

2A1 New Security Services Based on PKI

Antonio Gómez Skarmeta, Gregorio Martínez, and Óscar Cánovas, Universidad de Murcia, Spain

Abstract:

The basic job of a Public Key Infrastructure, PKI for short, is to define the mechanisms used both to allow a recipient of a signed message to trust a digital signature and to allow a sender to find the encryption key for a recipient. It is comprised of those elements needed to manage and enable the effective use of public key cryptography technology particularly on a medium and large scale.

Nowadays, PKIs are being considered a key element for providing security to new distributed communication networks and services. In this paper, we describe two of these innovative security services built over our own designed and implemented Java IPv6 PKI: a distributed security policy management architecture and a distributed credential management system.