amadeus

IDPMS 4.1.

PA-DSS implementation guide

Document version D01_IDPMS.1.1

By Dennis van Hilten

Amadeus
Breda
The Netherlands

Note

This PA-DSS Implementation Guide must be reviewed on a yearly basis, whenever the underlying application changes or whenever the PA-DSS requirements change. Updates should be tracked and reasonable accommodations should be made to distribute or make the updated guide available to users. Amadeus will distribute the IG to new customers together with the proposal.

Table of contents

Table of Contents

Notice

THE INFORMATION IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. AMADEUS MAKES NO REPRESENTATION OR WARRANTY AS TO THE ACCURACY OR THE COMPLETENESS OF THE INFORMATION CONTAINED HEREIN. YOU ACKNOWLEDGE AND AGREE THAT THIS INFORMATION IS PROVIDED TO YOU ON THE CONDITION THAT NEITHER AMADEUS NOR ANY OF ITS AFFILIATES OR REPRESENTATIVES WILL HAVE ANY LIABILITY IN RESPECT OF, OR AS A RESULT OF, THE USE OF THIS INFORMATION. IN ADDITION, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE SOLELY RESPONSIBLE FOR MAKING YOUR OWN DECISIONS BASED ON THE INFORMATION HEREIN.

NOTHING HEREIN SHALL BE CONSTRUED AS LIMITING OR REDUCING YOUR OBLIGATIONS TO COMPLY WITH ANY APPLICABLE LAWS, REGULATIONS OR INDUSTRY STANDARDS RELATING TO SECURITY OR OTHERWISE INCLUDING, BUT NOT LIMITED TO, PA-DSS AND DSS.

THE RETAILER MAY UNDERTAKE ACTIVITIES THAT MAY AFFECT COMPLIANCE. FOR THIS REASON, AMADEUS IS REQUIRED TO BE SPECIFIC TO ONLY THE STANDARD SOFTWARE PROVIDED BY IT.

1. Change log and approval

1.1. Change log

1.2. Document control

Security level	Confidential			
Company	Amadeus IT Group SA			
Department	Hospitality			
Author	Dennis van Hilten			
Reviewed by	Jan Paauwe		Date	23/11/2016
Approved by	[Name]		Date	[dd/mm/yyyy]
Version	Date	Change	Comment	By
1.0	01-10-2016		Initial version	DvH
1.1	01-11-2016			JP / DVH
1.2	04-01-2016	Change	Incorporated comments from PCI assessor	JP / DVH
1.3	23-02-2017	Change	Removed wildcard in minor version number	DvH
1.4	25-09-217	Change	Removed reference to PCI v1.2 and replaced by v3.2	DvH
1.5	06-11-2017	Change	Adjusted signature section	DvH

1.3. Approval and signatures

On behalf of Hotel	Name	Date

2. About this document

This document describes the steps that must be followed in order for your IDPMS installations to comply with Payment Application – Data Security Standards (PA-DSS). The information in this document is based on PCI Security Standards Council Payment Application Data Security Standards program (version 3.2 dated April, 2016).

Amadeus instructs and advises its customers to deploy Amadeus applications in a manner that adheres to the PCI Data Security Standard (v3.2). Subsequent to this, best practices and hardening methods, such as those referenced by the Centre for Internet Security (CIS) and their various "Benchmarks", should be followed in order to enhance system logging, reduce the chance of intrusion and increase the ability to detect intrusion, as well as other general recommendations to secure networking environments. Such methods include, but are not limited to, enabling operating system auditing subsystems, system logging of individual servers to a centralized logging server, the disabling of infrequently-used or frequently vulnerable networking protocols and the implementation of certificate-based protocols for access to servers by users and vendors.

If you do not follow the steps outlined here, your IDPMS installation will not be PA-DSS compliant.

3. Executive summary

IDPMS 4.1.x.x has been PA-DSS (Payment Application Data Security Standard) certified, with PA-DSS Version 3.2. For the PA-DSS assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):

Adsigo AG, Königsalee 43, 71638 Ludwigsburg, Germany

This document also explains the Payment Card Industry (PCI) initiative and the Payment Application Data Security Standard (PA-DSS) guidelines. The document then provides specific installation, configuration, and ongoing management best practices for using Payment Application as a PA-DSS validated Application operating in a PCI Compliant environment.

3.1. PCI Security Standards Council Reference Documents

The following documents provide additional detail surrounding the PCI SSC and related security programs (PA-DSS, PCI DSS, etc):

- Payment Applications Data Security Standard (PA-DSS)
  https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security
- Payment Card Industry Data Security Standard (PCI DSS)
  https://www.pcisecuritystandards.org/
- Open Web Application Security Project (OWASP)
  http://www.owasp.org

