DigiCert® Solutions
Infrastructure Security

digicert®

DigiCert® Solutions Infrastructure Security

Fortune 500 and Global 2000 organizations rely on DigiCert's 14-plus years of experience delivering digital trust solutions, including high-assurance TLS/SSL, PKI, IoT and signing solutions, to millions of their users and devices worldwide. DigiCert's solutions include DigiCert ONE, PKI Platform ONE and eIDAS[1]-compliant Qualified Website Authentication Certificates (QWACs). These solutions are designed to meet a range of business needs including on-premises, cloud and hybrid deployment. The DigiCert-managed solutions run on a secure infrastructure that is not only designed for high availability and fault tolerance but also complies with strict security processes and standards. DigiCert's secure infrastructure provides the performance, reliability and security that enterprises require for their authentication, encryption and digital signature needs.

Key Features

Stringent Physical, System, and Network Security

DigiCert's secure infrastructure for its cloud deployment includes the following features:

- **Physical security infrastructure:** Multi-factor authentication including biometric access control methods. Dual-person control on physical restriction into caged environment. Multiple security zones required to gain physical access to systems.
- **Restricted access to trusted employees:** Only DigiCert employees who have passed thorough background checks have access to DigiCert infrastructure.
- **Secure key management:** Cryptographic keys are generated on dedicated FIPS 140-21-compliant hardware security modules and stored in an encrypted format.
- **System and Network Security:** In addition to supporting security industry best practices, safeguards are in place to protect against DDoS, web application attacks, resource attacks and extensive other protections.
- **Role-based administration:** All IT services separate duties between personnel and prevent individual access to sensitive information and functions.

High Availability

DigiCert's secure infrastructure relies on data centers in different regions of the United States, Japan, Australia and Europe:

- **Redundant power and cooling systems:** In addition to redundant cooling, all IT equipment is dual-powered and served by multiple independent distribution paths.
- **Geographical distribution:** Load balancing of all critical web infrastructure globally.
- **Redundant infrastructure:** All critical network and system components are fault-tolerant.

Continuous Global Monitoring

- **Dedicated monitoring:** DigiCert Network Operations Center provides 24x7 monitoring of the DigiCert infrastructure, systems and network.
- **Third-party monitoring:** DigiCert employs external third-party global services to monitor its critical infrastructure, systems and networks.
- **Restricted access to trusted employees:** Only DigiCert employees who have passed thorough background checks have access to DigiCert infrastructure.
- **Secure key management:** Cryptographic keys are generated on dedicated FIPS[2] 140-2 compliant hardware security modules and stored in an encrypted format.

Independently Audited and Certi f

Applicability: Americas

Applicability: Europe

Product/ Scheme	Supervisory Authority	Trust Service Requirements	Accreditation Body/ Auditor	Description	Applicability
ZertES **Services Provider**	SAS[14]/BAKOM[15]	Swiss Law and ETSI[16] standards for Qualified Certification Service Providers (CSP) and Time Stamping Authorities	KPMG	Annual audits to ensure conformity with the requirements for qualified certificates.	Switzerland
Netherlands ETSI **for eIDAS Compliance**	Agentschap Telecom, Netherlands	ETSI EN 319 411-1 ETSI EN 319 411-2 v2.2.2[17] standards to issue Qualified Certificates for Electronic Signature, Electronic Seal and website authentication. EU Regulation (EU) No 910/2014 (eIDAS)	BSI	This is an annual audit for accreditation to be a QTSP in accordance with European Union Regulation No..910/2014 on electronic identification and trust services for electronic transactions in the internal market (also known as eIDAS).	Netherlands – but applies across the EU
Trust Service Provider (TSP) for PKIoverheid	Logius Policy				

Key Benefits of DigiCert ONE, a premier offering from DigiCert:

Unified PKI Management

With DigiCert ONE, customers can improve adherence to corporate policy and streamline management with unified PKI workflows including TLS, Enterprise PKI, Code Signing, Document Signing and IoT on one platform.

Scalability

DigiCert ONE, based on a containerized architecture, is highly scalable to support large deployment and growth needs of the business.

Deployment Flexibility

Customers have the flexibility of deploying DigiCert ONE solutions in the mode that meets their data policy and infrastructure requirements including cloud (public or private), on-premises or hybrid configurations

Fast Time-to-Value

With DigiCert ONE, customers can experience rapid CA/ICA creation through automation of infrastructure setup and management.