PCI DSS 2.0

Statement of Compliance

Relating to

Softdial Contact Center™ Version 10.6

statement

Contents

Introduction **1**

Statement of Compliance **2**

Compliance Comments **3**

§2.3 Encrypt all non-console administrative access. 3

§2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data. 3

§3 General comments on protecting cardholder data. 3

§3.4 Render PAN, at minimum, unreadable anywhere it is stored. 4

§3.5 Cryptographic key protection. 4

§3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary. 4

§3.5.2 Store cryptographic keys securely in the fewest possible locations and forms. 5

§4.1 Strong cryptography and public networks. 5

§5.1 Antivirus software. 5

§6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes. ... 5

§7 Restrict access to cardholder data by business need to know. 5

Re: Appendix A – Additional PCI DSS Requirements for Shared Hosting Providers. **6**

§A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment. 6

§A.1.2 Restrict each entity's access and privileges to its own cardholder data environment only 6

§A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10. 6

§A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider. 7

Introduction

This document states **Sytel Limited**'s position with respect to compliance with the **Payment Card Industry Data Security Standard version 2.0**.

Sytel is an OEM vendor of a call center platform called **Softdial Contact Center™ (SCC)**. Some implementations of SCC are delivered as a managed service by a service provider to an end-user by a third-party. Some implementations are delivered directly by Sytel.

Sytel attest that SCC is a PCI DSS 2.0 compliant platform.

It should be noted, however, that vendor compliance with PCI DSS does not automatically enable a service provider using SCC to assert that their implementation is PCI DSS compliant. **It is the responsibility of service providers and end-users** directly using SCC to validate their use of the SCC platform in order to ensure compliance. This document provides advice on areas of implementation where this is needed.

statement

Statement of Compliance

This statement of compliance relates to

- PCI DSS version 2.0
- Softdial Contact Center™ version 10.6

1. SCC is a hosted contact center and e-commerce enabling technology platform. It is deployed by hosted contact center service providers and end user contact center customers.

2. Sytel's end-user customers will invariably be card-not-present merchants who will need to assert compliance using Self-Assessment Questionnaire (SAQ) categories A, C or D. The category will depend on the end-user's business model.

3. **Sytel attests that its product Softdial Contact Center™ is PCI DSS 2.0 compliant** for the purposes of end-user Self-Assessment Questionnaire (SAQ) categories A, C and D.

4. It should be noted that SCC is a highly configurable and customisable call center platform. This means that it is possible for an end-user to abuse the software to make it behave in a manner that does not comply with PCI DSS. For example an end-user could produce a script that does not suspend recording of a call recording before capturing credit card details. Therefore, **it is the responsibility of service providers and end-users** directly using SCC to validate their use of the SCC platform in order to ensure compliance.

statement

Compliance Comments

The section references in this document refer to PCI DSS requirement numbers in the PCI DSS document.

§2.3 Encrypt all non-console administrative access.

Administrative access in SCC is facilitated by web-based administration applications, and by scripts developed using **Softdial Scripter**™. All forms of administrative access can be configured to use SSL/TLS, and should be in order to ensure compliance.

§2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data.

SCC implements application services that may be involved in dealing with cardholder data. SCC implements a model of separate service process instance for each tenant for all application services. This facilitates the hosting provider being able to comply with PCI DSS rules.

In addition, if hosting providers use Softdial Scripter™ to deliver applications to end-users, dual key encryption enables PAN data to be encrypted using a different key per tenant.

§3 General comments on protecting cardholder data.

SCC contains a powerful scripting environment that can be integrated with merchant service functions. It is possible for users to develop scripts that would not comply with the PCI DSS rules on protecting cardholder data, in exactly the same way that it is possible for a programmer to write programs that do not comply. **The script designer is responsible** for ensuring that scripts are developed in such a manner that PCI DSS rules are not compromised.

§3.4 Render PAN, at minimum, unreadable anywhere it is stored.

PAN, and other card data is captured either through agent-based audio capture or via DTMF detection or speech recognition. In order to enable compliance:

- SCC provides scripting primitives to pause call recording and resume call recording. These **must** be used for all forms of cardholder data capture, to avoid having recording files contain data that can be analysed to access cardholder data.