3.2. Application summary

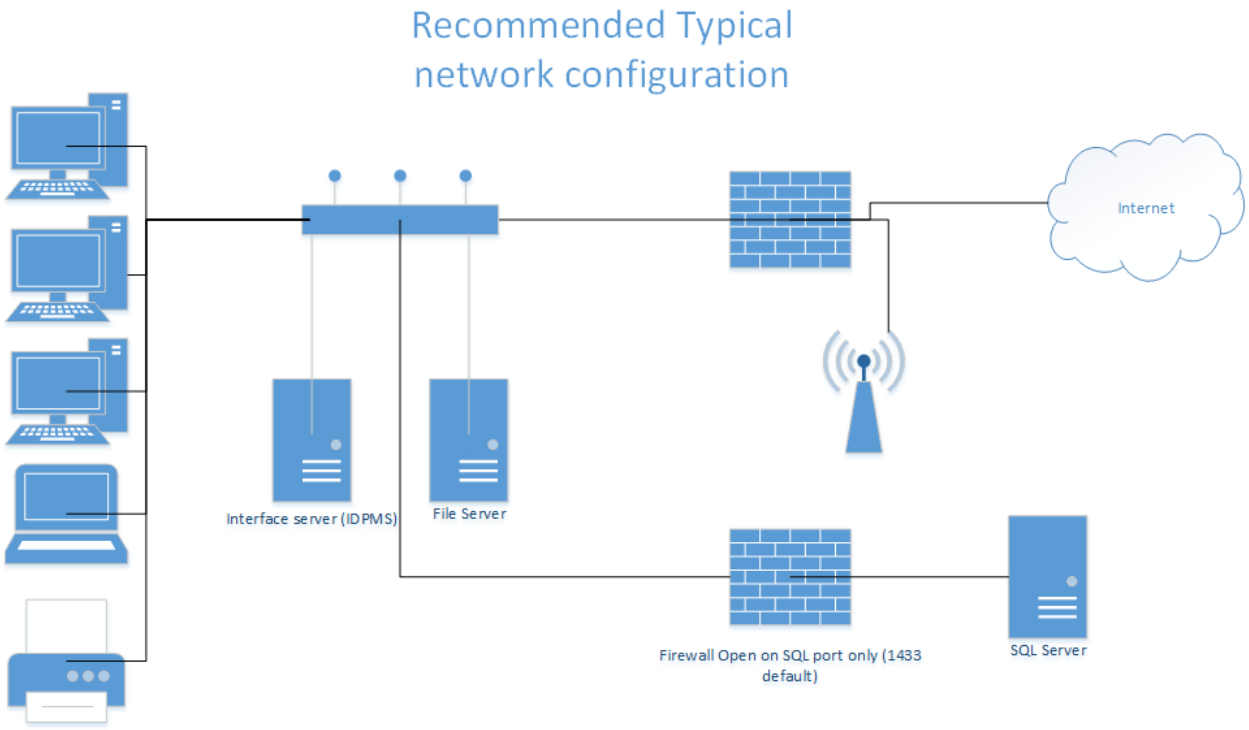
Payment Application Name:	IDPMS
Payment Application Version:	4.1.x.x
Application Description:	IDPMS, Integrated Distribution Property Management System, will help increase the yield and lower the cost for a hotel. It is a powerful set of software tools for efficient and effective management of hospitality operations, with special functionality for controlling distribution channels. The IDPMS Product Suite has a modular design so it caters to all types of properties
Application Target Clientele:	Hospitality
Components of Application Suite (i.e. POS, Back Office, etc.)	IDPMS consists of a single application that does all the tasks
Required Third Party Payment Application Software:	IDPMS uses Sixcards for Credit Card transactions
Database Software Supported:	IDPMS uses Microsoft SQL Server v2008 or Later
Other Required Third Party Software:	IDPMS uses Crystal Reports for reporting purposes
Operating System(s) Supported:	IDPMS runs on Microsoft Windows, including, but not limited to Windows 7 and Server 2008R2.
Application Functionality Supported	Reservations, front office, back office, reporting, etc.
Payment Processing Connections:	Credit cards are processed through the ProtoBase gateway, using a TCP/IP connection.
Description of Versioning Methodology:	IDPMS versioning has Four levels: Major version, Minor version, Release and Build: 4.1.x.x **Major version:** This changes when major / significant PCI impacting changes are made to the software. For example re-certification for a new version of the PA-DSS requirements. **Minor version**: Includes changes to the application that have a minor impact on PA-DSS requirements. These require additional documenting **Release**: changes include small changes or new features added to the application and may not have an impact on PA-DSS requirements. **Build**: changes include bug fixes and would have no negative impact on PA-DSS requirements.

4. Typical network implementation

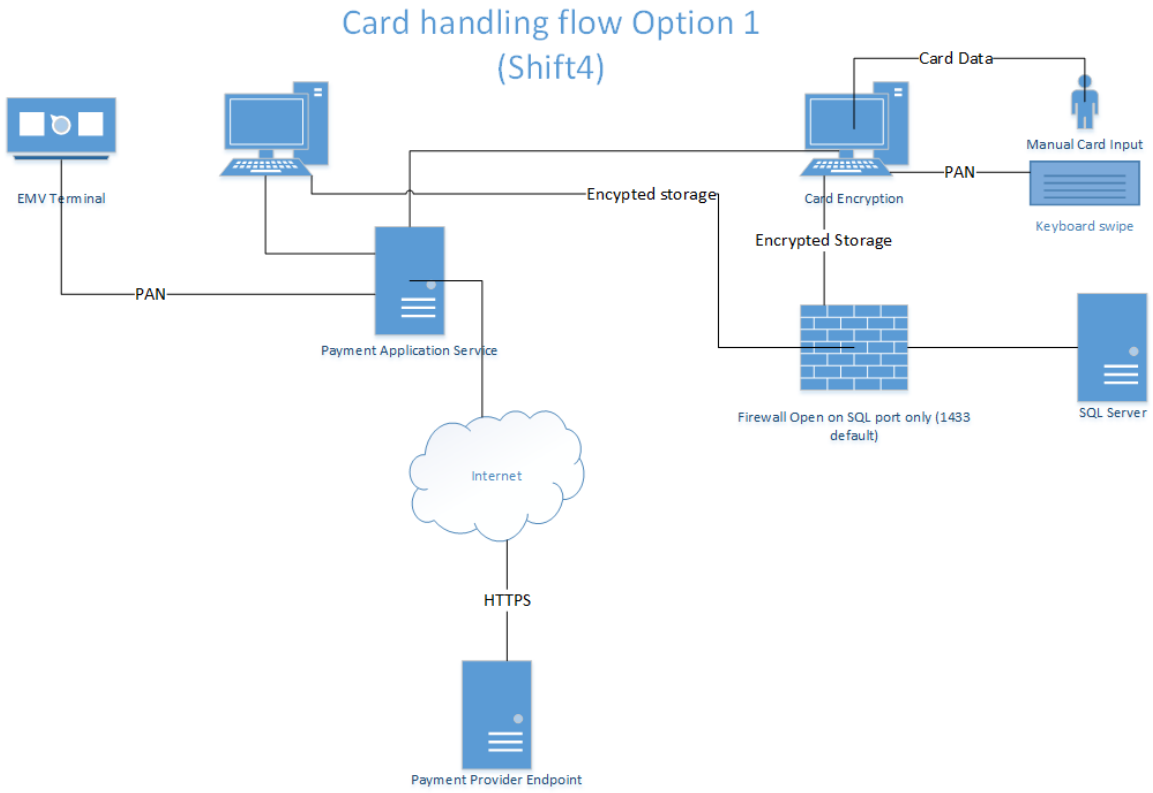
The PCI DSS requires that firewall services be used (with NAT or PAT) to segment network segments into logical security domains based on the environmental needs for internet access. Traditionally, this corresponds to the creation of at least a DMZ and a trusted network segment where only authorized, business-justified traffic from the DMZ is allowed to connect to the trusted segment. No direct incoming internet traffic to the trusted application environment can be allowed. Additionally, outbound internet access from the trusted segment must be limited to required and justified ports and services.

