The ID WORLD International Congress 2004

Identity for Public & Private Access Control

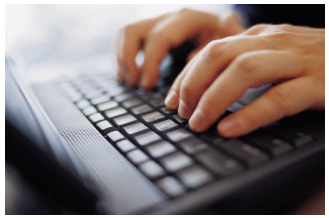
MODULE VI: Advanced Auto-ID Implementation

Examples for Trusted Identity

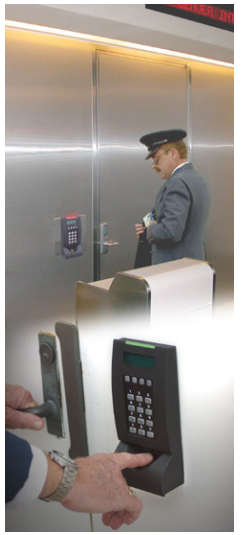
by
Ayman S. Ashour
ASSA ABLOY
Identification Technology Group

Identity for *Public* & *Private* *Access Control*

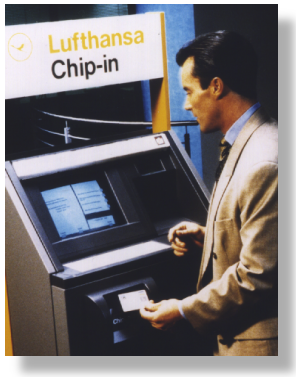
- Public:
  - Employee
  - Private contractor
  - Citizen
- Private:
  - Employee
  - Private contractor
  - Customer
- Access Control:
  - To a physical place
  - To information & logical place
  - To money & resources
  - To …….



What are the primary objectives of the identity system?



- Enhance security
  - Improve management of ID's
  - Enhance level of authentication
- Enhance productivity and lower costs
  - Faster & cheaper
  - Combine multiple applications on same ID



- Enhance privacy
  - Protect privacy of user
- Other …

Crucial considerations

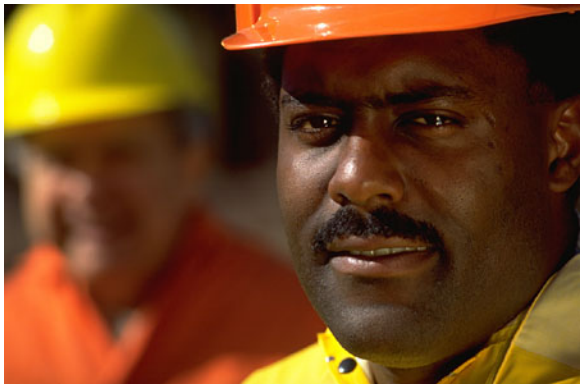
- Level of security
- Level of privacy
- Legacy systems and backward compatibility
- Transportability & interoperability
- Convenience, ease of use, speed
- On going maintenance
- Cost
- Who owns the ID?

Various levels of security

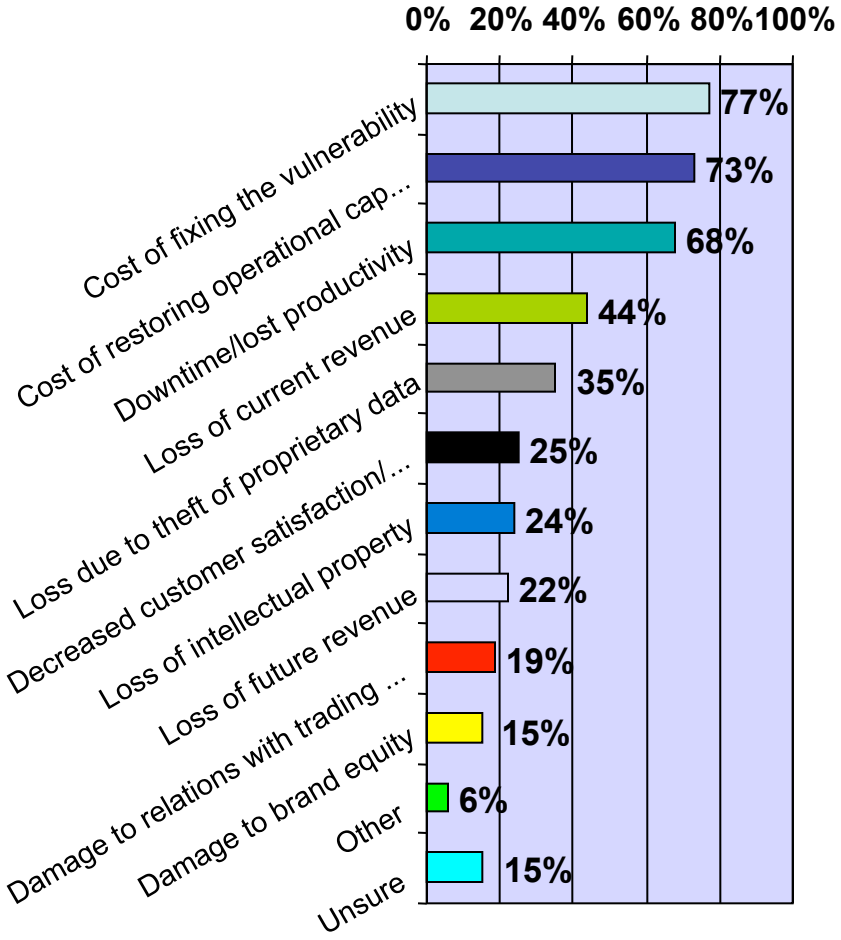
- Password / PIN
- ID card
- ID card w/ PIN
- Biometric
- ID card & biometric
- On card biometric
- Counterfeit proofing
  - Secure printing
  - Encryption

