



**NETWORLD+INTEROP** LAS VEGAS

[www.interop.com](http://www.interop.com)



# Updating Network Authentication: Taming the PKI Beast



Karl M. Wagner

[karl.wagner@us.pwc.com](mailto:karl.wagner@us.pwc.com)



PRICEWATERHOUSECOOPERS 

# Agenda

---

- About PwC
- Current Situation
- Challenge
- Key Decisions
- Key Insights
- Adopted Solution
- Lessons Learned
- Questions

# About PwC

---

- World's largest Public Accounting Firm
  - 125,000 Staff and Partners Worldwide
  - Partnerships in 142 Countries with over 850 locations
  - Organized as a "Partnership of Partnerships"
    - Each partnership is their own business unit
  - Provide Professional Services for:
    - Audit, Assurance and Business Advisory
    - Global Tax Services
    - Business Process Outsourcing
    - Corporate Finance & Recovery
    - Human Resource Services
  - Specialists in over 24 Industry Sectors
  - See <http://www.pwc.com> for more information

# About PwC

---

- Director of Global Networking & Telecommunications
- Responsible for supporting PwC's *Internal* network between the PwC country partnerships
- PwC's Global IT group
  - Coordinates and manages multi-country IT Services
  - Design and Operational work is "sub contracted" to larger PwC partnerships "at cost"
  - Global IT services are charged back to the PwC partnerships who use the service

# Current Situation

---

- Business Challenges

- Public Accounting Industry recently became regulated
  - Sarbanes-Oxley Legislation
  - Public Company Accounting Oversight Board (PCAOB)
  - Increased SEC involvement
- PwC Divested its Management Consulting Services
  - Reduction of nearly 30,000 staff and partners
  - As high as 30% in some countries
  - Great pressure to reduce overhead costs
    - IT is an overhead cost
- “Thin Global IT” model
  - Small staff to support cross-border, multiple partnership IT services

# Current Situation

---

- Relevant Deployed IT Services
  - Remote Access VPN – 40,000 active users Worldwide
    - 2-factor authentication with soft tokens
    - Triple DES or better encryption
    - Global LDAP Directory
  - PwC Web Portal
    - Consolidates Intranet (B2E), Customer (B2B) and Public (B2C) web sites
    - Extensive PMI (Permission Management Infrastructure)
    - Sophisticated LDAP Directory and Meta Directory tools
  - Peer-to-Peer Wireless LAN cards deployed for Audit teams

# Current Situation

---

- Demand for technology changes:
  - Wireless LANs in PwC offices
    - Growing use of IM pushing demand to remain connected during meetings in PwC office conference rooms
    - Wireless LANs (802.11b) are solution to tangle of sometimes working cables in crowded conference rooms.
    - Wireless LAN cards already available
  - PwC needed to update its VPN Gateways
    - Desire to move to VPN appliances rather than server based VPN to reduce costs and improve performance
    - Desire to support IETF standard IPSec to expand to devices beyond Windows laptops (e.g. PDAs)
    - Desire to use common network authentication to lower costs

# Challenge

---

*“Deploy Wireless LANs and update remote access VPN while keeping costs at the existing levels or lower.”*

