E-Business and PKI in Saudi Arabia

Regional Seminar on "E-Business"

for the Arab Region

Cairo - Egypt, 10 - 12 December 2002

Dr. Fahad Al-Hoymany
King Abdulaziz City
for Science & Technology
hoymany@isu.net.sa

د. فهد عبد الله الحويماني
مدينة الملك عبد العزيز
للعلوم والتقنية

Agenda

- **E-Business Overview**
- **E-business in Saudi Arabia**
  - E-commerce committee
  - Update on activities
- **PKI in Saudi Arabia**
  - Overview
  - Examples: confidentiality and digital signature
  - Structure of Saudi PKI
- **Conclusion**

E-Business
Main drivers worldwide

- ✓ Improved communication infrastructure…
- ✓ Ubiquitous networking (i.e., the Internet!)…
- ✓ High-speed processors, large storage capacities, better software…
- ✓ Multinational corporations, competition, globalization, outsourcing trends, alliances, partnering, acquisitions…
- ✓ Need for cost cutting, speed-to-market, short product life cycles, …
- ✓ Too much paper work…
- ✓ Poor market visibility (limited choices) and static prices …

E-Business
Saudi Environment

- About 500,000 Internet subscribers, about 1.25 million users
  - That's only 6% of the population
- About 250,000 PCs (desktops + notebooks) shipped annually
  - IDC puts the number of installed base of PCs in KSA at over 800,000 (Madar research puts it at 1.5 million!).
  - Large number but small in penetration compared to most GCC countries
- About 40% of IT spending in the Middle East comes from Saudi Arabia
- Largest GDP in the Middle East, about $175 billion (in 2002)

E-Business

Main Requirement

1) **Telecommunication infrastructure**

   The medium requirement

2) **National Public Key Infrastructure (PKI)**

   The security requirement

3) **Electronic Payment System**

   The money handling requirement

4) **Policies and Regulations**

   The law requirement

E-Business in Saudi Arabia

The E-commerce Committee

- **It is a national standing e-commerce committee, formed by council of ministers in 1997. Its members are:**
  - Ministry of Commerce
  - King Abdulaziz City for Science and Technology
  - Ministry of Finance and National Economy
  - Ministry of Post, Telegraph and Telephone.
  - Saudi Arabian Monetary agency
  - Ministry of Interior
  - Ministry of Information
  - Saudi Communication Authority

E-commerce Committee

Role of Each Member

- **Ministry of Commerce**
  - Drafting electronic transactions law
  - Reviewing and adapting current relevant policies and regulations to EC requirements
  - Awareness programs
- **King Abdulaziz City for Science and Technology**
  - Developing Public Key Infrastructure for use in Saudi Arabia
  - Developing the framework for regulating and managing certificates and use of digital signatures

E-commerce Committee

Role of Each Member

- **Ministry of Finance and National Economy**
  - Developing electronic government services to enable government agencies to offer services to citizens and to exchange data electronically
- Ministry of Post, Telegraph and Telephone.
  - Developing a robust telecommunications infrastructure capable of supporting EC
- Ministry of Interior
  - Defining the requirements for data security and privacy of personal data and information

E-commerce Committee

Role of Each Member

- **Saudi Arabian Monetary agency**
  - Development of payment systems for secure electronic collection of payments for electronic transactions between businesses, for both B2B and B2C.
- **Ministry of Information**
  - Development of Intellectual Property Rights in E-business contexts

E-commerce Committee

Role of Each Member

- **Others**
  - Providing support services such as delivery of parcels to businesses and homes (*Ministry of Municipalities and Rural affairs*)
  - Training and education of required manpower resources (*Ministry of Higher education and Vocational Training Institutes*)
  - Developing a business portal for serving SME's (*Chambers of Commerce*)

PKI in Saudi Arabia
KACST's Role

- **Build and operate the root certification authority, Root CA**
- **Define some national PKI policies, standards and regulations, including:**
  - digital signature policies and laws, and
  - the rules and regulations governing certification authorities
- **Define the requirement for data security and privacy with other agencies**

PKI in Saudi Arabia

What is PKI?