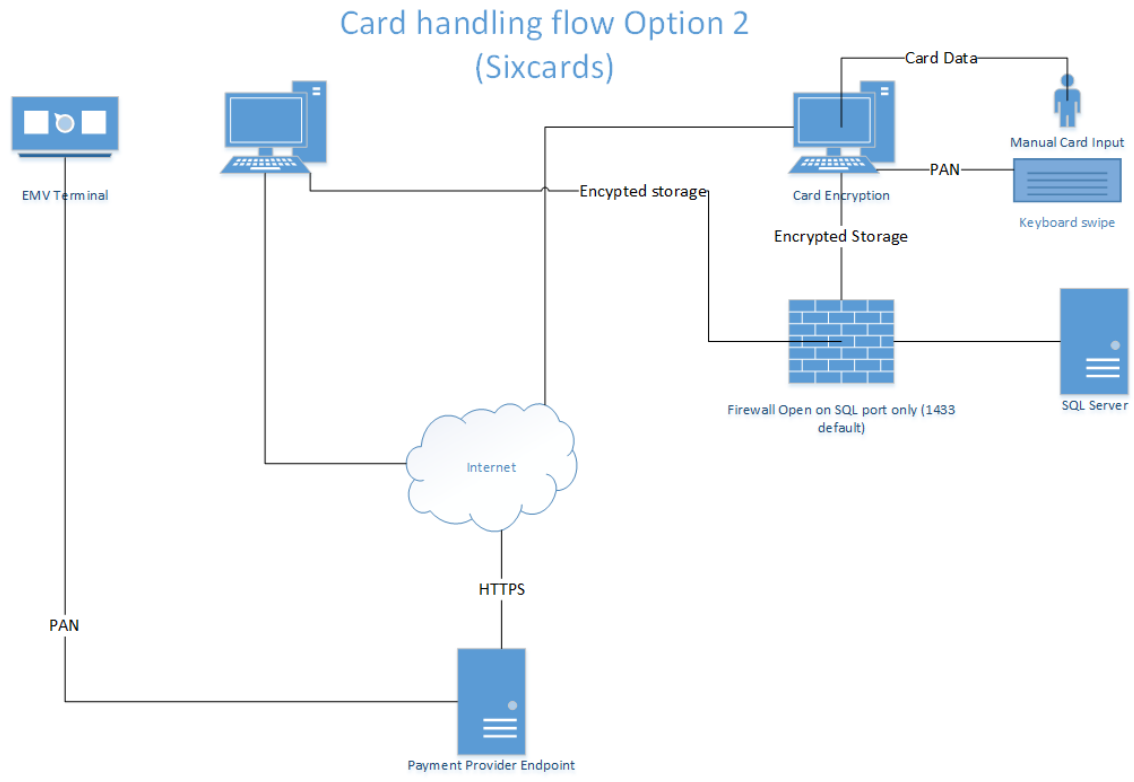
As of PCI-DSS 3.0 Card Holder data should be stored on a server that has no connection to the internet. To accomplish this the SQL server should be separated from the file server and connected through a firewall. For IDPMS only the SQL port (1433 or other configured port) is needed, and RDP support should only be accessible from the file Server.

