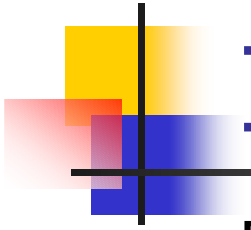
New Security Services Based on PKI

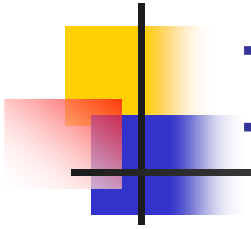
Presented by Jordi Palet
jordi.palet@consulintel.es
Consulintel



Introduction

- PKIs ... key element for providing security to distributed and dynamic networks and services
- New context/new services: End-end security , Mobility, distributed services, resource access control, …

- Actual centralized security paradigm is no more valid in the framework of distributed services. New security model based on "decentralized" architectures.
- Increase the PKI functionalities with support for credentials and authorization support for objects and resource control access.
- IPv6 introduce new needs in the security services



IPv6 needs

- IPsec mandatory for IPv6: need to fully support security services
- IPsec in IPv6 will enable host to server, gateway to gateway and host-2-host, due to abundant supply of address space
- Full range of address allows the end-end communication and the end-end security support
- IPv6 large address space enables new security models, i.e. assign multiple addresses to a single host; local address for local access and global address for Internet access

New Needs

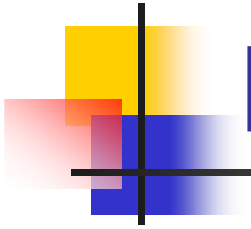
- Pervasive networks need a mechanism to allow users to have seamless, transparent and trusted access to the network resources. Manage not only with authentication aspects but also with privileges and authorization has introduced the need of Authentication and Authorization Infrastructures (AAIs),

- Ad-hoc networks because of their nature they are clearly untrusted, must be also complemented with security phases in order to support real uses of this kind of network. ”Security for automatic configuration of ad-hoc networks”

New needs (II)

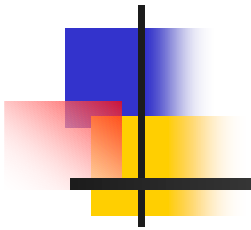
- Enable users to connect to any network access provider, whatever the provider of the subscription may be, an inter-domain security infrastructure like AAA (Authentication, Authorization, Accounting).

- Discovery/advertisement phase in home networking. An incoming node must find out where to connect to the net and should notify its position to the other members in the network "Securing Network Discovery"



PKI support

- PKI and its extension Authentication and Authorization Infrastructures (AAIs) key component
- PKI linked to a Policy Management and distributed environments
- PKI supporting new protocols to query, enforce and manage the security services
- PKI and IPv6
- Mobility, ad-hoc and in general Pervasive networks support



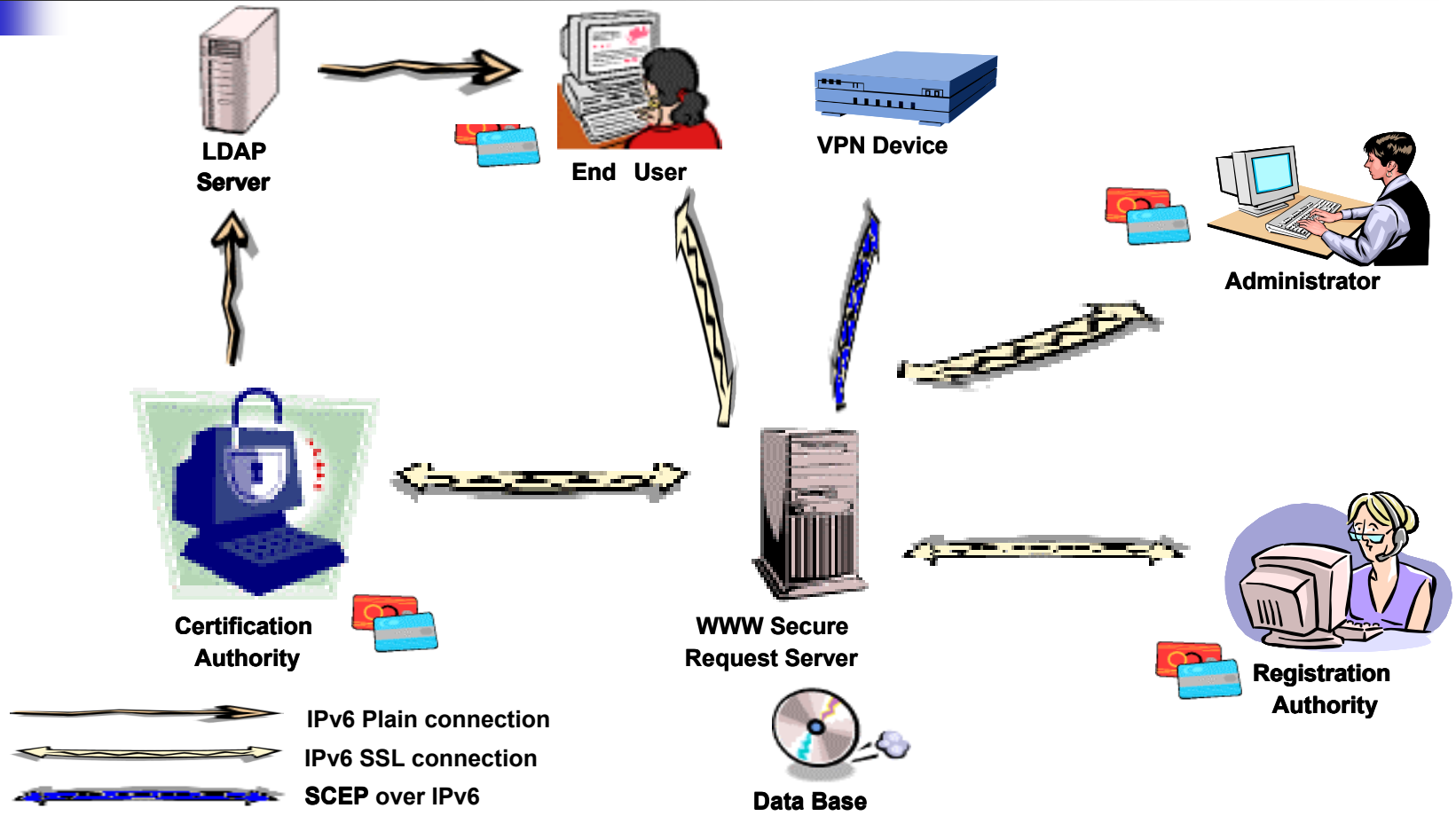
The UMU IPv6 PKI (UMU-PKIv6)

