PCI DSS Compliance When Recording Calls In Contact Centres

Introduction

Anyone doing business in what's known as the call centre or contact centre sector, regardless of their vertical market focus, will be aware of the Payment Card Industry standards. That is: the Payment Card Industry Data Security Standard (PCI DSS); and the associated Payment Application Data Security Standard (PA-DSS).

Furthermore, anyone looking to develop a business application to serve the contact centre market will be aware of the need to comply with the PCI DSS and PA-DSS standards.

Specifically, many will be concerned with technology solutions, either from a user point of view, or from the perspective of a vendor or solutions provider.

This application note looks at one form of technology solution to solve the issue of tone elimination in recordings of calls between customers, clients or subscribers and contact centre agents or other staff members.

It is addressed, primarily, at application developers – those developing business focused contact centre applications for both business-to-consumer (B2C) and business-to-business (B2B) deployments.

PCI DSS Compliance

> *Anyone looking to develop a business application to serve the contact centre market will be aware of the need to comply with the PCI DSS and PA-DSS standards.*

PCI standards

The global PCI DSS mandates that any business, of any size, that stores, processes or transmits cardholder data obtained from payment cards, and/or sensitive authentication data (SAD), adheres to its information security best practices. Those are identified in a framework – a minimum set – of 12 specific requirements for protecting cardholder data.

Those requirements are supported by the three-step process of assess, remediate and report, facilitating an ongoing process for continuous compliance. The PCI DSS applies to all entities involved in payment card processing, including merchants, payment card processors, financial institutions, and service providers.

Legislation

Significantly, the PCI DSS is not designed to supersede local, regional or sector laws, legislation, or other legal and regulatory requirements. On the other hand, its impact may well be reinforced by additional controls and practices, to further mitigate risks.

The needs of developers

An application developer, implementing a contact centre platform, will need a technology solution to enable the delivery of the controls and practices necessary to ensure ongoing compliance with the PCI DSS.

An essential technology for developers of contact centre applications is that of media processing for telecommunications; what are often referred to as telephony resources. As many credit card transactions are conducted via telephone, whether through the legacy PSTN or over a next generation, IP-based network, the processing, storage and transmission of cardholder data naturally occurs during telecommunications.

The sections of the PCI DSS relevant to a telephony-based transaction refer to sensitive authentication data (SAD), which includes magnetic-stripe data (or the equivalent on a chip), the 4/3-digit card security code, and personal identification numbers (PINs) or PIN blocks.

Security requirements

PCI DSS security requirements include the common sense obligation to protect stored cardholder data, by restricting access to system operators that have a business need to know and by restricting physical access to such data. Specific requirements go further in that they require that cardholder data must not be stored after authorisation, even if encrypted.
Prior to authorisation, the temporary storage of SAD may be permitted by individual payment brands (e.g., Visa or Mastercard).

The requirements apply to all system components included in or connected to the cardholder data environment (CDE), which spans people, processes and technologies. Those system components include network devices, application servers, and contact centre applications, whether internally provisioned or provided as a service by a third party.

PCI DSS Compliance

Call recording

The implications extend to components or devices located within or connected to the CDE, and a classic example of one such device is the call recorder. Those are used to monitor and record conversations between calling (or called, in the case of an outbound dialler application) customers and call centre agents. The practice of call recording is widespread, not least in the financial services sector, and is governed by other legislation and requirements, such as the Sarbanes-Oxley Act (in the United States), and the Regulation of Investigatory Powers Act 2000 (RIPA) and the Telecommunications (Data Protection and Privacy) Regulations 1999 (in the [still] United Kingdom). When a call, during which a customer enters h[is/er] PIN using the keypad on a telephone, is recorded, the dual-tone, multi-frequency (DTMF) digital signature that represents the PIN is naturally captured automatically, together with the audio voice signal. That is, unless deliberately, something is done to remove or extract the DTMF digits from the recording.

Tone elimination

The need to suppress the DTMF in the recording is explicit in the PCI DSS, which requires that cardholder data, and that includes the PIN, must not be stored after authorisation. That means anyone involved in contact centre solutions needs a technology solution that will enable their system to eliminate DTMF tones in recordings, and so comply with the PCI DSS.

Technology options

In a telecommunications environment, which means any call centre, the technology solution involves telephony resources, which can be implemented in two ways. For those prepared to integrate third party telephony resources into their solutions, typically by means of a vendor API, the result will be a seamless, built-in system option that can be readily activated by the end user organisation. For developers who would rather shy away from such activity, the alternative is to employ an in-line, intermediary device as part of their solution.