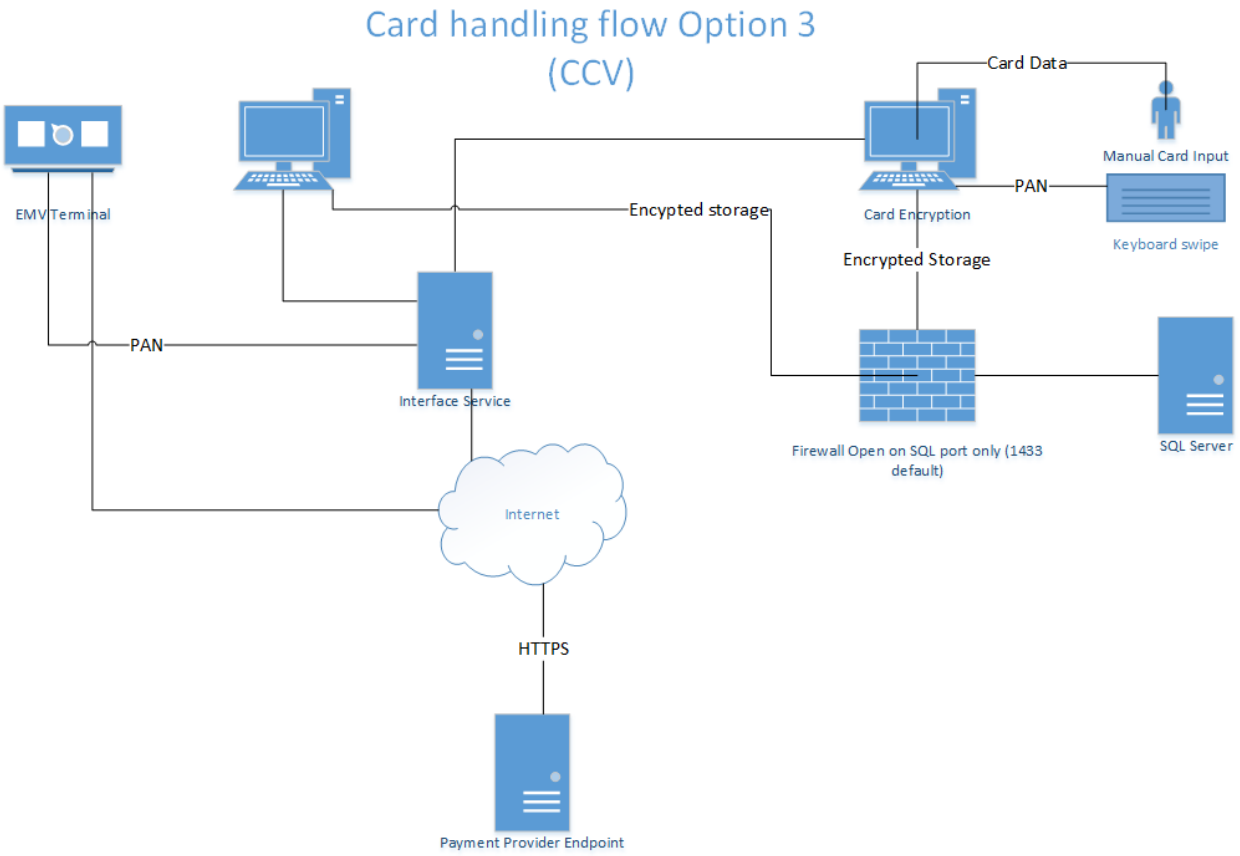
For maintenance it's required that SQL server management studio is installed on the file server.



5. Dataflow diagram







6. Difference between PCI compliance and PA-DSS Validation

As a software vendor, our responsibility is to be "PA-DSS Validated".

We have performed an assessment and certification compliance review with our independent assessment firm, to ensure that our platform does conform to industry best practices when handling, managing and storing payment related information.

PA-DSS is the standard against which Payment Application has been tested, assessed, and validated.

PCI Compliance is then later obtained by the merchant, and is an assessment of your actual server (or hosting) environment.

Obtaining "PCI Compliance" is the responsibility of the merchant and your hosting provider, working together, using PCI compliant server architecture with proper hardware & software configurations and access control procedures.

The PA-DSS Validation is intended to ensure that the Payment Application will help you achieve and maintain PCI Compliance with respect to how Payment Application handles user accounts, passwords, encryption, and other payment data related information.

The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The security requirements defined in the DSS apply to all members, merchants, and service providers that store, process or transmit cardholder data.

The PCI DSS requirements apply to all system components within the payment application environment which is defined as any network device, host, or application included in, or connected to, a network segment where cardholder data is stored, processed or transmitted.

6.1. The twelve requirements for PCI DSS

These are the twelve requirements of the PCI-DSS

Build and Maintain a Secure Network

1. *Install and maintain a firewall configuration to protect data*
2. *Do not use vendor-supplied defaults for system passwords and other security parameters*

Protect Cardholder Data

3. *Protect Stored Data*
4. *Encrypt transmission of cardholder data and sensitive information across public networks*

Maintain a Vulnerability Management Program

5. *Protect all systems against malware and regularly update anti-virus software or programs*
6. *Develop and maintain secure systems and applications*

Implement Strong Access Control Measures

7. *Restrict access to data by business need-to-know*
8. *Identify and authenticate access to system components*
9. *Restrict physical access to cardholder data*

Regularly Monitor and Test Networks

10. *Track and monitor all access to network resources and cardholder data*
11. *Regularly test security systems and processes*

Maintain an Information Security Policy

12. *Maintain a policy that addresses information security*

7. Considerations for the Implementation of Payment Application in a PCI-Compliant Environment

The following areas must be considered for proper implementation in a PCI-Compliant environment.

- Sensitive Authentication Data requires special handling
- Remove Historical Cardholder Data
- Set up Good Access Controls
- Properly Train and Monitor Admin Personnel
- Key Management Roles & Responsibilities
- PCI-Compliant Remote Access
- Use SSH, VPN, or TLS for encryption of administrative access
- Log settings must be compliant
- PCI-Compliant Wireless settings
- Data Transport Encryption
- PCI-Compliant Use of Email
- Network Segmentation
- Never store cardholder data on internet-accessible systems
- Use TLS for Secure Data Transmission
- Delivery of Updates in a PCI Compliant Fashion

7.1. Remove Historical Sensitive Authentication Data

Versions before 3.12.4xx stored sensitive authentication data.

- Historical data must be securely deleted (magnetic stripe data, card validation codes, PINs, or PIN blocks stored by previous versions of the software) – removal is absolutely necessary for PCI compliance

Notice that it is absolutely necessary for PCI DSS to securely delete any historical sensitive authentication data from the system.

The following steps describe how sensitive data is permanently erased from the system:

Remove all copies and backups of IDPMS/IDCRS and IDPMS_STORED_DOCS on the SQL data server and/or backup server of the customer. Scan the network for .bak and .trn files and delete them all using Eraser software 6.2.*.* (https://eraser.heidi.ie/download/)

Remove all logs (*.log) from credit-card interfaces such as 3c, Shift4 and others. For removal use Eraser software 6.2.*.*

After all files have been securely removed a new SQL back-up must be made in order to have a new backup and to empty the SQL Log file as the SQl log file may still contain uncrypted PAN data from before the update to the PCI compliant IDPMS version (version > 3.12)

Version 3.12.4xx is a PA-DSS v1.2 validated applications and for this version no extra sweep actions are needed.