*AKA – Keep the unit cost of the “IT Utility” under control.*

# Key Decisions

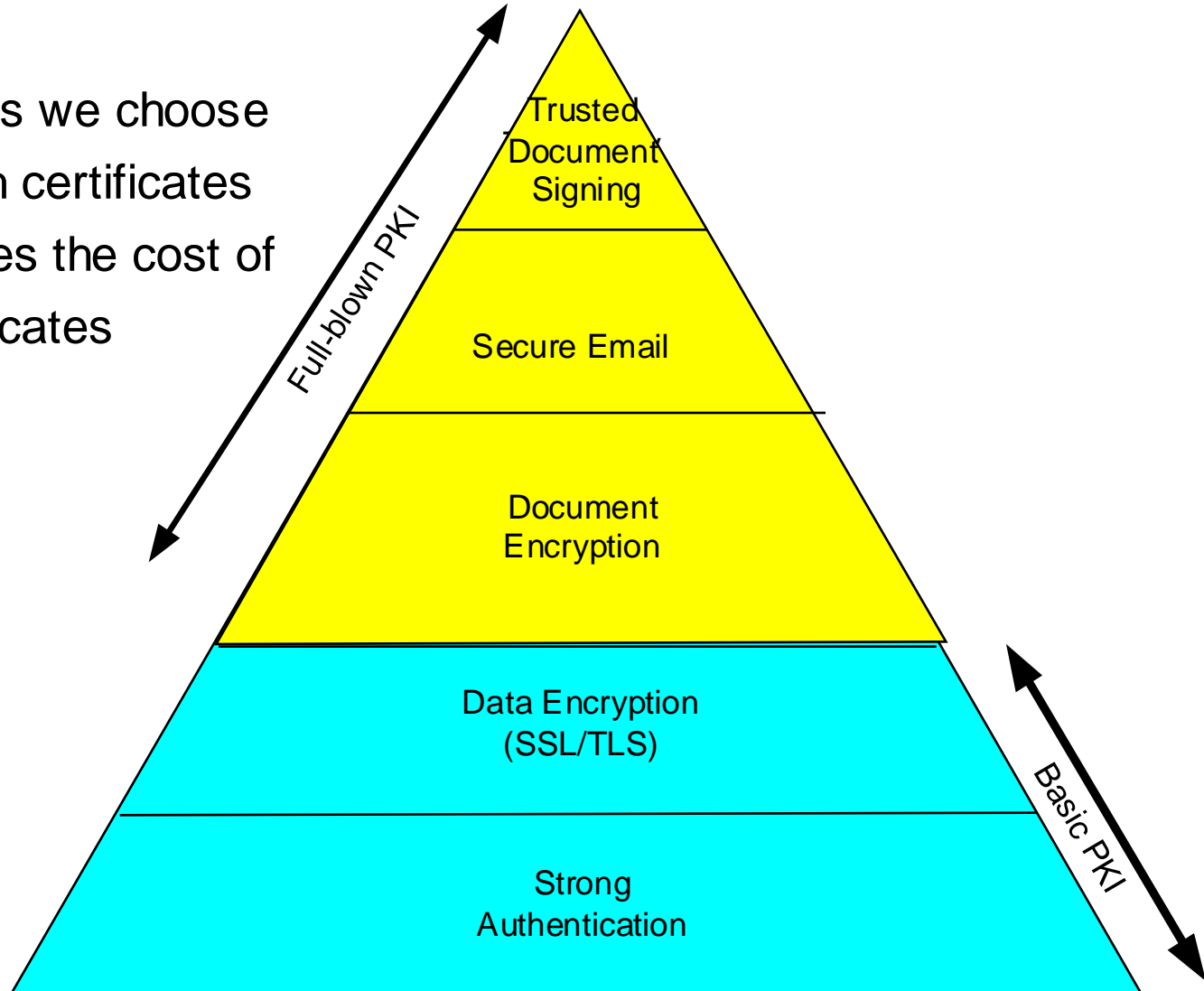
---

- Wireless LANs Deployment strategy?
  - Two modes meet security needs (2-factor authentication)
    - Wireless LANs with Remote Access VPN
      - Limits performance of local office applications
      - Increased gateway costs & deployments
    - 802.1x EAP authentication – “WAP = VPN Gateway”
- What type of credential to use?
  - 2-Factor Authentication: “Something you know and something you have”
  - The thing “you have” is your credential
  - PwC has deployed “software” tokens
  - X.509 Certificates have technical advantages
    - “Native” protocol support
  - X.509 Certificates have reputation of being expensive

# Key Insights

---

- The things we choose to do with certificates determines the cost of the certificates



# Key Insights

---

- Eliminating:
  - Document Signing
    - Removes the need to keep old certificates to verify documents signed by people who had left PwC
  - Secure e-mail
    - Removes the need to provide external people to verify a PwC certificate
  - Document Encryption
    - Removes the need to escrow old private keys to decrypt documents

# Key Insights

---

- Choose to:
  - Not alter the basic “Identity Process”
    - Token distribution system relies on the existence of a Lotus Notes ID Certificate
    - Use the same process for certificate distribution
    - If/When PwC moves away from Notes IDs, certificate/token distribution systems will have to change
    - Required some programming on PwC’s part to splice into the existing distribution system.
  - Use Microsoft Certificate Server 2003
    - No additional cost – included in existing contract
    - Does not depend on Active Directory adoption

# Key Insights

---

- Tokens (Soft)
  - PwC had purchased a license and fully depreciated the initial software investment
  - Distribution system was already built and in place
  - Only remaining costs are servers and software maintenance
  - Additional costs would be needed to use tokens for Wireless LANs
    - Users would increase to 70K, up from 40K

# Key Insights

---

## Certificate Costs

### One-time:

- New CA Servers
- Hardware Security Modules
- Cost to write modified distribution software

### Recurring costs:

- Hardware maintenance

## Token Costs

### One-time:

- Desktop Wireless LAN software to support tokens

### Recurring costs:

- Software maintenance
- Software upgrade costs
- Hardware maintenance

# Adopted Solution


---

- Updated IPSec VPN with certificate based authentication and username/password authentication.
- Wireless LANs with 802.1x EAP TLS authentication with certificates
- Microsoft Certificate Server
  - w/o Active Directory implemented
  - Auxiliary Hardware Security Modules for key storage, signing and key generation
- Push certificates via desktop software distribution process

# Adopted Solution

- PwC in house developed “RA Pro”:

**raPRO Validation (Beta 16)**



A digital certificate will now be installed on your PC. This certificate will offer enhanced security for many of the systems and applications you already use.