Departamento de
Ingeniería de la Información
y las Comunicaciones

UMU-PKIv6 Description

- Main Objective ... to establish a high security infrastructure for distributed systems
- Main Features:
  - First PKI supporting the IPv6 protocol
  - Developed in Java ➔ running on every Operating System
  - Issue, renew and revoke certificates for every entity belonging to one organisation
  - Final users can use either RAs or Web browsers to make their own certification operations
  - LDAPv6 directory support
  - Use of smart cards (file system, RSA or Java Cards) ... allowing user mobility and increasing security
  - PKI Certification Policy support
  - VPN devices certification support (using the SCEP protocol)
  - Support for the OCSP protocol and Time Stamp
  - Web administration

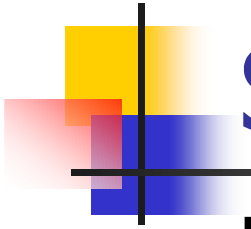
UMU-PKIv6 Architecture



https://pki.ipv6.um.es

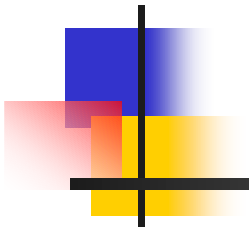
Security Policies

- There is ...
  - high interest in policy-based networking, but
  - no complete systems supporting the specification and deployment of these policies
- Policies used to manage distributed communication systems ... "IF certain *conditions* are present, THEN specific *actions* are taken"
- Security is vital ➔ we sign every policy (using X.509 certificates issued by our own PKIv6)
- We use policies for managing
  - The UMU-PKIv6 itself
  - Secure IPv6 VPNs

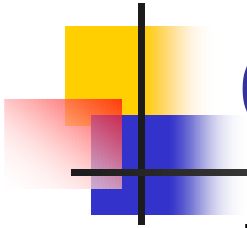


Security Policies for PKIs

- UMU-PKIv6 policies
  - Drive the way the PKIv6 itself works
  - Digital implementation of a Certification Practice Statement (CPS) ... they specify which rules must be applied to requested or existing certificates
  - Digitally signed (integrity and authentication) normally by the CA private key
  - Centralised creation process driven by the PKI admin
  - Distributed use by RAs and other PKI components
  - Categories:
    - Certification rules
    - Re-issuance rules
    - Revocation rules



Conclusions



Conclusions

- New security network management paradigm based on policies
- New Architectural elements for authorization management
- End-End security needs and distributed security environments
- PKI and AAI as one of the central component of the security framework
- UMU-PKIv6 ... provides a common trustworthy point for new distributed services

Departamento de Ingeniería de la Información y las Comunicaciones

New Security Services Based on PKI

Antonio F. Gómez Skarmeta
Gregorio Martínez Pérez
{skarmeta,gremar}@dif.um.es

University of Murcia
SPAIN