- **It is a system that creates a trust environment for conducting transactions over public networks, by developing a framework for issuing certificates to be used for:**
  - Confidentiality,
  - Integrity,
  - Authentication,
  - Non-repudiation,
  - Digital signatures, access control, creation of original documents, among others.
- **PKI is well-recognized as a main instrument for solving many security problems over public networks.**

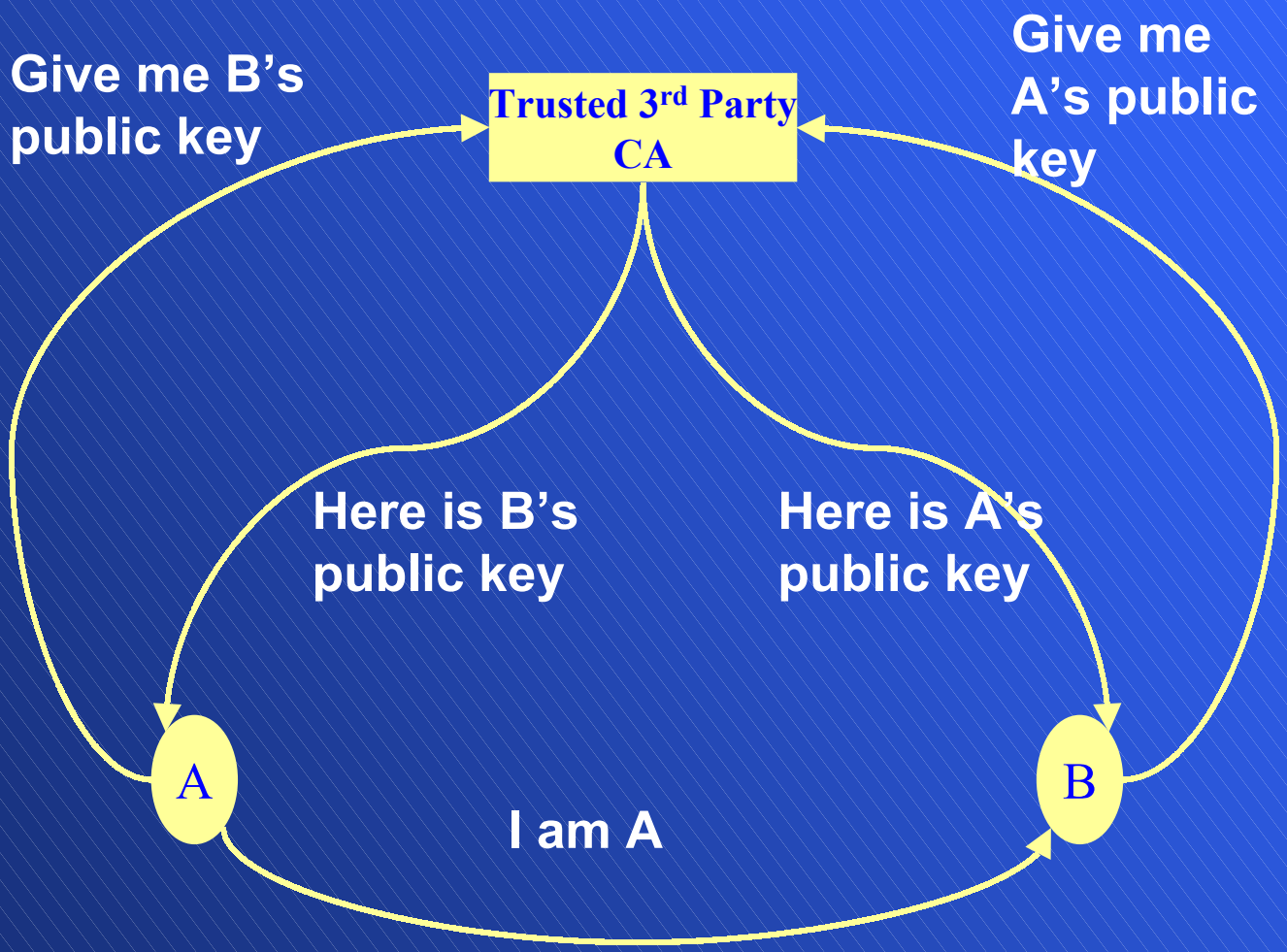
PKI in Saudi Arabia

Example of issues addressed by PKI

- How can two or more people communicate via the Internet without letting others read their communication?
- How can one know that a received message did indeed come from person X (the expected person)?
- How can you know that the web site you are going to is the right web site?
- How can the web site know that you are indeed the right person?
- How can one sign a contract online?
