Upotrebom digitalnih sertifikata do sigurnog pristupa servisima

Dokument sadrži uputstvo za postupak zahtevanja serverskih SSL digitalnih sertifikata u AMRESu, njihovu instalaciju na Linux i Microsoft platformama i korištenje u svrhu zaštite pristupa web, mail i radius servisima.

AMRES BPD no	**106**
Tematska grupa/Working group	Sigurnost/Security
Kategorija dokumenta/Category	Uputstvo/Cookbook
Naslov originala	**Upotrebom digitalnih sertifikata do sigurnog pristupa servisima**
Originalna verzija/datum	Revizija 1 (dokumenta iz septembra 2010.)/ 21. april .2011.
Originalna verzija dokumenta na srpskom jeziku	PDF
Title	**Cookbook for securing a service access with digital certificates**
Version/date	Revision 1 (of the document dated September 2010)/ 21. April 2011
English version	PDF
Dodaci/Appendices (Serbian only)	
Dodatak B	SSL protokol
Dodatak C	EAP-TTLS protokol

Rezime

Dokument promoviše usvajanje digitalnih sertifikata u institucijama ?lanicama Akademske mreže Srbije kao na?ina za uspostavljanje sigurnih kanala komunikacije.

Da bi korisnici prilikom preuzimanja ili slanja podataka na neki server imali zašti?enu komunikaciju, moraju biti sigurni da su zaista pristupili onom serveru kojem su imali nameru da pristupe i da niko ne može pro?itati i/ili promeniti podatke koji se šalju ili primaju. Upotreba digitalnih sertifikata u kombinaciji sa SSL tehnologijom omogu?ava pomenutu sigurnost.

Opisane su komponente PKI infrastrukture, ali i na?in realizacije PKI funkcija na primeru uklju?ivanja AMRESa u TCS (TERENA Certificate Service) servis. Navedene su i razli?ite potrebe za korištenjem PKI u NRENu, koje zahtevaju razli?ite tipove digitalnih sertifikata, ali je posebna pažnja posve?ena korištenju PKI infrastrukture, odnosno digitalnih sertifikata u kombinaciji sa SSL tehnologijom u svrhu me?usobne autentifikacije servisa i njihovih korisnika.

U dokumenta je objašnjen postupak pribavljanja serverskog sertifikata – generisanje klju?a, formiranje sertifikata, priprema za/i podnošenje zahteva za potpisivanje serverskog sertifikata. U

završnom delu dokumenta nalaze se uputstva za instalaciju digitalnih sertifikata na Linux serverima.

Summary

This document promotes the adoption of digital certificates in the member institutions of the Academic Network of Serbia (AMRES) as a means of establishing secure communication channels.

In order to establish secure communication when receiving or sending data from/to a server, users must be sure that they are indeed accessing the resources they intended to access and that no one can read and/or change the data that is sent or received. Such security is provided by the use of digital certificates in conjunction with Secure Sockets Layer (SSL) technology.

The document outlines the components of a Public Key Infrastructure (PKI), and also the implementation of PKI functions to include AMRES in the TERENA Certificate Service (TCS). The document specifies various needs for PKI in a National Research and Education Networking organisation (NREN), which require various types of digital certificates, while special attention has been given to the use of PKI and digital certificates in combination with SSL technology for the purpose of the mutual authentication of services and their users.

The document explains the procedure for obtaining a server certificate – key generation, the creation of certificates and the preparation and submission of the request for signing a server certificate. The final part of the document contains instructions for installing digital certificates on Linux servers.