Certification and Compliance

Contents

Overview

This article provides a breakdown on the levels of compliance for industry standards that the Swivel product can provide. It also includes information on the level of security and standards certification achieved. By buying a Swivel product this does not necessarily make you instantly compliant. For example with PCI compliance a risk assessment must be carried out. You achieve compliance by having the correct protection in place.

Certification

CCTM

The CESG Claims Tested Mark (CCTM) scheme provides a government quality mark for the public and private sectors based on accredited independent testing, designed to prove the validity of security functionality claims made by vendors. In more colloquial terms, the CCTM is designed to assure public bodies that a product or service does ?what it says on the box?.

http://www.cctmark.gov.uk/

Test Lab Report Reference: U090922

Compliance

PCI User Access 8.2

In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:

- Password or passphrase
- Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)

Compliance can be achieved with Swivel Single Channel or Dual Channel authentication

PCI Employee Remote Access 8.3

Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

Compliance can be achieved with Swivel Dual Channel authentication

ISO-27002:2005 Section 11.4.2 User Authentication for External Connections

Appropriate authentication methods should be used to control remote access to the network.

Compliance can be achieved with Swivel authentication

Gramm?Leach?Bliley Act

Section 501(b) of the Gramm?Leach?Bliley Act, 15 USC 6801, require banks and savings associations to safeguard the information of persons who obtain or have obtained a financial product or service to be used primarily for personal, family or household purposes, with whom the institution has a continuing relationship.

Compliance can be achieved with Swivel authentication

USA PATRIOT Act

The regulations implementing section 326 of the USA PATRIOT Act, 31 USC § 5318(l), require banks, savings associations and credit unions to verify the identity of customers opening new accounts.

Compliance can be achieved with Swivel authentication

The Federal Financial Institutions Examination Council (FFIEC)

Financial institutions offering Internet-based products and services should have reliable and secure methods to authenticate their customers. The level of authentication used by the financial institution should be appropriate to the risks associated with those products and services. Financial institutions should conduct a risk assessment to identify the types and levels of risk associated with their Internet banking applications. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks. The agencies consider single-factor authentication, as the only control mechanism, to be inadequate in the case of high-risk transactions involving access to customer information or the movement of funds to other parties.

Compliance can be achieved with Swivel authentication, subject to a risk assessment

Sarbanes Oxley

Section 404, unlike some other federal regulations, does not specifically set out technological requirements. Nonetheless, strong authentication technology will necessarily play a major role in achieving compliance.

Compliance can be achieved with Swivel authentication

Health Insurance Portability and Accountability Act (HIPAA)

Covered entities must also authenticate entities it communicates with. Authentication consists of corroborating that an entity is who it claims to be. Examples of corroboration include: password systems, two or three-way handshakes, telephone callback, and token systems.

Compliance can be achieved with Swivel authentication

Code of Connection (CoCo)

For connection to the Government Connect Secure Extranet (GCSX). Local Authorities must comply with the Code of Connection (CoCo), drawn up between GC, OGC Buying Solutions, CSIA and Communications Electronics Security Group (CESG), prior to connection. The LA CoCo submission is authorised by OGCbs as advised by CESG. CoCo specifies 2 factor authentication

Compliance can be achieved with Swivel Dual Channel authentication

Code of Federal Regulations Title 21 CFR Part 11

The Food and Drug Administration (FDA) in the United States designed Part 11 of Title 21 of the Code of Federal Regulations (21 CFR Part 11) to help ensure that life sciences companies can use electronic records and signatures that are equivalent to those based on paper and ink. Strong or two factor authentication is not specified, but can be used to verify the digital signature: ?The agency decided not to make the required extent and stringency of controls dependent on the type of record or transactions, so that firms can decide for themselves what level of controls are worthwhile in each case?, (3) the circumstances under which extra security and authentication measures are warranted in open systems?

http://www.fda.gov/ora/compliance_ref/part11/FRs/background/pt11finr.pdf#page=36

Compliance can be achieved with Swivel authentication

Basel II

The Basel II Accord, which went into affect in member countries by year-end 2006, is based on three pillars, designed to ensure that banks effectively monitor risk and implement sufficient risk-management practices to protect the institution. The committee defines operational risk as "loss resulting from inadequate or failed internal processes, people and systems or from external events."

Authentication is not specified but would help to minimise the operational risk.

Compliance can be achieved with Swivel authentication

FIPS 200

The minimum security requirements cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: (vii) identification and authentication.

Identification and Authentication (IA): Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Compliance can be achieved with Swivel authentication

FIPS 140-2

Swivel uses the Java Secure Random number generator for all random numbers within Swivel. This class provides a cryptographically strong random number generator (RNG). A cryptographically strong random number minimally complies with the statistical random number generator tests specified in FIPS 140-2 Security Requirements for Cryptographic Modules, section 4.9.1. Additionally, SecureRandom must produce non-deterministic output and therefore it is required that the seed material be unpredictable and that output of SecureRandom be cryptographically strong sequences as described in RFC 1750: Randomness Recommendations for Security.

Compliance can be achieved with Swivel authentication

NIST Special Publication 800-53

Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. NIST Special Publication 800-63 provides guidance on remote electronic authentication including strength of authentication mechanisms.

Compliance can be achieved with Swivel for some levels of authentication

NIST Special Publication 800-63 Electronic Authentication Guideline Level 1

No Identity Proof Required

Compliance can be achieved with Swivel authentication

NIST Special Publication 800-63 Electronic Authentication Guideline Level 2

Single Factor Remote Network Authentication

Compliance can be achieved with Swivel authentication

NIST Special Publication 800-63 Electronic Authentication Guideline Level 3

Multi Factor Remote Network Authentication

Compliance can be achieved with Swivel authentication