Photo courtesy of Recognition Systems

Private access control for employees



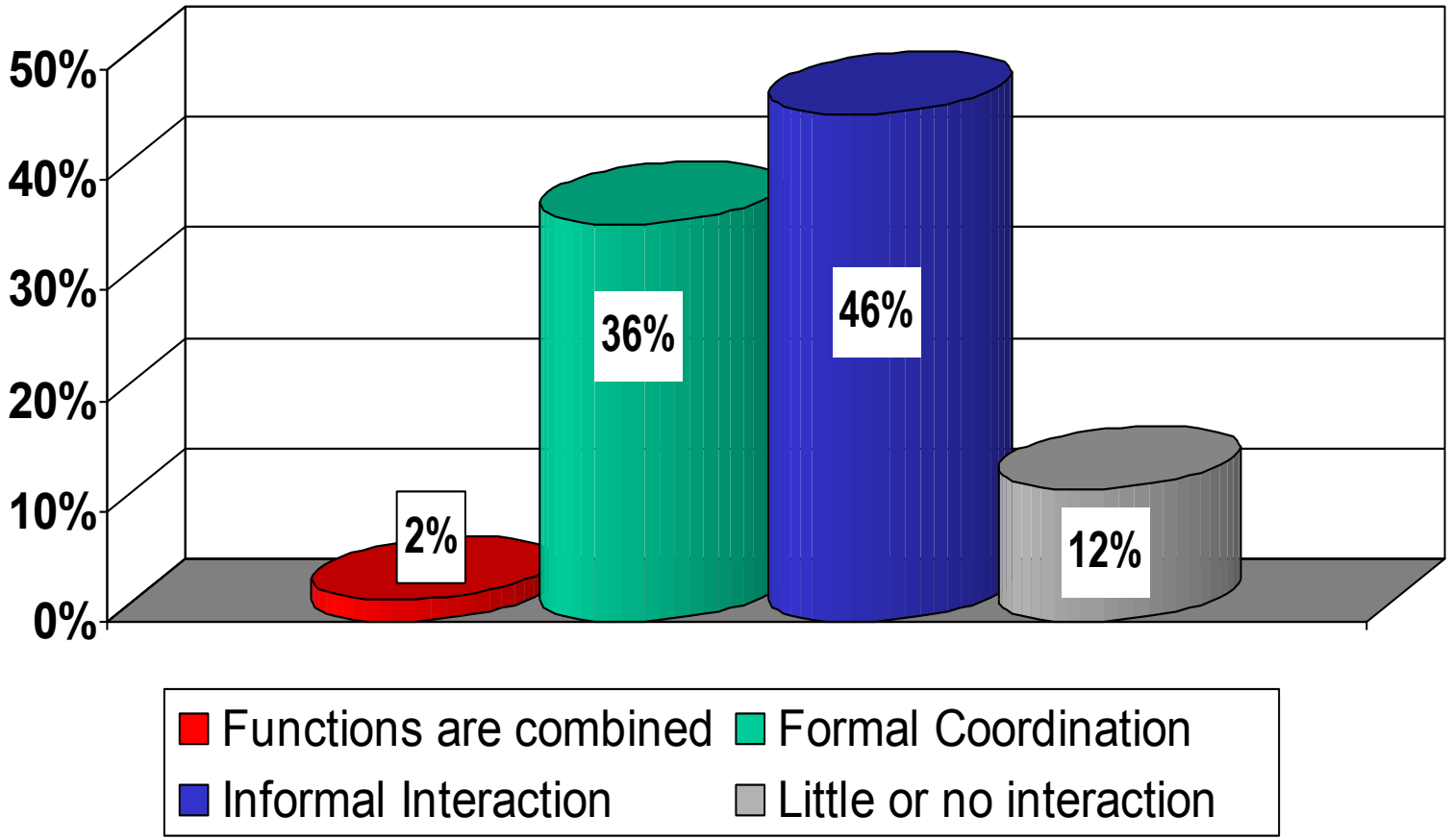
IT security costs led to change of behavior



