

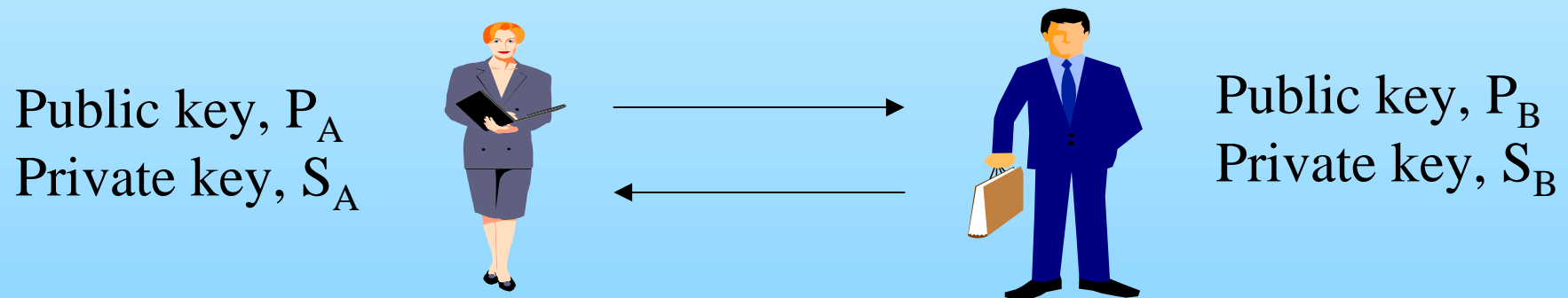
# Security Policies and Trust Management

T. Pedersen  
Cryptomathic A/S  
Denmark

# Outline

- Public Key Infrastructure
  - Need for certificates
  - Roles in a PKI
- Need for trust management
  - reasons for (not) using a certificate/CA
- Goals for trust management
- Design considerations
- Demonstrator

# Public Key Infrastructure



Sign using  $S_A$   
Encrypt under  $P_B$

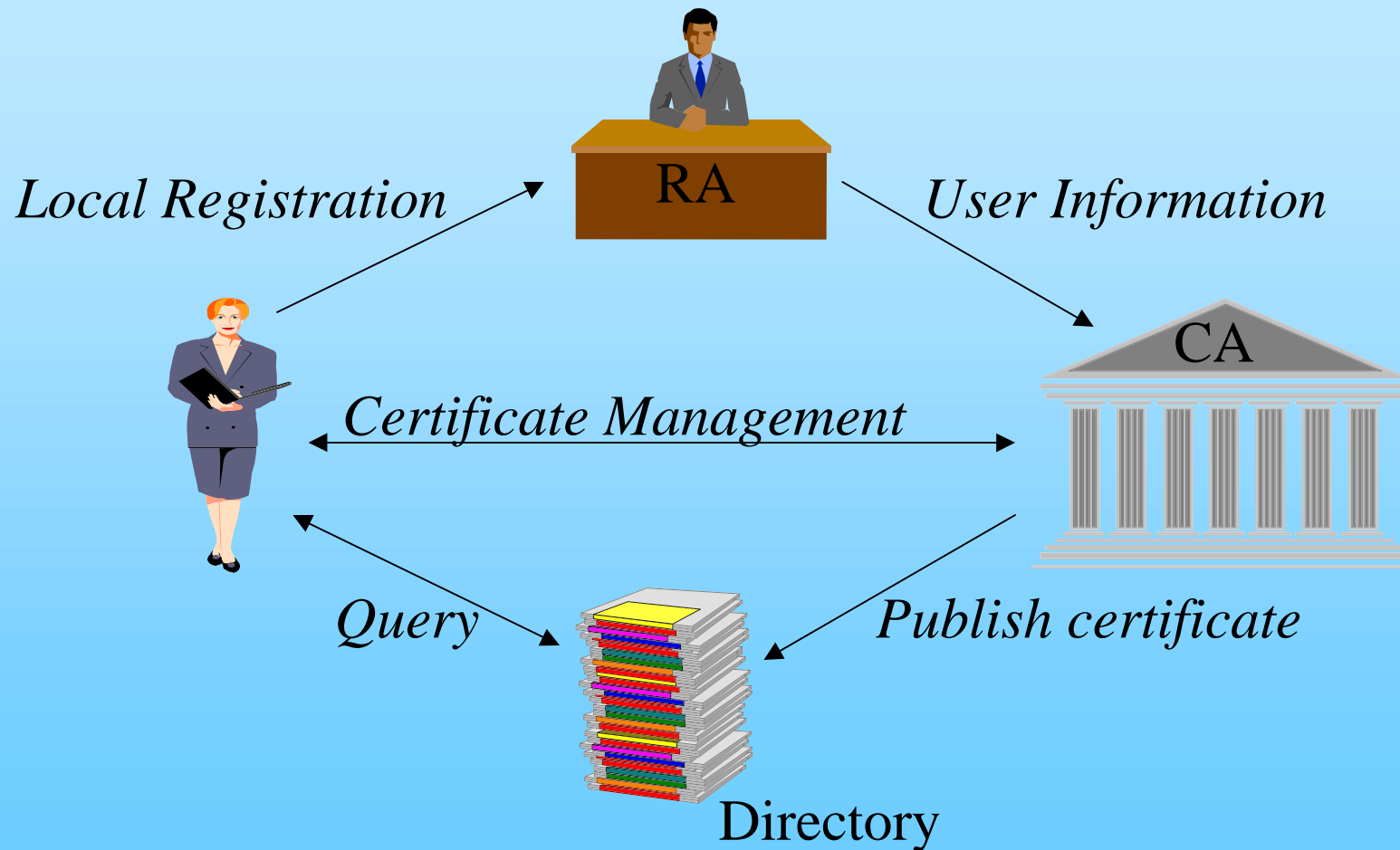
Decrypt using  $S_B$   
Verify signature using  $P_A$

