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

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 0TJ-17.S9 (s sepedministr)20.4 (tioyyr7.2pr)8.G d[dutTw 0[n additB0 1 Tf[Al0.6)/b ted f (ptionfun (teTw 0])0.09 0.45 0.73 sc3/TT0 3

	Product/ Scheme	Supervisory authority	Trust service requirements	Accreditation body/Auditor	Description	Applicability	
	SSAE-16 SOC 2 Type II and III	AICPA3	Detail operational effectiveness of systems to manage customer data based				
			principles"—security, availability, processing			Global	
					Global		
			perf	ormed on	Clobal		
			Digi	Cert's ke53 8 ý } J0	-1.444 Talfahagement	cyğ4 ¢le ĴrJ0 -1.444 Td(manage	ement
	CA/E	3 Forum5					
		WebTrust™ for		_			
		Code Signing					
		-		-			
		-		_			

)[

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 and General Services Administration	NIST SP800-53, 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	with the U.S. FBCA for issuance of - Interoperable smart cards to organizations that do business with the U.S. government.		of products used in credentialing systems, physical access control to enable for placement on the GSA's ⁹ Approved Products List	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	of Practice for Information Security EESSI1713 and		maintain accreditation as a provider of Bermuda subsidiary, is the only authorized CSP in Bermuda.	Bermuda

Applicability: Europe

Product/ Scheme	Supervisory authority	Trust service requirements	Accreditation body/Auditor	Description	Applicability
	SAS ¹⁴ /BAKOM ¹⁵	Swiss Law and ETSI			
Services Provider					
		Stamping /alt I/TT2 1 Tf0 1	1 25 Td\$m0 oA 41 40	97 255.375 cm0 0 m 8 .75 0 l1	LE Td C or) r) rCorCor
				yAEE ESEI€BAAGARN)/1DBogusAE570ar	

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.

solutions in the mode that meets their data policy and

© 2025 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.