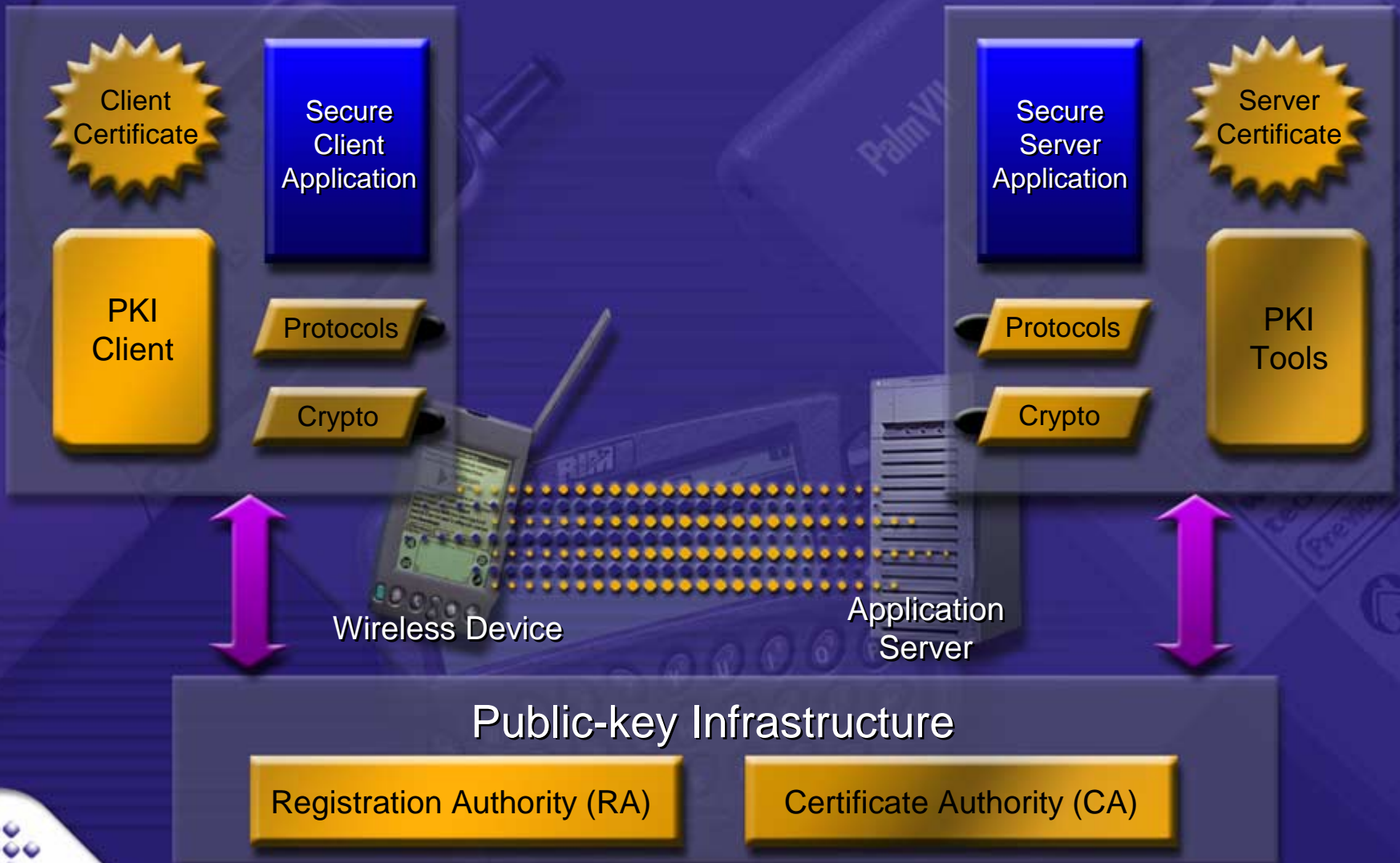
Traditional Key Size (Bits)	ECC Key Size (Bits)	Symmetric Key (Bits)	
1,024	163	80	<b>DES</b>
3,072	283	128	
7,680	409	192	<b>AES</b>
15,360	571	256	

