Trust Models In ICE-TEL

Andrew Young
Nada Kapidzic Cicovic
David Chadwick

Interworking Public Key
Certification Infrastructure for
Europe

European IVth Framework Project under the TELEMATICS Programme

THE UNIVERSITY OF SALFORD

COST
Computer Security Technologies

Overview

- A quick look at public key authentication
- Comparison of existing trust models
- ICE-TEL, the best of both worlds
- Examples

Public Key Authentication

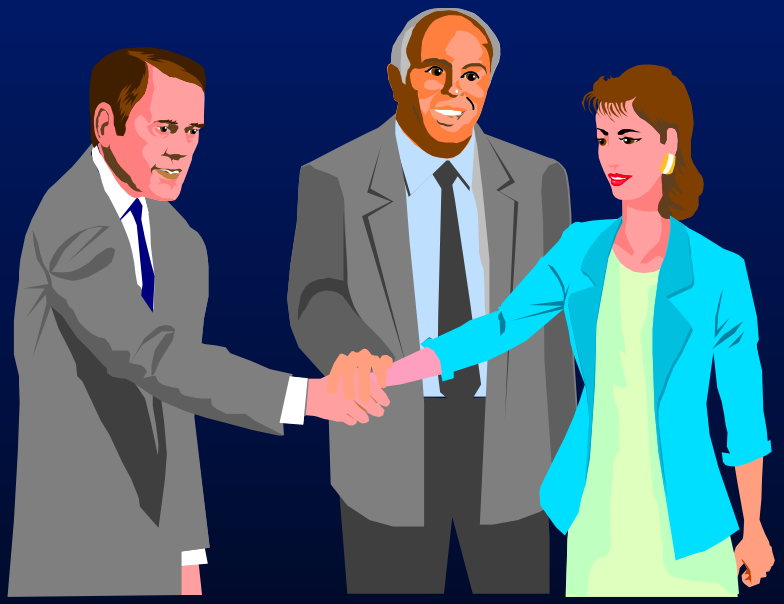
- To verify a digital signature, I need
  - the signer's public key
  - to be sure who "owns the public key"
    - (i.e. who knows the corresponding private key)
- Certification
  - Third party assertion of "who owns which public key"
- Which third parties do I trust?
  - On what basis do they make their assertion?
  - What guarantees do they give? Liability?

Certification

- Third party issues certificate, comprising:
  - Who is doing the asserting (issuer)
  - Who is the subject of the assertion
  - What is being asserted (public key)
  - The small print (certification policy)
  - Digital signature
- Syntactic check of certificates tells me if the public key is accurate
- Semantic check of policies tells me who the public key belongs to
  - or what can be done with it

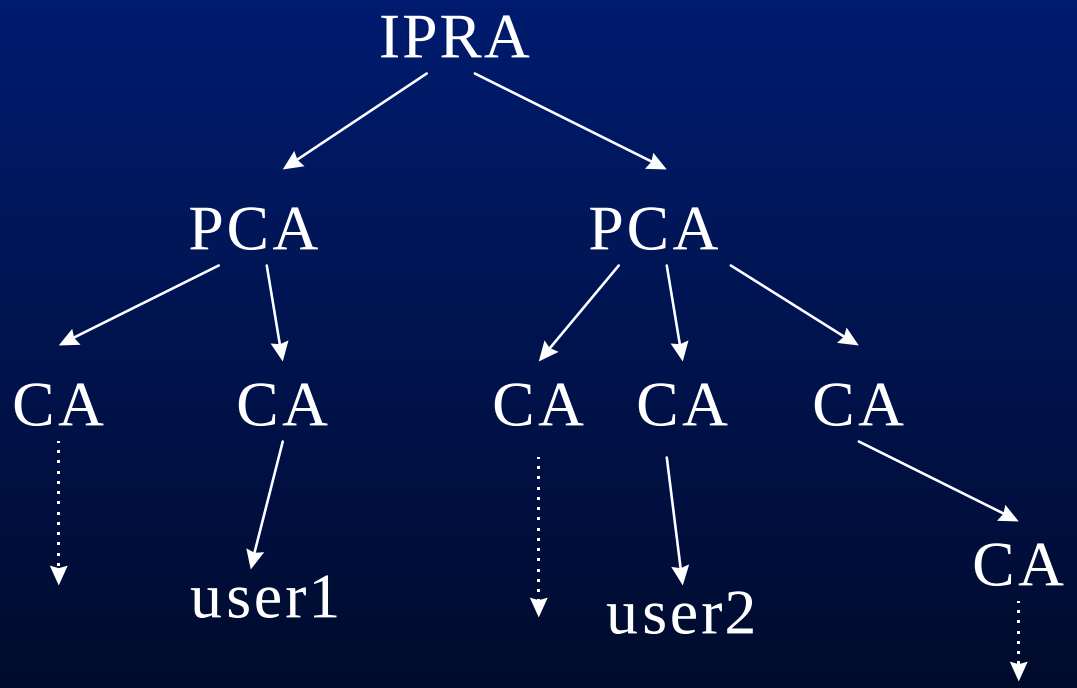
PGP Trust Model

- Web of trust
- Third party is “Trusted Introducer”
- Introducer does not have a “policy”



