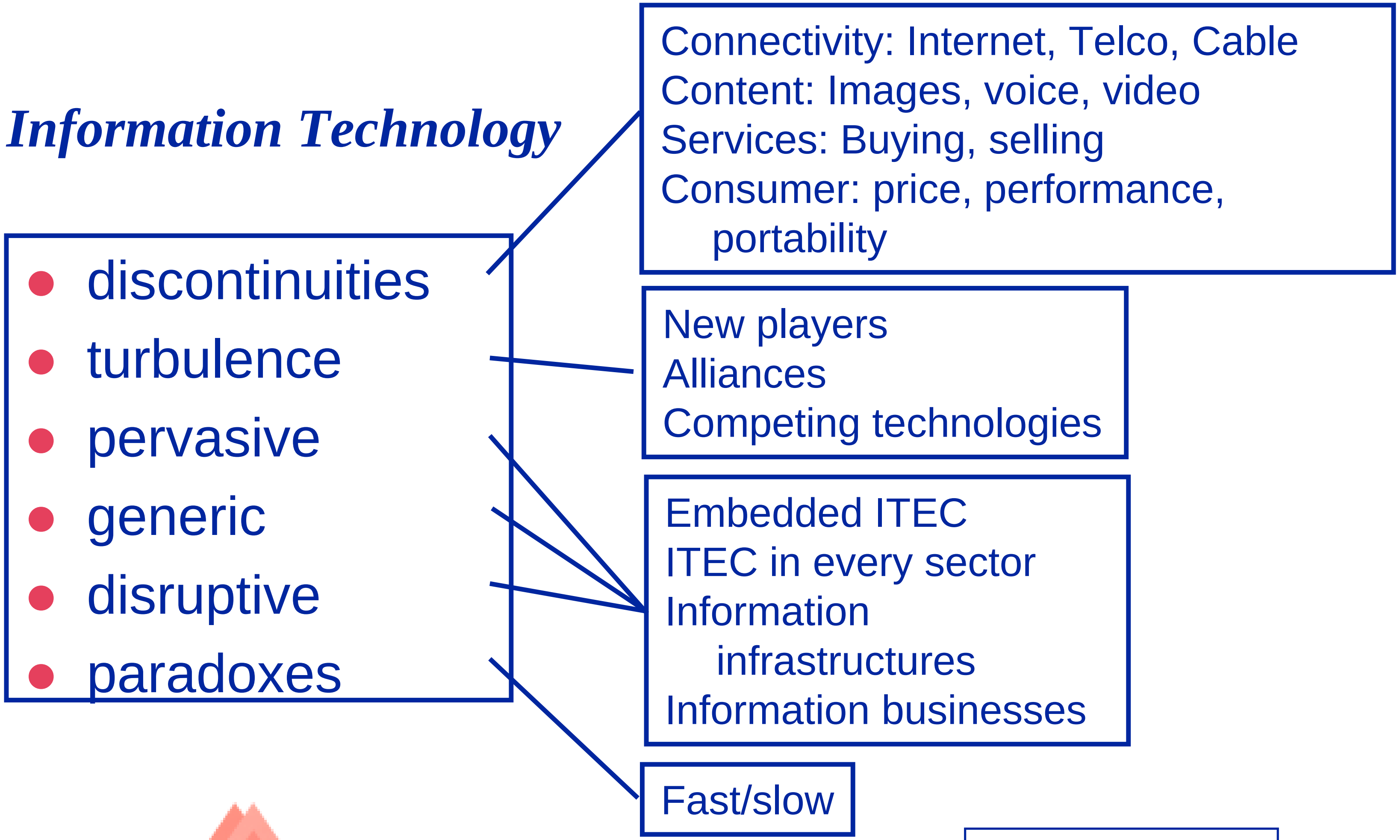
End to End Security for Internet Electronic Commerce

