How GlobalSign Secures Its Environment

WHITE PAPER

At GlobalSign, the security of our services and customer data is our highest priority. This white paper generally describes the practices and controls we implement to ensure the integrity, confidentiality and availability of our environment.

GlobalSign's Approach to Information Security

As one of the longest operating and largest publicly trusted Certification Authorities (CAs), GlobalSign has a long track of providing high security Public Key Infrastructure (PKI) solutions. Information security is an important topic on the agenda at the board level and senior management is heavily involved in defining and ensuring implementation of security policies that guarantee the confidentiality, integrity and availability of the services we provide.

We have a dedicated global security and compliance team that is in charge of operating our information security management system. The system is based on the ISO 27001 standard and the WebTrust Principles and Criteria for Certification Authorities - the globally recognized framework for operating a publicly trusted CA. Our management system addresses all common areas of information security, including but not limited to the following:

- Information security governance and strategy
- Continuous threat profiling, risk assessments and risk management
- Personnel awareness and trustworthiness
- Physical and environmental security
- Security operations and monitoring
- Access management
- System development and maintenance
- Incident management and breach response
- Business continuity and disaster recovery

Apart from having defined and distributed the necessary policies throughout the firm, we have deployed procedural and technical security controls in order to protect our PKI services:

- Multi-factor authentication on all our applications and systems
- Multi-layer networks with strong filtering controls
- Advanced malware detection controls
- Air gapping of critical key material such as root CA keys
- Military-grade physical access barriers restricting access to our data centers
- Intrusion detection and prevention systems in both our office and data center networks
- Full disk encryption of our IT equipment
- Recurring vulnerability assessment (quarterly) and penetration testing exercises (annually)
- Review source code of critical applications
- Responsive patch management

Next to pursuing the highest security of our own environment, GlobalSign is a proud and long-standing member of the most critical, standards-driven bodies and organizations, including the Certification Authority (CA) / Browser Forum, the Certificate Authority Security Council (CASC) and the Industrial Internet Consortium (IIC), and is compliant with the North American Energy Standards Board (NAESB), the National Institute of Standards and Technology (NIST) and the National Cybersecurity Center of Excellence (NCCoE).

Employee Awareness and Trustworthiness

As information security threats quickly evolve, so must the information, guidance and training we offer towards our employees. Ensuring awareness of threats to data privacy and information security is a continuous process. This is reflected not only in professional training for employees, but in numerous other activities to drive awareness within the entire organization. In order to ensure a mindset of constant vigilance, our employees are recurrently subjected to phishing tests and simulation of other social engineering attacks.

GlobalSign also verifies trustworthiness of employees performing critical functions within the organization. Employee verification includes skills, education, previous employment, professional reference, and criminal background checking (where allowed in local jurisdiction of the employee).

Business Continuity and Disaster Recovery

Our environment has been built in a resilient way and is capable of withstanding major environmental disasters, organized or deliberate disruption, and loss of utilities and services. Our methodology for business continuity management and disaster recovery is based on the ISO22301 standard and incorporates the following:

- Business impact analysis to quantify business impact and determine appropriate continuity strategies
- Alignment of service recovery time and point objectives with key performance indicators (KPIs) desired by our customers
- Emergency communication and notification procedures to inform our customers and other relying parties
- Continuous on- and off-site back-ups of information
- Yearly re-evaluation of the business continuity strategy and business continuity plans
- Regular testing of the business continuity plan and recovery procedures to ensure recovery time and point objectives can be met
- Dedicated recovery processes and plans for CA-specific disasters such as key compromise

To ensure high availability, we have data centers around the world. Should one of these experience either a natural disaster or man-made event, then operations will fail over to another location within the defined recovery time and recovery point objectives. Additionally, those data centers, as well as the issuance facility, are all subject to the standard precautionary measures, such as multiple detection systems, multiple connectivity lines and 24x7x365 monitoring. This means we will be alerted at the very earliest opportunity to any such events either taking place or about to take place to best position us to react in the most appropriate and effective way.

Data Privacy

GlobalSign respects the right to privacy of its customers. Our privacy policy is in line with the European Union General Data Protection Regulation (GDPR) and applies to the entire GlobalSign network and to all the information collected for issuing the whole range of GlobalSign products and services:

- We protect personal data using appropriate physical, technical and organizational security measures.
- We request explicit consent for all the personal data subjects may submit.
- We collect no personal data unless the subject submits it.
- We use the data the subject submits only for purposes defined within our privacy policy.
- We securely dispose personal data after use.
- Subjects have the right to review the personal data that GlobalSign holds and check it for consistency.
- Subjects have the right to correct data in the remote case that errors may be found in our records.

Compliance and Audit

To assess and demonstrate compliance, GlobalSign's environment is subjected to multiple internal and external audits, including:

- Independent annual ISAE3000 SOC3 Type II audits against the industry-leading frameworks for certification authorities, by which we have been certified since 2001 – the second longest in our industry: WebTrust for Certification Authorities, Extended Validation, SSL Baseline Requirements, Code Signing and EV Code Signing.
- Bi-annual eIDAS conformity assessment based on the eIDAS regulation and ETSI standards for European qualified trust service providers
- Vulnerability scans, which focus on network filtering, configuration management, patch management, application security and infrastructure security
- Continuous monitoring of control effectiveness to ensure compliance and security controls are effectively designed and implemented
- Annual independent assessment against ISO27001:2013 (Information Security Management System) & ISO22301:2012 (Business Continuity Management System). GlobalSign is the first global CA to complete both ISO27001 and ISO22301 certifications.

All the assessment reports are publicly available at https://www.globalsign.com/en/repository/

About GlobalSign

GlobalSign is the leading provider of trusted identity and security solutions enabling businesses, large enterprises, cloud service providers and IoT innovators around the world to secure online communications, manage millions of verified digital identities and automate authentication and encryption. Its high-scale Public Key Infrastructure (PKI) and identity solutions support the billions of services, devices, people and things comprising the Internet of Everything (IoE).

US: +1 877 775 4562
UK: +44 1622 766766
EU: +32 16 89 19 00

sales@globalsign.com
www.globalsign.com

GlobalSign®
GMO INTERNET GROUP