TRUST SERVICES

Seacert Customer Benefits

- **Cost Effective.** Customized trust services available at lower costs than in-house development or other commercially available Certification Authorities (CA) vendors. The practical solution for those who want to avoid up-front development and training costs and be assured that they satisfy all deployment requirements.
- **Scalable.** A scalable architecture that produces millions of provisioning credentials a month, and which can be easily expanded.
- **Customizable.** Provisioning software that is highly configurable and can easily be modified to support custom specifications. This flexibility surpasses what is available to those who rely on vendor-supplied software.
- **Conforming to Industry Security Standards.** Operations and controls designed to meet or exceed the North America AICPA/CICA WebTrust Program standard for CA criteria. This criteria provides a valuable framework for assessing adequacy of CA controls and issuing independent opinions.

Seacert provides Public Key Infrastructure (PKI) services, such as provisioning digital certificates, identities and cryptographic keys for device makers and service providers. Seacert supports media content distribution for movies, television shows and video games. In addition, Seacert provides device registration and identification credentials to IoT and Big Data services.

Seacert supplies cryptographic services to provide for quick, secure and cost-effective deployments. Through Trust Services, we support a variety of cryptographic standards and protocols and have the expertise to provide reliable, customizable implementations. With over 60 global customers, Seacert supports a variety of business process flows, credentials, and event response mechanisms.

Standard Services

- Core cryptographic services include: registration authority (RA); root generation and management; certificate signing; device and service provider provisioning; certificate revocation list (CRL) signing and hosting; secure storage and backup; and test PKI management.
- Certificate signing services for client authentication, service authentication, application authentication (code signing) and data protection (encryption).
- General business services include: reporting, archiving, billing, audit management and business continuity.

Custom Services

- Public key infrastructure (PKI) design and implementation, including PKI hierarchy definition, profile definitions and requirements documentation. We work with you to take a specification and determine how to implement it with cryptographic credentials. We have the expertise to offer alternatives and explain the implications for event response techniques, performance, complexity and cost.
- Response systems design and implementation. Event response services beyond the standard CRL are available, along with specialized tools to manage such functions. Renewability services also available.
- Provisioning services that enable your implementers to purchase compliant credentials in bulk, just as they would other component parts. Easy-to-use ordering forms and delivery processes.

SEACERT SERVICES

Seacert offering includes:

Industry-leading security. Seacert employs multiple-custody security protocols to protect sensitive keys. The protocols rely on the K-of-N threshold smart card technology and access control technology provided by FIPS-140 certified hardware security modules. Operations are conducted in a high-security facility with redundant, offsite backups.

Configurable tools.

- The CA Tools handle the issuance of root and subordinate certificates; CRLs and other revocation lists and signing of Certificate Signing Requests (CSR).
- Cryptographic Provisioning Tool (CPT) generates packets (i.e., logical set of key, certificates and assertions to be associated with a single device or service) for multiple types of devices or services. CPT enables efficient and error-free electronic ordering and fulfillment.
- The Order Processing Tools include an order unwrap/decrypt tool and a CSR tool.

Comprehensive and reliable operations. Seacert follows industry best practices for operations, thus providing customers with credentials that are secure, of highest quality, and are available with a short turnaround time.

Supported Standards

Supports a variety of cryptographic standards and protocols. Offers standard and/or custom extensions or implementations.

Standards and Protocols	
Cryptographic keys	RSA 1024 bit or 2048 bit modulus AES (Advanced Encryption Standard) Others available upon request
Certificates and Certificate Revocation Lists	x.509 v3 RFC5280 (with direct or indirect CRLs)
PKI	PKCS #7, PKCS #8, PKCS #10, PKCS #12 (syntax standards)
Other	SAML, XML (authentication, authorization language constructs) FIPS 186-2, FIPS 140-2 (digital signature standards) SP800-22, SP800-90, and RFC 1750 (random number generator standards)

Deployment Service Models

Seacert offers flexible deployment models. The Direct Service supports an adopter outsourcing provisioning; the Branded Service supports provisioning through a separate service; and the Trust Authority Service s upports provisioning through the Trust Authority (TA).