

# Symantec Identity and Authentication Solutions Infrastructure Security

Secure, reliable, audited cloud-based authentication infrastructure

## Fact Sheet: Authentication

Leading organizations rely on Symantec's 20 years of experience delivering cloud-based authentication solutions to hundreds of millions of users and devices around the world.

Designed for high-availability, fault-tolerance, and adherence to the strictest security processes and standards, Symantec cloud-based authentication solutions deliver the performance, reliability, and security your organization requires to power its authentication projects.

### Key Features

#### *Stringent Physical and System Security*

Symantec cloud infrastructure is operated from multiple Tier 4 data centers—the most stringent level of data center defined by ANSI/TIA<sup>1</sup>-942—featuring:

- **Network isolation:** Data centers are physically and logically separated from Symantec's corporate network.
- **Redundant, controlled infrastructure:** Fully redundant subsystems and compartmentalized security zones controlled by biometric access controls methods.
- **Restricted access to trusted employees:** Only Symantec employees who have passed thorough background checks have access to Symantec cloud infrastructure.
- **Secure key management:** Cryptographic keys are generated on dedicated FIPS<sup>2</sup> 140-2 compliant hardware security modules, and stored in an encrypted format.

#### *Service Management Best Practices*

Symantec follows a rigorous set of IT maintenance and information security best practices, including:

- **Role-based administration:** All IT services separate duties between personnel and prevent individual access to sensitive information and functions.
- **Incident management process:** Extensively documented incident management processes and procedures, and

regular “fire drill” exercises ensure IT personnel can effectively respond to security incidents.

#### *High Availability*

Symantec infrastructure relies on multiple data centers on the East and West coasts of the United States to deliver:

- **Uninterrupted operations:** Active-active configuration provides uninterrupted operation during maintenance or in the event of a failure at any one data center.
- **Redundant power and cooling systems:** All IT equipment is dual-powered, and served by multiple independent distribution paths. Cooling infrastructure is independently dual-powered, and fault-tolerant site infrastructure features electrical power storage and distribution facilities.
- **Binding SLAs:** Symantec Service Level Agreements guarantee 99.95 percent availability.

#### *Continuous Global Monitoring*

- **Dedicated systems monitoring:** Symantec's dedicated Network Operations Center provides 24 hours a day, seven days a week monitoring of host intrusion and network intrusion detection systems examining the Symantec infrastructure, IT systems, and network activity.
- **Third-party monitoring:** Symantec employs an independent external global service to monitor its critical services and perform daily vulnerability scans.

#### *Independently Audited and Certified*

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

- **AICPA SOC<sup>3</sup> 2 Type 2:** Annual attestation of the AICPA SOC 2 to provide assurance to customers in areas including

1. American National Standards Institute/Telecommunications Industry Association

2. Federal Information Processing Standards

security, following the retirement of the legacy SAS 70 reporting standard.

- **AICPA/CICA WebTrust™ for Certification Authorities and WebTrust™ for Certification Authorities – Extended Validation:** Annual examinations performed for Symantec’s key management and certificate life cycle management operations, certificate authority (CA) business practices disclosures, and CA environmental controls supporting Symantec’s public and managed PKI CA services.
- **Federal PKI Shared Service Provider Program:** Symantec PKI has been certified for compliance with the requirements of NIST<sup>4</sup> SP800-53, which specifies security controls for information systems supporting the executive agencies of the U.S. federal government.
- **FIPS-201 Certified:** Symantec has been approved for cross-certification with the U.S. Federal Bridge Certification Authority for issuance of PIV(Personal Identity Verification)-Interoperable smart cards to organizations that do business with the US government.

### Key Benefits

#### *Faster Time-to-Value*

With Symantec cloud-based solutions, everything a customer needs to deploy and activate their strong authentication solution is included. No hardware to purchase, no software to deploy—customers can have a working solution up and running quickly with a minimum amount of planning.

#### *Lower Cost of Ownership*

Symantec cloud-based approach to authentication eliminates the costs associated with purchasing, deploying, and maintaining a dedicated in-premise authentication solution.

#### *Proven Operational Excellence*

Symantec is a proven leader in delivering a world-class, reliable, and secure cloud-based infrastructure. With over 1 billion credentials issued and 20 years of operational

experience, Symantec cloud-based solutions put the experts on your team without you having to hire them.

### More Information

#### *Visit our website*

<http://enterprise.symantec.com>

#### *To speak with a Product Specialist in the U.S.*

Call toll-free 1 (800) 745 6054

#### *To speak with a Product Specialist outside the U.S.*

For specific country offices and contact numbers, please visit our website.

#### *About Symantec*

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world’s largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives. To learn more go to [www.symantec.com](http://www.symantec.com) or connect with Symantec at: [go.symantec.com/socialmedia](http://go.symantec.com/socialmedia).

#### *Symantec World Headquarters*

350 Ellis St.  
Mountain View, CA 94043 USA  
+1 (650) 527 8000  
1 (800) 721 3934  
[www.symantec.com](http://www.symantec.com)

<sup>3</sup>. American Institute of Certified Public Accountants Service Organization Controls

<sup>4</sup>. National Institute of Standards and Technology