## PKI (cont.)

- Public key is the digital identity
- Questions
  - Sender: who can decrypt message?
  - Recipient: who signed message?
- Public key certificate provides link:

Public key  $\longleftrightarrow$  Identity

# PKI (cont.)



# Trusting (using) a PKI

Is the information in the certificate correct?

- How did the RA validate the information
- Is the information still valid
  - how can a certificate be revoked
  - distribution of information about revoked certificates

Quality of PKI essential

# Using a certificate

What can the certificate be used for

- restrictions on usage
- liability

Information in the certificate:

- real name (versus pseudonym)
- personal ID number
- account number

# Goals for trust management

Specify and use requirements on

- which certificates can be used - and when
  - users own certificates
  - certificates received from other users
- when new certificates from a CA can be accepted
- is on-line verification necessary (directory or CA)



# Goals (cont.)

## Option 1: Always ask user

- to select a certificate to be used
- before accepting a new certificate

## Option 2: Let user specify default certificate (always selected)

## Option 3: Let user specify

- which certificates to use when
- requirements on accepting new certificates

## Goals (cont.)

Option 3 allows for automatic certificate handling:

- server side
- client side

However, manual trust management can (should) not be excluded

# Design Considerations

What does it mean to specify when a CA/certificate can be used

- User certificates
  - certain (types of) applications
  - in sessions with certain users
- CAs and received certificates
  - certain (types of) applications

# Design (cont.)

Need functionality for

- installing new CAs
- specifying policy (for CAs and certificates)
- viewing policy
- selecting certificates, that can be used
- deciding if received certificate are acceptable
- negotiation of certificates

# Design (cont.)

## Situation class:

Describes situation where target (certificate/CA) may be used

## Policy:

List of Situation objects associated with target

## Requirement (interaction with user):

Given target find all Situation objects

Given Situation object find all targets

# Design (cont.)

## Testing if policy is met

- Need description of session (the actual situation)
- Methods for testing if actual situation satisfies situation object in Policy

# Selection of Certificates

Possible to select certificates based on users policy.

