## 2A2 PKIX-based Certification Infrastructure Implementation Adapted to Non-End Entities

Eduardo Jacob, Fidel Liberal, and Juanjo Nunzilla, University of the Basque Country, Spain

**Abstract:**

Public Key Infrastructures are considered the most suitable systems to provide basic security services through the use of digital certificates. Nevertheless, the traditional way of operation, based on web interface and asynchronous interactions, as well as the cost and difficulty of registration processes, have caused their replacement by another systems in many of the scenarios for which PKIs were conceived. These more efficient solutions generally present laxer security mechanisms and require too much user knowledge. The system we propose tries to provide a bridge between both approaches by defining an automated PKI focused on specific application scopes by using on-line interaction procedures. We will explain a PKI system we have developed that is oriented to provide advanced certification services. This work tries to be compliant with protocols defined in PKIX standards. One very important point in our work is that these RAs, after performing user authentication and validation, will mark users' requests as valid and forward them to the CA, which will process them automatically, with no human agent intervention. The rationale behind this is to try to automate and speed the generation, transport and installation of the certificates in applications.

The system will also provide validation services through OCSP protocol use. The RA will again have a proxy-capability, acting as an authorised OCSP responder. In addition to providing on-line validation methods, our CA will periodically issue appropriate CRLs that will be stored in the repository (a LDAP directory service) with issued certificates. In contrast to traditional architectures, typically oriented to provide final services to human users (generally through a web interface) our PKI is focused on easy integration of applications or services that might benefit from the use of a certification infrastructure.