



Seacert™

Scalable Key Provisioning and Personalization for Large Networks of IoT Devices

SERVICES

- **High Volume Key Provisioning.** We deliver X.509 certificates in large volumes to create unique identities for millions of devices every month.
- **Managed PKI Services.** We create and manage root certificates and certificate authorities, ensuring security and business continuity
- **Custom PKI Services.** We work with you to develop PKI services that meet your needs. Seacert provides the tools and expertise you need to solve your business problems, whether that's custom X.509 extensions, specialized CRLs, or signed authorization certificates.

SEACERT MAKES IT PERSONAL

The biggest barrier to deploying IoT projects is providing robust scalable security to a large number of distributed devices. The core security challenge is **device personalization**. Devices need to be provisioned with unique, trusted identities and the rights needed to interact in the complex ecosystems of industrial and consumer IoT. Seacert is the only security service that provides device personalization at the massive scale you need to launch your project and manage risk. Whether you want to deliver credentials on the factory floor or from an online cloud-enabled service, Seacert makes scalable device personalization easy.

Focus on Your Core Business

Running a large-scale key management operation requires specialized facilities, processes, technology and skills. Seacert's experts can run your keying operations so that you can focus on your core business. Seacert was developed for large networks of consumer electronics devices around the world. Its unique architecture, developed specifically for large networks of service-enabled devices is a natural platform for IoT devices. Our world class operation delivers the most scalable and secure PKI services in the industry.

Go with a Trusted Leader

Since 2008, Seacert has issued billions of personalization credentials to leading global consumer electronics device makers and content service providers. Our credentials are embedded in hundreds of millions of devices worldwide.

USE CASES: Let Seacert help you make your IoT security project personal.



Media & Entertainment

Seacert provides the credentials that protect video and audio content for millions of world-wide users every day.



Industrial IoT

Seacert provides unique identities for each device, application, service and user to secure operations and prevent hacker exploits.



Smart City

Seacert can help maintain the end-to-end integrity of smart infrastructure for cities at a fraction of the cost of alternative approaches.



Connected Cars

Seacert delivers a trusted identity for each component within a car to secure end-to-end communications and make cars safe

FEATURES

Managed PKI Services

- **Root CA Flexibility.** We can create and manage a root Certificate Authority (CA) specifically for you, or you can use a Seacert or third-party root CA.
- **Bulk X.509 Certificates.** Delivered in batches of any size, from hundreds to millions, along with their corresponding private keys to satisfy any scale of project.
- **Revocation.** We manage certificate revocation lists, OCSP, and other revocation mechanisms should a private key become compromised.
- **Storage and Backup.** Ensure business continuity by letting Seacert manage your root keys in secure facilities and HSMs, backed up across multiple physical locations.
- **Test and Production Environments.** Allow development and test activities to proceed without affecting production operations.

High Volume Provisioning Services

- **Offline Key Provisioning.** We deliver batches of customized X.509 certificates for you to provision on your factory floor or in your own online field provisioning system. Our highly scalable services can deliver millions of credentials in a single order.
- **Online Key Provisioning.** Provision identities to your apps and devices by obtaining credentials from a Seacert hosted secure, multi-tenant cloud-based repository at initialization time.

Custom PKI Services

- **Ecosystem PKI Design.** We can design the PKI hierarchy for your entire implementation, including root, subordinate CAs, services, devices, applications, platform providers, OEMs, remediation and whatever else you need. Seacert can provide all or part of the associated credentials to fit your needs.
- **Easy to Manage PKI.** Back-end services are provided through a battle-tested and fully audited web portal for ordering, deploying, revoking and managing credentials.

- **SAML Assertions.** We can deliver SAML Assertions signed by your specified X.509 certificate, to facilitate authentication by a SAML-compliant identity provider.
- **Signed XML and Blobs.** XML documents and blobs that are digitally signed with the X.509 certificate can be delivered in bulk.
- **Symmetric Keys.** Can be provisioned in bulk to enable high-speed encryption of data and data computation.
- **Secure TLS Communications.** X.509 certificates can be used to establish point-to-point, secured TLS communications between devices, applications and users.

Security and Standards Compliance

- **WebTrust Compliant.** Seacert defends against insider or intruder attacks via secure facilities, processes and technologies, including FIPS 140-2 validated HSMs.
- **Auditable Reporting.** All operations are logged, and actionable reports are created to help meet compliance and regulatory requirements.
- **Cryptographic Standards & Protocols.** RSA 1024/2048 bit, Elliptic Curve 150 to 528 bit, AES 128/192/256 bit, x.509 v3, RFC 5280, RFC 4325, FIPS 140-2, FIPS 186-2, PKCS #7, #8, #10, #12, Signed SAML assertions, Signed or Encrypted XML or blobs, SP 800-22 & SP 800-90, and RFC 1750.

Complementary Products



whiteCryption® Code Protection™

Shields mobile apps and code that operates on untrusted devices to foil hackers and protect code secrets.



whiteCryption® Secure Key Box™

Stores your keys for mobile apps, IoT devices and services, even when there is no dedicated hardware security device.

Provision Devices with Identities when Manufactured or when they Boot