7.2. Sensitive Authentication Data requires special handling

IDPMS does not store Sensitive Authentication, not even for trouble shooting purposes. IDPMS does also not ask for any sensitive authentication data at all.

7.2.1. Collect sensitive authentication

Sensitive data should not be used to find / solve problems in the application. In the rare case that live data is required the PCI DSS related procedures must be followed.

7.2.2. Store such data with limited access

The data that is collected from a live (customer) environment should only be stored on the specific development network location that is available to those software engineers that are working on IDPMS.

7.2.3. Collect only the limited amount of data

Only collect the data that is necessary to pin-point the specific issue, like only a specific date or a specific guest related record or data set.

7.2.4. Encrypt sensitive authentication data while stored

The data used is always encrypted, using the mechanism used throughout the entire product for encrypting sensitive data.

7.2.5. Securely delete such data immediately after use

After the problem has been resolved the data of entire environment is wiped out using Eraser.

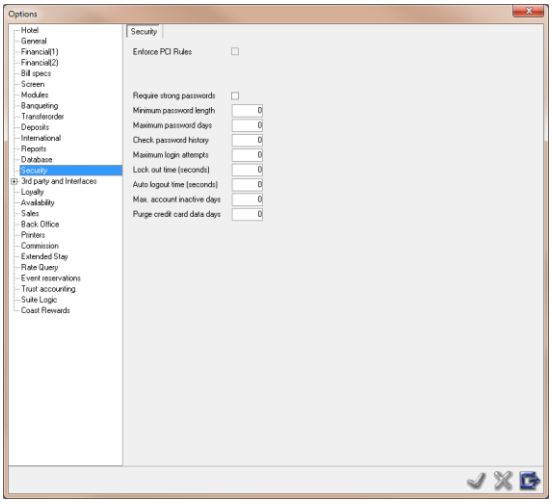
7.3.6 Securely remove all back-ups from IDPMS database and OS

To guarantee the retention policy of card holder data it is mandatory to securely remove all back-ups related to IDPMS or the OS within the set retention policy. (See chapter 7.3)

7.3. **Cardholder Data**

The cardholder data is stored in the IDPMS SQL database. Fields in the Resfol, Groupfol, Event_resfol, CreditCard_log, Credidcard_auth, CRS_Resfol. Distr_resfol, Posting tables as well as in the Guest Table contains PAN data in encrypted or masked format.

The number of days for purging PAN data is set in the IDPMS settings under "Number of days for purge." See screenshot.



The maximum value that can be set is 90 days.

The purging process is automated task during night audit, and cannot be switched off or started manually.

7.4. **Removal of Cryptographic material**

All deletions of cryptographic materials are wiped with the eraser tool. No historical data is encrypted again with a new key. Historical data is saved during a limited time frame, see previous paragraph.

7.5. **Set up Good Access Controls**

The PCI DSS requires that access to all systems in the payment processing environment be protected through use of unique users and complex passwords. Unique user accounts indicate that every account used is associated with an individual user and/or process with no use of generic group accounts used by more than one user or process. The following should be followed:

- Do not use administrative accounts for application logins (e.g., don't use the "sa" account for application access to the database).
- Assign strong passwords to these default accounts (even if they won't be used), and then disable or do not use the accounts.
- Assign strong application and system passwords whenever possible.
- Create PCI DSS-compliant complex passwords to access the payment application, per PCI Data Security Standard 8.5.8 through 8.5.15
- Changing the "out of the box" settings for unique user IDs and secure authentication will result in non-compliance with the PCI DSS

The PCI standard requires the following password complexity for compliance (often referred to as using "strong passwords"):

- Do not use group, shared, or generic user accounts (8.5.8)
- Passwords must be changed at least every 90 days (8.5.9)
- Passwords must be at least 7 characters (8.5.10)
- Passwords must include both numeric and alphabetic characters (8.5.11)
- New passwords cannot be the same as the last 4 passwords (8.5.12)

PCI user account requirements beyond uniqueness and password complexity are listed below:

- If an incorrect password is provided 6 times the account should be locked out (8.5.13)
- Account lock out duration should be at least 30 min. (or until an administrator resets it) (8.5.14)
- Sessions idle for more than 15 minutes should require re-entry of username and password to reactivate the session (8.5.15)

These same account and password criteria must also be applied to any environment, applications or databases included in payment processing to be PCI compliant. IDPMS, as tested to in our PA-DSS audit, meets, or exceeds these requirements.

IDPMS must require unique usernames and complex passwords for all administrative access and for all access to cardholder data.

[Note: These password controls are not intended to apply to employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by employees with administrative capabilities, for access to servers with cardholder data, and for access controlled by the application.]

- Control access, via unique username and PCI DSS-compliant complex passwords, to any PCs or servers with payment applications and to databases storing cardholder data.

Use rights and roles can be reviewed using the Configuration reports (Reports/Settings/Users)

With the first use of IDPMS 4.1 each user will be forced to change password.