# Certicom Technology

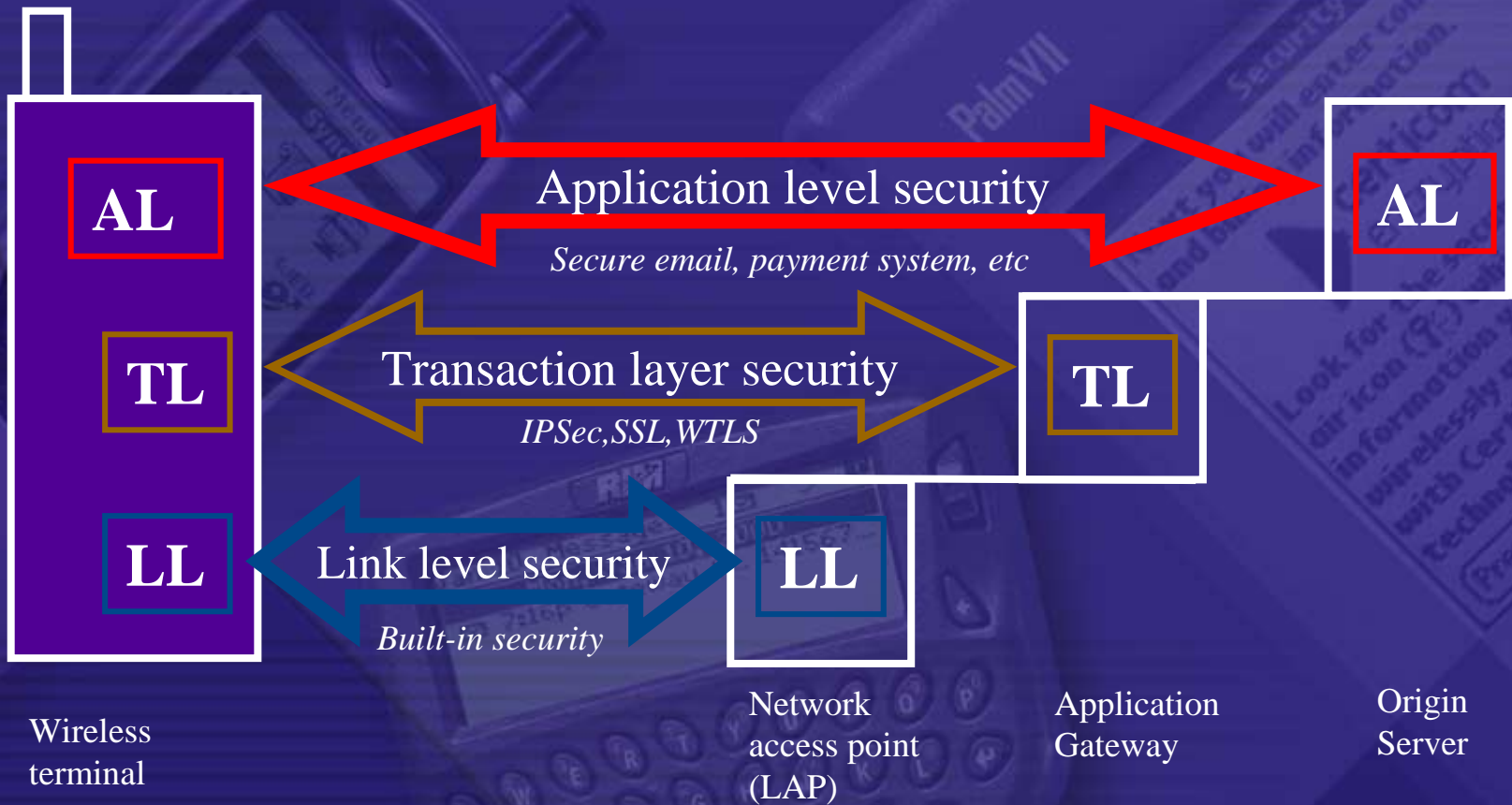
- ◆ Digitally Signed Transaction on a Palm VII Using Certicom ECC Technology



