digicert®

DigiCert® ONE Infrastructure Security

Fortune 500 and Global 2000 organizations rely on DigiCert's 25-plus years of experience delivering digital trust solutions to over 100,000 customers and billions of devices worldwide. The DigiCert ONE platform delivers digital trust for machines, software, connected devices, and content from a secure infrastructure. This infrastructure is purpose-built for high availability and fault tolerance, and it adheres to the strictest security processes and standards.

Stringent physical, system and network security

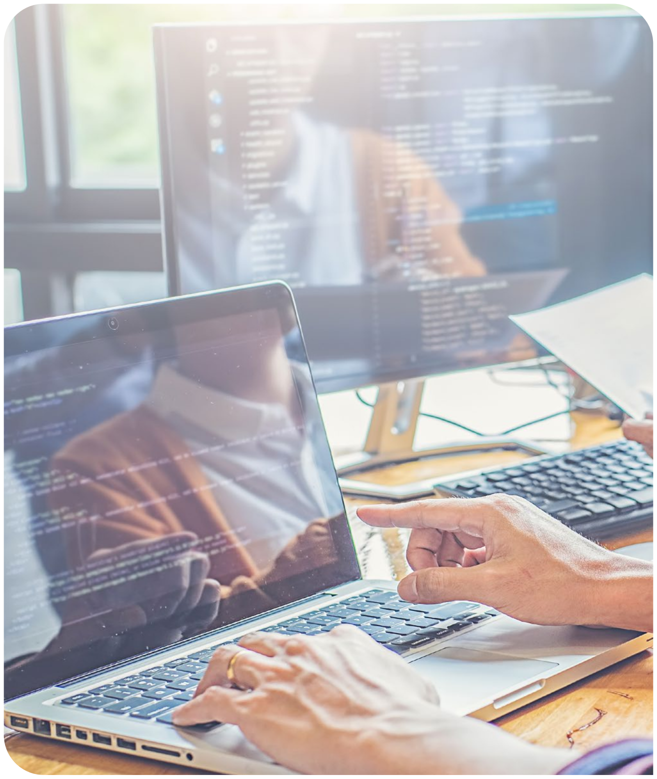
DigiCert's secure infrastructure includes the following features:

- **Physical security:** Multi-factor authentication including biometric access control methods. Dual-person control required for access to caged environment. Multiple security zones must be passed through 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-compliant Hardware Security Modules (HSM) and stored in an encrypted format.
- **System and Network Security:** In addition to supporting security industry best practices, safeguards protect against DDoS, web application attacks, resource attacks and other possible remote threats.
- **Role-based administration:** All IT services separate duties between personnel, preventing individual access to sensitive information and functions.
- **Dedicated monitoring:** DigiCert Network Operations Center provides 24x7 monitoring of the DigiCert infrastructure, systems, and networks.
- **Third-party monitoring:** DigiCert employs external third-party global services to monitor its critical infrastructure, systems, and networks.

Global high availability

DigiCert operates its secure infrastructure from data centers across the globe:

- **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.



Independently audited and certified

DigiCert solutions are regularly audited by independent third parties. DigiCert has achieved:
Applicability: Global