Access user rights can be reviewed by The User Menu Access report in report->Settings-> Users

7.6. **Properly Train and Monitor Admin Personnel**

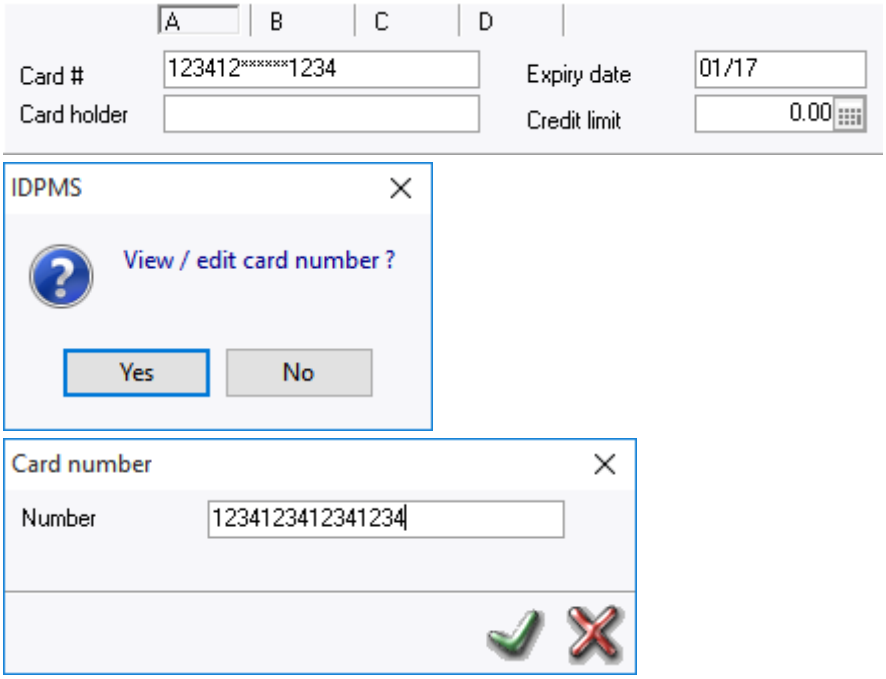
It is the merchant's responsibility to institute proper personnel management techniques for allowing user access to cardholder data, site data, etc. You can control whether each individual user can see the full credit card PAN (or only the masked data).

In most systems, a security breach is the result of unethical personnel. So pay special attention to whom you trust into your admin site and who you allow to view full decrypted and unmasked payment information.

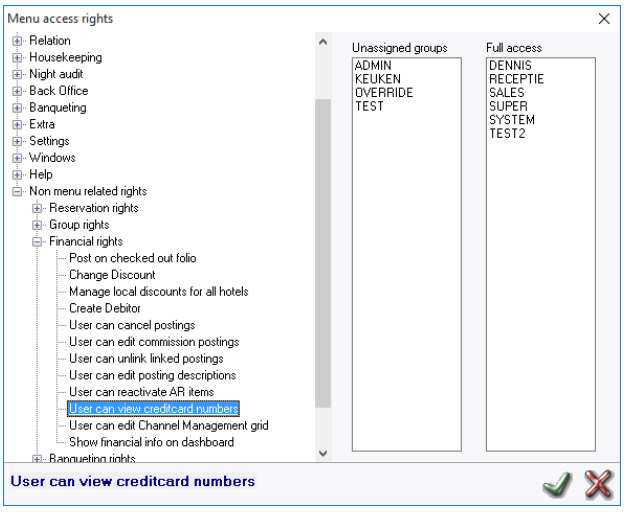
7.7. **Setup user access to view unmasked PAN**

By default, all display of Credit card numbers will show as a masked PAN, only users with a need to know should have access to the full PAN.

Each access to the full PAN will be logged.



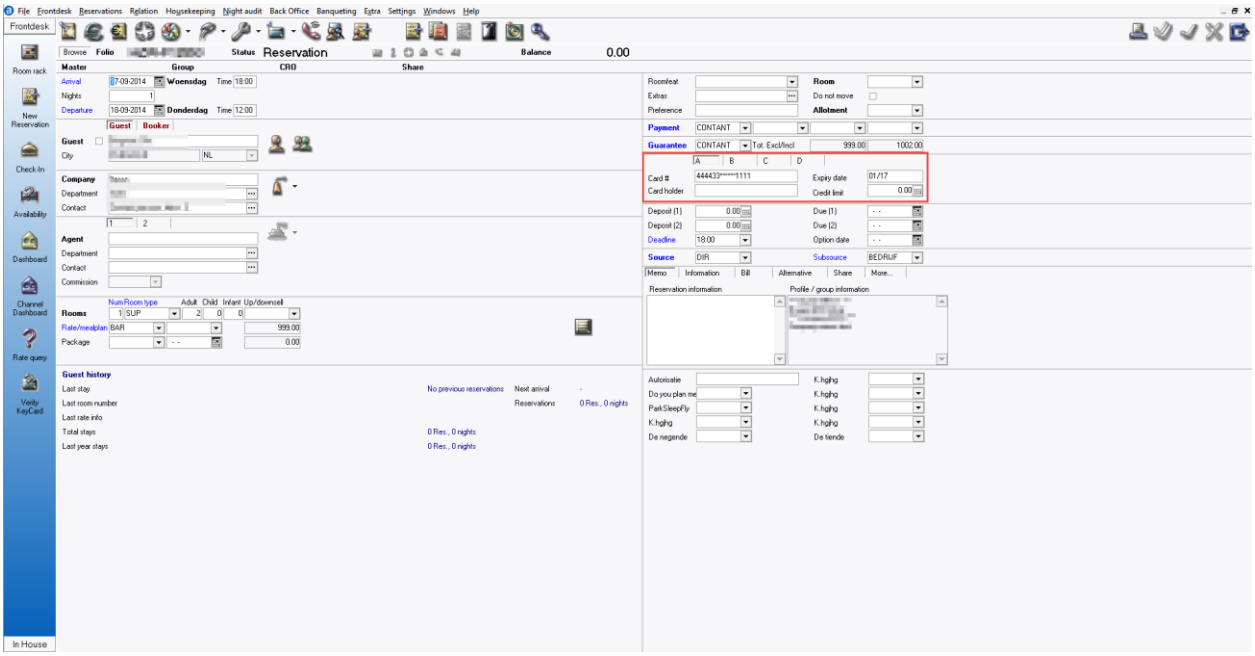
User rights can be configured in the user right configuration



