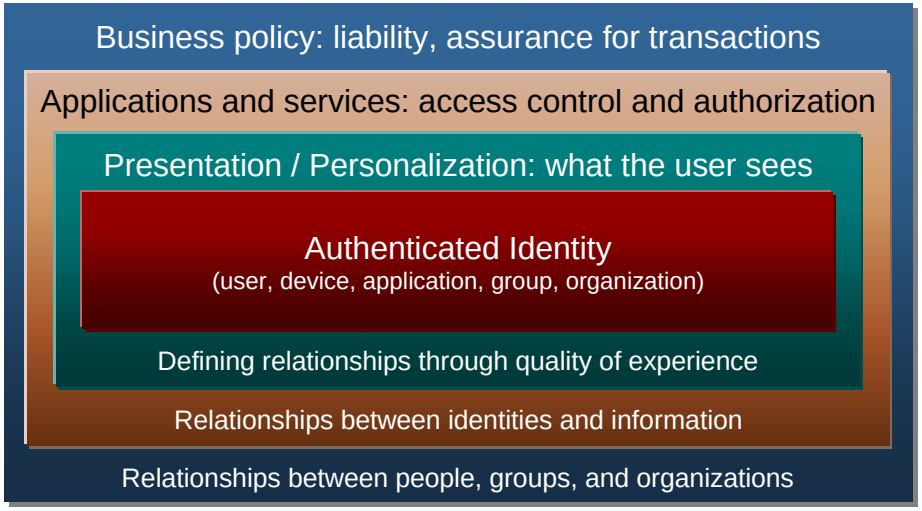
Infrastructure for Trusted Computing

Kevin LeBlanc
Product Marketing Manager, RSA Keon and Smart Badging Solutions

Why is Authentication Important?

- Authentication is the essential foundation for trusted computing
  - Establishes trust by proving identities of the participants in a transaction
  - "On the Internet, no one knows you're a dog"

- Authentication is the foundation for other critical services
  - Personalization
  - Authorization / Access Management
  - Identity Management
  - Audit



Source of graphic: Burton Group, "Enterprise Identity Management", October 2002

Authentication Market Drivers

- Expanding access
  - Increasing numbers of mobile workers, telecommuters & devices
  - Extension of the enterprise network to third parties
    - Partners
    - Customers
  - Increasing network size and complexity
  - Need for portable credentials
- "Willy Sutton effect"
  - Increase in sensitive information accessed remotely
  - High levels of internal compromise/theft
  - Growing security awareness

Source: RSAS, adapted from Frost & Sullivan

How does One Decide?

- Many authentication technologies are available
  - How objectively to position alternatives?
  - How objectively to help customers choose the most appropriate?
- Market buzz ≠ Market reality, e.g.,
  - Biometrics get hugely disproportionate share of press coverage relative to actual deployment
  - "Year of the _____"
  - "Smart Card for Everyone"
  - "Tokens are Dead" vs. "Tokens Rule"

Simplifying the Challenge
Scorecard Approach

	UserID / Password	RSA SecurID Hardware Tokens	RSA SecurID Software Tokens	RSA Mobile	Digital Certificates	Smart Cards + Certificates	Biometrics
Strategic Fit - Corporate Systems							
Relative Security	○	●	●	●	⊙	●	⊙
Interoperability/Back-End Integration	●	⊙	⊙	⊙	⊙	⊙	○
Robustness / Scale	○	⊙	⊙	⊙	⊙	⊙	○
Future Flexibility	○	⊙	⊙	⊙	●	●	○
Strategic Fit - Users							
Convenience/Ease of Use	○	⊙	⊙	●	⊙	⊙	●
Portability	●	●	⊙	⊙	○	⊙	⊙
Multi-Purpose	○	○	○	○	⊙	●	⊙
Total Cost of Ownership (TCO)							
Acquisition Cost	↓	■	■	↓	↓	■	↑
Deployment Cost	↓	■	■	↓	■	■	↑
Operating Cost	↑	↓	■	↓	■	■	■

Key

Strategic Fit	Total Cost of Ownership
●- Best	↑- High
⊙- Better	■- Medium
○- Good	↓- Low