Integrated API-based option

Technology platforms such as Aculab's Prosody S and Prosody X offer APIs that enable developers to readily integrate the functionality needed to suppress DTMF signals. Aculab's vast experience in telephony signal processing, and its knowledge and expertise in the field of DTMF handling (generation and detection), is second to none. Very many contact centre systems and solutions around the world are underpinned by Aculab's renowned Prosody X DSP boards and chassis, or its SIP-based Prosody S host media processing software.

Intermediate device option

Aculab also offers an intermediary solution, which is based on an application of its ApplianX IP Gateway, which can be used as a stand-alone, in-line, intermediary device for the purpose of eliminating the DTMF tones that are used to convey cardholder data, including PINs.

" Aculab's vast experience in telephony signal processing, and its knowledge and expertise in the field of DTMF handling (generation and detection), is second to none."

PCI DSS Compliance

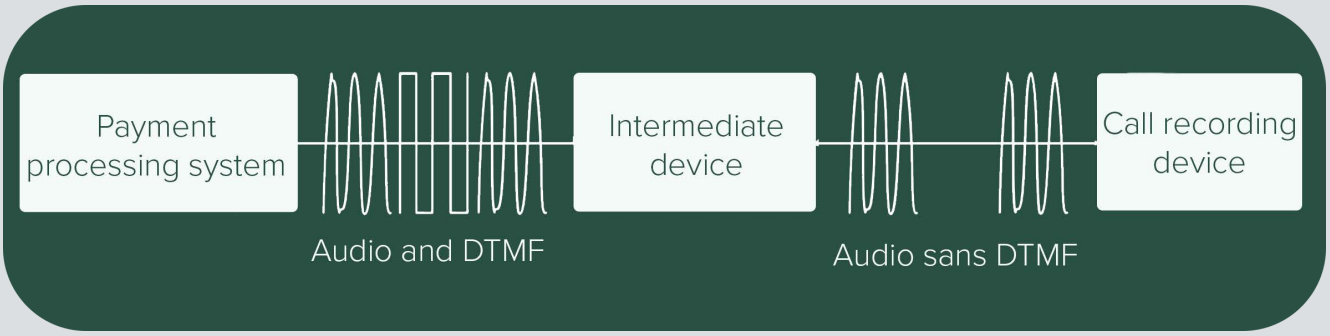

Figure 1: Basic principle of DTMF elimination

ApplianX IP gateway

The ApplianX IP Gateway's tone elimination (also known as DTMF clamping) feature can be applied to suppress DTMF signals during a call that is being recorded. By installing the gateway in-line, between the contact centre system and a call recorder, DTMF signals can be readily prevented from reaching the recorder. The gateway's DTMF clamping feature is a user configurable option that can be applied to suppress tones, in real-time.

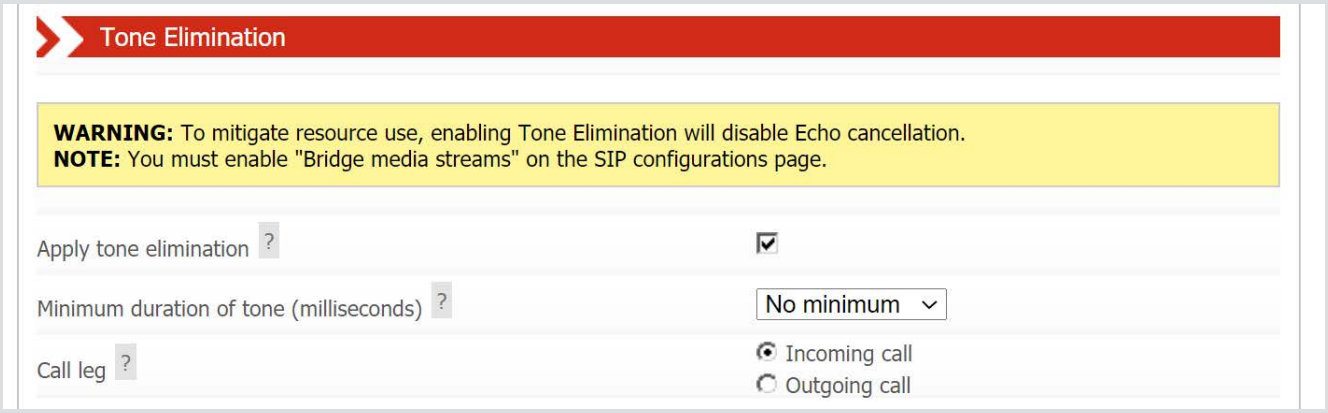

Figure 2: Tone elimination configuration

DTMF elimination

To see how DTMF clamping can be configured, see the Tone Elimination section on pages 32 and 33 of the ApplianX IP Gateway user guide. That presents user options to customise the elimination of DTMF tones from calls. The following image represents a screenshot from the user guide, which shows the configuration options.

Note that configurations for tone elimination are applied on a per route basis.