# Public Key Infrastructure



# Security levels

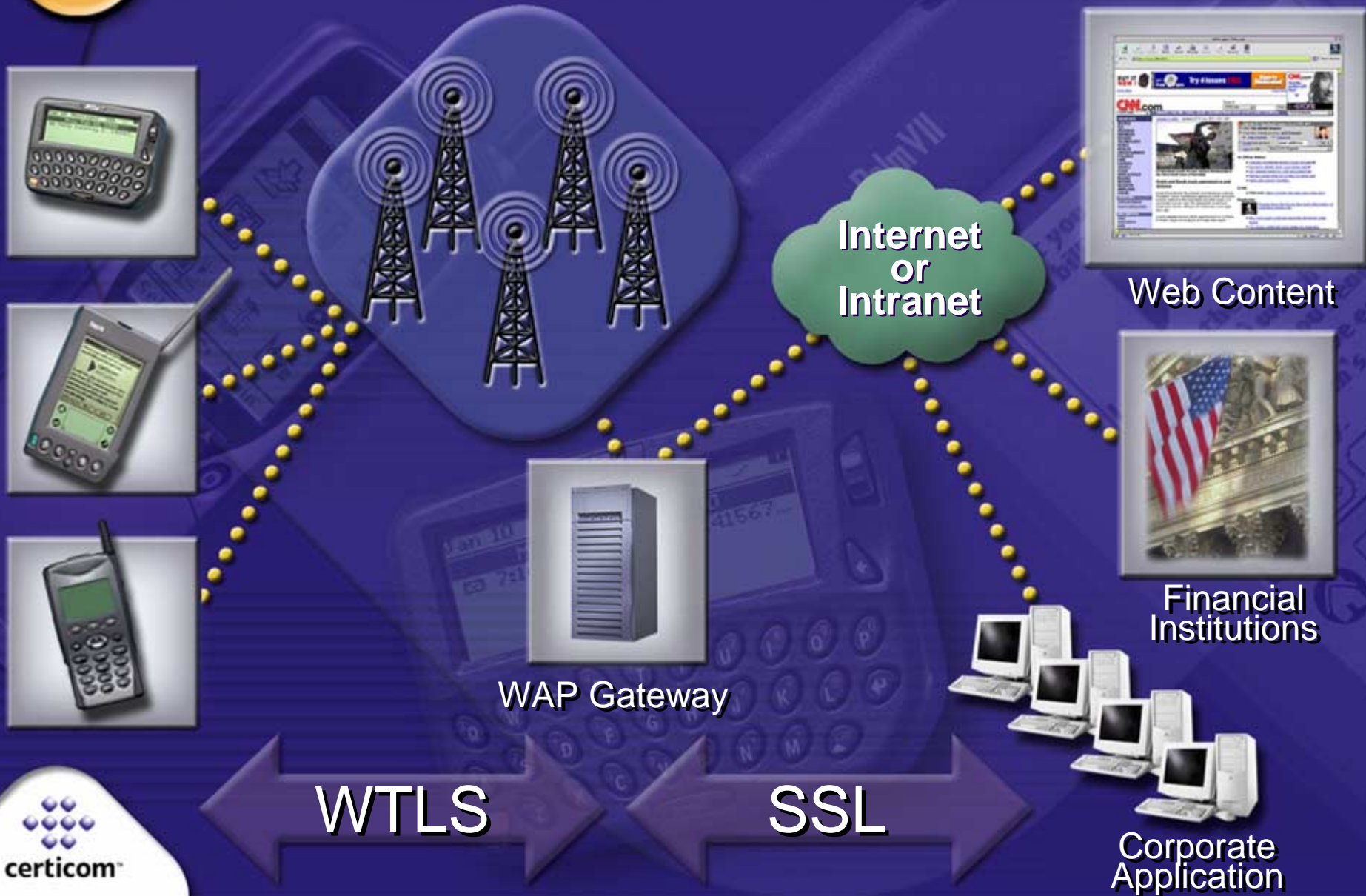


# Europe / Asia



- ◆ Standards Based Market - GSM with SMS
- ◆ m-Commerce Driven by Financial Service Applications
- ◆ Slow Transition to WAP