- **Businesses that quantify the financial cost of cyber crimes have an average loss of more than $1.4 million in 2002**
- **Financial costs include items such as:**
  - **Remediation**
  - **Restoration**
  - **Lost downtime / productivity**
  - **Loss of revenue**
  - **Customer satisfaction**
  - **Brand value**
  - **Relationships**

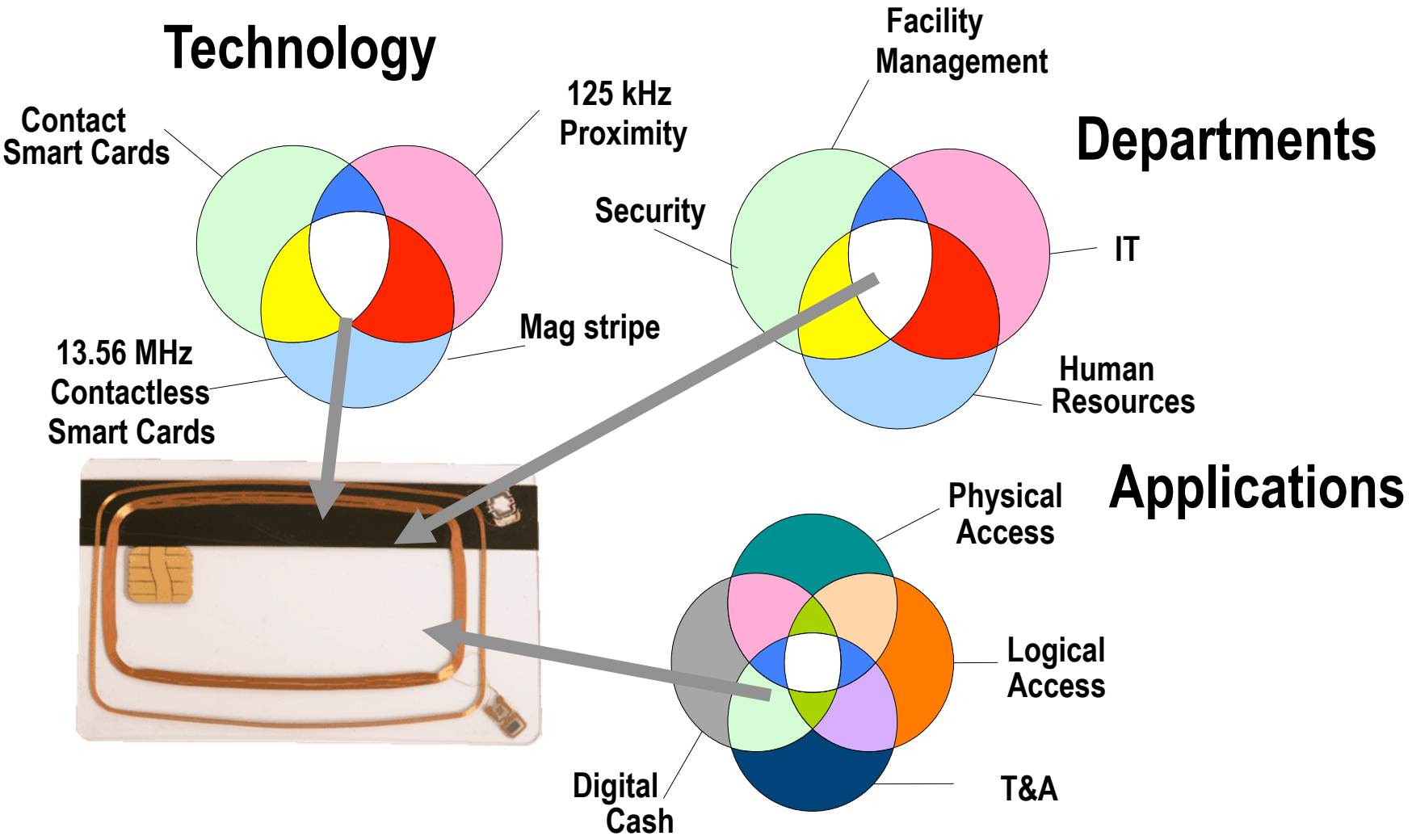
Source: CSO Security Sensor III, May 2003

