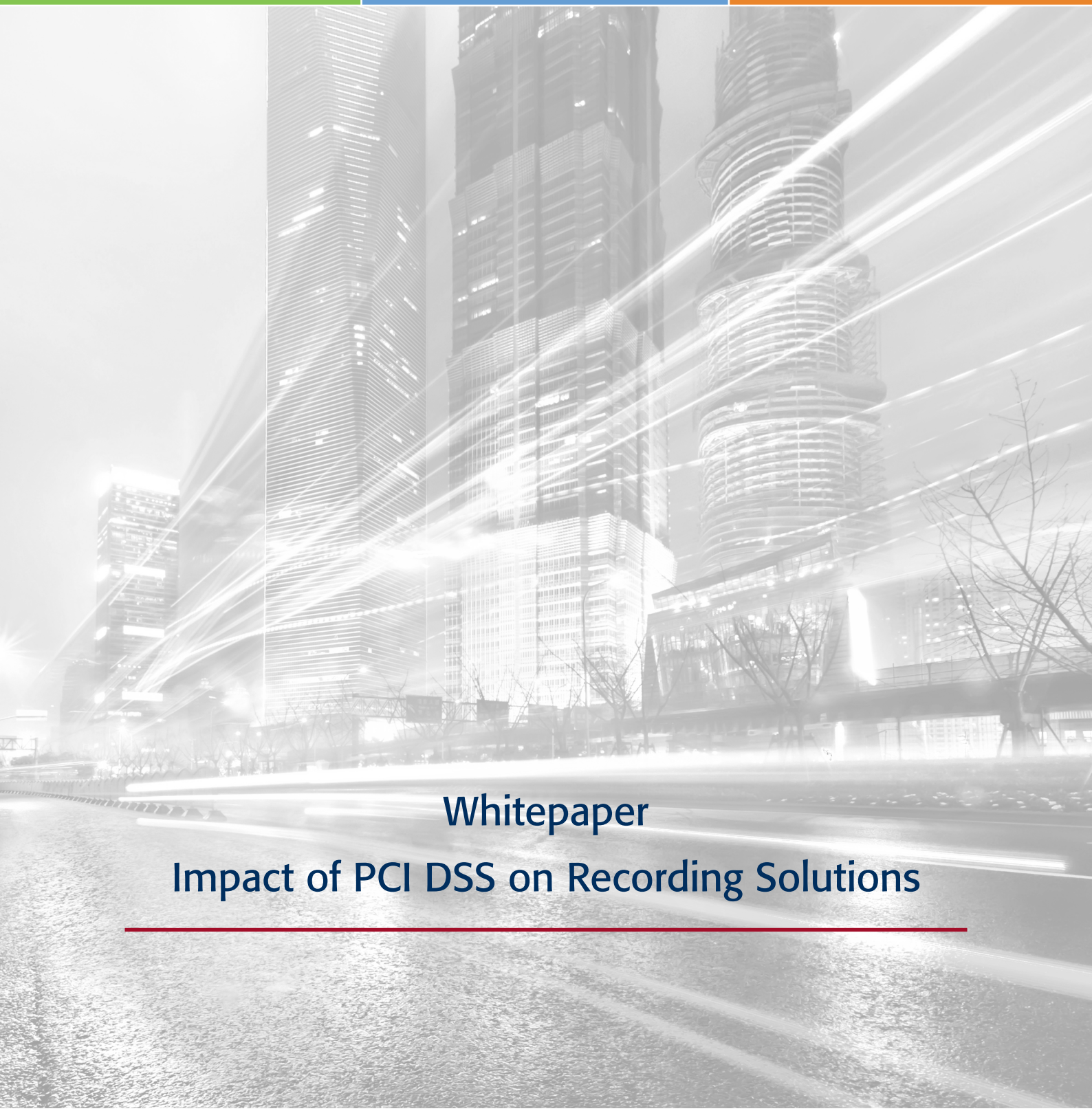

Whitepaper

Impact of PCI DSS on Recording Solutions

We record & analyze communications

ASC

1 What is PCI DSS?

PCI DSS stands for Payment Card Industry Data Security Standard, and is a worldwide security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). (http://www.pcisecuritystandards.org) The standard was created to help organizations that process card payments prevent credit card fraud, hacking and various other security vulnerabilities and threats. A company processing, storing, or transmitting payment card data must be PCI DSS compliant. Non-compliant companies who maintain a relationship with one or more of the card brands, either directly or through an acquirer risk losing their ability to process credit card payments and being audited and/or fined. All in-scope companies must validate their compliance annually. This validation can be conducted by auditors - i.e. persons who are PCI DSS Qualified Security Assessors (QSAs), however smaller companies have the option to use a self-certification questionnaire. Whether this questionnaire needs to be validated by a QSA depends on the requirements of the card brands in that merchant's region.