- How can a broker prevent an investor from denying a stock transaction?
- How can you be sure that the recipient received the message? And that he does not deny it?
- How can the recipient prove that you did send the message?
- How can you know that an Internet document is original?

PKI in Saudi Arabia: Trusted 3rd Party

Example: A wants to send private message to B



Both A & B have positively identified each other

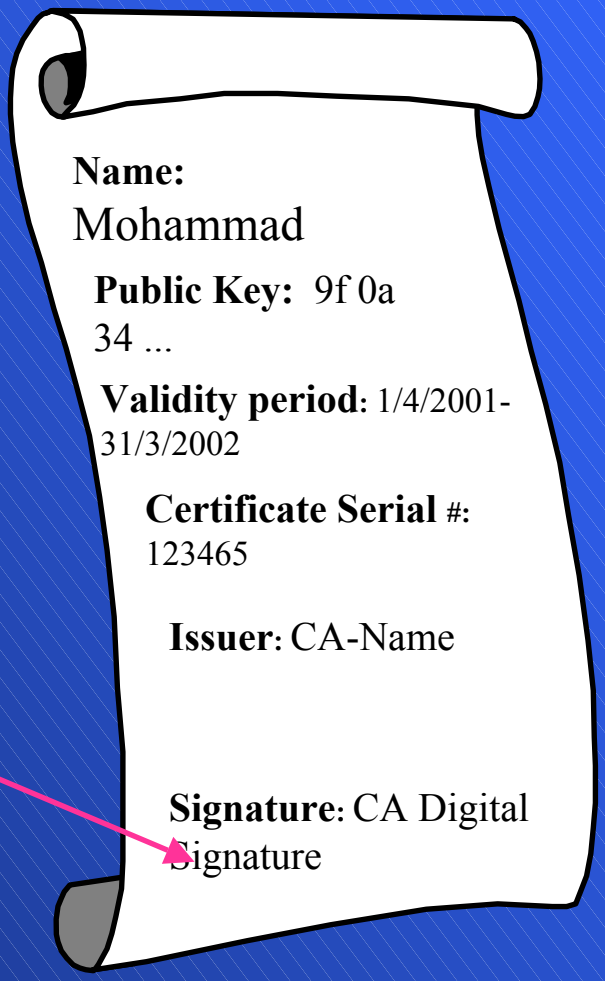
PKI in Saudi Arabia

How PKI works

1) You identify yourself to a CA (or registration authority) so that you can be identified officially as person X with public key K.
2) You get your private key (which you keep secret) and public key (which goes with your public certificate).
3) Anyone that needs to identify you can check the "official" certificate which has a CA's signature on it.
4) If a user trusts a given CA, then he should trust the certificates issued by that CA.