Security's Interaction with IT / MIS Departments

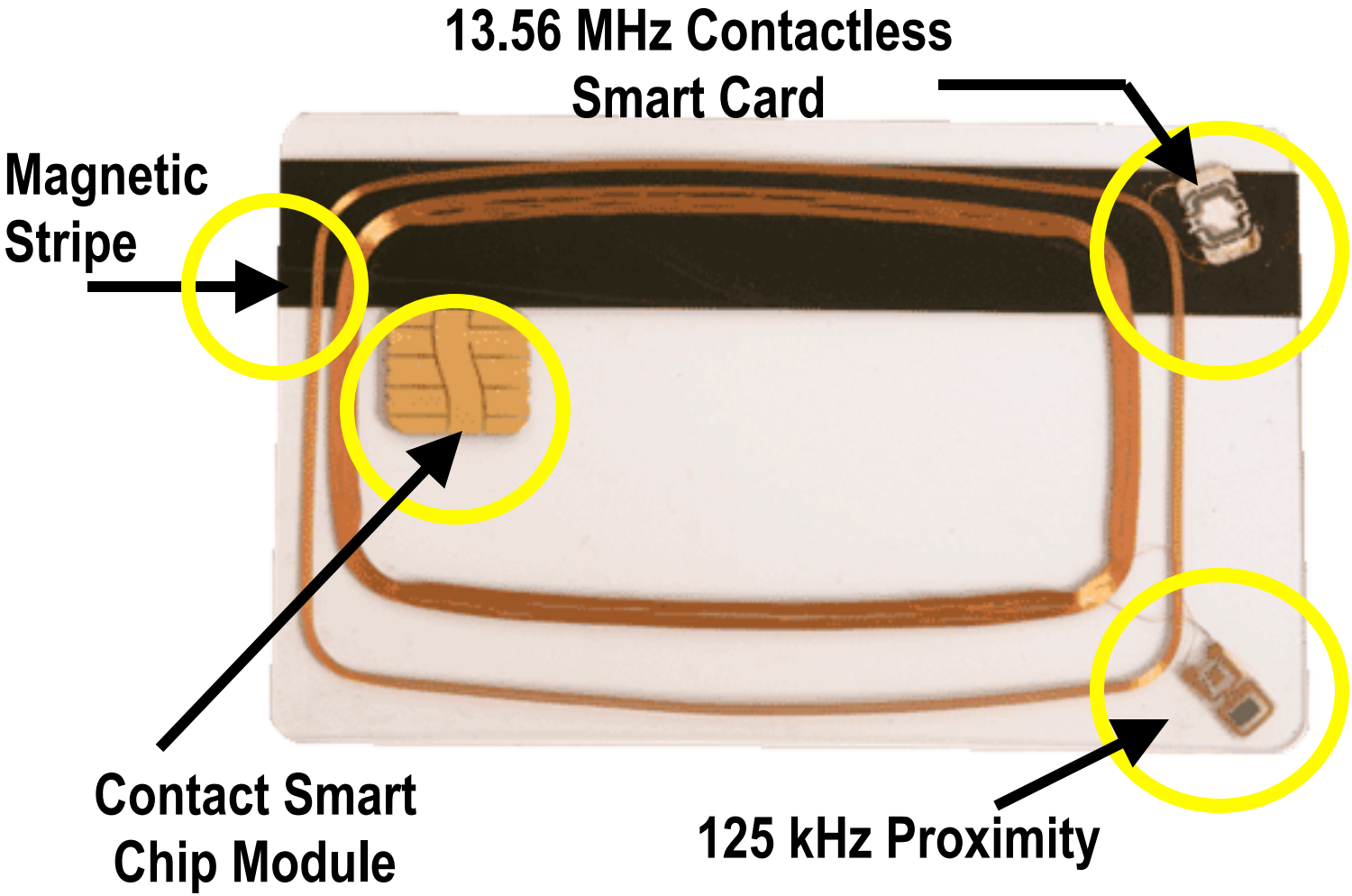


Source: Top Security Threats, Pinkerton 2003 