Hierarchical Organization of Certification Authorities for Secure Environments

Lourdes López Santidrián
Justo Carracedo Gallardo
Objectives

MAIN OBJECTIVE
To propose a Hierarchical Organization of CAS

Aims:

• General MODEL
• Open MODEL
• Easy solution for Certificate Path Validation
Pilot Experiment

EUJT de Telecomunicación

UNIVERSIDAD DE MADRID

Developments:

• Seckit
• SecServer
SecKit

- Generation of keys (DES, RSA)
- Sending of secure files
- Reception of secure files
- Access to the Directory
Pilot Environment
MODEL [3]
Certificate Path Validation [1]
Certificate Path Validation [2]

CertificationPathIdentifier ::= SEQUENCE OF NewAuthorityKeyIdentifier

NewAuthorityKeyIdentifier ::= SEQUENCE {
  autyType [0] CertificateType,
  autyKeyIdentifier [1] KeyIdentifier OPTIONAL,
  autyCertIssuer [2] GeneralNames,
  autyCertSerialNumber [3] CertificateSerialNumber}

CertificateType ::= BIT STRING {
  groupAuthority (0),
  subgroupAuthority (1),
  certificationAuthority (2),
  user (3) }

NewSubjectKeyIdentifier ::= SEQUENCE {
  subjectType [0] CertificateType,
  subjectKeyIdent [1] KeyIdentifier OPTIONAL}
Certificate Path Validation [3]

[number] represents GeneralName
<Cnumber> represents CertificateSerialNumber

Conclusions and Future Work

- Certificate v3 important step ahead
- Go to a general model
- Formal specification of the policy statements