**INSUFFICIENT!**

Applications may have additional requirements, such as

- SECA
- special PKI properties (e.g., on-line verification)

## Selection (cont.)

Input for selection (generated by calling entity):

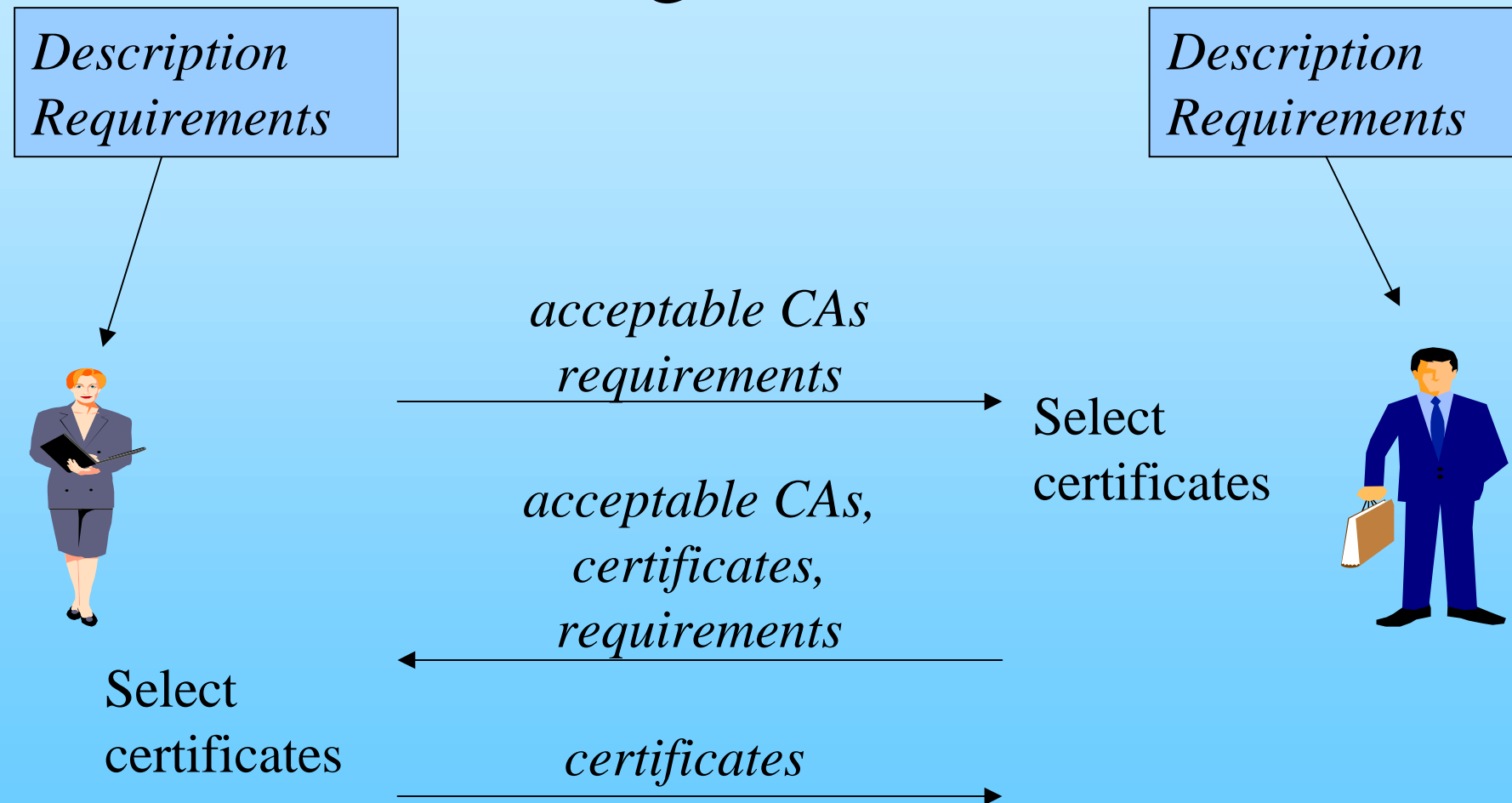
- Description of actual situation
- Requirements from application