Configuration details

The 'Minimum duration of tone' specifies the amount of DTMF tone to be present before it is considered to be DTMF tone and hence eliminated, and by default, that is set to 'No minimum'. That default value will trigger the gateway into eliminating tones as soon as a sample of audio can be identified as containing tone.

Other valid values will require at least 40 milliseconds or 64 milliseconds of tone before identifying that a sample of incoming audio contains a DTMF tone, and only then excluding the tone from the outgoing audio.

The 'Call leg' option should be set according to whether tones are expected to arrive on the incoming or outgoing (from the perspective of the gateway) leg of a call.

If an incoming call is expected to carry DTMF then 'Incoming call' should be selected as the call leg on which to eliminate tones. If an outgoing call is expected to carry DTMF then 'Outgoing call' should be selected as the call leg on which to eliminate tones.

PCI DSS Compliance

Tone elimination

The following figure illustrates the process of elimination of DTMF tones. The upper waveform shows DTMF and audio, whereas the lower waveform contains no DTMF signals.

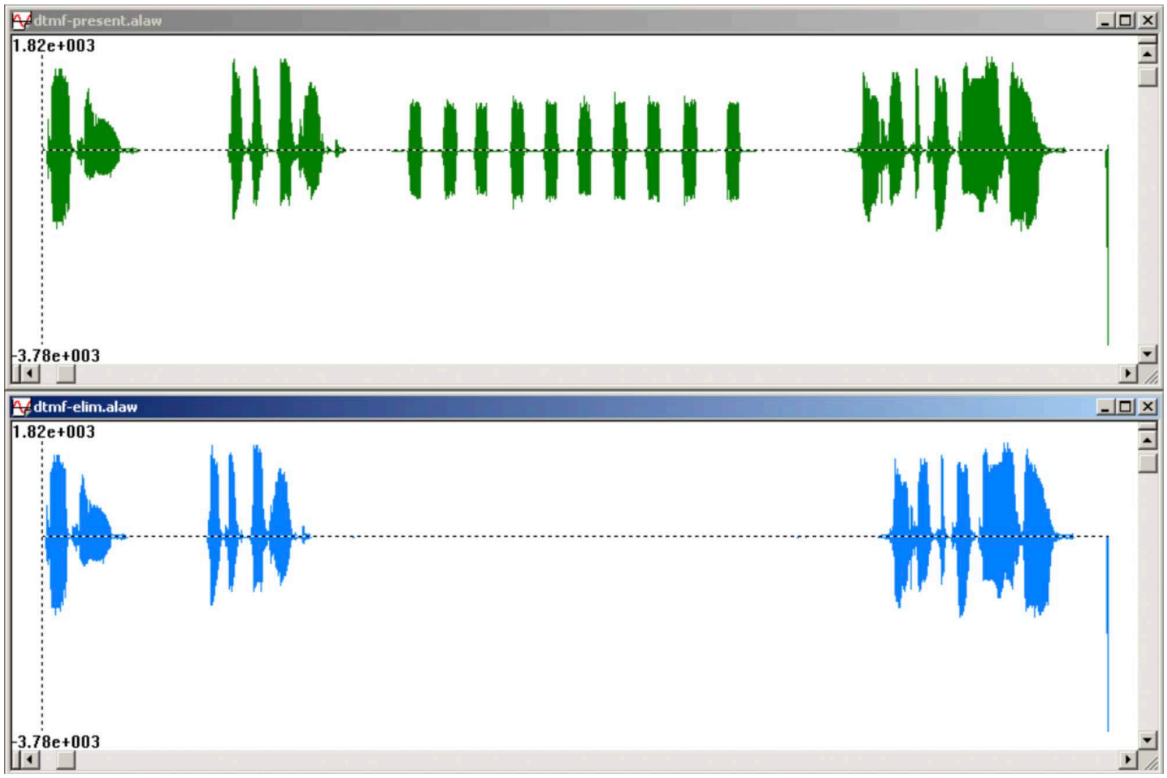

Figure 3: Showing tones present and eliminated

Application example

The ApplianX IP Gateway can be deployed between a contact centre system and a call recorder as shown in Figure 4 below.

In this case, the system is controlled by the call centre agent who passes the caller to a secure, payment processing sub-system, by means of a hot-key. Whilst the agent is not a party to the call, the caller makes the payment by using the telephone keypad to enter card details. If successful, the caller is informed via the sub-system IVR and the database is updated, before the transaction details are sent to a payment gateway and the call is automatically returned to the agent. The process is effectively the same in an outbound dialler scenario.

The system is secure, because the agent is not exposed to the card details and the card details are not stored. Therefore, the opportunities for fraud are reduced considerably. Furthermore, the agent's session is recorded from start to finish, with no breaks or pauses, and critically, without the DTMF signals representing the caller's data, which are suppressed by the ApplianX IP Gateway.

