



Ascertia PKI-as-a-Service

Enterprise-grade managed PKI for governments, TSPs, and enterprises.

Secure identities, devices, and digital transactions, without the complexity of running your own PKI. Ascertia PKI-as-a-Service (PKIaaS) delivers certificate issuance, validation, and lifecycle management from a fully managed, high-availability cloud service, powered by ADSS CA/PKI Server and Web RA Server.

Digital Trust Made Simple with PKI-as-a-Service

Digital business requires trust. Every online interaction — whether purchasing goods, conducting financial Every digital interaction — buying goods, conducting financial transactions, streaming content, or accessing enterprise systems — relies on trust. That trust is established by digital identities, issued and managed through Public Key Infrastructure (PKI).

However, deploying PKI internally is a significant challenge. Organizations must invest in specialized hardware, configure secure and resilient environments, maintain compliance with demanding standards, and hire teams with rare PKI expertise. The result is often a costly, time-consuming, and fragile infrastructure that can become a bottleneck to business agility. For many, the complexity of ongoing operations — certificate lifecycle management, availability monitoring, disaster recovery, and keeping pace with cryptographic advances — makes PKI difficult to sustain.

PKI-as-a-Service eliminates these challenges. Delivered as a fully managed offering, it provides the same robust, standards-based trust infrastructure without the overhead. The service handles certificate issuance, lifecycle automation, validation, and compliance, all backed by resilient cloud architecture and operated by PKI specialists.

With PKI-as-a-Service, organizations gain a secure, scalable, and future-proof trust platform — ready to use without the complexity of building and running it themselves. This enables businesses, governments, and service providers to focus on digital transformation while ensuring authenticity, integrity, and confidentiality across all digital interactions.

Key Features

- **Standards Compliance:** Fully compliant with RFC 5280, RFC 6960 and RFC 5019, has undergone FIPS 201 certification.
- **Third Party Certifications:** Common Criteria EAL 4+ ALC_FLR.3 certified, meeting the requirements of the NIAP Protection Profile for Certification Authorities Version 2.1 (2017)
- **Support for Classic and Quantum Resistant Cryptography:** ADSS PKI Server provides support for generating keys and certificates using the following algorithms:
 - RSA & ECDSA
 - FIPS 204 (CRYSTALS Dillithium)
 - FIPS 203 (Kyber)
 - FIPS 205 (SPHINCS+)
 - Classic McEliece
- **Multi-Tenant & Dedicated Models:** Choose the deployment model that fits your security requirements..
- **Certificate Lifecycle Automation:** REST APIs, SCEP, CMP, EST, ACME for integration into IT and DevOps pipelines.
- **Integration with Active Directory:** Seamlessly integrate certificate enrolment into Active Directory and Group Policy for certificate issuance.
- **Flexible Certificate Validation:** Chose the certificate validation model that works for you, OCSP or CRL's.
- **Flexible Certificate Templates:** Chose from standard certificate templates, or easily create your own..

Ascertia PKI-as-a-Service Architecture

ADSS PKI-as-a-Service enables customers to choose the right hierarchy they need for their enterprise, built using Ascertia ADSS Server and Web RA, customers get the world's most flexible trust services platform without the complexity of an on-premise deployment. Sit back and let us do all the heavy lifting.

The Ascertia PKI-as-a-Service is built on a cloud-native, multi-layered architecture designed for scalability, high availability, and secure operations. The managed service abstracts away the underlying complexity of PKI, while still delivering all the essential components required to establish digital trust.

PKI-as-a-Service Core Components

Root and Issuing Certification Authority (CA) Services

Hosted and operated by the provider, these generate and sign digital certificates for users, devices, and applications. Multiple logical CAs can be provisioned within the service to meet diverse business and compliance needs.