How PKI works

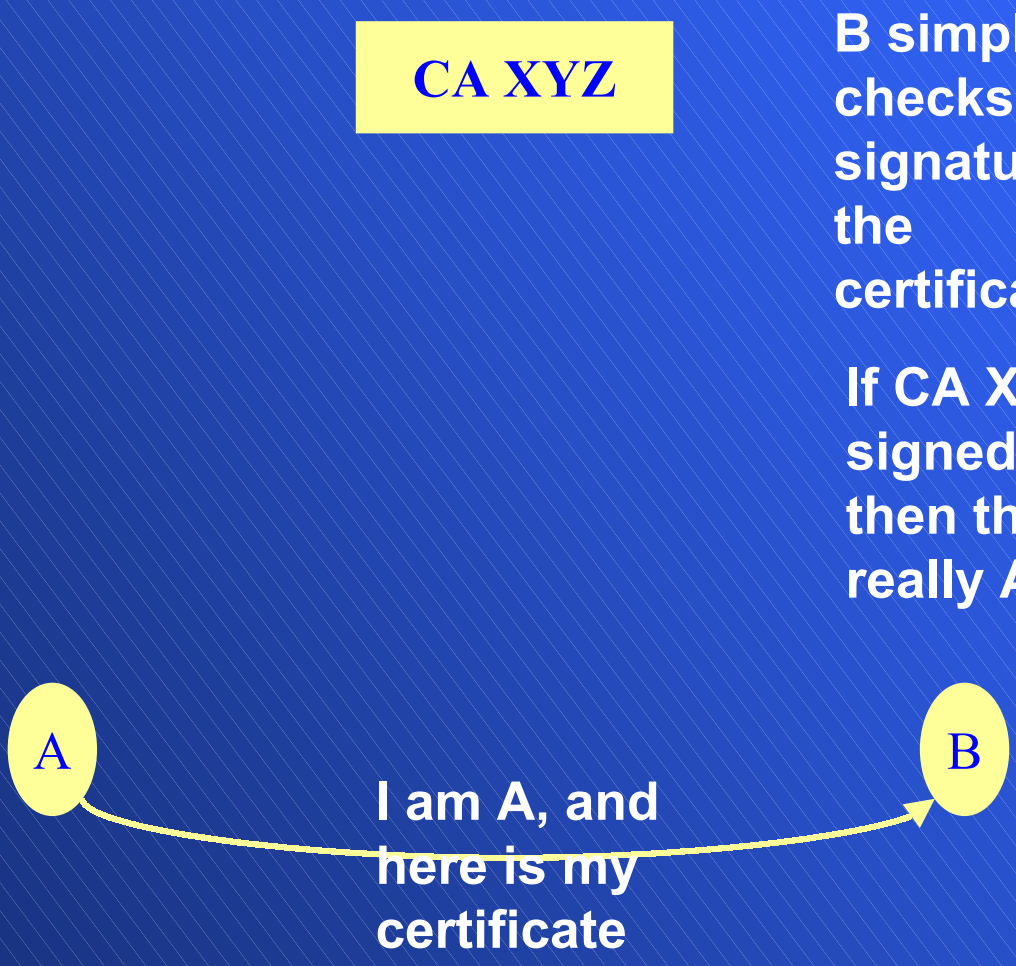
Certificate



Signature of CA means that Mohammad is associated with this public key

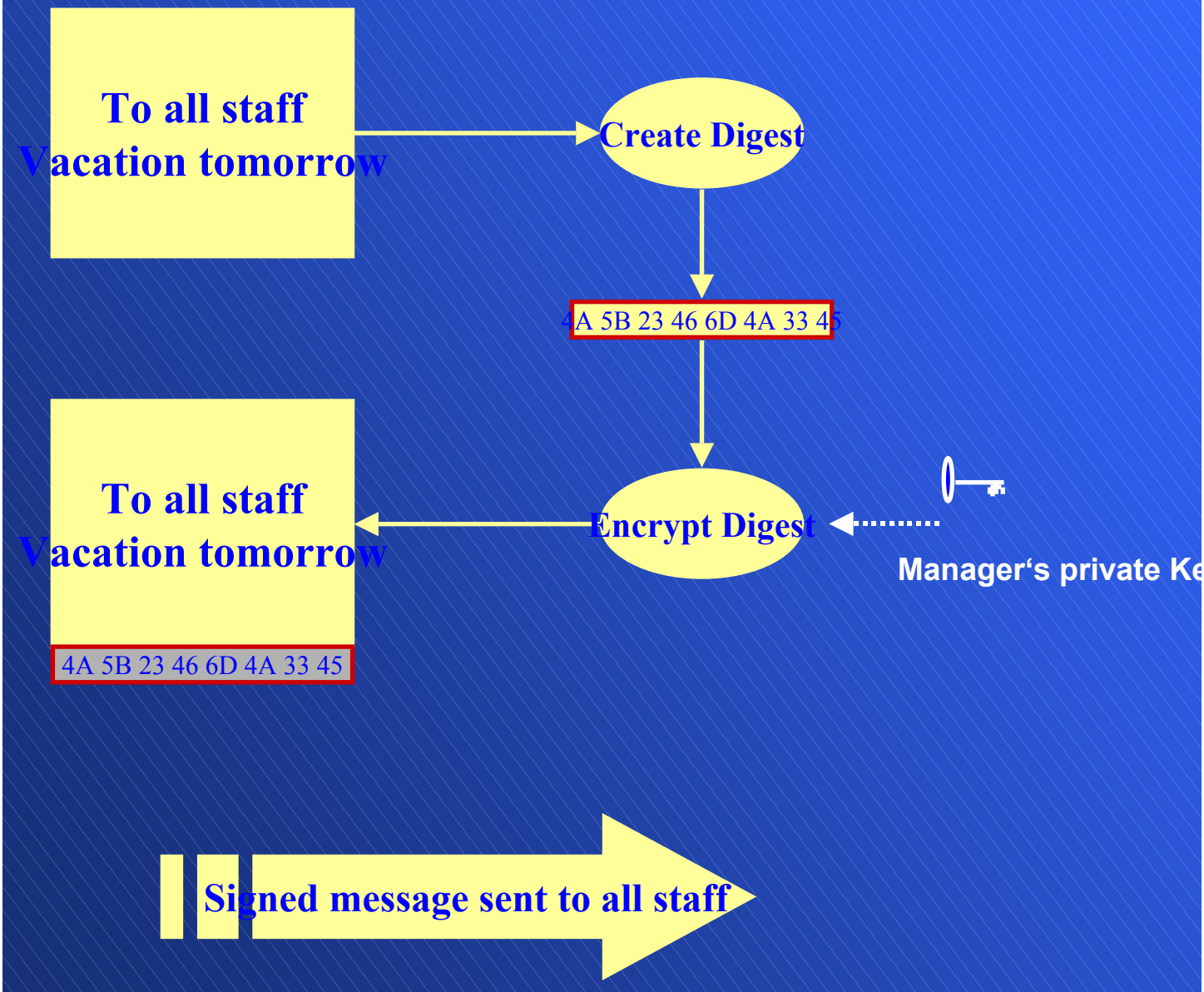
How PKI works

Example: A wants to send private message to B



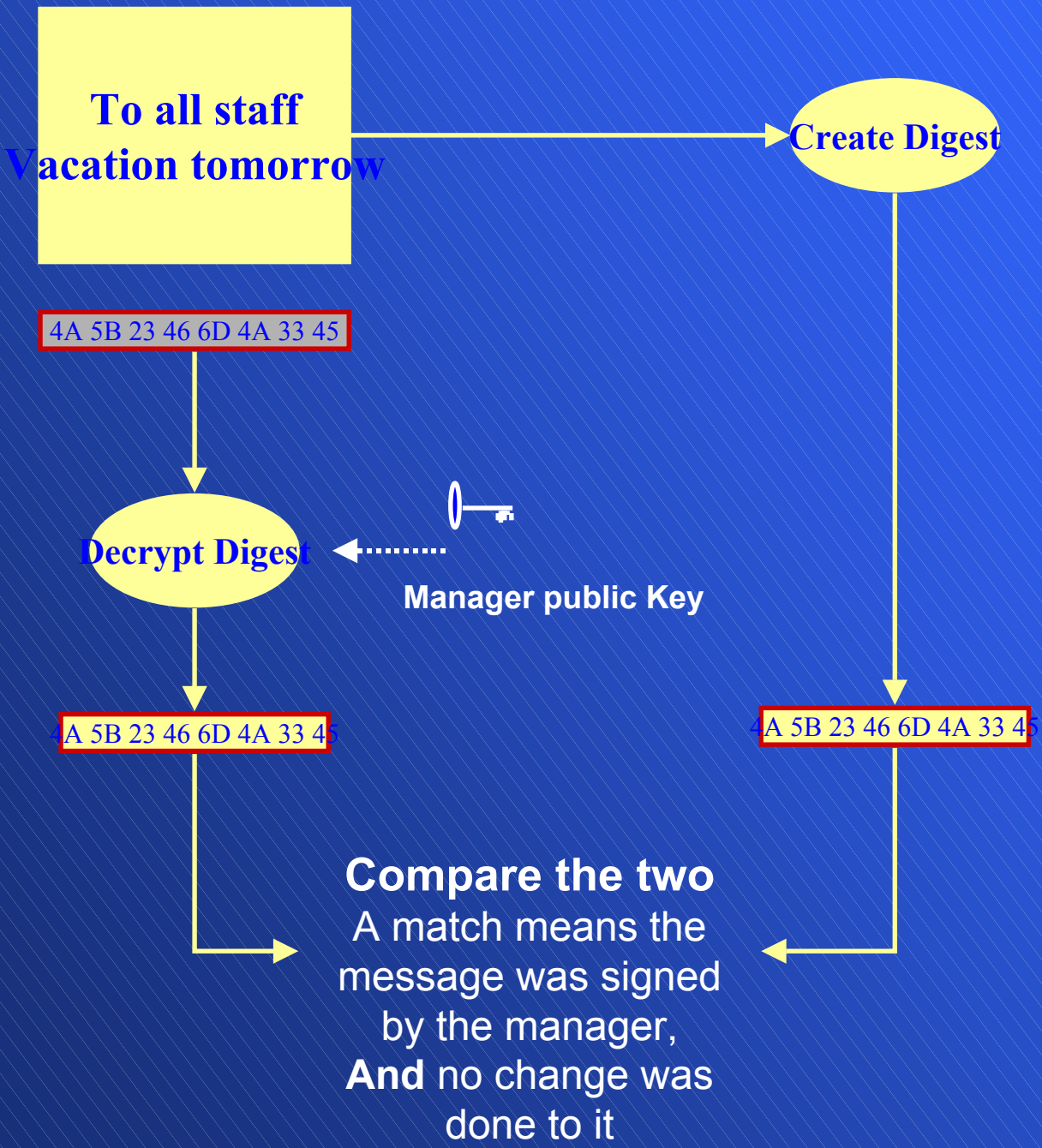