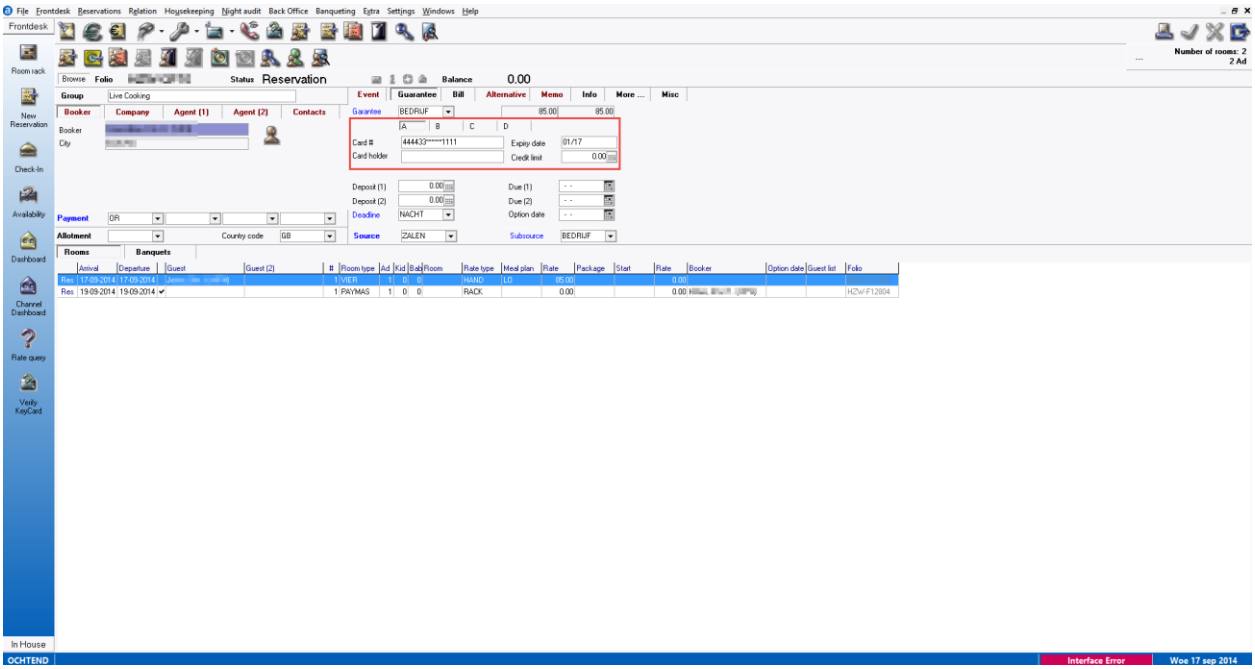
7.7.1 Display of PAN data

Pan data is displayed in the following screens

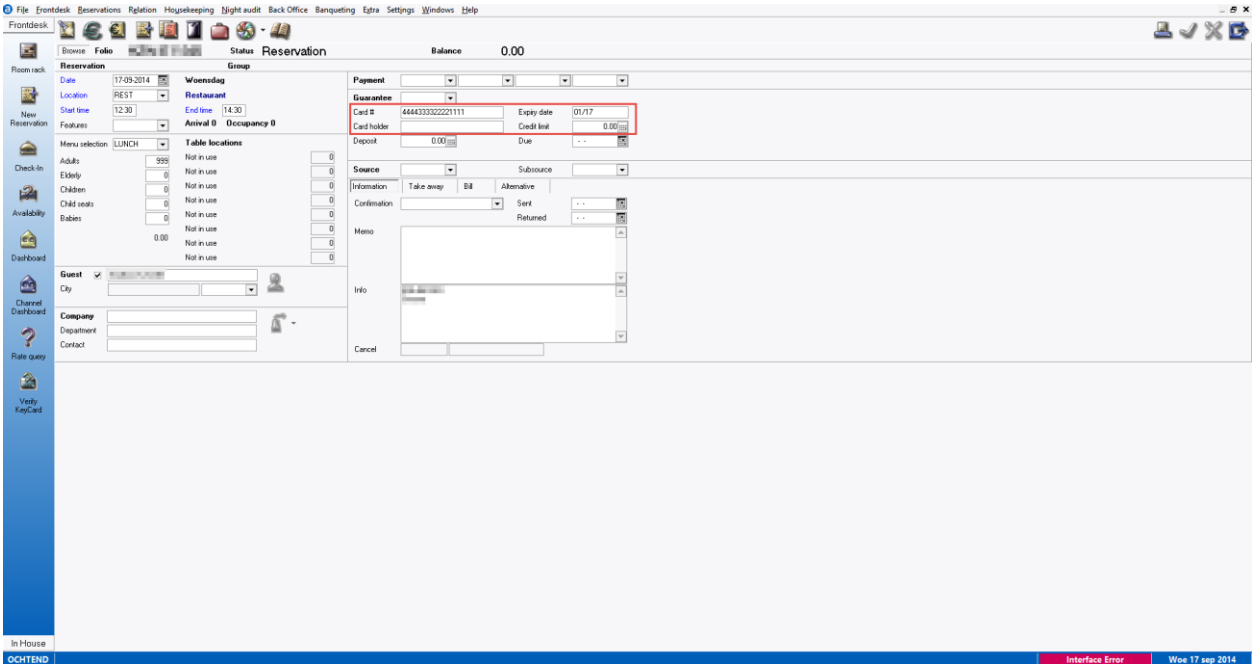
1. Reservation screen:



2. Group reservation screen



3. Event reservation screen



7.8. **Key Management Roles & Responsibilities**

IDPMS uses the Advanced Encryption Standard (AES), sometimes referred to as Rijndael Encryption. IDPMS uses the 256 bits key variant, which is the maximum under the current AES standard.

IDPMS uses a unique dynamic key approach where the encryption key is different for each transaction. On top of that the IDPMS customer is able to renew the key at any desired moment. The key renewal process can only be started from within IDPMS by a user that has been assigned the right to do so. During the training the Amadeus consultant clearly explains the customer this part and adds that this right should be granted to a very limited number of users.