PEM Trust Model

- CA hierarchy
- PCAs publish a “certification policy”
- IPRA ties the PCAs together



The Gap in the Market

- PGP is user-centric
- PGP does not scale up to large communities
- PEM is organisation-centric
- PEM does not scale down to small communities

The ICE-TEL Trust Model

- Supports diverse security domains
  - single users
  - simple groups or small organisations
  - complex organisations
- Supports organic growth, allowing reorganisation of domains
- Trust between domains is by choice, and need not be mutual or transitive
- No central infrastructure

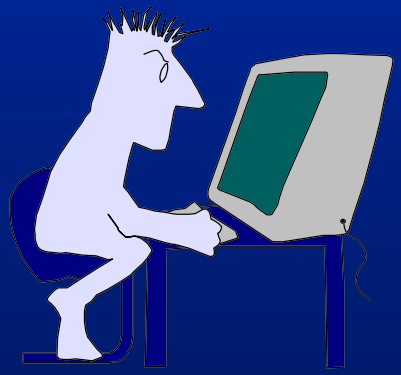
Trust Points

- Each security domain contains trust points
- A trust point is a CA with an advertised policy
- Security domains interlinked by cross-certification among trust points
- User advertises certification path to trust point
- Trust point advertises the cross-certificates it has issued

Personal Security Environment

- Each user securely stores
  - the public key of a trusted user
  - the public key and policy of a trusted CA

Example - two users

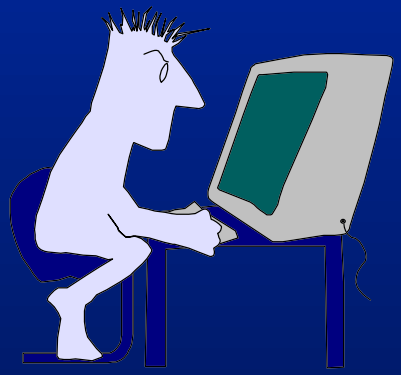


User A

User B

- User A obtains user B's public key by "secure means" and stores it in his PSE.
- User A can autheticate messages from user B
- User B need not do anything
- No policies involved

One user and a small company

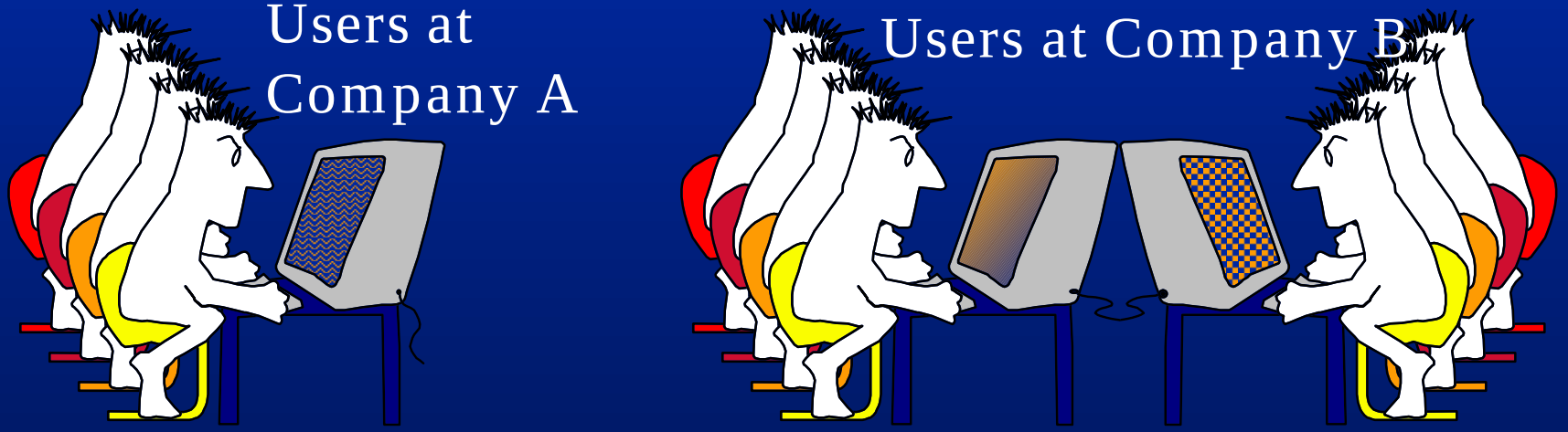


User A

Users at Company B

- Company B creates a CA and publishes a policy
- User A obtains company B's CA's public key and policy and stores it in his PSE.
- User A can autheticate messages from users in company B