Andrew Herbert

ajh@ansa.co.uk

The Opportunity

Information Technology



- discontinuities
- turbulence
- pervasive
- generic
- disruptive
- paradoxes

Connectivity: Internet, Telco, Cable
Content: Images, voice, video
Services: Buying, selling
Consumer: price, performance, portability

New players
Alliances
Competing technologies

Embedded ITEC
ITEC in every sector
Information infrastructures
Information businesses

Fast/slow

Securing the Internet

- Unlimited scale
- Complex configuration
- Huge variety
- Distributed
- Continual evolution
- Concurrent operation
- Creeping bureaucracy
- Inherent unreliability
- Uncertain availability
- Different regulations

- many components
- many details
- many choices
- many places
- many changes
- many conflicts
- many chiefs
- much that can go wrong
- many demands
- many legal systems

=> We can’t assume a secure infrastructure

Why “end-to-end” security

- No uniformity
- No ubiquitous infrastructure
- No global security policy
- No global administration or control
- No static relationships

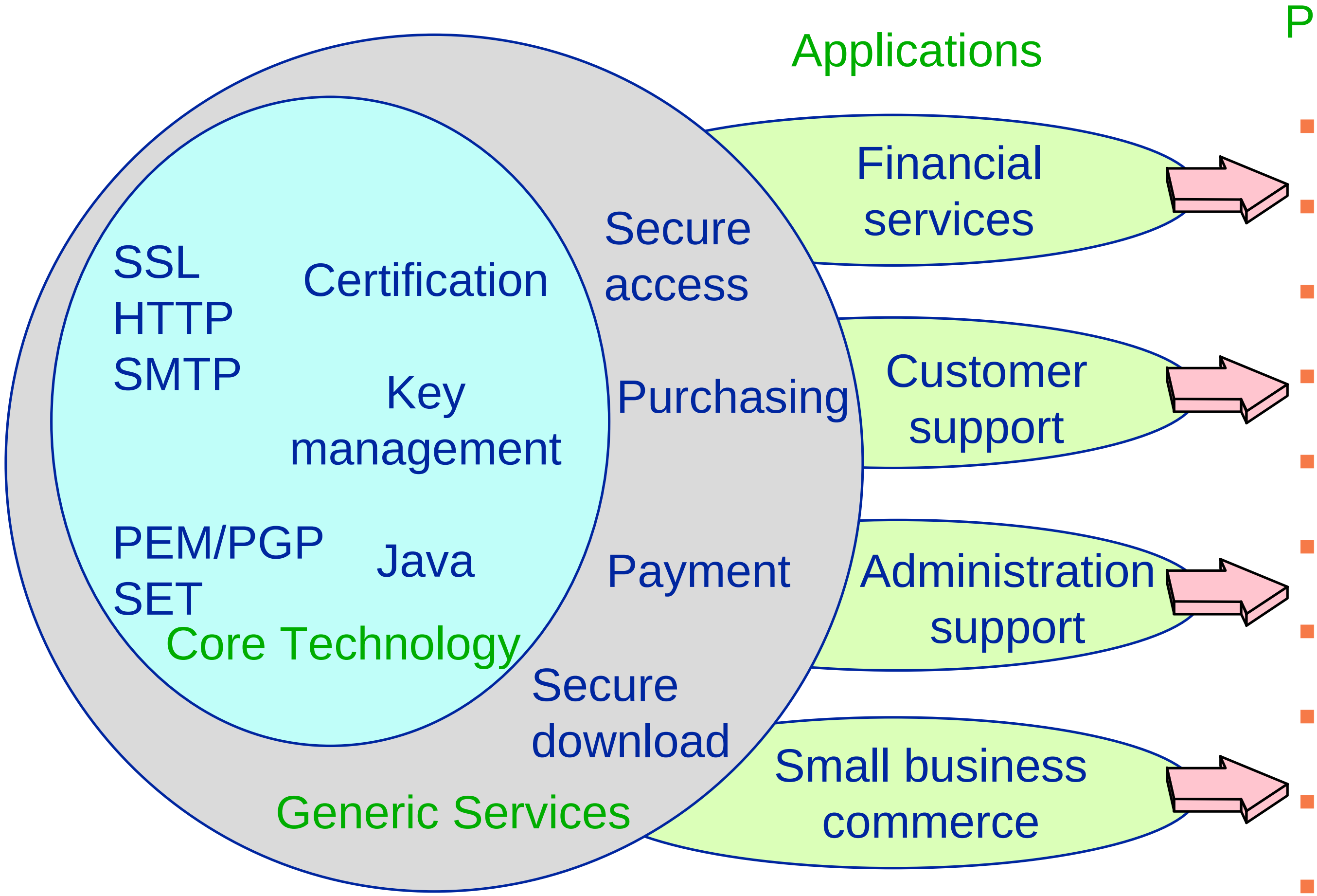
Self-defence is the only way

Provide tools and components
for engineering self-protection
and keeping audit trails

Objectives

- *Secure electronic commerce on the Internet*
  - viable business models
  - common architecture
  - pilot demonstrators
  - prototype infrastructure components
  - standards
- *Strong European dimension*
  - different business cultures
  - international commerce
- *User forum*

The project in one slide!



Partners

- APM
- HP Labs
- HP WCSO
- Tech. Univ. Berlin
- GMD
- GEMPLUS
- Swiss Bank
- Smart Card Forum
- Octacon
- Visa International

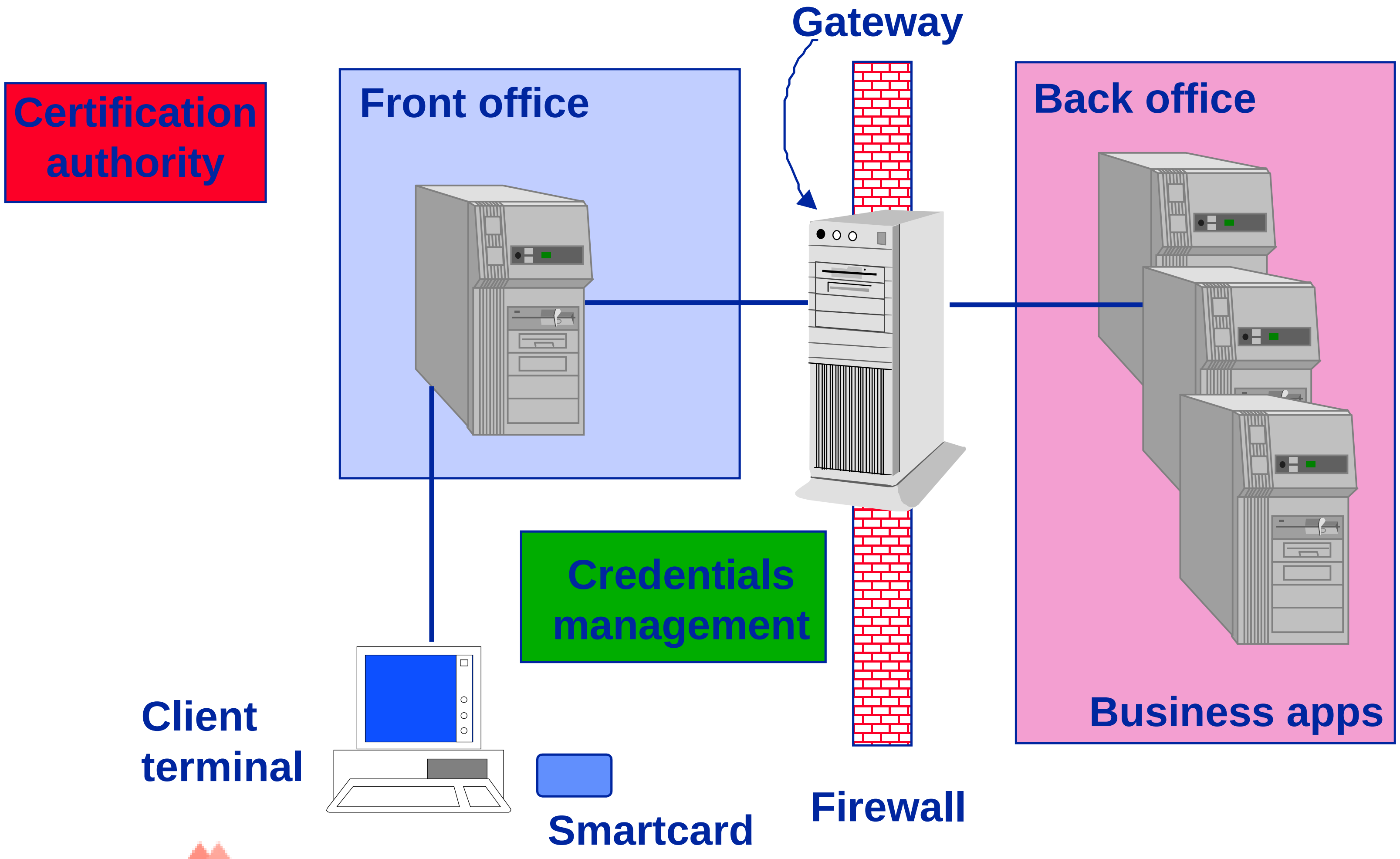
Why now?