Product/ Scheme	Supervisory authority	Trust service requirements	Accreditation body/Auditor	Description	Applicability
SSAE-16 SOC 2 Type II and III	AICPA	Detail operational effectiveness of systems to manage customer data, based on five trust service principles—security, availability, processing integrity, confidentiality, and privacy	BDO U.S.	Annual audits to ensure data is securely managed to protect the interests of organizations and clients. SOC 2 replaces legacy SAS 70 reporting standard	Global
WebTrust™ for Certification Authorities	AICPA/CICA	Adequacy and effectiveness of controls deployed by a Certification Authority (CA)	BDO (DigiCert) EY (DigiCert Europe)	—	Global
WebTrust™ for Baseline Requirements	CA/B Forum	CA/B Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates	—	Annual audits performed on DigiCert's key management, certificate authority (CA) business practices, disclosures and CA environmental controls supporting DigiCert public and managed PKI CA services	Global
WebTrust™ for Extended Validation	CA/B Forum	CA/B Forum[5] Guidelines for the Issuance and Management of EV Certificates.	—	—	Global
WebTrust™ for Code Signing	CA/B Forum	Code Signing Working Group's Minimum Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates.	—	—	Global
WebTrust™ for VMC	AuthIndicators Working Group	Based on the Minimum Security Requirements for the Issuance of Mark Certificates	BDO U.S.	Annual audits performed on DigiCert's issuance of Mark Certificates	Global
WebTrust for Network Security	CA/B Forum		BDO	Annual audit performed on DigiCert's Network and Certificate Systems Security compliance against the CA/B Forum Baseline Network Security Requirements	Global
WebTrust for S/MIME	CA/B Forum		BDO	Annual audits performed on DigiCert's issuance of S/MIME Certificates	Global
WebTrust for MATTER			BDO	Annual audit performed on DigiCert's key management, certificate authority (CA) business practices, disclosures and CA environmental controls supporting DigiCert private and MATTER PKI CA services	Global
WebTrust for AATL	Adobe		BDO		

Applicability: Americas

Product/ Scheme	Supervisory authority	Trust service requirements	Accreditation body/Auditor	Description	Applicability
Registration Authority - Accreditation - MP and Certificate Authority - Accreditation	DirectTrust	–	BDO	Accreditation program to demonstrate adherence to data processing standards and compliance with security infrastructure, integrity and trusted identity requirements	United States
FBCA for EPCS	FPKIPA (FPKI Policy Authority)		FPKI		United States

Applicability: Europe

Product/ Scheme	Supervisory authority	Trust service requirements	Accreditation body/Auditor	Description	Applicability
ZertES Qualified Certification Services Provider	SAS/BAKOM	Swiss Law and ETSI 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 Certification for eIDAS Compliance	Agentschap Telecom, Netherlands	ETSI EN 319 411-1 ETSI EN 319 411-2 v2.2.2:27 standards to issue Qualified Certificates for Electronic Signature, Electronic Seal and website authentication. EU Regulation (EU) No 910/2014 (eIDAS)	BSI	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 Management Authority for PKIoverheid	ETSI EN 319 411-1, ETSI EN 319 411-2 v2.2.2 and PKIoverheid Program of Requirements standards to issue Qualified Certificates for Electronic Signature, Electronic Seal and Website Authentication under the Staat der Nederlanden Root	BSI	Annual audits to maintain accreditation as a TSP for the Dutch government	Netherlands
Belgium Qualified Trust Services Provider	Belgian FPS Economy - Quality and Safety	ETSI EN 319 411-1, ETSI EN 319 411-2 standards to issue Qualified Certificates for Electronic Signature, Electronic Seal. EU Regulation (EU) No 910/2014 (eIDAS)	BSI	Annual audits to maintain accreditation as a provider of Qualified certificates for electronic signatures by individuals as well as electronic seals for corporate entities in Belgium	Belgium, also applies across the EU

Applicability: Asia/Pacific

Product/ Scheme	Supervisory authority	Trust service requirements	Accreditation body/Auditor	Description	Applicability
ISAE 3402	IAASB/IFAC	ISAE 3402	BDO Sanyu	Annual audits on internal controls over financial reporting	Japan
ISO/IEC 27001	–	Compliance with ISO/IEC 27001 Information Security Management Systems Requirements Specification (formerly known as BS7799-2)	–	Annual audits to evaluate how securely an organization manages and stores its information and data in our Japan Data Center	Japan
Gatekeeper Accreditation	Digital Transformation Agency (DTA)	Australian Government's Protective Security Policy Framework (PSPF) and Australian Government Information Security Manual (ISM)	CyberCX	Annual audits that cover protective security governance, personnel security, information security, and physical security	Australia

Compliance with industry data privacy regulations

DigiCert complies with applicable privacy regulations including the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA).

Additional information is available at:
https://privacy.digicert.com/policies/

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management, to secure infrastructure, software, devices, messages, AI content and agents. Learn why more than 100,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com.