intertrust®

Datasheet

Intertrust PKI

Scalable key provisioning for large networks of IoT devices

Secure IoT devices with Intertrust PKI

The biggest barrier to deploying IoT projects is providing a trusted ecosystem across a large number of distributed devices. The core security challenges are device personalization, trust, and lifecycle management. Devices need to be provisioned with unique, trusted identities that can interact in complex ecosystems of industrial and consumer IoT only with trusted entities.

Intertrust Public Key Infrastructure (PKI) service provides device personalization at the massive scale you need to launch your project and manage your risk effectively. Whether you want to deliver credentials on the factory floor or from an online cloud- enabled service, we make trusted device identity management scalable and easy.

Focus on your core business

Running a key management operation requires specialized facilities, processes, technology and skills. Intetrust PKI has the expertise to run your key operations, allowing you to focus on your core business. Intertrust PKI was purpose-built for large networks of consumer electronics devices around the world. Today, this 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

Intertrust PKI has issued more than 2 billion cryptographic credentials to leading global consumer electronics device makers and service providers. Our credentials are embedded in hundreds of millions of devices worldwide.

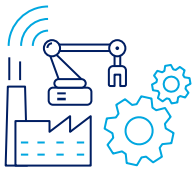
Services

- **High and low volume key provisioning.**
- **High volume X.509 certificates** to create unique identities for millions of devices each month.
- **Managed PKI services** to create and manage Root CAs, Subordinate CAs, and end-entity certificates (or key pairs) for the entire ecosystem while ensuring security and business continuity for the end-to-end lifecycle.
- **Intertrust PKI provides all the keys you need** for secure access control, mutual authentication, secure over-the-air updates and data protection and privacy.
- **Custom PKI services** – we work with you to develop PKI services that meet your needs.

Intertrust PKI provides the tools and expertise you need to solve your business problems, whether that's custom X.509 certificate extensions, specialized remediation methods, code signing services, factory floor integration, or custom encryption or digital signing of unique data structures. Intertrust PKI is the ideal solution for secure PKI services.

Handle complex device identities at scale

Use cases



Industrial IoT

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

Smart city

Maintain the end-to-end integrity of smart infrastructure for cities at a fraction of the cost of alternative approaches.

Connected cars

Deliver trusted identities to components within a car to secure end-to-end communications and make cars safe.

Features

Managed PKI services

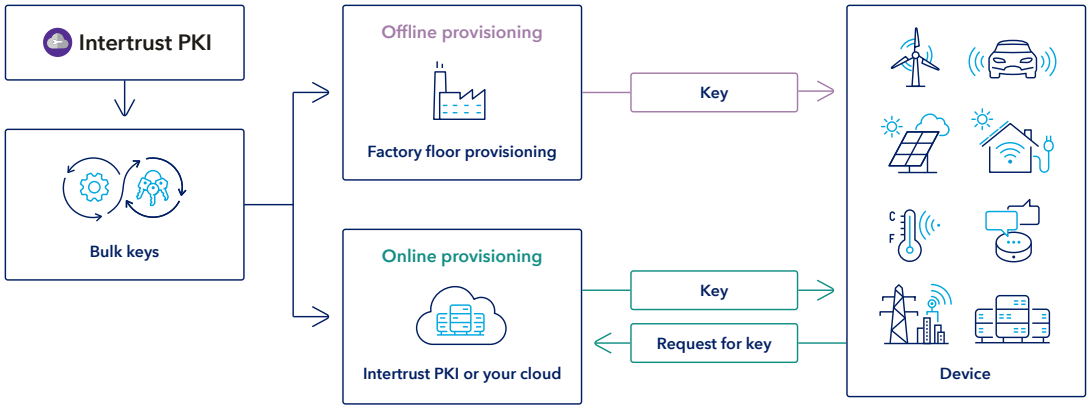
- **Root CA flexibility.** You have the option to let us create and manage a Root Certificate Authority (CA) specifically for you, or to use an Intertrust PKI Root CA.
- **Bulk X.509 certificates.** We can deliver X.509 certificates in batches of any size from hundreds to millions, along with their corresponding private keys to satisfy any scale of project.
- **Revocation.** We manage certificate revocation lists, OCSP, and other revocation mechanisms if private keys become compromised.
- **Storage and backup.** Intertrust PKI manages your root keys in secure facilities and HSMs, backed up across multiple physical locations to ensure business continuity.
- **Test and production environments.** Allow development and test activities to proceed without affecting production operations.

High volume provisioning services

- **Simple certificate enrolment protocol (SCEP -- RFC 8894).** A PKI protocol that leverages existing technology by using Cryptographic Message Syntax (CMS, formerly known as PKCS #7) and PKCS #10 over HTTP.
- **Offline key provisioning.** Deliver batches of customized X.509 certificates so you can 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 applications and devices by getting credentials from an Intertrust PKI 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 CA, Subordinate CAs, services, devices, applications, platform providers, OEMs, remediation and whatever else you need. Intertrust PKI can provide all, or part of the associated credentials to fit your needs.
- **Easy to manage PKI.** Back-end services are provided through a pen-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 and services.



Provision devices with identities when manufactured or when they boot.

Security and standards compliance

- **WebTrust compliant and ISO 9001:2015 certified.** Intertrust PKI defends against insider or intruder attacks via secure facilities, processes and technologies, including HSMs and having in place tested business continuity capabilities. A robust Quality System ensures ongoing process quality and continual improvement.
- **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.

intertrust®

Building trust for the connected world.

Learn more at: intertrust.com/platform
Contact us at: +1 408 616 1600 | dataplatform@intertrust.com