Selection procedure:

- Retrieve target satisfying actual description and matching requirements from application



# Negotiation

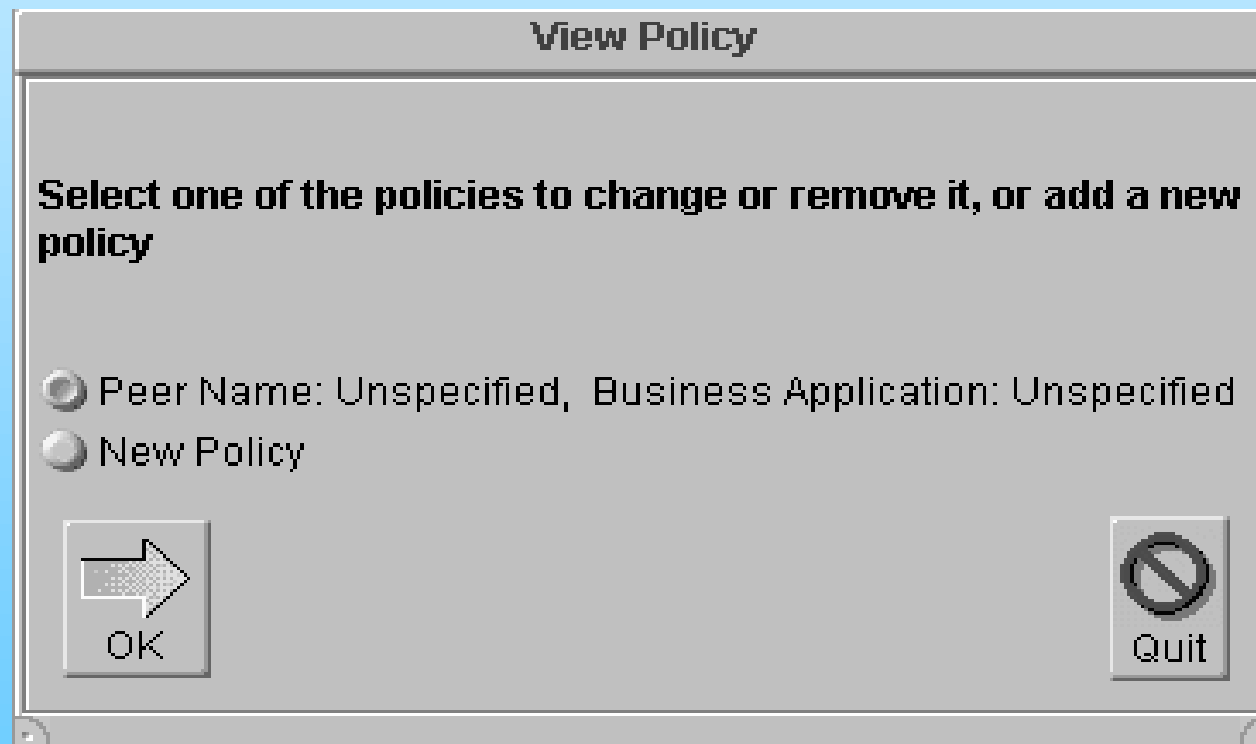


# Other Approaches

Some trust management in browsers and email clients

- Example (Netscape):
  - specify that CA can be trusted for e-mail, network sites
  - certificates for signed applets
  - SEMPER trust management is a natural extension

# Some screens




## Some screens (cont.)

**Change Policy**

Enter changes.  
To remove the policy leave the fields blank.

Peer Name

Business Application

## Some screens (cont.)



# Conclusion

- Define purpose of trust management
- What is needed for certificate selection
- Partly implemented
  - specification of policy
  - selection/negotiation
- Natural and necessary extension of trust management in browsers