# WAP Architecture



# i-Mode Architecture



Conversion  
to TCP/IP



Specialized i-Mode Content

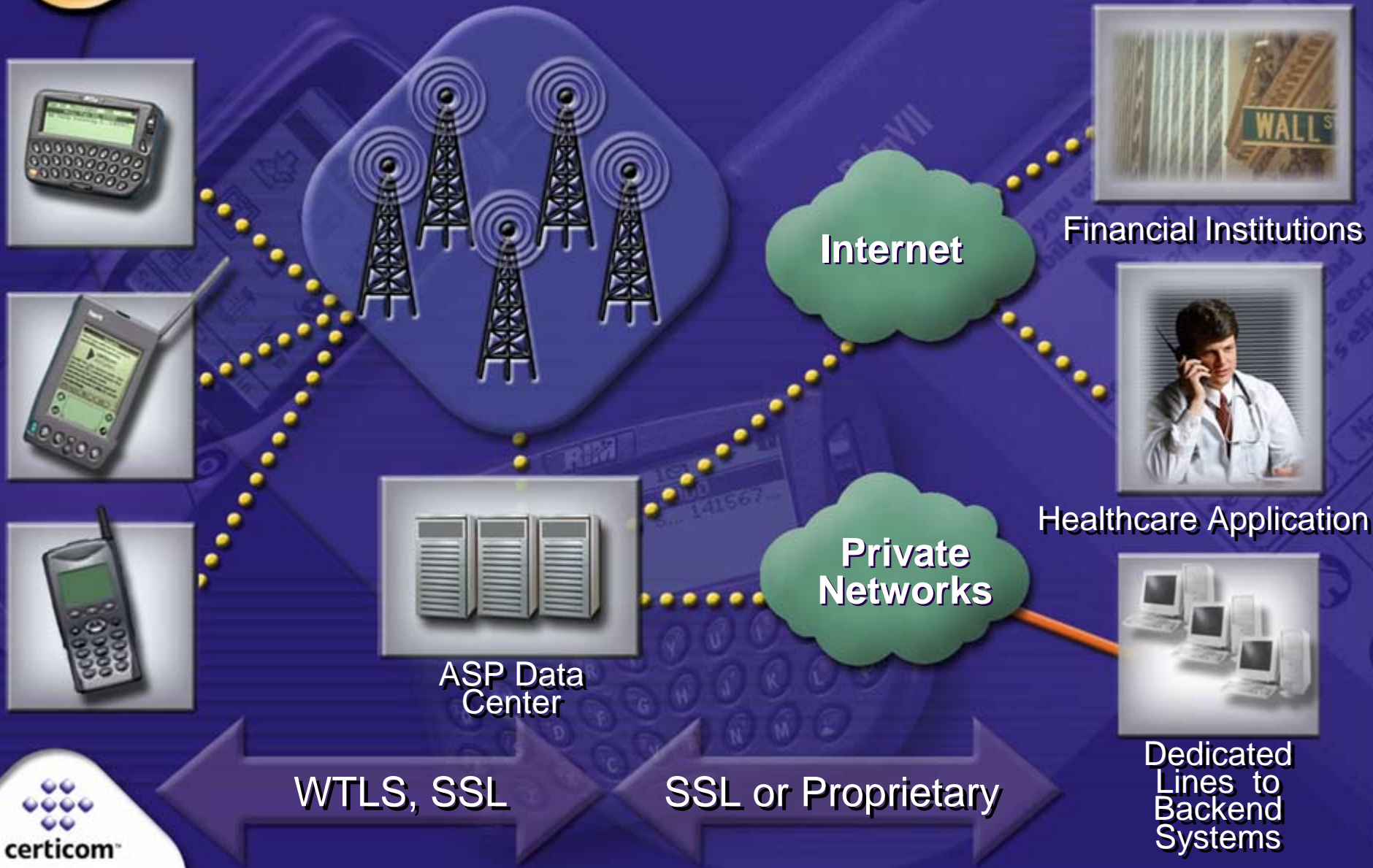
SSL

# North America

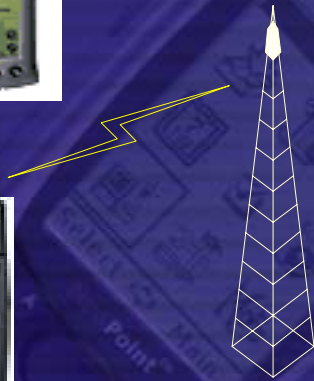


- ◆ Internet Far Exceeds Mobile Penetration
- ◆ Greater Emphasis on High Value m-Commerce Transactions
- ◆ Greater Diversity of Devices, Networks and Application Developers

# ASP Architecture



# Case Study: 724 Solutions



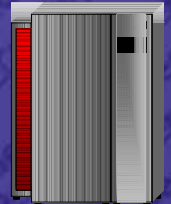
Wireless Gateway



724's Financial Services Platform



Application Server  
Financial Institution



Standard Browser

- Certicom Security:**
- WTLS Plus™ Client
  - Trustpoint PKI Client

Content Translation  
Transaction Processing

- Certicom Security:**
- WTLS Plus™ Gateway
  - Trustpoint™ PKI Portal

Application Host  
Content Storage

- Certicom Security:**
- Trustpoint™ CA or MobileTrust™ CA Service or (Legacy PKI/CA)

