Integrated and Full System for issuance of Digital Signature

PKA device, model SA renders all integrated digital signature services in one device. This device has provided different services including data timestamped, digital signature issuance center for XML messages and digital signature issuance center with CS context, all in one device. This device can be used as secure and integrated center for issuance of digital signature and timestamped in the organization and renders services to other servers and systems in context of web services. As such it is possible that all the documents and data of the organization to be signed digital in context of PDF standards. Also it is possible to add digital signature on the data with XML template existing in the database and/or between two services and any data to be signed digitally with CMS standard base.

Support of Hardware Security Module (HSM)

The internal HSM is for secure production and maintenance of private keys of data timestamped, PDF signer, XML signer and CMS signer which provides higher levels of security. In this device a system as Key Management System (KMS) has been provided that is responsible for full management of life cycle of keys including manufacturing, maintenance, providing, support, retrieving and transfer. Also for more security, for maintenance of support version of private keys, one special smart card is used. On the other hand this device can be connected to various HSM devices under network based on standard PKCS#11.
Performance
- Up to 32 Concurrent Connections
- Timestamp Service: 600 tps
- PDF Signing: 150 tps
- XML Signing: 150 tps
- CMS Signing: 150 tps

Software Development Kit
- J2EE and J2SE SDK
- .Net Framework SDK
- Web-Service API (SOAP)

Hardware Security Module (HSM)
- Includes embedded HSM with FIPS 140-2 Level 3 Certificate
- Embedded HSM 25/220/600 tps (1024 bit RSA signature/second)
- Supporting various Network HSMs by PKCS#11 Interface (SafeNet, nCipher, Utimaco, Boll, etc.)

PKI Standards
- RFC 3161 (Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP))
- RFC 3778 (The application /pdf Media Type)
- RFC 4330 (Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI)
- FIPS 180-4 (Secure Hash Standard (SHS))
- FIPS 140-2 (Security Requirements for Cryptographic Modules)
- PKCS#1 (RSA Cryptography Standard)
- PKCS#7 (Cryptographic Message Syntax Standard)
- PKCS#10 (Certification Request Standard)
- PKCS#11 (Cryptographic Token Interface)
- XML-Sig (XML Signature Syntax and Processing)

Physical Characteristics
- Connectivity: 1 Gbps Ethernet
- Dimensions: 426 x 365 x 44 mm
- 1U Rackmount

Timestamped CA (TSA)
PKA device, model SA is able to be used as TSA. This device can add the timesatmped by receiving the data package and to sign the final complex digitally. This process is conducted according to TSP protocol and standard RFC3161. On the other hand this device can receive the sync time from the introduced references by NTP protocol.

Digital Signature Issuance Center in context of PDF
PKA device model SA can have role of integrated server for production of digital signature on documents with PDF format. In this condition, the device can receives various standard setup of PDF file like warning text and/or logo of the envisaged organization and to insert it in the envisaged coordinates. The produced digital signature in PDF files is standard and can be read and validate in all software and PDF tools like Adobe Acrobat Readers and/or Foxit Reader.

Connectable to other Software Systems
PKA device has been designed in a manner it can be connected easily to other software of the organization; by this device all the software systems can be equipped with PKI-enabling. For this purpose, various connections with this device have been predicted for development of software. This device can render its different services in context of web-services and has programming library (SDK) for two platforms of Net Framework and JavaJ2EE/J2SE. By these tools, the other software systems can be equipped with PKI-Enabling easily and in shortest possible time.