SiNAM
IT's our business

SINAM Public Key Infrastructure Solutions

SPKIS
E-SIGNATURE SOLUTIONS

- Building many type of Certification Authorities in one physical server;
- Support of strongest symmetric and asymmetric cryptographic and hash algorithms such as RSA, ECDSA, AES, SHA1, SHA256, SHA512, etc.
- System allows the certificate owner to generate public/private keys and send a certificate request to the CA for certification purposes; As well as depending on the certificate policy, CA can generate keys for the certificate owner too.
- Multifunctional Java and C# libraries for the integration of different information systems with digital signature and CA;
- Full support of SmartCard, eToken, HSM and other similar cryptographic devices;
- Mobile services and tools for signing and encryption of electronic documents as well as financial transactions.
- EİDAS qualified Remote Signing Service Provider(RSSP) for signing documents.
- 100% compatibility result of cybersecurity assessment by Deloitte on the based of compiled criteria as well as WebTrust requirements.

Background

Security and protection of data integrity are one of the main problems on the development of modern information technologies. Solution for identification, confidentiality and other security issues are possible by application of digital signature and cryptography methods. In this sence, Public Key Infrastructure (PKI) is one of the significant elements in the area of information Technologies. PKI settles many tasks by use of asymmetric cryptographic algorithms according to public key technology. Identification of people, protection of data integrity, determination of data source issues are solvable on information environment. The main leading element of PKI is a Certification Authority (CA) hierarchical chain of trust. CA - as a trusted source, carries out of people identification by using of digital certificates and assymetric keys. The process of secure exchange of keys among people on PKI technology based on asymetric cryptographic algorithm is provided and this ensures data integrity and safely delivery by encryption. As a guarantor of establishment of digital certificates providing identification on keys, their control and as well as other security princiles, CA fully provides security on electronic environment. Settled by digital certificates, digital signature is deemed to be equal to hand signature and sets issues as protection of data integrity and source determination. Pursuant to performing cryptography of data by asymmetric keys, loss of data is impossible in any case.

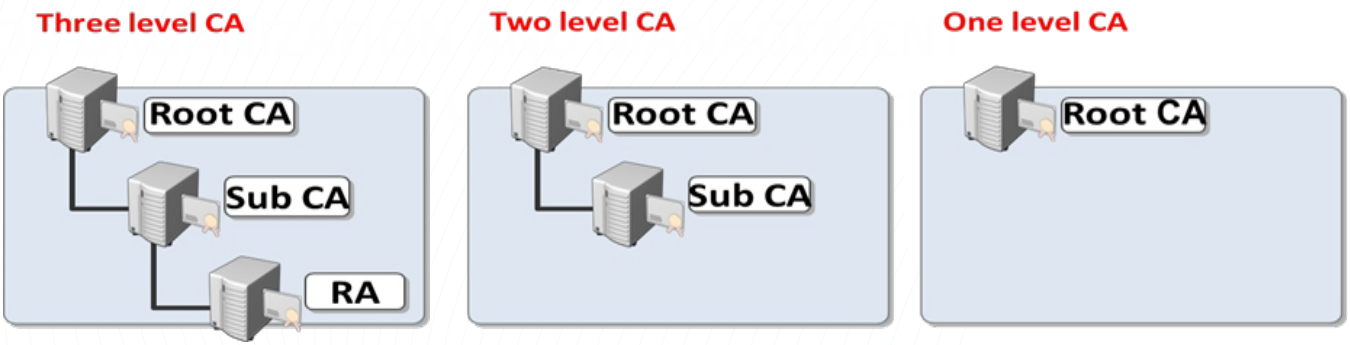
The major functions of Public Key Infrastructure (PKI)

- Confidentiality
- Authentication
- Integrity
- Non repudation

This document, provides information on SPKIS solutions created duly to the principles of PKI technology. SPKIS solutions consists of CA founded in accordance with the regulations of PKI technology and other components. Based on these components, information is given on other substantial sides of PKI technology.

