Инфраструктура открытых ключей (PKI)

Инфраструктура открытых ключей (ИОК, англ. PKI - Public Key Infrastructure) — набор средств (технических, материальных, людских и т. д.), распределённых служб и компонентов, в совокупности используемых для поддержки шифрования на основе закрытого и открытого ключей. В основе PKI лежит использование системы шифрования с открытым ключом и несколько основных принципов:

- закрытый ключ (private key) известен только его владельцу;
- удостоверяющий центр создаёт электронный документ — сертификат открытого ключа, таким образом удостоверяя факт того, что закрытый (секретный) ключ известен эксклюзивно владельцу этого сертификата, открытый ключ (public key) свободно передаётся в сертификате;
- никто не доверяет друг другу, но все доверяют удостоверяющему центру;
- удостоверяющий центр подтверждает или опровергает принадлежность открытого ключа заданному лицу, которое владеет соответствующим закрытым ключом.

PKI на OpenSSL

PKI на OpenSSL

XCA

XCA

EJBCA

http://www.ejbca.org UCLA Anderson School of Management and PrimeKey is conducting a survey regarding the use of EJBCA and PKI. It would be very beneficial to the project if you could spare a few minutes to take this short survey.

Развертывание PKI на базе EJBCA

OpenXPKI

http://www.openxpki.org/

The OpenXPKI Project

The OpenXPKI project has the vision to publish a software stack that provides all necessary components to manage keys and certificates primarily based on the X509v3 cryptography standard.

OpenCA

Open Source PKI Management Software OpenCA v1.5.1 Download the latest version!

The OpenCA PKI Project is a collaborative effort to develop a robust, full-featured and Open Source out-of-the-box Certification Authority implementing the most used protocols with full-strength cryptography world-wide. OpenCA is based on many Open-Source Projects. Among the required software there are OpenLDAP, OpenSSL, Apache Project, Apache mod_ssl.

The project development is divided in two main tasks: studying and refining the security scheme that guarantees the best model to be used in a CA and developing software to easily setup and manage a Certification Authority.

https://pki.openca.org/projects/openca/

CAFL63

Приложение Удостоверяющий Центр (УЦ) ФЗ-63

Ссылки

https://ru.wikipedia.org/wiki/Инфраструктура_открытых_ключей

Pro-LDAP.ru - Руководство по выживанию — TLS/SSL и сертификаты SSL (X.509), подписанные УЦ и самоподписанные

https://sysadminmosaic.ru/pki/pki

2019-07-15 12:00