Survey of Fortune 1000 Companies

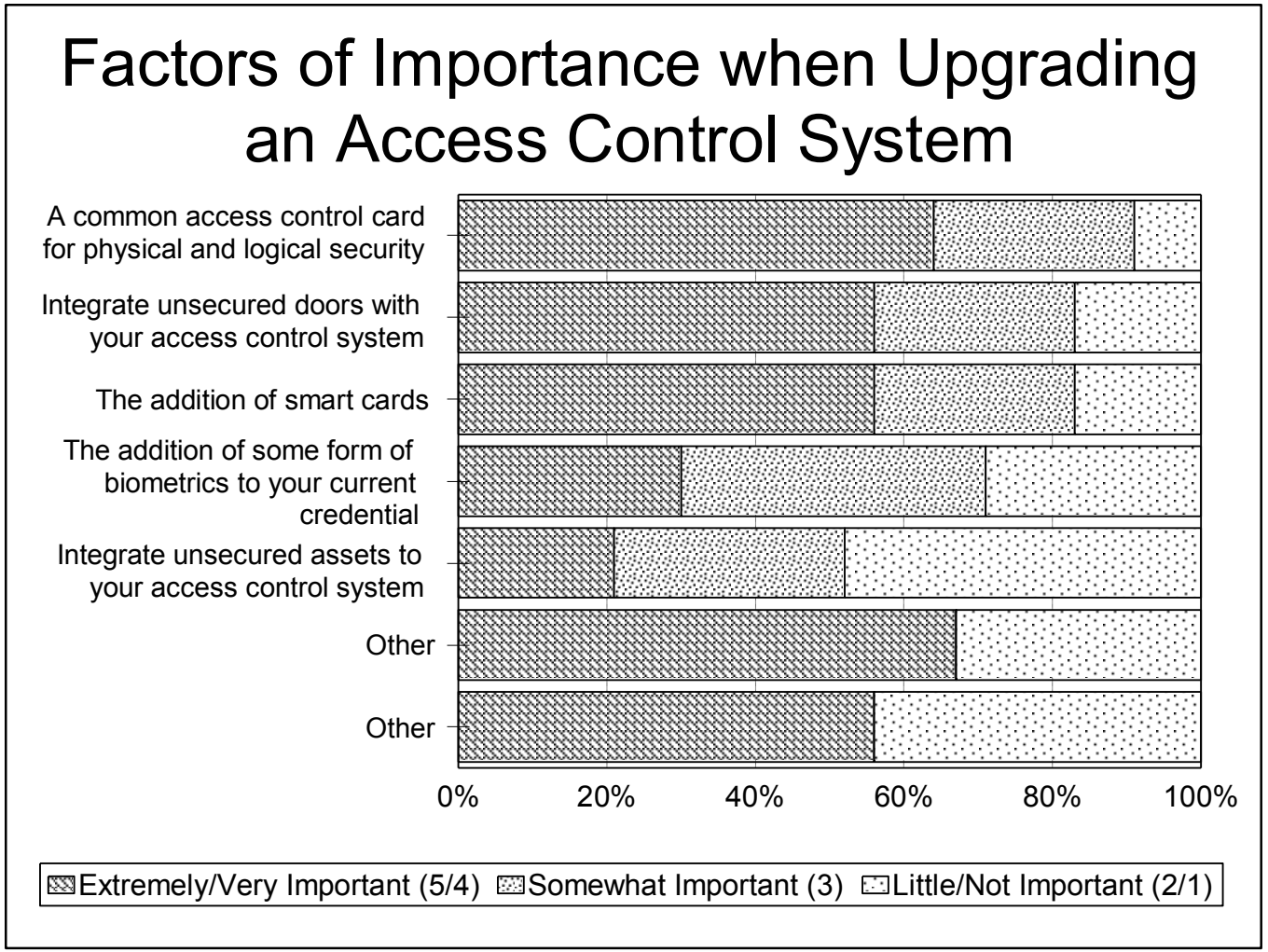
Implications for **private access control** for **employees**



