DigiCert® Solutions
Infrastructure Security

digicert®

DigiCert® Solutions Infrastructure Security

Fortune 500 and Global 2000 organizations rely on DigiCert's 14 plus years of experience with delivering PKI, IoT & TLS/SSL solutions to millions of their users and devices worldwide. DigiCert PKI Platform, a cloud-based solution, runs on a secure infrastructure that is not only designed for high-availability and fault-tolerance, it also complies to 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 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 140-2 [1] 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:** All IT equipment is dual-powered and served by multiple independent distribution paths. In addition to redundant cooling.
- **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.

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:

[1]Federal Information Processing Standards

Certification	Accreditation Body	Requirements	Auditor	Description	Applicability
AATL	Adobe	Requirements set forth by Adobe for participation in their Approved Trust List embedded in Acrobat and Reader	BDO US	WebTrust™ for Certification Authority audit is leverage for this annual requirement	Global
Microsoft Trusted Root Program	Microsoft	Requirements set forth by Microsoft for participation in their trusted root store program	BDO US	WebTrust™ suite of audits (Certification Authority, Baseline Requirement, Extended Validation and Code Signing) are leveraged for this annual requirement	Global
Mozilla Root Store Policy	Mozilla	Requirements set forth by Mozilla for participation in their trusted root store program	BDO US	WebTrust™ suite of audits (Certification Authority, Baseline Requirement and Extended Validation) are leveraged for this annual requirement	Global
WebTrust™ for Baseline Requirements and Network Security	AICPA/CICA[2]	CA/B Forum[3] "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" and "Network and Certificate System Security Requirements"	BDO (Digicert) EY (QuoVadis)	Annual audits performed on DigiCert's key management and certificate life cycle management operations, certificate authority (CA) business practices disclosures, and CA environmental controls supporting DigiCert public and managed PKI CA services	Global
WebTrust™ for Certification Authorities		Adequacy and effectiveness of controls deployed by a Certification Authority			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 Extended Validation		CA/B Forum "Guidelines for the Issuance and Management of EV[4] Certificates"			Global

[2] Canadian Institute of Chartered Accountants [3] Certification Authority/Browser Forum
[4] Extended Validation

Certification	Accreditation Body	Requirements	Auditor	Description	Applicability
PCI-DSS SAQ D	PCI Security Standards Council				United States
DirectTrust	DirectTrust			An accreditation program to demonstrate adherence to data processing standards and compliance with security infrastructure, integrity, and trusted identity requirements	United States
Federal PKI Shared Service Provider Program	Federal Public Key Infrastructure Policy Authority (FPKIPA) and General Services Administration (GSA)	NIST SP 800-53, 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 US government		Annual certification of products used in credentialing systems, physical access control systems (PACS) and PKIs to enable for placement on the GSA's[5] Approved Products List (APL)	United States
FISMA[6]	OMB[7]	NIST[8] SP 800-53 r4, FIPS 199, FIPS 200	ElectroSoft	Annual security reviews to ensure an up-to-date security plan, documented controls and risk assessments required to maintain a PKI platform ATO with the U.S. Federal Government	United States
SSAE-18 SOC 2 Type II and Type III	AICPA[9]	Examination of the operational effectiveness of controls relevant to the Security "trust services criteria"	BDO US	Annual audits to ensure data is securely managed to protect the interests of organizations and clients. SOC 2 replaces legacy SAS 70 reporting standard	United States

[5] General Services Administration [6] Federal Information Security Management Act
[7] Office of Management and Budget [8] National Institute of Standards
[9] American Institute of Certified Public Accountants

Certification	Accreditation Body	Requirements	Auditor	Description	Applicability
EUgridPMA[10] Managed CA	IGTF[11] (include APGridPMA[12] and TAGPMA[13])	Authentication Profile of the IGTF		Accreditation to operate the Managed CA for EuroGridPMA, the trust grid for e-Science Grid authentication in Europe	Europe
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
EU Qualified Trust Service Provider (QTSP)	Agentschap Telecom, Netherlands	ETSI EN 319 411-1, ETSI EN 319 411-2 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
Netherlands e-Recognition/ eHerkenning	Netherlands e-Recognition	ISO 27001 (limited scope - NL eHerkenning)	Kiwa	Facilitate business-to-government identity and authorisation	Netherlands
Trust Service Provider (TSP) for PKIoverheid	Netherlands PKIoverheid	ETSI EN 319 411-1, ETSI EN 319 411-2 and PKIoverheid Program of Requirements standards to issue Qualified Certficates 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

[10] European Policy Management Authority for Grid Authentication [11] Interoperable Global Trust Federation
[12] Asia-Pacific Grid Policy Management Authority [13] The Americas Grid Policy Management Authority

Certification	Accreditation Body	Requirements	Auditor	Description	Applicability
ZertES Qualified Trust Services Provider	SAS[14]/BAKOM[15]	Swiss Law and ETSI[16] standards for Qualified Trust Services Provider and Time Stamping Authorities	KPMG	Annual audits to ensure conformity with the requirements for qualified certificates	Switzerland
ZertES Qualified Trust Services Provider – Remote Signing	SAS/ BAKOM	CEN EN 419 241-1 Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements	KPMG	Meets the requirements of Swiss Law for remote signing where the private signing keys are managed by a Trust Service Provider	Switzerland (Swiss Regulated / Qualified certificates)
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)		Annual audits that covers protective security governance, personnel security, information security and physical security	Australia
Bermuda Authorised Certificate Services Provider (CSP)	Ministry of Energy, Telecommunications and E-Commerce	Bermuda Electronic Transactions Act and includes elements ISO 17799 (Code of Practice for Information Security Management), EESSI[17] 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

[14] Swiss Accreditation Service [15] Swiss Federal Office of Communications [16] European Telecommunications Standards Institute [17] European Electronic Signature Standardisation Initiative

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/digicert-privacy-policy/

Key Benefits

Faster Time-to-Value

With DigiCert cloud-based solutions, everything a customer needs to deploy and activate their authentication, encryption and digital signature solutions are included. Customers can have a working solution up and running quickly with a minimum amount of planning.

Lower Cost of Ownership

DigiCert cloud-based approach to PKI, IoT & TLS/SSL eliminates the costs associated with purchasing, deploying, and maintaining a dedicated on-premises solution.

Proven Operational Excellence

DigiCert is a proven leader in delivering a world-class, reliable, and secure cloud-based infrastructure. With over 5 billion validations happening every year, DigiCert has proven its operational excellent for the past 14 years by delivering the expertise, ease of use, and security that customers love.

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

digicert®