- 24M Internet users
- Reducing telecoms costs
- Credit card infrastructure for payment
  - international clearing and risk management
  - international purchasing as well as payment
- Key service providers emerging
  - for example Verisign certification authority
- Many small-to-medium enterprises
  - direct sales world wide via the Web
  - outsource accounts, Web sales and marketing

Project Structure

- *Pilot demonstrators*
  - HP WSCO: product sales and service contracts
  - Swiss Bank: portfolio management
  - TUB: telecooperation (in academic administration)
  - Octacon: secure market place provider
- *Infrastructure components*
  - HP/Visa: corporate purchasing
  - APM: secure access and download, strong crypto
  - GemPlus: smartcard support
  - GMD: key management
- *User forum*
  - Smartcard Forum

Common Architecture



Gateway

Certification authority

Front office

Back office

Credentials management

Business apps

Client terminal

Smartcard

Firewall

WCSO Pilots

- Online service for VARs
  - secure access to contract and price data
    - Web server-based
    - Initially no direct link to back office
- Online support to customers
  - customers with contracts
    - internal certification
  - casual customers
    - requires external certification authorities
- => More responsive, targeted service
- => More business, reduced admin costs

TUB Pilot

- *University administration applications*
  - within departments, between departments
  - strong privacy culture
- *Secure access to student records and institutional data*
- *Secure telecooperation*
- *Secure information dissemination*
  - distribution of ordinances etc
- *E-mail foundations*
- => More responsive and informed administration

Swiss Bank Pilot

- *Deploy SwisKey product across the Internet*
  - portfolio management
  - current product is a closed private network
- *Download "branded" application to user*
  - better user interface than WWW
- *Secure hole punching through to back office applications*
- *Do own key management*
- *Strong security as a selling point*
- => significantly more SwisKey business

