



# **Centralised Trust Management in Applications**

**Amsterdam, 16 Feb 2004**

**Massimiliano Pala  
Politecnico di Torino**

**- TF-Emc2 Meeting -**



# How Trust is Built into Applications

- Today Applications still rely on Trust Lists
  - Browsers
  - MUAs
- Two main effects of Trust Lists
  - There is no way for the final user to verify all the policies of the pre-installed certificates
  - Users are scared when prompted for a new certificate to be added to the list
- Trust Lists push users to accept certificates by “faith” (i.e. Wrong Reasons)
- Is the name “Trust Lists” really suitable ?



# Trust Models

- **What Trust Models are available today?**
  - **Trust Lists (Most Diffused in Apps)**
  - **Hierarchies (Easy for Developers)**
  - **Bridge-CAs**
  - **Cross-Certification**
  
- **Is there a way to avoid Trust Lists by using currently supported trust models supported by today applications ?**



# Introduction

- **We would like to:**
  - **Avoid the usage of Trust Lists**
  - **Single Point of Trust**
  - **Centralised Trust Management for Apps**
  - **Available in Today Applications**
  
- **Requirements:**
  - **Our solutions best fits into organisations (such as NRENs or Universities) where a PKI is already established**



# The Scenario

- **Let's imagine EuroPKI wants its users to be able to verify all the TACAR's Root certificates**
- **For each of the TACAR's Root CA Certificates, EuroPKI issues a corresponding certificate**
  - **It is a sort of Cross-Certificate**
  - **It does not need agreements between the two parties (it is one-way cross-certification)**
  - **It is centrally managed**
  - **It is easy to implement (just issue n certs)**

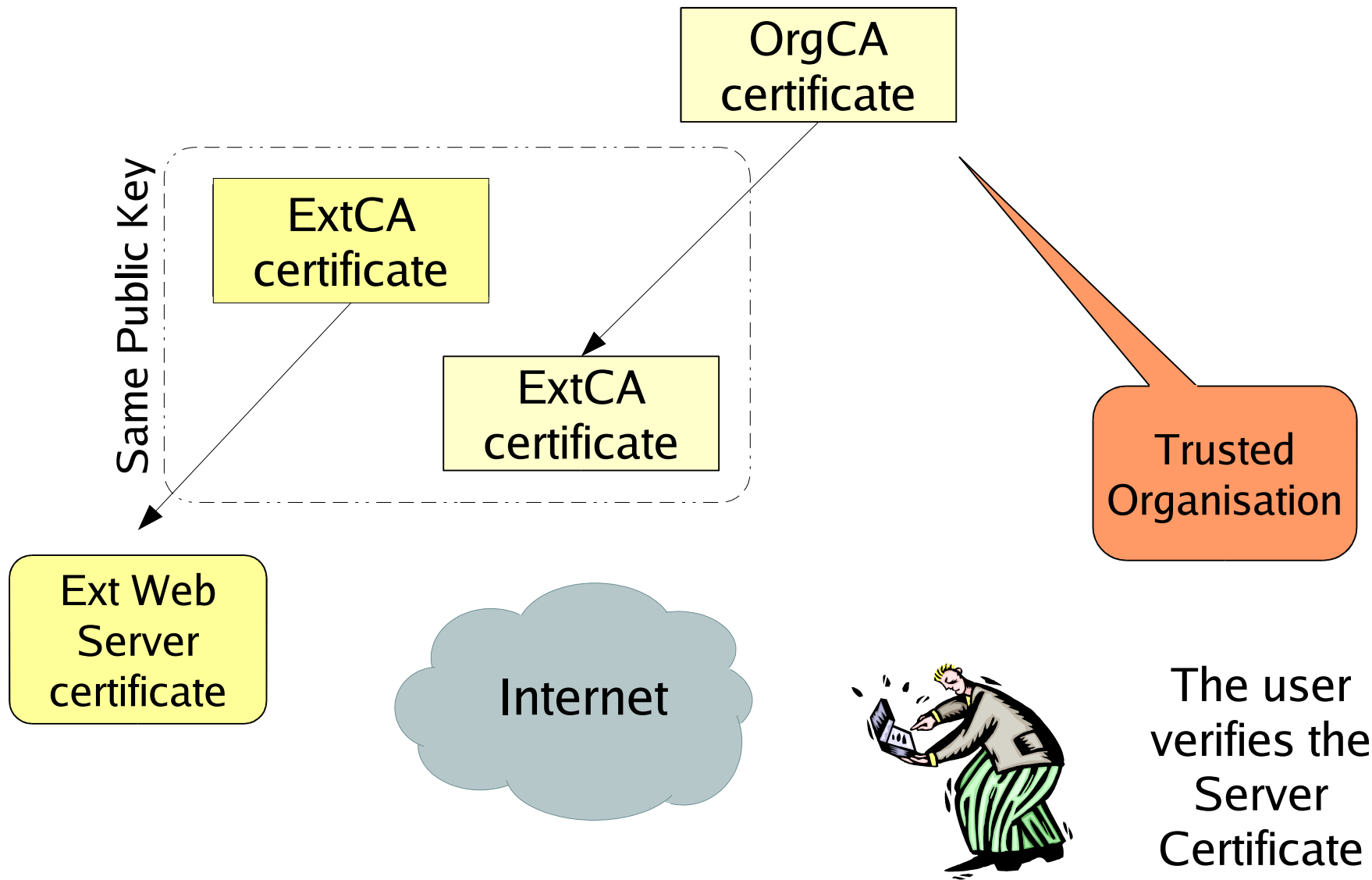


## Example (1/2)

- **My Organisation CA**
  - CN=Organisational Root CA, O=My Organisation, C=IT
- **External Organisation CA**
  - CN=External Root CA, O=Other Organisation, C=IT
  - CN=User Certificate, O=Other Organisation, C=IT
- **My Org Issues the Cross Cert for the External Organisation**
  - **Subject:**  
CN=External Root CA, O=Other Organisation, C=IT
  - **Issuer:**  
CN=Organisational Root CA, O=My Organisation, C=IT



# Example (2/2)





# A good Solution ?

- **No need of Trust Lists into Applications**
- **Central Management of Trust**
- **Fingerprint verification actually performed**
- **Supported on Windows Systems  
(2000/Xp/2003)**
  - **IE**
  - **Outlook**
- **Easy to integrate in OpenSSL based applications**
  - **Statically linked apps will need re-compilation**
  - **Applications using shared libraries just work (e.g. Kmail or Konqueror)**



# Still Open Issues...

- **Cross-Certification not available on Mozilla-Based browsers and MUAs (developers needed)**
- **Policy/Path/Name Constrains Issues (same as in Cross Certification?)**
  - **How to verify the certificate chain by applying RFC-3280 ?**
- **Revocation of “Semi-Cross-Certificates”**
  - **Better to issue certs with short validity period, or**
  - **Revoke Cross-Certificates if no more trusted**



# Still Open Issues...

- **Distribution of “Semi-Cross-Certificates” issues:**
  - **By using os-specific applications (e.g. Pushing all the cross-certificates into the registry)**
  - **By pushing certificates when the organisational portal is accessed by users?**
  
- **More ?**



# Future Plans

- **Better Understanding of Cross-Certification support into applications**
- **Study of specific extensions usage for constrains mediation in semi-cross-certificates**
  
- **It is only an initial work and deep investigation is needed**
  - **Ideas ? Proposals ? Contributions ?**