Such a system is very easy for the agent to understand and helps to reduce the average cost per transaction, in addition to preventing the agent from being exposed to callers' credit card details.

PCI DSS Compliance

The ApplianX IP Gateway receives inbound SIP or TDM signalled calls from the contact centre system, eliminates the DTMF signals in real-time and makes a corresponding outbound SIP call to the recorder. The RTP audio media reaching the recorder contains no
DTMF and so the recording can be stored or archived in full compliance with the PCI DSS. In this scenario, the ApplianX IP Gateway can be configured for TDM-to-TDM, TDM-to-SIP or SIP-to-SIP calls, with a capacity of up to 4 E1/T1 trunks and 120 SIP calls.

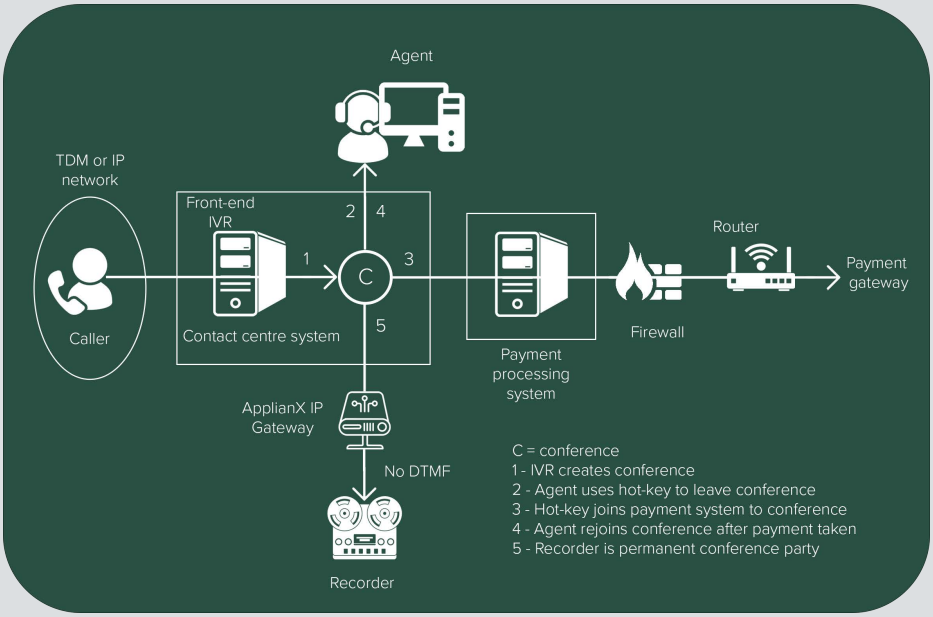

Figure 4: Application example

Conclusion

In any contact centre offering payment processing functionality via telephone, whether calls are handled by legacy TDM-based or next generation, SIP-based systems, there will be DTMF digital signatures present in the audio signals received as a result of data input by the caller. Those DTMF signals represent sensitive data, such as a customer's PIN.

When calls are recorded, for whatever purposes, by the contact centre, in order to protect customer data and comply with the PCI DSS, those DTMF signals must be excluded from all call recordings.

Unless such a capability is built in to the contact centre's payment processing system, an intermediate device will be needed to perform that function i.e., suppress or eliminate the DTMF signals so that they are not present in stored recordings.

Clearly, the tone elimination feature of Aculab's ApplianX IP Gateway means it can be used as a stand-alone, in-line, intermediary device for eliminating the DTMF tones used to convey cardholder data, including PINs.

The ApplianX IP Gateway's tone elimination or DTMF clamping feature will suppress, in real-time, any DTMF signals in the audio of calls fed to a recording device. By installing the gateway in-line, between the transaction processing system and the call recorder, DTMF signals can be prevented from reaching the recorder.

With such a ready made, off-the-shelf solution, the contact centre manager can gain peace of mind, secure in the knowledge that customer data is protected and PCI DSS compliance is assured.

About Aculab

Aculab is an innovative company that offers deployment proven technology for any telecoms related application. Its enabling technology serves the evolving needs of automated and interactive systems, whether on-premise, data centre hosted, or cloud-based.

Over 1000 customers in more than 80 countries worldwide, including developers, integrators, and solutions and service providers, have adopted Aculab's technology for a wide variety of business critical services and solutions.

Aculab offers development APIs for voice, data, fax and SMS, on hardware, software and cloud- based platforms, giving a choice between capital investment and cost-effective, 'pay as you go' alternatives.

For more information

To learn more about Aculab Cloud and Aculab's extensive telephony solutions visit:
www.aculab.com

Contact us

Phone
+44 (0) 1908 273800 (UK)
+1 (781) 352 3550 (USA)

Email
info@aculab.com
sales@aculab.com
support@aculab.com

Social
@aculab
aculab