# B2C Financial Services

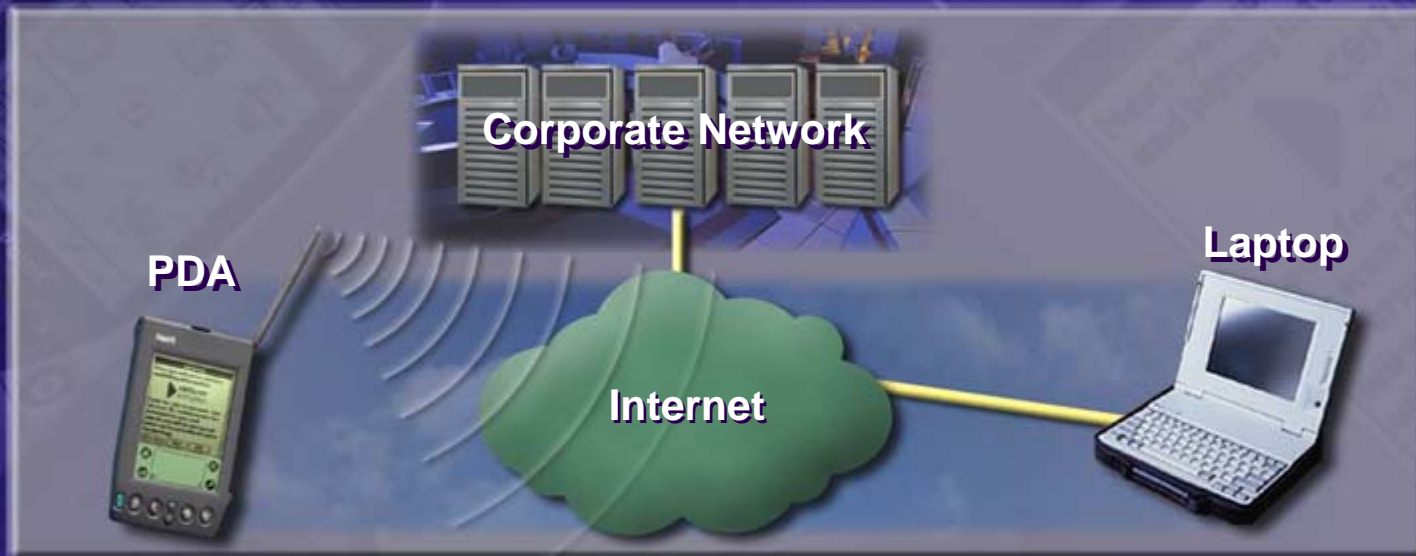
Banking and Stock Trading  
Anytime, Anywhere!



- ◆ Aether Systems & Schwab
- ◆ Cingular Interactive (BellSouth WD) & Fidelity
- ◆ 724 Solutions & Wells Fargo

# Network Security

90% of Remote Workers Will Connect to the Office through a VPN



- ◆ Mobile VPN: Cisco, Check Point, Nortel, others
- ◆ Beta Test: FedEx, Proctor & Gamble ... 64 total

# *mCommerce Growth Requires Security*

- ◆ Global mCommerce predicted at \$200 Billion by 2004 (Gartner Group)
- ◆ Individuals' electronic identities need to be trusted in eBusiness transactions
- ◆ Password protection still dominant in 2001
  - 4% use certificates, PKI, or SmartCards for online authentication
- ◆ By 2005, stronger authentication will be built into applications and devices
  - Tokens, SmartCards w/Certs, PKI, Location based, Two factor authentication, Mobile VPNs

# *Multiple Identities/Multiple Devices*

- ◆ Consumers want choice
  - Desktop, PDA, pager, phone
  - Multiple platforms with larger variety of applications
- ◆ Merchants/service providers want to give consumers that choice
- ◆ Each device has unique needs for identity for that consumer
  - A single consumer will likely have *multiple identities* for a single account relationship
- ◆ This increases total cost of the secure solution for the merchant/service provider

# "Multiple Identity" Problem



Corporate Information



Internet Content or Service



PIN or BIOMETRICS



B2B Supply Chain

## Goal

- ◆ Anytime, Anywhere
- ◆ Any Device

## Challenge

- ◆ Multiple Identities (Private Keys & Digital Certificates)

# “Nomadic Identity”

## Value Proposition

- ◆ Card Carries Identity
- ◆ Superior Convenience
- ◆ Lower Cost

... *Stay Tuned!*



# Summary

- ◆ Myth: Wireless is “less secure” than wired
- ◆ Fact: Perception is reality
- ◆ Fact: We have to work harder
- ◆ Myth: Security = Privacy
- ◆ Fact: Application level security reduces e-Fraud
- ◆ Fact: Just starting
- ◆ Myth: People want security
- ◆ Fact: People want to be secure ... it’s an “entitlement”
- ◆ Fact: Need built-in, transparent implementations