- SCC encrypts all DTMF digits and captured speech stored in its log files, and for sessions subject to paused call recording have such logging turned off altogether.

- If it is necessary for the user to store PAN data, SCC provides a scripting library with dual-key encryption which enables PAN data to be stored using strong encryption with tenant-specific keys. In order to minimize the risk of exposure through reverse engineering, this library is only available on request.

§3.5 Cryptographic key protection.

Sytel provides a means to set a private crypto key for each installation and a private key per tenant. The end customer is expected to provide a public key to be used for encryption of data that may be stored. Validating hashes can only be achieved by using both public and private keys together.

§3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.

Private cryptographic keys are automatically generated by the system using a form of Globally-Unique Identifier (GUID) with a checksum. Private keys are not user-configurable in order to mitigate custodianship issues.

The process for private key change involves a nominated service provider or end-user custodian requesting a new private key via Sytel Support. The outcome of this process is a new key and the supply to custodian of the old private key to enable archive decryption.

statement

The key generation software is only available to Sytel support staff in object code form and custodianship of the key generation source code is limited to 2 trusted personnel within Sytel, both of whom have a minimum of 10 years' service within the company.

§3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.

Sytel does not publish this information except to service providers subject to the requirements of §3.5.2b

§4.1 Strong cryptography and public networks.

All public network interfaces within SCC are configurable to use SSL. Private network interfaces (for example signalling between Softdial CallGem™, Sytel's predictive pacing and ACD engine, and Softdial Telephony Gateway™ (STG), a softswitch and media processor application) would normally be deployed securely within the same LAN. If such interfaces traverse public networks they must do so via a secure VPN tunnel to ensure compliance.

§5.1 Antivirus software.

SCC contains 2 real-time applications; Softdial CallGem™ and STG. Real-time applications require uncontended access to operating system resources. This means that any antivirus software installed on the systems hosting these services must remain non-resident during the operating day, and that scans should be run as part of nightly scheduled outage.

§6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes.

Sytel attests that it fulfils industry best practice requirements in respect of SCC. SCC is also an application scripting platform upon which third-parties can build applications. **The user is responsible** for ensuring that security flaws are not introduced.

§7 Restrict access to cardholder data by business need to know.

Sytel attests that its own authentication scheme conforms to the technical requirements needed to implement strong access control measures, as defined in section 7. SCC provides a user authentication scheme that enables role-based access. New users set up in the system have a basic minimum set of privileges. **The user is responsible** for using this scheme to set up a compliant set of access control measures.

Re: Appendix A – Additional PCI DSS Requirements for Shared Hosting Providers.

SCC is an OEM contact center hosting product, and is used extensively by third parties to deliver shared contact center hosting. SCC facilitates compliance with the requirements listed in Appendix A, subject to the following comments:

§A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.

The tenant-side services within SCC should to be run on a dedicated host (or virtual server) to ensure compliance.

Compliance can still be achieved running multiple tenants services on one host but this requires significant security configuration effort. The easiest way to achieve this is for service providers who need to provide PCI DSS compliant services to their users to provision a VM per tenant.

§A.1.2 Restrict each entity's access and privileges to its own cardholder data environment only

The SCC authentication model is segregated by tenant. Each tenant manages their own user/administrator community. Tenant access to resource is managed by the hosted service provider. **The hosted service provider is responsible** for ensuring that limits are set per tenant so that resources cannot be monopolised or security vulnerabilities exposed.

Again the easiest way for the service provider to do this for a SCC installation is to adopt a 'VM-per-tenant' approach.

§A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.

The logging facilities within SCC are compliant, with an out-of-the box installation. The service provider does not need to make changes to logging behaviour to comply.

§A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.

In a compromise situation timely remedy is important. The Sytel support organisation needs to be part of this process. Service providers need to certify Sytel to be able to gain remote access on demand in order to assist with forensic investigation. Having a codified trust relationship in place is necessary for prompt resolution of such issues and will be required to be in place as part of any service provider attestations in respect of PCI DSS compliance.

statement

statement

www.sytelco.com
info@sytelco.com
+44 (0)1296 381 200

Sytel Limited 1 Cromwell Court New Street Aylesbury Buckinghamshire HP20 2PB UK