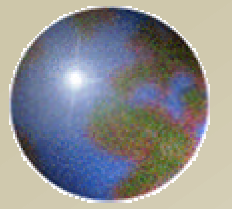
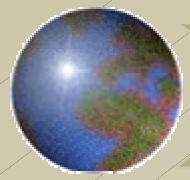


Secure Messaging Workshop

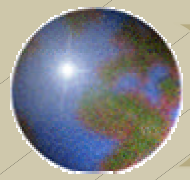
The Open Group Messaging Forum

February 6, 2003



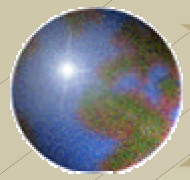
Workshop Facilitators

- Russ Chung, *American Eagle Group*
- Stephan Wappler, *noventum Consulting GmbH*
- *Wen Fang, The Boeing Company*



Welcome and Introductions

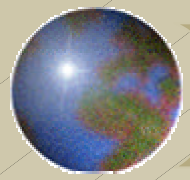
- Name
- Employer
- Job title or duties
- Secure messaging experience:
  - User
  - Messaging administrator
  - PKI administrator
- Specific questions/issues/problems about secure messaging



Workshop Objectives

Upon completion of this workshop, participants will be familiar with:

- Components of a PKI
- Establishing and maintaining trust relationship
- Installation, configuration of certificate servers
- Issuing certificates
- Installation of client certificates
- LDAP schema, database, and records management



Workshop Scenario

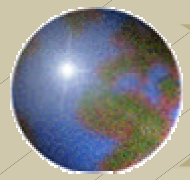
- We start with an unencrypted messaging network:
  - Exchange 2000 / Outlook 2002
  - Lotus Domino R 5.0.10 / Notes R5.0.10
- During the workshop, we will install/configure:
  - Certificate servers
  - LDAP servers
  - Client certificates
- During the workshop, we will discuss/demonstrate:
  - Open LDAP
  - Open SSL
  - Boeing LDAP Proxy

Agenda

Components of PKI	Russ
Establishing Trust Relationship	Stephan
Domino - Certificate Authority	Russ
Domino - LDAP	Stephan
Notes - Client Certificate Install	Russ
Windows 2000 Certificate Server	Stephan
Exchange 2000 Key Management Server	Wen
Outlook - Client Certificate Install	Wen
Boeing LDAP Proxy	Wen
Open SSL	Wen
Open LDAP	Wen
Purchasing a Commercial Certificate	Stephan
Notes work-around: Sending encrypted e-mail	Stephan

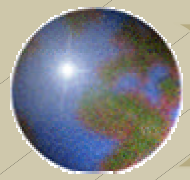
Basis for Secure Messaging

- Encryption: public key algorithms and hash functions
- Secure public key infrastructure (PKI), which supports key exchange
- Software which supports secure messaging functionality (e.g. email-clients or plug-ins)
- Policies, procedures and agreements to establish and maintain trust in the system
- Optional: special devices e.g. a smart card and a smart card reader or an USB token



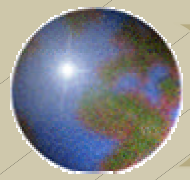
Components of a PKI

- Encryption
  - Symmetrical keys
  - Asymmetrical keys
  - Encryption algorithms
- Digital Signatures
  - Hash functions



Components of a PKI

- Certificates
- Certificate Policy
- Certification Practice Statement
- Relying Party Agreement



Components of a PKI

- Certificate Authority (CA)
- Registry Authority (RA)

  - or -

  Local Registry Authorities (LRA)
- Directory Service
- Time Stamping (as an additional service)

Certificate Authority Tasks

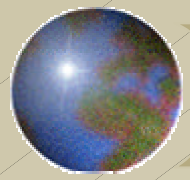
- A CA has to generate the certificate based on a public key. Typically a CA generates the pair of keys on a smart card or a USB token.
- It guarantees the uniqueness of the pair of keys and links the certificate to a particular user.
- It manages published certificates.
- Lastly, a CA is part of cross certification with other CAs

Registration Authority Tasks

- A RA has two main functions:
  - To verify the identity and the statements of the claimant
  - To issue and handle the certificate for the claimant

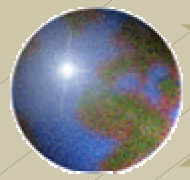
Directory Services

- The directory service has two main functions:
  - To publish certificates
  - To publish a Certificate Revocation List (CRL) or to make an online certificate available via the Online Certificate Status Protocol (OCSP)



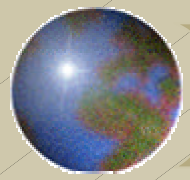
Notary / Time Stamping

- Time Stamping is a special service.
- Time Stamping confirms the receipt of digital data at a specific point in time.
- Time Stamping is used for contracts or other important documents where a receipt needs to be confirmed.



Implementation

- Many technical and organizational activities have to be performed before secure messaging is possible.
  - The organizational work is the larger and the more critical part.