Overview

SINAM company works more than 10 years on the area of digital signature and information security. SPKIS – digital signature solutions were created in consequence of great experience and long-term practice. This solution owns moduls which supports all possible functionalities on digital signature and cryptography. The main direction of this solution is a building of corporate and government CA and proposing the services for information security. As well as management of digital certificates, CA management system is able to provide services such as OCSP, TSA etc. International standards and local legislations are considered while the establishment of the system and have a chance of adoption to internal legislation of any country. Certificate center might be established on diversified structure by SPKIS solutions.



SmartCard and eTokens are used for creation and storage of public/private keys for digital signature certificates. As well as other carriers (Microsoft, Java containers) and external memory devices are useable. Hardware Security Module (HSM) device can be used for generation and protection of CA keys and signing of subscriber certificate. Additionally, in case of non existance of HSM, CA keys might be reserved in databse of CA. System possess integration opportunities with the products of HSM, SmartCard and eTokens of diferent vendors.

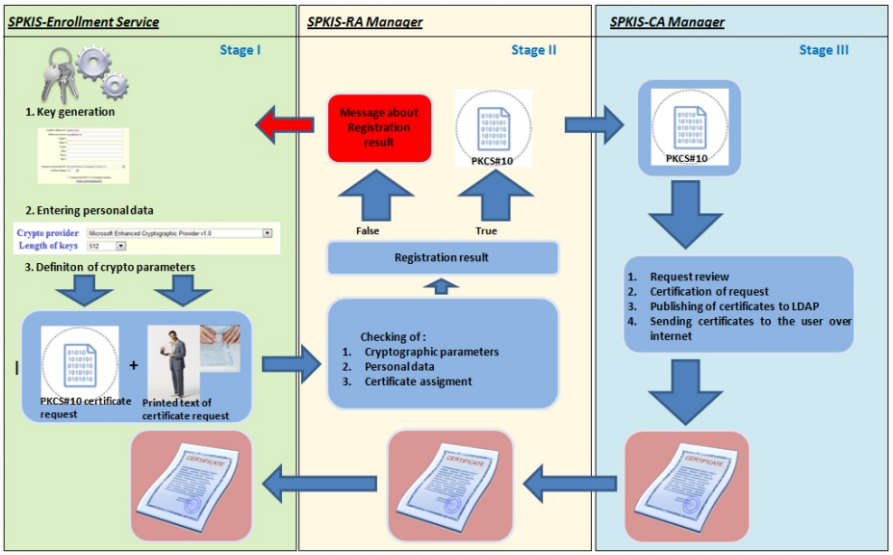
System Basic Features

- creation and management of more than one certification center in one server;
- creation of public/private key and submission of digital certificate request by web enrollment service of certification centre;
- full integration with HSM for the purpose of security of CA keys;
- user keys can be generated and stored in smartcards and eTokens;
- the secure management service for registration authority;
- registration of all transactions log;
- system is developed on the base of international standards and local legislation for digital signature;
- software for generation of digital signature and library for cryptographic methods;
- technical functionalities for accreditation with government Root CA;
- support of different range of cryptographic algorithms(RSA, DSA, SHA1, SHA2, ECDSA);
- online Certificate Status Protocol (OCSP) service;
- time Stamp Authority(TSA) service.
- Mobile application for creation of digital signature and encryption data
- EİDAS qualified Remote Signing Service Provider(RSSP

There are diferent mechanisms for the creation of digital signature keys on the system. Creation of keys can be set up by the certificate owner on his own computer or by the system administrator at the certificate center. PKCS10 for the certificate requests and for digital certificates X509 standard are used. It is possible to use CRL mechanism alongside with the status check service created through OCSP protocol in order to check the status of the certificate. For giving the TimeStamp services CA can use TSA module of SPKIS solutions. CA can issue many type of certificates such as digital signature, code signing, ssl certificate, mail security etc. Having outstanding experience on establishing and management of Corporate and nationally significantCA, SINAM corporation offers preparation of CP, CPS and other technical documents and auditing services.

System architecture and components

The main direction of "SPKIS" solutions is creation and management process of CA . For this purpose many softwares included in solution. Furthermore, there are certain additional softwares and libraries in the area of digital signature and cryptography. In order to create corporate and government CA, SPKIS solutions offer CA building architecture. The principle of submission of user certificates mainly performed by 3 modules. Generation, acceptance, certification of certificate requests and submission certificate to user has been described in the diagram below:



Mentioned diagram can be changed depending on requirement for CA. It is possible to set up CA chain with several levels and varied RA architecture. In order to provide TSA and OCSP services, SPKIS-TSA and SPKIS-OCSP modules are available to use. System architecture makes possible to insert existing CA into another CA chain. Besides, to set new RA's or revoke current RA's. All these will not effect to sustainable labor process. Due to system was built on Service oriented Architecture(SOA), all components can be easily integrated with other information systems.

