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 eIDAS1-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 function

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 dualpowered 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 FIPS2 140-2 compliant hardware security modules and stored in an encrypted format.

Independently audited and certified

In addition to DigiCert's own extensive information security policies and practices, DigiCert solutions are regularly audited by independent third parties and have achieved the following:

Applicability: Global

Product/ Scheme	Supervisory authority	Trust service requirements	Accreditation body/Auditor	Description	Applicability
SSAE-16 SOC 2 Type II and III	AICPA[3]	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 Authorities	AICPA/CICA[4]	Adequacy and effectiveness of controls deployed by a Certification Authority (CA)	BDO (DigiCert) EY (QuoVadis)		Global
WebTrust™ for Baseline Requirements		CA/B Forum[5] "Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates"		Annual audits performed on DigiCert's key management cycle management 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 "Guidelines for the Issuance and Management of EV[6] Certificates."			Global
WebTrust™ for Code Signing		Code Signing Working Group's Minimum Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates.			Global
WebTrust™ for VMC	No	Based on the Minimum Security Requirements for the Issuance of Verified Mark Certificates	BDO U.S.	Annual audits performed on DigiCert's issuance of Verified Mark Certificates	Global

[3]American Institute of Certified Public Accountants ; [4]Canadian Institute of Chartered Accountants ; [5]Certification Authority/Browser Forum ; [6]Extended Validation

Applicability: Americas

Product/ Scheme	Supervisory authority	Trust service requirements	Accreditation body/Auditor	Description	Applicability
FISMA[7]	OMB[8]	NIST[9], SP800-53, FIPS 199, FIPS 200	DataLock	Annual security reviews to ensure an up-to-date security plan, documented controls and risks assessments.	United States
Federal PKI Shared Service Provider Program:	Federal Public Key Infrastructure Policy Authority (FPKIPA) and General Services Administration (GSA[10])	NIST SP800-53, which specifies security controls for information systems supporting the executive agencies of the U.S. federal government. Adherence to Common Policy		Annual audits of services, procedures and practices as part of the identity federation agreement with the U.S. Government to provide services.	United States
FIPS-201	U.S. Federal Bridge Certification Authority (FCBA)	Cross-certification with the U.S. FBCA for issuance of PIV (Personal Identity Verification) - Interoperable smart cards to organizations that do business with the U.S. government.		Annual certification of products used in credentialing systems, physical access control systems (PACS) and PKIs to enable for placement on the GSA's [9]Approved Products List (APL).	United States
Full accreditation to DTAAP[11]	EHNAC[12]			An accreditation program to demonstrate adherence to data processing standards and compliance with security infrastructure, integrity and trusted identity requirements.	United States
Bermuda Authorised Services Provider (CSP)	Ministry of Energy, Telecommunications and E-Commerce	17799 (Code of Practice for Information Security Management), EESSI1713 and WebTrust for CAs		Biennial certification to maintain accreditation as a provider of Bermuda Authorised Certificates. QuoVadis, a DigiCert subsidiary, is the only authorized CSP in Bermuda.	Bermuda

[7]Federal Information Security Management Act ; [8]Office of Management and Budget ; [9]National Institute of Standards ; [10]General Services Administration ; [11]Direct Trust Agent Accreditation Program ; [12]Electronic Healthcare Network Accreditation Commission ; [13]European Electronic Signature Standardisation Initiative

Applicability: Europe

Product/ Scheme	Supervisory authority	Trust service requirements	Accreditation body/Auditor	Description	Applicability
ZertES Qualified Certification 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 Certification 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 accordancewith 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
Netherlands e-Recognition/ eHerkenning	Logius Dutch Government (Operator Agentschap Telecom (Dutch Telecommunications Agency) (Supervisor)	ISO 27001 (limited scope - NL eHerkenning) Compliance with ISO/ IEC 27001 Information Security Management Systems Requirements	KIWA	Provision of registration for eHerkenning products for access to Dutch Government Services on behalf of an organization	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
EUgridPMA[18] Managed CA	IGTF[19] (include APGridPMA[20] and TAGPMA[21])	Authentication Profile of the IGTF		Accreditation to operate the Managed CA for EuroGridPMA, the trust grid for e-Science Grid authentication in Europe.	Europe

[14]Swiss Accreditation Service ; [15]Bundesamt für Kommunikation ; [16]European Telecommunications Standards Institute ; [18]European Policy Management Authority for Grid Authentication ; [19]Interoperable Global Trust Federation ; [20]Asia-Pacific Grid Policy Management Authority ; [21]The Americas Grid Policy Management Authority

Applicability: Asia/Pacific

Product/ Scheme	Supervisory authority	Trust service requirements	Accreditation body/Auditor	Description	Applicability
ISAE[22] 3402	IAASB/IFAC[23]	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://www.digicert.com/digicertprivacy- policy/

[17]Policy and Security Requirements for Trust Services Provider issuing certificates; Part 1: General Requirements. Policy and Security Requirements for Trust Services Provider issuing certificates; Part 2: Requirements for Trust Service Providers issuing EU qualified certificates. These TSP component services are being provided for the following qualified trust service(s) as defined in EU Regulation 910/2014 (eIDAS): - Issuance of qualified certificates for electronic signatures (qualified trust service), in accordance with the policies: QCP-n, QCP-n-qscd - Issuance of qualified certificates for electronic seals (qualified trust service), in accordance with the policy: QCP-l, QCP-lqscd - Issuance of qualified certificates for website authentication (qualified trust service), in accordance with policies QCPw, QCP-w-psd2; [22]International Standard on Assurance Engagements; [23]International Auditing and Assurance Standards Board/International Federation of Accountants

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.

For more information, email our security experts at pki_info@digicert.com