Please enter your GUID (e.g. JSMITH001), your GUID password, and your Lotus Notes password below.

GUID:

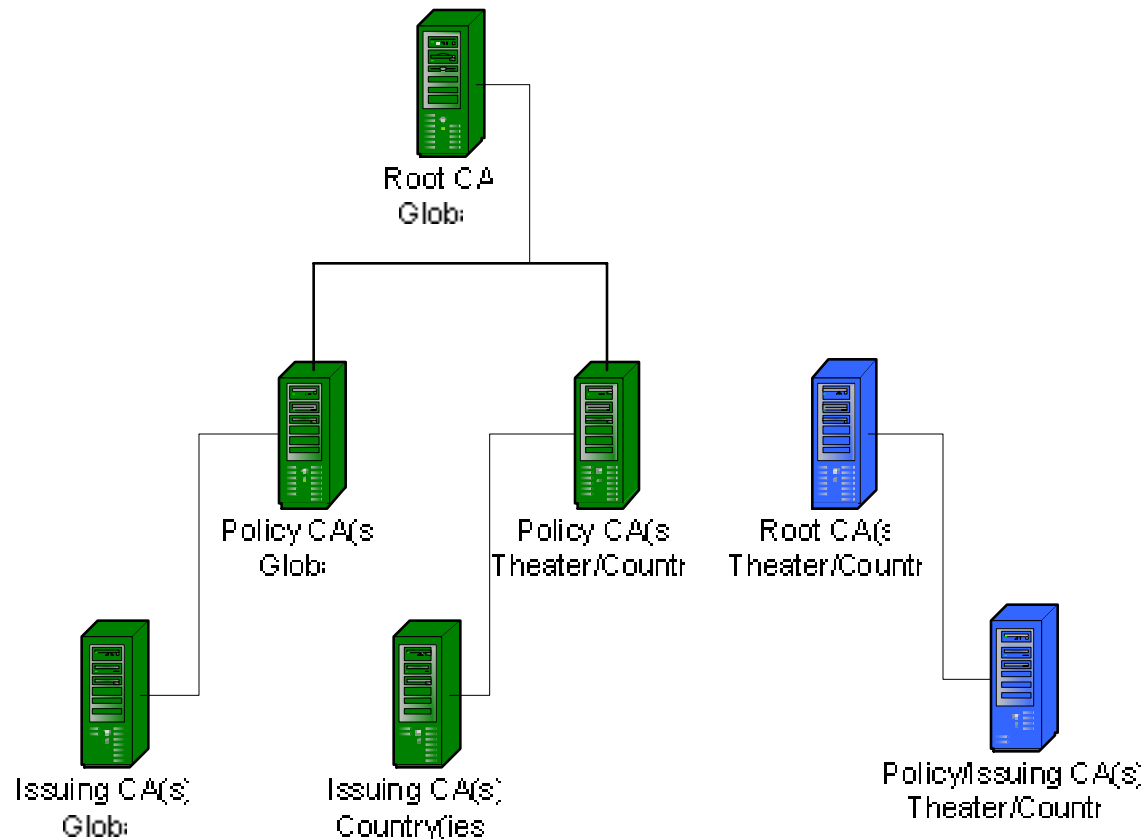
GUID password:

Lotus Notes password:

OK

# Adopted Solution

- Global, Country and “Island” Certificate Structure



# Lessons Learned

---

- Just because something is supposed to be expensive, doesn't mean it is
- Take a critical look at your requirements to see if you *really* need them all
  - Justify each requirement based upon incremental cost it adds to the solution
- A common authentication system will cost less than separate authentication systems
- A common [cost savings] mantra is:  
*Reuse before buy, buy before build*
  - But sometimes IT IS less expensive to build – so run the numbers before you decide!

# Questions

---

Questions?

Acknowledgement and Thanks to:

Steve Goldberg, PwC US IT

Fred King, PwC Global IT

Many others from the PwC US IT staff