SPKIS solutions consist of following components

"SPKIS – CA Manager" – Management system for Certification Authority.

"CA_Manager" module performs the function of creation and management of certificate requests, user certificates, certificate templates, registration centers, CRLs and as well as other objects. With the help of this module it is possible to create root and intermediate CAs and insert the corporate CA into another trusted CA chain(accreditation of CA). CA_Manager issues certificates, based on certificate requests which formed by certificate owners and approved by RA. Issued certificates are delivered to subscribers and published to LDAP/HTTP directories. CA private keys can be stored in HSM or CA Database during creation of CA. Furthermore, management of LDAP and HTTP directories are performed by this module.

"SPKIS - RA Manager" – Management system for Certification Authority.

Organization and management of certificate requests registration problems are experienced on private and state agencies which have substantially certificate users. In this kind of enterprises, itis the most convenient method to create registration centers (RA) in order to ncrease security levels by minimizing the quantity of trusted parties – certificate issuing odies. RA-Manager is the module for management of registration center. With the help of his odule RAs registered by CA performs the management of certificate requests. System dministrators check incoming requests and make a decision for issuing certificate via RA-anager module. Subsequently this decision, CA administrator can certify the request. This nsures management of large-scale certification request issue more punctual and fast rocessing n turn. Limited certificate requests received by CAs, can be done through CA_Manager.

"SPKIS – Enrollment Service" – registration of certificate requests.

"SPKIS – ES" module lets certificate owners to create public/private keys on their computers, send certificate request to RA and or CA, obtain certificate prepared due to the request and such other functions. Subscribers are able to prepare and send certificate requests as PKCS#10 format via online and or offline form to registration and or certification center. The generation of the keys is implementable by user on its computer or on SmartCard or eToken that belongs to him. Along with stated, there are such possibilities to obtain certificates of CA, information regarding to certification center, apply for revocation of certificates, obtain certificate revocation lists(CRL) of CA. System is a web-based software and available on any internet browser.

"SPKIS - eSigner" – software for signing and encrypting of electronic documents.

eSigner is a web based software for signing/verifying and encryption/decryption of files. Software can sign any type of files not depending on size and creates signature package file. All the EIDAS signature formats(XADES, PADES, CADES, ASIC) is supported in the process of signing documents. For creating of digital signature any certificate can be used which is stored in SmartCard, eToken, windows container etc. Besides the signing process document encryption and decryption functions can be used using this software. The algorithms for encryption and signing can be defined by user. Software has functionality for getting the public certificates from computer memory or LDAP directories for data encryption.

mSigner is a mobile version of eSigner is created for android OS and does the same functionalities. This application also can use SmartCards with mobile devices. Signing and encryption of any files inside the mobile device is possible through SmartCards connected to mobile devices by USB, MicroUSB and or Bluetooth readers.

"SPKIS - AzTrustCryptoLib" – Java and C# crypto library for integrating systems with digital signature. The library contains the methods such as digital signing, verifying, encryption, decryption, certificate status checking, search of certificates through LDAP directory and other methods. Library including Java and C# librariesis designed for information systems used on different platforms.

"SPKIS-LDAP" – System for deployment of CRLs to LDAP directories. Management of LDAP directories which is used for publishing of CRL and certificates is executed by CA_Manager software. Microsoft Active Directory and or other LDAP applications can be used as LDAP directories. Publish of certificate and CRL is automatically done by the system at certain time intervals. System lets LDAP to publish objects to directory at the same time.

"SPKIS – OCSP Server" – OCSP server responder. OCSP is an online certificate status checking service. Every CA using this software can create OCSP service as alternative to CRL for checking the status of certificates. Services and systems working with OCSP protocol can use this service for cheking certificate status online without downloading the CRL.