Multi-technology ID card to address legacy and interoperability

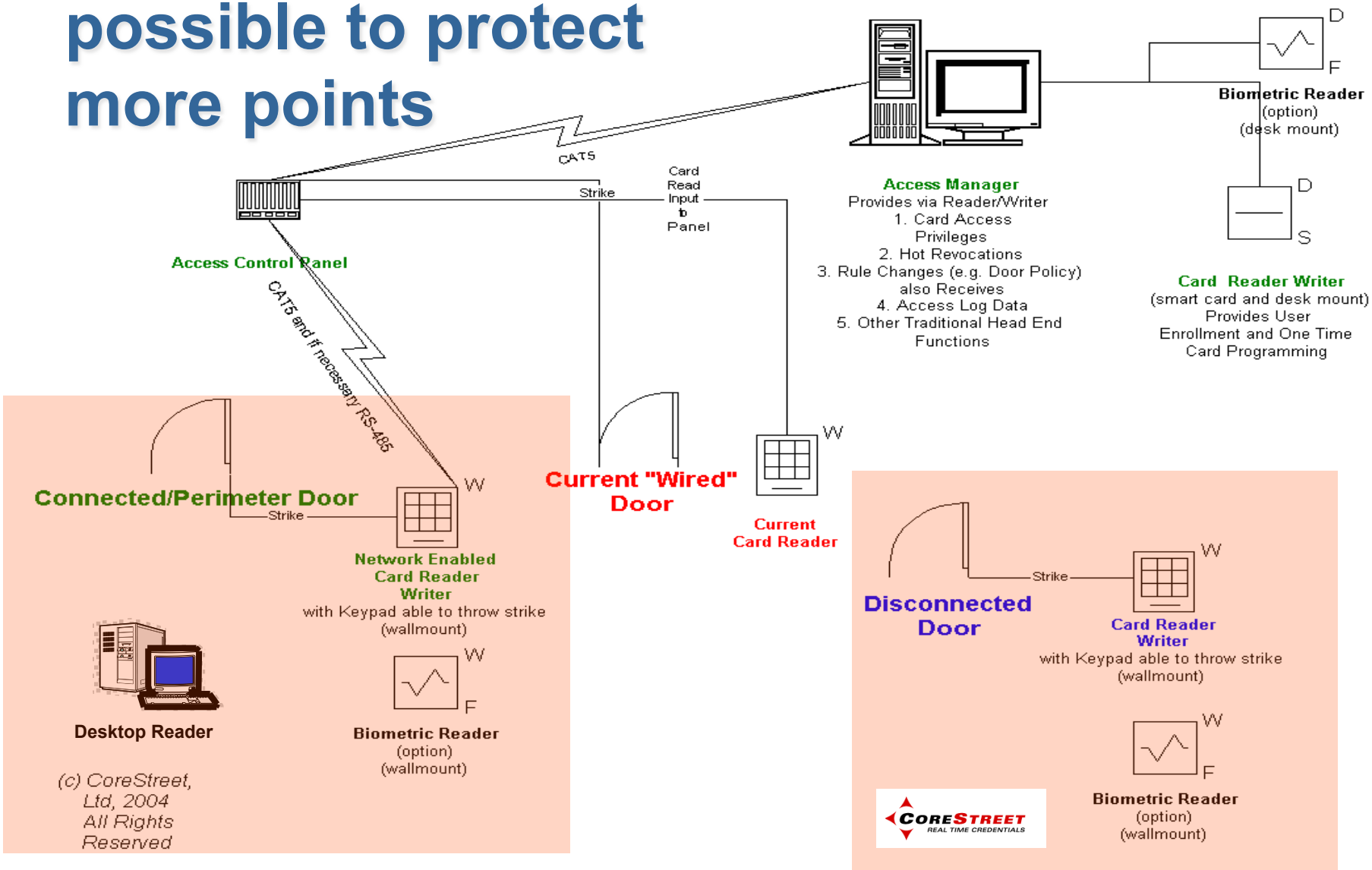


ID convergence & unsecured doors



BNP Market Research Survey July 2004 supplied courtesy of CoreStreet , Ltd.

