SAP Digital Payments
Configuration Guide

Non-Disclosure Statement

Intended audience

This document is intended for Systems Architects, Developers or Technical managers who are considering using CardEasy in their organisation with SAP Digital Payments.

Document revisions

V1	Initial release
V1.5	Updated SAP configuration screenshots
V1.6	Updated Configuration steps
V1.7	Change of wording in configuration steps

Audience

This document is intended for those involved in planning, defining, and designing PCI compliance solutions in call centres. It aims to provide a high-level general understanding of the Syntec CardEasy PCI-DSS Solution and how it can be deployed within the SAP Digital Payments solution.

It should be noted that the document refers to PCI-DSS Compliant payment processing within the telephone channel only and does not cover PCI-DSS payments taken via other contact centre channels (e.g. web chat), although Syntec also has payment solutions that can meet these needs.

PCI-DSS

PCI DSS is the worldwide Payment Card Industry Data Security Standard that was set up to help businesses process card payments securely and reduce card fraud. This is achieved through enforcing tight controls surrounding the storage, transmission and processing of cardholder data that merchants handle.

Achieving and maintaining PCI-DSS compliance in the call centre is expensive and complex. Failure to do so risks heavy fines and reputational damage in the event of a data breach. CardEasy avoids both the business impact and the expense of audit, completely removing the call centre from scope while eliminating operator keying errors and speeding up the payment process.

CardEasy Overview

CardEasy aims to de-scope the contact centre from PCI-DSS to the fullest extent possible by stopping sensitive card data from entering the environment at the network edge.

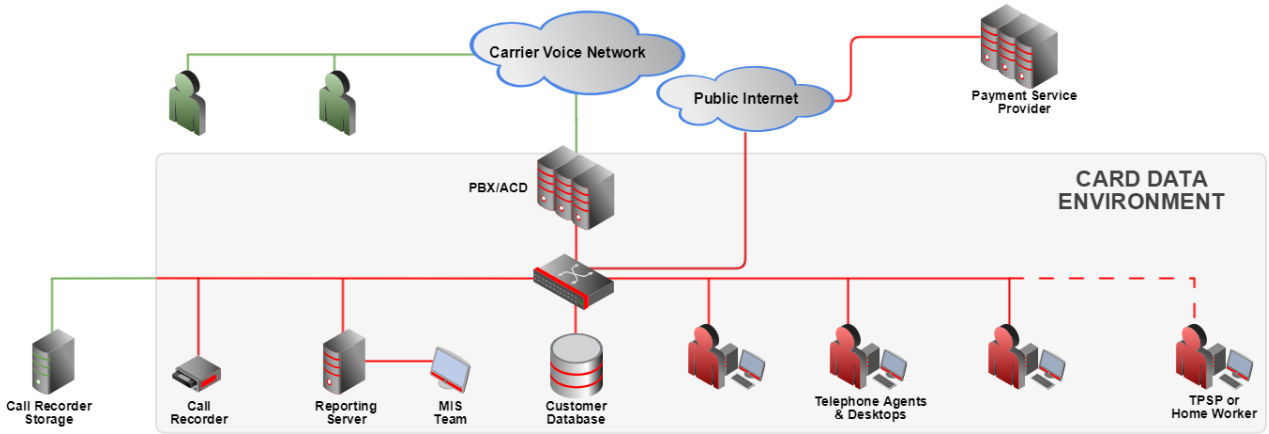
It works by having the customer enter their card details by touch tone (DTMF) on their telephone handset during the call without interrupting the call flow. The agent remains on hand to assist the customer throughout. There is no need to transfer the call to an external system. DTMF tones containing card data are blocked at the network edge preventing downstream equipment from being drawn into scope.

The agent controls the system by way of a Virtual Terminal launched from SAP. The VT is provided by CardEasy and will make a submission to the merchants PSP and return the PSP token back to SAP Digital Payments. SAP Digital Payments will then use this token to complete the payment journey directly with the merchants PSP.

This document deals with the SAP Digital Payment add on setup. CardEasy MUST also be positioned within the merchant's telephony voice call flow which we have a number of ways to do depending on the merchants telephony setup.