Authentication Scorecard

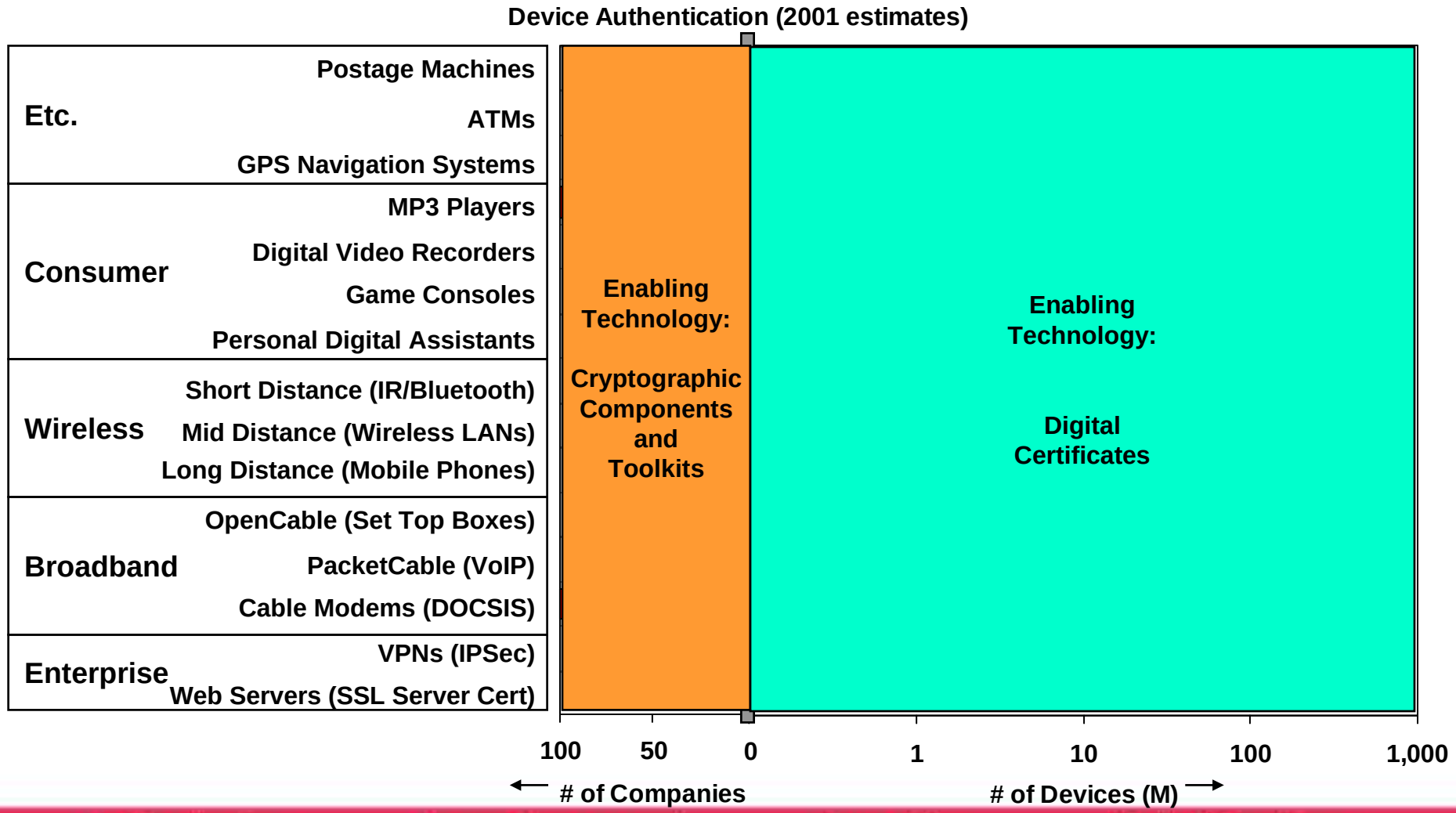
Three Major Categories – Ten Attributes

- Total Cost of Ownership
  - Acquisition cost
  - Deployment cost
  - Operating cost
- Strategic Fit (users)
  - Convenience / Ease of Use
  - Portability
  - Multi-purpose
- Strategic Fit (corporate/system)
  - Relative Security
  - Interoperability / Back-end Integration
  - Robustness / Scale
  - Future Flexibility

"Three-Legged Stool"

Trusted Computing Beyond the PC

Device Authentication



Authentication | Access Management | Encryption | Digital Signatures

Source of Device Estimates: PKI Forum Technical Working Group, March 2002

Device Authentication

Value Add: Reduce Fraud

Market Segment	Unit Value of Service ($/mo)	Units Shipped in 2002 (000)	Total Value of Service ($M/mo)	Assumed Fraud Rate	Potential Business Value ($M/mo)
Cable Modems	$45	11,096	$499	5%	$25
Digital Cellular Handsets	$35	438,920	$15,362	5%	$768
PDAs	$40	16,043	$642	5%	$32
Video Game Consoles	$50	38,000	$1,900	5%	$95
Digital Set Top Boxes	$45	49,154	$2,212	5%	$111
Digital Video Recorders	$13	4,845	$63	5%	$3
DVD players	$19	44,350	$843	5%	$42

$M per month!

Example: Remote Software Upgrades

- Automated Teller Machines
  - NCR Encrypting PIN Pad (EPP) module, for use in all NCR Personas ATMs
  - Signature
    - Developer signs software upgrade using private key
    - Service provider may also sign software upgrades for devices on their network
  - Download
    - Consumer downloads software upgrade, or more likely ...
    - … Service provider distributes software upgrade directly to device
  - Verification
    - Device processes and verifies an X.509 digital certificate to retrieve public key
    - Device uses public key from digital certificate to verify the signature attached to software upgrade
    - Device installs software upgrade

Source: NCR, “NCR Offers Greater Security for ATM Customers”, December 2001

Example: Protect Against Malicious Code

- Business problem
  - Customers frequently questioned the integrity and authenticity of virus definition files
  - Negative publicity has direct revenue impact

- Solution
  - Digitally sign virus definitions using Internet standards based digital certificates

Example: Digital Tachograph

- As of August 2004, all new Heavy Goods vehicles in EU will be required to run with a “smart” digital tachograph
  - Collects information on driving, work and rest times for drivers
- Four types of smart cards
  - Driver card
  - Company card
  - Workshop card
  - Control card
- Certificate-based solution
  - Each EU member nation is responsible for its own digital certificate management solution

SECURITY®

The Most Trusted Name in e-Security®