Smart cards make it possible to protect more points



ITG Identification Technology Group

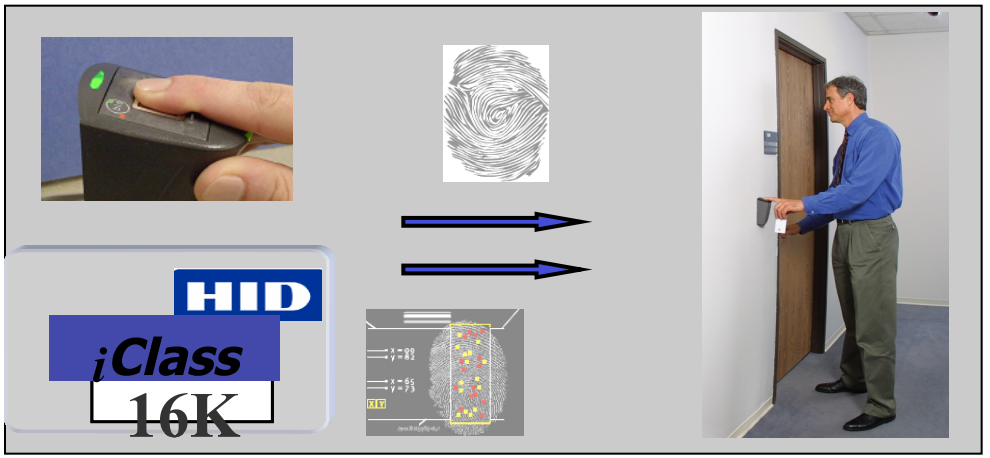
ASSA ABLOY

Private access control for customers

- Security important, but costs, privacy and ease of use generally take precedence
- Biometric & PKI less used for transport only applications
- As expected for access to money security returns to a bigger role
- Multi-application cards are increasing as as new private alliances subscribe to one ID card solution for multiple different isolated private transactions
- The customer almost always owns the ID

Public access control for employees

- Similar concepts to private access control for employees
- Interoperability issues are looming large
- CAC and TWIC are two major smart card programs in US
- US Government Smart Card Handbook offers excellent background material and very helpful design and implementation guidance



Public access control for citizens

- e-Government offer excellent opportunities for reducing costs, improving productivity
- Significant experience with health cards in several European countries
- On-going trials in US including a cross state project covering health and welfare
- Privacy considerations *are* important and smart card technology offers great opportunities for enhanced privacy

Public access control for citizens

- Terrorism worry driving major upgrade of travel security
- “Breeder” documents critical for integrity of “chain of trust”
- National ID cards and ePassports (eMRTD) based on ICAO standards calling for contactless microcontroller smart cards
- USA Trusted Traveler program – on going trials

ID systems are often subsystems within larger systems

- Authentication at the issuance stages of ID is often an area of weakness
- Authentication of readers and authorized users in multiple applications
- On-going development in technology to improve maintenance of ID systems and fast removals of revoked ID's

Conclusions

- RFID & smart card industries have developed sufficiently and converged to provide a large and diversified offering to meet the needs of most applications ..be them private or public, employee or citizen
- It is crucial when launching an ID project to be clear on objectives and to recognize trade offs between various system attributes
- Smart cards offer users unparalleled levels of security and privacy while significantly enhancing productivity and solving traditional problems of managing multiple ID's and remote locations
- Excellent documentation and background information exist to allow virtually every organization to benefit from new technology

Resources

- US General Services Administration – Government Smart Card Handbook
- Smart Card Alliance Reports:
  - Secure Identification Systems: Building a Chain of Trust
  - Privacy & Secure Identification Systems: The Role of Smart Cards as a Privacy Enabling Technology
- CoreStreet, Ltd. White Paper
  - KeyFast Technical Overview: An introduction to the architecture and usage of KeyFast Technology
- Web Sites
  - www.smartworldacademy.com