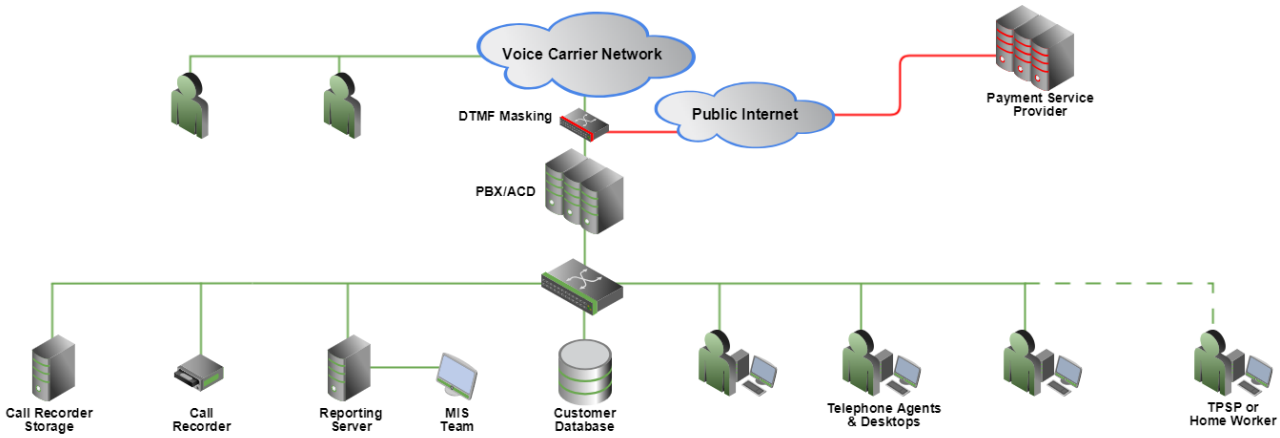
Typical Merchant environment without CardEasy

In the diagram below the elements coloured in red are all subject to PCI controls either because of direct contact with card data causing them to be considered part of the 'Card Data Environment' (CDE) or because they fall into the classification of 'connected systems' under PCI-DSS definitions. The merchant's functions from the PBX down, including Agents systems, call & screen recordings, workstations and networks are all exposed to PAN and CVC. In a flat network topology, the number of machines involved can be huge. PCI Controls should be deployed to secure this environment – a very time consuming and costly to implement task with high ongoing maintenance implications.



Typical Merchant environment with CardEasy

The graphic below illustrates how CardEasy removes the need for PAN and CVC to enter the merchant's network and thus removes it from scope. The CDE is now restricted to the CardEasy DTMF Masking server (fully managed by Syntec and located in the AWS cloud) and PCI controls are largely eliminated.



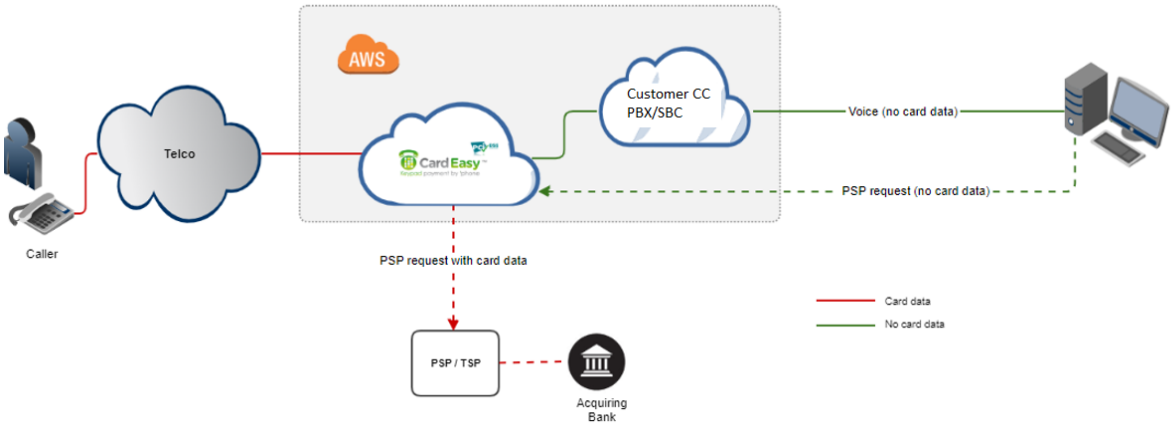
High level functional overview

CardEasy consists of three main functional components; DTMF removal from the voice call, SAP Digital Payments interaction and PSP tokenization submission.

