Strategy and Synergy for Security

SETS Certification Authority Software

e-Abhedya
ई-अभेद्य

A Security Solution Developed by SETS

About SETS

Society for Electronic Transactions and Security (SETS) is an initiative of the Office of the Principal Scientific Advisor (PSA) to the Government of India.

SETS has been engaged in providing cyber security solutions in different verticals of cyber security including (a) Cryptology & Computing which includes Algorithms and Protocols design, Cryptanalysis, Post Quantum Cryptography, Quantum Key Distribution and High Performance Computing, (b) Hardware Security which includes Secure Hardware Design and Side Channel Analysis, (c) Network Security which includes Perimeter & Application Security and Intrusion Detection & Prevention along with (d) Services and Training with Vulnerability Analysis & Penetration Testing and providing assistance in framing Security Policy & Audit.

About e-Abhedya

SETS e-Abhedya software offers PKI services to the users based on the state-of-the-art Elliptic Curve Cryptography (ECC) along with RSA techniques. The benefit of using ECC over RSA is that the keys and digital certificates based on ECC leads to achieve higher security as compared to traditional RSA based digital certificates without compromising the operational time. At present, Digital Signing Certificate (DSC) services are being offered with ECC support whereas encryption certificates and combo certificates are being offered with RSA support. e-Abhedya at present, support services like E-mail signing & encryption, electronic document signing & verification and digital signatures creation for the users.

Secure Web Services
E-mail Encryption
E-mail Signing
e-Document Signing
Society for Electronic Transactions & Security
Certification Authority
e-Abhedya
ई-अभेद्य
Public Key
Private Key
A Public Key Infrastructure Solution by SETS
Confidentiality
Non-Repudiation
Integrity
Authentication

General Features

e-Abhedya Services
- E-mail Signing & Encryption
- e-Document Signing
- Creation of Digital Signature for users
- Encryption Certificate with RSA
- Combo Certificate with RSA
- Web Server Certificate
- Wildcard Certificate
- Code Signing Certificate with RSA

Key Generation
- Key pair and CSR generation for DSC by user only
- User's Private Key Generation and Storage in self custody

Digital Certificate
- Choice-based EC-key size selection
- Off-line Verification of Users through RA
- Multiple Certificates of different class type
- OCSP Support
- CRL and Certificate Renewal

e-Abhedya Software Features
- Responsive Design
- Simple and Attractive GUI for User Interfaces
- E-mail and Mobile Verification of Users
- Indigenous Product Development

Documentation
- Operational Help through ReadMe files
- Comprehensive Documentation with Manuals and Technical Report

Technical Features

- Very high elliptic curve key sizes in the range of 256, 384 and 521 bit supported
- RSA 4096 bit key size supported
- NIST/SECG recommended elliptic curves for digital certificates/digital signatures generation and document signing
- Strong Hash Function (SHA256, SHA384 and SHA512) supported
- Strong Symmetric Encryption Algorithm like AES-256 used for Private Keys Encipherment
- HTTPS protocol for CA and RA Servers connectivity
- LDAP Server to store records
- Efficient session handling during various operations performed by the user/RA
- Robust Software Design to handle exceptions including link failure etc.
- Responsive Design of the product software
- Best Software Engineering Practices adopted in product development
- User is exposed to information on “need-to-know” basis only
- OCSP support
- Hardened OpenSSL
- Transparent Software Code
- No use of any pre-compiled binaries in the product development
- Windows/Linux platform supported

Contact

Society for Electronic Transactions & Security
(SETS)
MGR Knowledge City, C.I.T. Campus
Tramani, Chennai - 600 113
☎ 044-66632520
044-66632501
✉ kunal@setsindia.net

Genesis of the Name e-Abhedya

Abhedya in Hindi language means "Non-penetrable". In Public Key Infrastructure, e-Abhedya asserts its meaning by providing an environment and mechanisms to realize a world of safe communication.