How PKI works

Digital Signature Example: Manager signs announcement



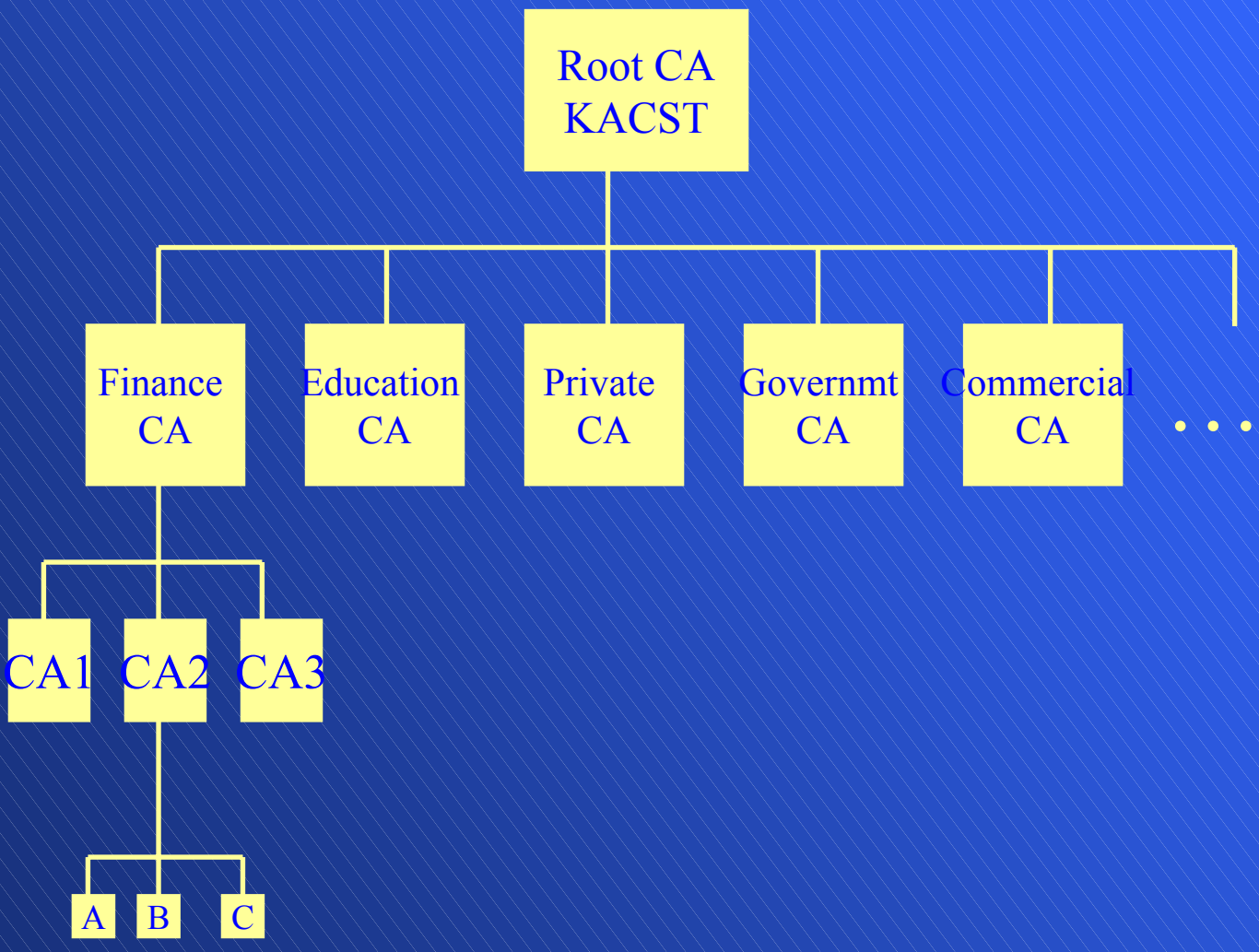
How PKI works

Digital Signature Example: Staff verifies signature



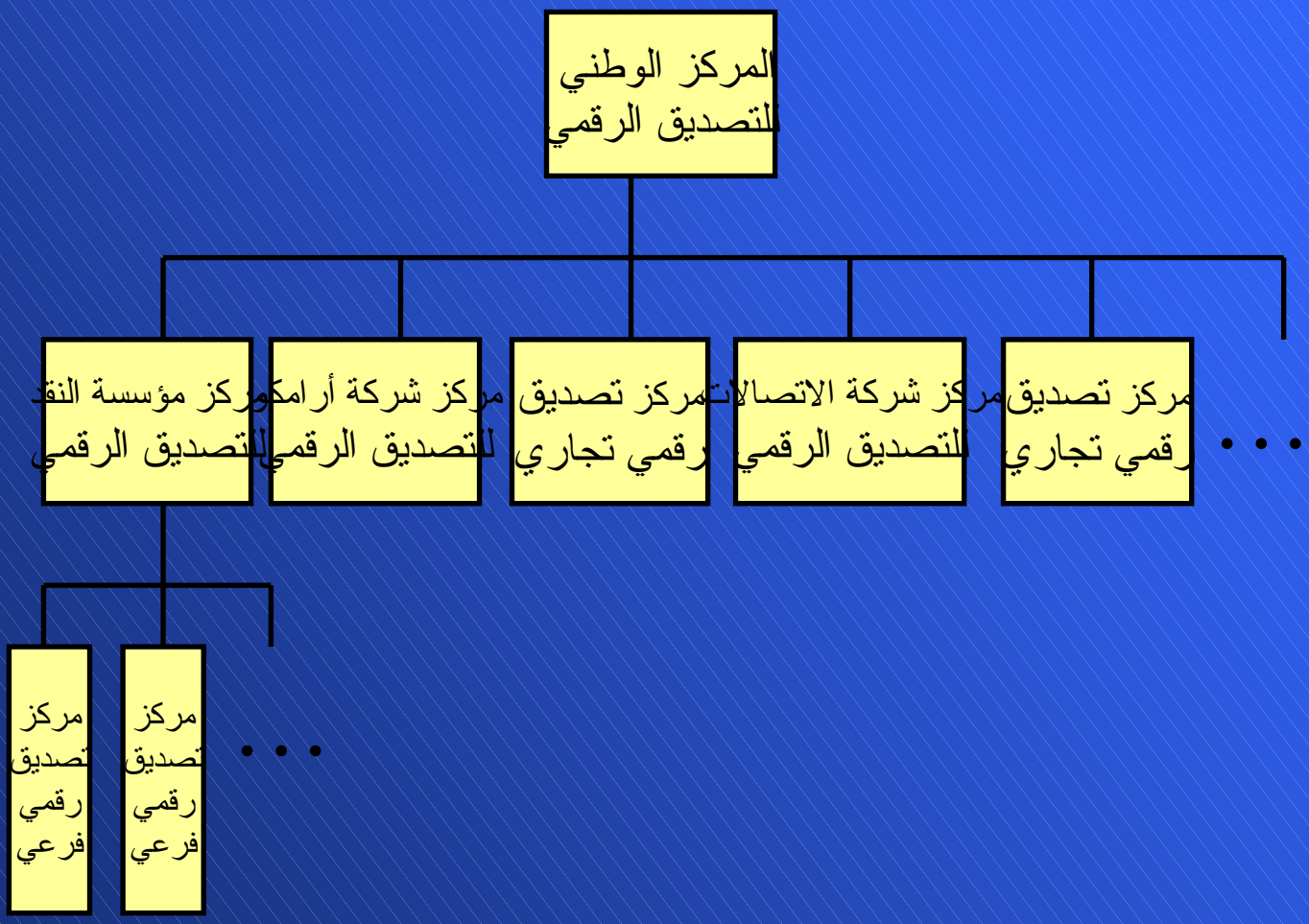
PKI in Saudi Arabia

PKI Structure



PKI in Saudi Arabia

PKI Structure



PKI in Saudi Arabia

Conclusion

1) **There is a high-level committee in charge of overseeing E-business activities in the country**
2) **A number of achievements have been recorded thus far**
   - A number of ongoing PKI projects
   - An electronic transactions act in progress
   - A digital signature law underway
   - Certification policy has been drafted
   - EDI project under-development
   - Government E-procurement system being developed
   - Payment for some public transactions already enabled via Internet
   - A number of awareness programs, conferences, training have been done
3) **There is a need for coordination with other E-business/PKI projects in the Arab world**
   - Similar digital signature laws, E-Business acts, PKI compatibility, etc.