"SPKIS – TSA Server" – TSA server responder, offers time stamp service. Using this software CA can create Time Stamp Authority for giving service of time stamp. Time stamp service is formed on the basis of TSA protocol. Private keys of TSA certificate can be stored and used in HSM and DB while providing TSA service.

"SPKIS – RSSP" – EIDAS qualified Remote Signing Service Provider. RSSP is a latest technology for signing documents easily not using private key storages by certificate owner. Instead of traditional key storages, RSSP iis responsible for generating, storing and using private keys for creation of digital signature under de sole control of key owner. This service was created on the base of EIDAS regulation documents and standards which is relying to internationl cybersecurity standards.

Advantages of the system

There are different information systems in the areas of E-signature and certification centre. During the development of SPKIS system similar systems were analyzed and their shortcomings were investigated and these issues were taken into consideration in the process of system development. The main distinctive features of "SPKIS" system from the other certificate centre systems are the following:

- It is possible to create and use any number of root and intermediate certification centre in one physical server
- The registration of certficate requests in the system is done not on paper, but electronically over the internet which serves for maximum simplification of the process
- The strongest symmetric and asymmetric cryptographic and hash algorithms are used in the system. RSA, ECDSA, AES, SHA1, SHA256, SHA512, etc. can be shown as an example
- The system allows certificate owner to generate public/private key and send certificate request to the centre for certification purposes
- There are multifunctional Java and C# libraries in the system meant for integration of different information systems inside the system with e-signature
- The system works in the integration environment with SmartCard, eToken, HSM and other similar cryptographic devices

Main organizations and activity of areas for application of SPKIS Solutions:

- Taxes services
- Customs control
- Ministries
- Financial organizations
- Universities
- Electronic elections
- e-Commerce
- Payment systems
- Strong authentication services (two factor authentication)
- Electronic document management
- Mail security
- SSL certification

Success stories

National Certification Services Center

- Building Root, Policy, Issuing Certificate Authorities;
- Building Remote Signing Services for Issuer Cas$
- Building OCSP, TSA services;
- Using HSM and Smartcard/eToken for protection of private keys.

Central Bank of the Republic of Azerbaijan

- Building Certificate Authority
- Accreditation of CA with National Root CA of Azerbaijan Republic
- Building Registration Centres
- Using HSM and Smartcard/eToken for protection of private keys
- Integration of corporate information systems with digital signature

The State Customs Committee of the Republic of Azerbaijan

- Development of software for digitally signing of electronic documents and application of cryptographic API
- Application of SmartCard and eToken for digital signing

State Social Protection Fund of Azerbaijan Republic

- Building a corporate Certificate Authority
- Development of software for digital signature and encryption of electronic documents
- Development of system for exchange of signed document packages

RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols
https://www.rfc-editor.org/info/rfc2510

RFC 2511 Internet X.509 Certificate Request Message Format
https://www.rfc-editor.org/info/rfc2511

RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile
https://www.rfc-editor.org/info/rfc2459

RFC 2314 PKCS #10: Certification Request Syntax Version 1.5
https://www.rfc-editor.org/info/rfc2314

RFC 2587 Internet X.509 Public Key Infrastructure LDAPv2 Schema
https://www.rfc-editor.org/info/rfc2587

RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
https://www.rfc-editor.org/info/rfc3280

RFC 7512 The PKCS #11 URI Scheme
https://www.rfc-editor.org/info/rfc7512

RFC 7292 PKCS #12: Personal Information Exchange Syntax v1.1
https://www.rfc-editor.org/info/rfc7292

RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5
https://www.rfc-editor.org/info/rfc2315

RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
https://www.rfc-editor.org/info/rfc6960

RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
https://www.rfc-editor.org/info/rfc3161

RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
https://www.rfc-editor.org/info/rfc3647

RFC 5911 New ASN.1 Modules for Cryptographic Message Syntax (CMS) and S/MIME
https://www.rfc-editor.org/info/rfc5911

SPKIS

E-SIGNATURE SOLUTIONS

SINAM Public Key Infrastructure Solutions

SiNAM
IT's our business

68, B. Vakhabzadeh Str.,
AZ1141, Baku, Azerbaijan

+994 12 510 11 00
+994 12 497 51 96

office@sinam.net
www.sinam.net