DTMF removal can be performed by a SIP proxy server sited normally in the AWS cloud between the Telco and merchants PBX/SBC or by using a physical CardEasy SIP appliance on the merchants site. Everything downstream of the CardEasy SIP service is descoped from PCI-DSS as no card data passes beyond this point.

SAP Digital Payments interaction Launches the CardEasy Virtual Terminal for PAN and CVC capture and provides confirmation that the PSP result has been received by SAP

The initial PSP tokenization submission is performed by the CardEasy service which runs in the AWS cloud and builds the PSP tokenization submission and handles the response



Configuration Steps:-

1. The merchant provides CardEasy with their test and production PSP Server to Server API Credentials

2. The merchant to complete the relevant PSP SAP Digital payment instructions:-

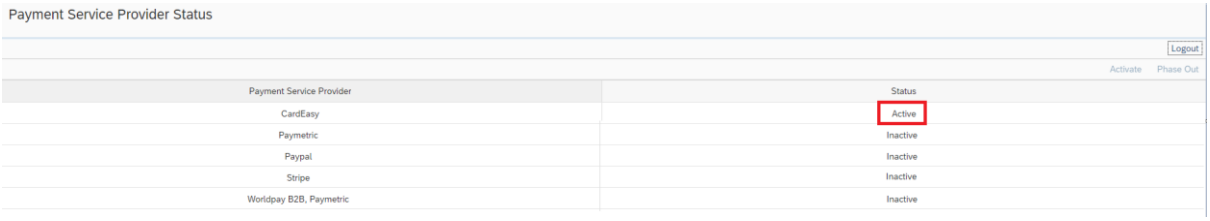
   SAP Help Portal page of SAP digital payments add-on below

   https://help.sap.com/docs/DIGITALPAYMENTS

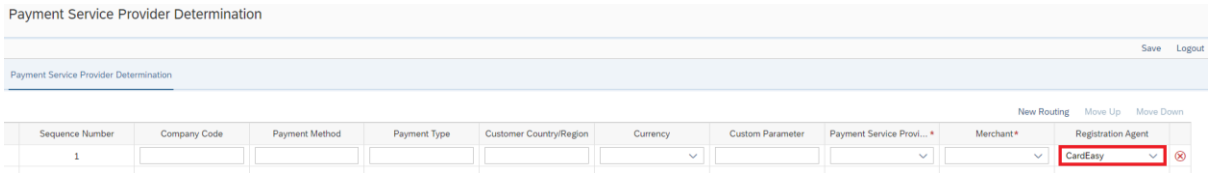
   Then select

   Administration Guide => Setup Activities => Connecting the SAP Digital Payments Add-On and the PSP

3. As part of the SAP Digital Payments add-on setup for CardEasy the merchant must Activate CardEasy in the SAP Digital Payments Service Provider Status page



4. Make sure you select CardEasy as the Registration Agent in the SAP Digital Payments add-on Payment Service Provider Determination page

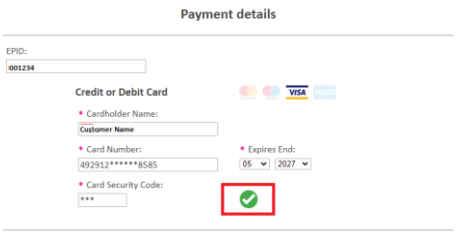


5. Provide CardEasy with your SAP tenantID to associate it with your CardEasy account.

6. Wait for CardEasy to confirm setup is complete before proceeding to step 7

7. Within your SAP system you will be able to launch the CardEasy secure page.

8. You should now be able to capture PAN and CVC by clicking in the relevant field to initiate the capture. The Green tick indicates that the PSP token has been received by SAP Digital Payments.



Currently supported PSP's are Cybersource, Moneris, Stripe, Worldpay, Paypal

Support for Novalnet, PayFabric from EVO Payments and SnapPay from Fiserv will be provided as required