Octacon Pilot

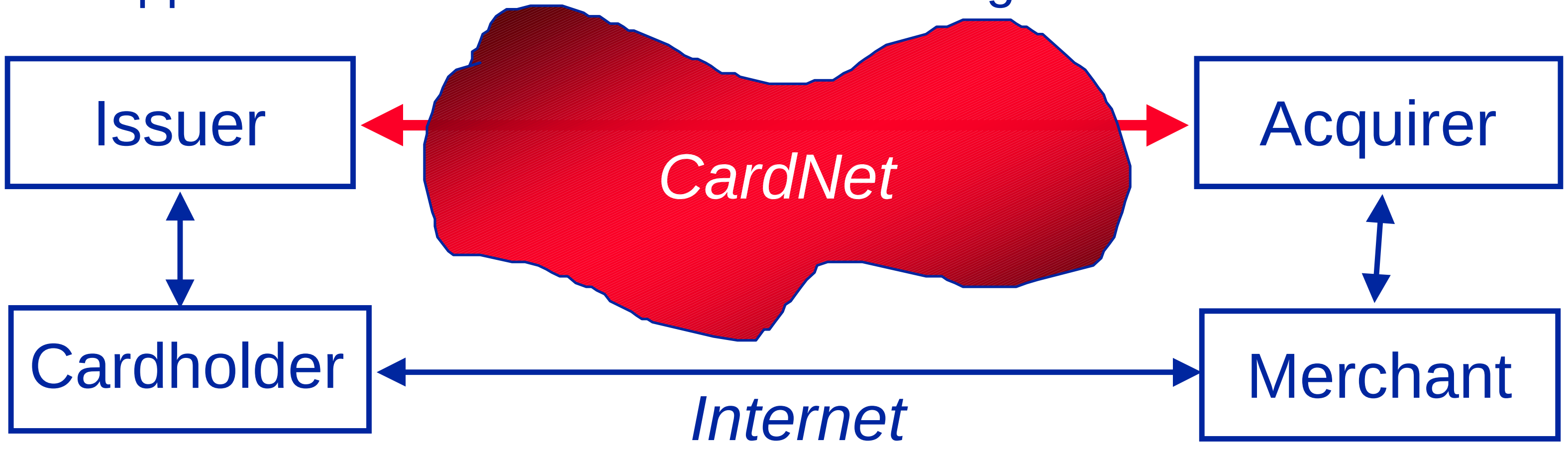
- *Host Web front office for other businesses*
  - especially SMEs
- *Catalogue*
  - find suppliers by product, by area etc
- *Purchasing*
  - provide a “one-stop internet shop”
- *Payment reconciliation*
- => Business service provider
- => Valued added services
- => Internet “outsourcing”

Corporate purchasing infrastructure

- *Corporate card for office purchasing*
  - capture MOTO business for office supplies
  - enforce controls, reduce paperwork costs
  - consolidated MIS reports to managers
- *Leverage Secure Electronic Transactions*
  - joint VISA / Mastercard standard
  - roll-out through 1996
- *Leverage Smartcards*
- *Build live system in 3-4 countries*
- => Real banking infrastructure for pilots

Secure Electronic Transactions

- Protocol for secure credit card transactions
- Industry-wide standard
- Public keys for authentication (not identification)
- Symmetric session keys for privacy
- Certification hierarchy rooted at card agency
- Supports both online and offline working



Why credit cards for payment?