Registration Authority (RA) Services

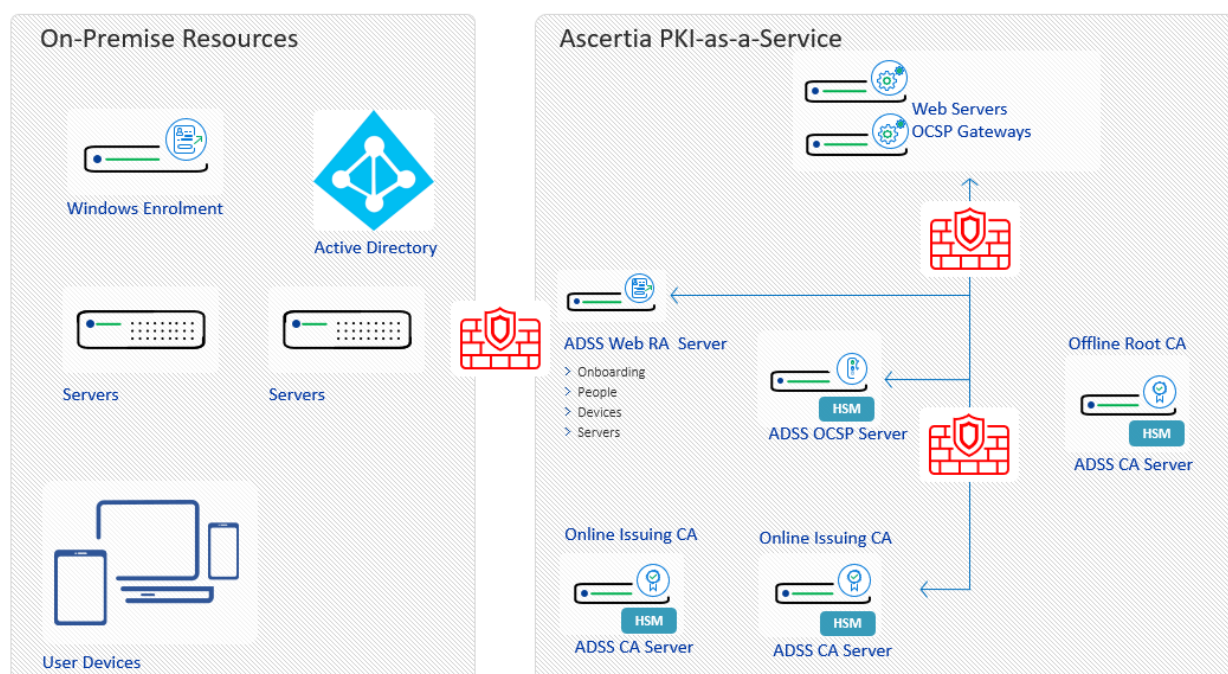
Integrated workflows handle identity vetting, enrolment requests, and approval processes. This ensures that every certificate is issued to a verified and authorized entity.

Certificate Validation Services (OCSP & CRL)

OCSP and CRL endpoints ensure real-time, low-latency validation of certificate status. These services maintain high throughput and redundancy to support large-scale deployments.

Key Management & Hardware Security Modules (HSMs)

All cryptographic keys are generated and protected within FIPS 140-3 certified HSMs, ensuring strong separation of duties and secure lifecycle management.



Offering Highlights

Simplifies Deployment: We know how hard building a PKI can be, sit back and we do all the heavy lifting.

Flexible Enrolment Options: Ascertia PKI-as-a-Service offers the full range of certificate enrolment methods to cover all of your enrolment needs.

Management Control and Reporting: Detailed role-based access controls makes it easy to give your staff the rights they need, for instance allowing help-desk staff to access log information so they can help customers whilst ensuring that they cannot view or change any configuration data.

PKI at Scale: With more and more use cases requiring certificates and with certificates moving to shorter life spans. Ascertia PKI-as-a-Service is a highly efficient cloud-based solution that can scale with nearly limitless capacity.

ADSS PKI-as-a-Service built on Ascertia's advanced trust services platform and provides a multi tenanted cloud native solution for delivering keys and certificates to enable digital trust.

Built by PKI experts, the Ascertia managed service team take all of the stress and complexity away from designing, building and maintaining your PKI.

- > **Round the clock support:**
24 x 7 support and system availability.
- > **Bring Your Own Root Support:**
Enables customers to leverage their existing Root CA to sign issuing or policy CA's beneath existing trust anchors if required.
- > **Extendable Use Cases**
Simple to add new use cases and services, PKI-as-a-Service enables you to add more digital trust use cases as and when you need to.
- > **Ready for the future**
Ascertia PKI-as-a-Service is PQC algorithms ready.



Mike Hathaway | Chief Product Officer

About Ascertia

Ascertia provides digital trust for people, devices, data and documents for everybody from individuals to Enterprises and Governments. Ascertia's PKI and digital signature technologies serve a global customer base and partner network via direct and indirect sales channels.

For more info

info@ascertia.com

www.ascertia.com