Distributed Private Key Generator for ID-Based Public Key Infrastructure

Pance Ribarski and Ljupcho Antovski

Faculty of Computer Sciences and Engineering,
Skopje, Macedonia
{pance.ribarski,ljupcho.antovski}@finki.ukim.mk

Abstract. We recognize the need of certificateless PKI to reduce the step of obtaining the public key. This leads to ID-Based cryptography where we have PKI with full power to generate private keys for any identity. We solve this problem by implementing distributed key generation to form a group of players which will act as private key generator for ID-Based PKI. The implementation is done on the Android platform, showing the possibilities of running PKI on cheap and widely available hardware.

Keywords: distributed key generation, ID-Based cryptography, PKI, implementation, Android