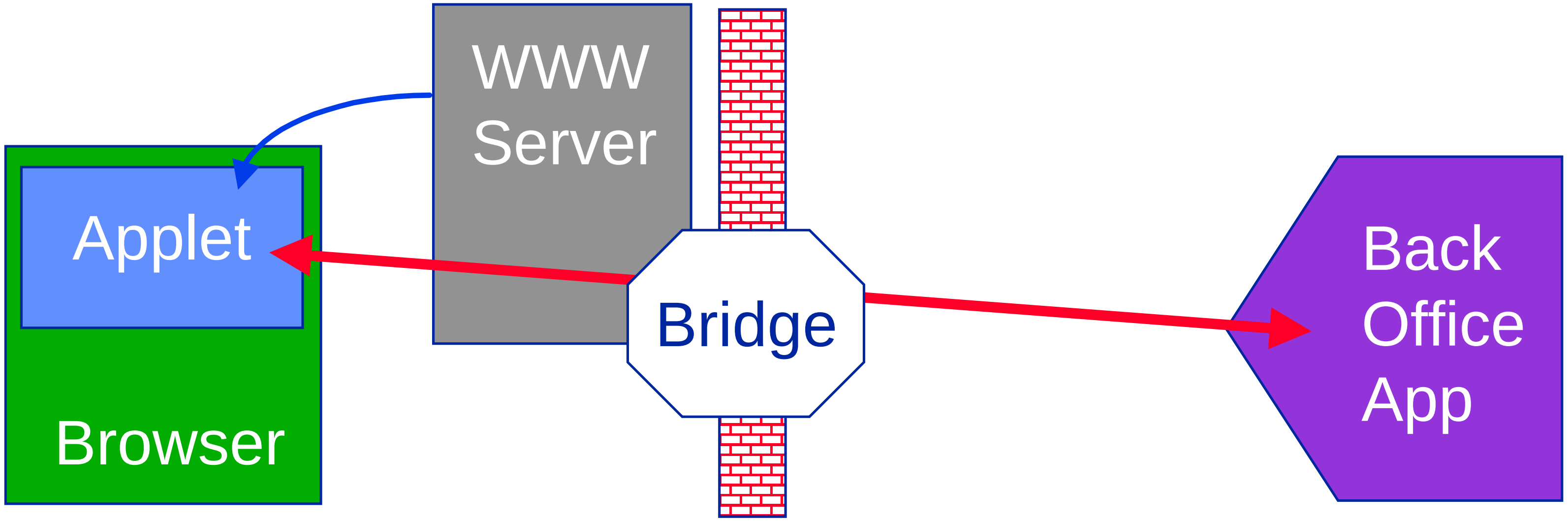
- electronic cash
  - *anonymous, instant payment, contains value, no prior legal contracts*
  - *not yet international, risks unquantified*
- electronic cheques
  - *signed instruction to pay, no guarantee of payment*
  - *not international*
- electronic credit cards
  - *guarantees authorised payments, depends on prior legal contacts*
  - *international, can work offline*
- electronic funds transfer
  - *direct transfer of value between accounts*
- subscription
  - *usage is accounted against a prepaid budget*

Secure purchasing

- catalogue searching
- browsing product details
  - possibly confidential
- ordering products
  - probably confidential
- negotiation
  - price, delivery, payment method, payment terms
  - probably confidential
- payment
  - authenticated, authorised and probably confidential

Secure Download

- Only download authorised client “applets”
- Authenticate applet to server and vice versa
- Securely distribute privileges to punch through firewall and access back office services



Strong Cryptography

- *Export, patent and prohibition issues*
- *Demonstrate where strong crypto is essential*
- *Explore non-cryptographic techniques*
  - one-way functions (see next talk)
    - signature
    - authentication
    - authorisation
- *Architect interfaces to enable alternate cryptos*
- *Show PGP strong crypto in SwisKey pilot*

Smartcard support

- *Use Smartcards for key distribution*
  - Keep keys outside unsafe computers (e.g. PC’s)
- *PCMIA reader, Smartcard ready modem*
- *GPK200card*
  - RSA, DSA, DES algorithms
  - SHA, MD5 hashing
  - true random numbers
  - RSA signature 150ms, verification 50ms
  - capacity for 2Kb of stored application data
- *Software for client and host*
  - includes secure channel set up.

Key management infrastructure

- *Systems to manage relationships between identities and keys*
- *Based on SecuDE toolkit*
  - PEM, X.509
- *Investigate*
  - federated as well as hierarchical relationships
  - role and attribute-based keys
- *Integrate* with HTTP, SSL, Smartcard etc

User Forum

- *User members of consortium*
- *Smartcard Forum*
  - US-based consortium
  - Over 400 members
  - briefings, demonstrations, business strategies
  - main sectors:
    - financial
    - public administration
    - telecoms operators
- *Other projects*
  - SEMPER (e-cash), ICE

Summary

- *End-to-end security*
- *Electronic Commerce*
- *Pilot demonstrators*
  - *real business applications*
- *Key infrastructure components*
  - *secure hole-punching, Smartcards*
  - *key management, payment*