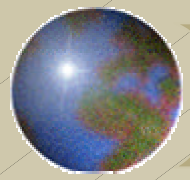


Technical Activities

- Gather the technical requirements for a PKI solution and secure messaging software
- Decide on whether to buy or develop
- Select the hardware and software for the PKI solution and secure messaging solution
- Install and test the system
- Upgrade the network infrastructure and implement the selected solutions

Organizational Activities

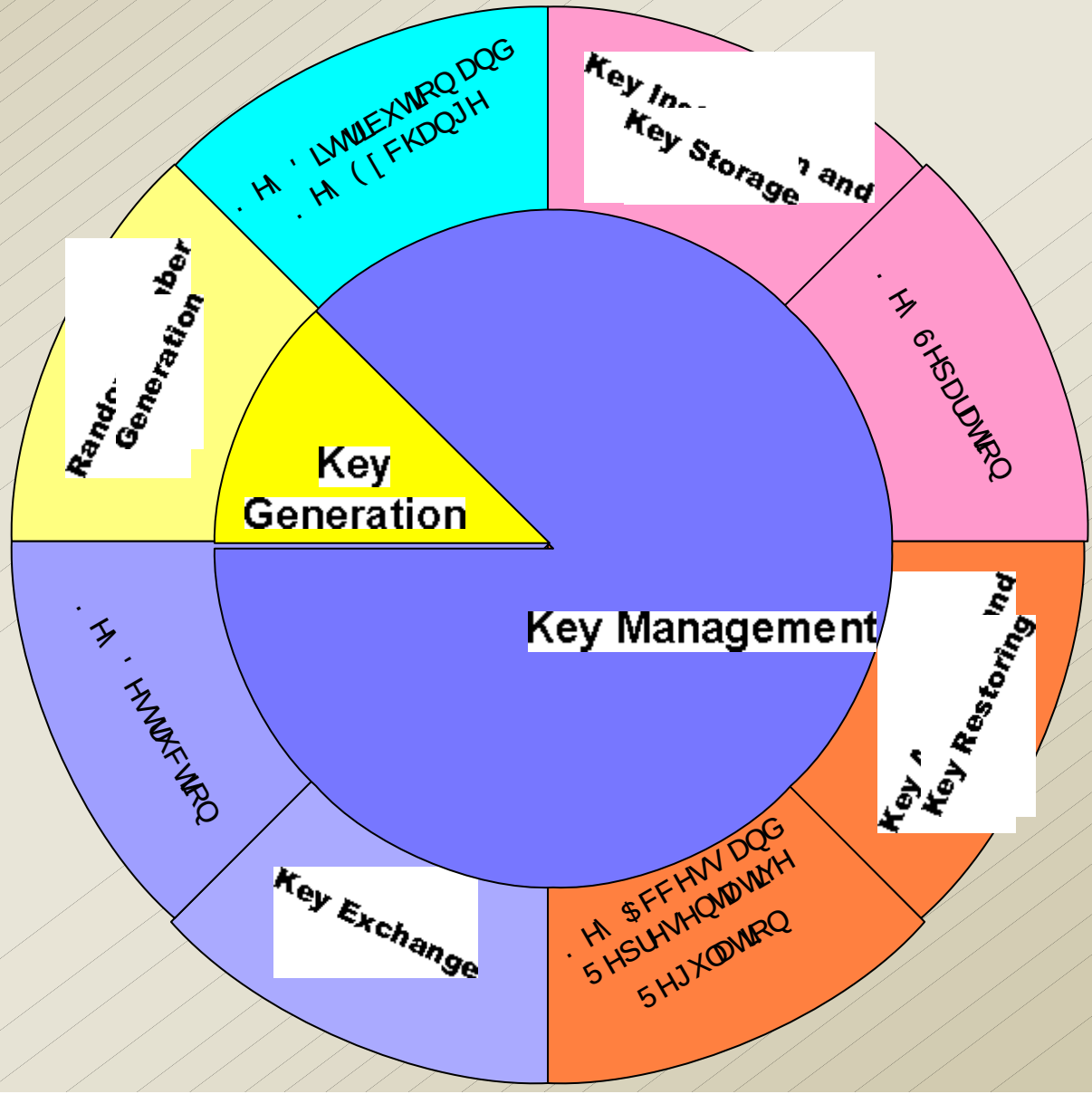
- Compile the requirements and come up with a concept of how to operate with and utilize keys:
  - Key generation
  - Key management
    - Distribution and exchange of certificate and private key
    - Key separation
    - Archiving of the certificate, and if necessary, the private key
    - Change and validation of certificate and if necessary, the private key
    - Manage the access to and representative use of the certificate and private key
    - Freezing and destruction of certificates



Organizational Activities

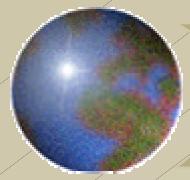
- Definition of Certification Practice Statement (CPS)
- Development of a security concept for the CA and security policies
- Actions in case of suspected or recognized compromise of the Private CA Key
- Responsibility, representative regulation, storage, validity of Private CA Signing Key

Summary



Let‘s talk about…

- Parts of a PKI - Solution
- Key Generation and Key Management
- Conclusion of the necessary Measures



Parts of a

PKI - Public Key Infrastructure