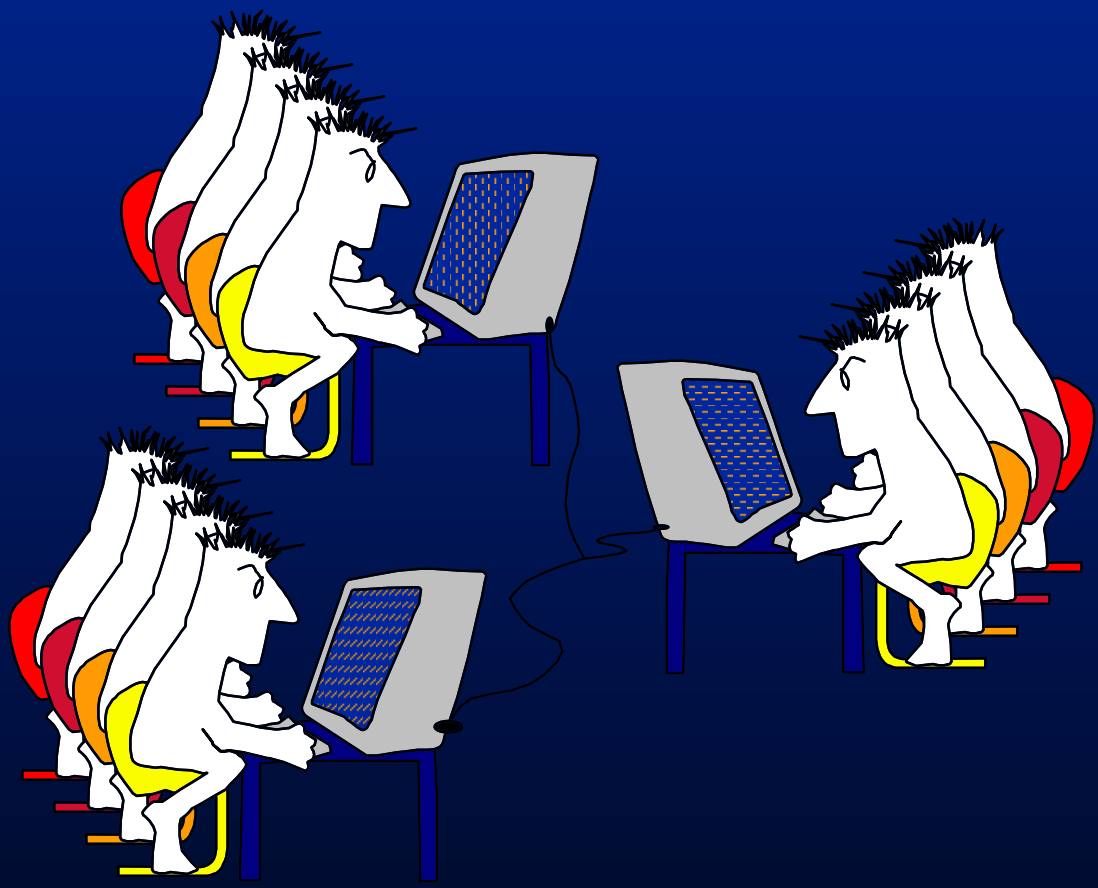
A small company and a big company



- Company B creates a CA hierarchy and publishes a policy for the root CA.
- Company A's CA issues a cross-certificate for Company B's root CA
- Users in company A know their CA's public key and policy.
- Users in company A can autheticate messages from users in company B

Organic growth

Users at Company B



Conclusions

- Scalable deployment model
- Flexibility permits reorganisation
- Supports embedded high security domains
- Explicit use of CA policy

For more information on ICE-TEL

http://www.darmstadt.gmd.de/ice-tel/ice-home.html

Interworking Public Key Certification Infrastructure for Europe

European IVth Framework Project under the TELEMATICS Programme

- 17 partners from 13 countries
- Build and operate CA infrastructure
- Build and pilot secure applications WWW, S/MIME, X.500
- Software from Cost, GMD, Isode, SSE