2 How are ASC recording solutions affected by the PCI DSS standard?

ASC recording solutions may unintentionally record and store communications containing credit card data (account numbers), if e.g. a customer reads out his credit card account number (also called Primary Account Number (PAN)) to the call center agent via the telephone. Even more sensitive is the so-called card validation code (CVC) also called card verification value (CVV) or card security code (CSC) (or Kartenprüfnummer (KPN)). This information must not be stored in any case according to the PCI standard.

When screen recording is used, the PAN and CVC may also be captured unintentionally and stored on the recorder.

3 Solution

The primary goal shall be to avoid the recording of credit card data in the first place by muting audio and excluding credit card data input from screen recording.

In order to achieve this goal ASC will provide detailed instructions on how to configure the audio and screen recording to avoid the capture of credit card information. In addition templates for Standard Operating Procedures (SOP) for the customers will be provided, detailing the procedures for muting audio.

As long as the system is configured correctly and the users adhere to the SOPs the recording of credit card information will be reduced to exceptional recording due to human error. In order to reduce the potential security vulnerabilities even further a couple of measures will be taken within the ASC recording solution to avoid the misuse of such unintentionally and exceptionally recorded credit card data. These measures comprise of:

- Encrypted storage of audio data (Industry standard AES encryption)
- Encryption of audio transmission to players
- Hardening of ASC's recorders by the means of port scanners and ongoing thorough security threat assessment
- Virus scanner (upon request)
- Firewall
- Deletion of unintentional recorded credit card information (with two person integrity)
- Central logging of system and security events

Please note that despite some statements made by other players in the marketplace, encryption (even so-called end-to-end encryption) will not automatically make a recording solution PCI DSS compliant. As stated before there is credit card information which must not be recorded at all (CVC), even encrypted.

Encryption will only help to reduce the leakage of unintentionally recorded credit card information.

PCI DSS compliance can only be testified for merchants or service providers i.e. existing installations dealing with cardholder data. ASC provides solutions which are designed in a way that they can be part of an overall system which meets the PCI requirements and can hence be PCI DSS certified.

Appendix:

High level description of the 12 PCI DSS requirements and ASC's comments

Requirement Number	Description	ASC's comment
1	Install and maintain firewall configuration to protect cardholder data.	Firewalls shall be configured according to ASC's product documentation.
2	Do not use vendor-supplied defaults for system passwords and other security parameters	ASC systems are deployed with specific accounts and passwords.
3	Protect stored cardholder data	The primary goal is to not record cardholder information in the first place. Exceptional cardholder data stored due to human error is encrypted and protected by access rights.
4	Encrypt transmission of cardholder data across open, public networks	ASC's programs use secure transmission mechanisms (HTTPS, SFTP, SSL/TLS) for all communication across the network.
5	Protect all systems against malware and regularly update antivirus software or programs	Virus scanners can be installed on ASC recorders.
6	Develop and maintain secure systems and applications	▪ ASC will include latest patches of third-party software in every new release ▪ ASC software will be checked with static code analyzer ▪ ASC development regularly executes code reviews ▪ System security will be checked with security scanner for every new release ▪ ASC systems will be checked by independent security experts at regular intervals
7	Restrict access to cardholder data by business need-to-know	The primary goal is to not record cardholder information in the first place. Exceptional cardholder data stored due to human error can only be accessed following a two person integrity mechanism.
8	Identify and authenticate access to system components	Support of LDAP and two person integrity login as well as a detailed audit trail are available.
9	Restrict physical access to cardholder data	Physical access to the recorders can only be restricted by the customer. E.g. by placing recorders in server rooms with restricted access. Archives of communication are stored in a proprietary format and are encrypted i.e. unauthorized obtained archive media cannot be played back.
10	Track and monitor all access to network resources and cardholder data	ASC systems provide a detailed audit trail.
11	Regularly test security systems and processes	At customer's discretion.
12	Maintain a policy that addresses information security for all personnel	At customer's discretion.

ASC Technologies AG
Seibelstraße 2 - 4 | Phone +49 6021 5001 0
63768 Hösbach | Fax +49 6021 5001 310
Germany | hq@asctechnologies.com