There is no access to any key material by the customer.

A new key is generated when the user chooses to do so and the user is given the opportunity to store the binary file, where the key is generated from, on a memory stick and store that in their vault. When a new key is generated, all encrypted data in IDPMS is decrypted against the old key and then encrypted against the new generated key. This process is done per credit card entry, first a decryption with the old key and then an encryption with the new key. Once all records are encrypted with the new key, the old key is destroyed.

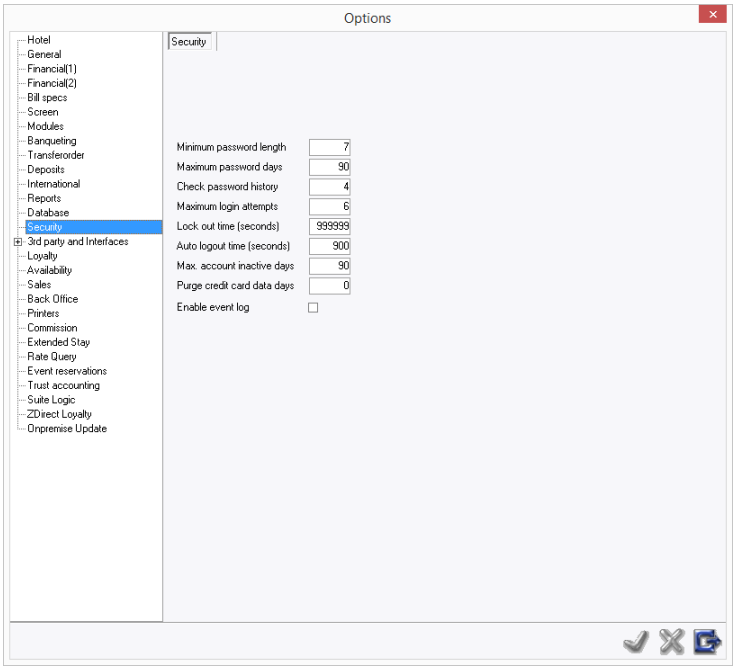
Key renewal must be done yearly by the administrator of the system (See 7.10)

7.9. **Logs**

The PCI logs are stored in a SQL server table, see the below for the events that are logged.

From IDPMS these events can be reviewed Extra->Tools->Show System Log

Logging can also be send to the Windows event log by enabling the following parameter:



This logging is also send to Microsoft Event Logging and the format of the Event Logging is *not* configurable in IDPMS. In The Settings -> Options ->security parameters the event log can be turned on

The Microsoft Event Log can be configured to send event log information to a centralized server, the Windows Event Collector. The Windows Event Collector functions support subscribing to events by using the WS-Management protocol.

Event collection allows administrators to get events from remote computers and store them in a local event log on the collector computer. The destination log path for the events is a property of the subscription. All data in the forwarded event is saved in the collector computer event log (none of the information is lost). Additional information related to the event forwarding is also added to the event.

How to fully configure the Microsoft Event Collector is beyond the scope of this document, please see the Microsoft website under "Windows Event Collector" (http://msdn.microsoft.com/en-us/library/windows/desktop/bb427443(v=vs.85).aspx).

Amadeus IDPMS has logging that cannot be turned off as per PCI DSS 10.2 and 10.3 as follows:

Implement automated assessment trails for all system components to reconstruct the following events:

10.2.1 All individual user accesses to cardholder data

10.2.2 All actions taken by any individual with root or administrative privileges

10.2.3 Access to all assessment trails

10.2.4 Invalid logical access attempts

10.2 5 Use of identification and authentication mechanisms

10.2.6 Initialization of the assessment logs

10.2.7 Creation and deletion of system-level objects.

Record at least the following assessment trail entries for all system components for each event from 10.2.x:

10.3.1 User identification

10.3.2 Type of event

10.3.3 Date and time

10.3.4 Success or failure indication

10.3.5 Origination of event

10.3.6 Identity or name of affected data, system component, or resource.

Disabling or subverting the logging function of IDPMS in any way will result in non-compliance with PCI DSS.

7.10. PCI-Compliant Wireless settings

IDPMS does not support wireless technologies. However, should the merchant implement wireless access within the cardholder data environment, the following guidelines for secure wireless settings must be followed per PCI Data Security Standard 1.2.3, 2.1.1 and 4.1.1.

1.2.3: Perimeter firewalls must be installed between any wireless networks and systems that store cardholder data, and these firewalls must deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

2.1.1:

- All wireless networks implement strong encryption (e.g. AES)

- Encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions
- Default SNMP community strings on wireless devices were changed
- Default passwords/passphrases on access points were changed
- Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2)
- Other security-related wireless vendor defaults, if applicable

4.1.1:

- Industry best practices are used to implement strong encryption for the following over the wireless network in the cardholder data environment (4.1.1):
- Transmission of cardholder data
- Transmission of authentication data
- Payment applications using wireless technology must facilitate the following regarding use of WEP:
- For new wireless implementations, it is prohibited to implement WEP as of March 31, 2009.
- For current wireless implementations, it is prohibited to use WEP after June 30, 2010.

Amadeus Support uses Fastviewer as secure connection with the customer. Fastviewer use a remote technology where the connection is secured with 256 bit AES encryption. As each employee has its own credentials logging of access can be secured.

Fastviewer remote connects from the merchant's network to the Amadeus Fastviewer servers. No direct connectivity from the internet is required for this solution.

The merchant is responsible for creating a dedicated Amadeus Support Account on their network applying the Password requirements as described in Chapter 7.5

7.11. Encryption Key Renewal

The end-user of IDPMS can at any time replace the key that is in use for PCI related data encryption. The key-renewal process can only be started by those users that are granted the right to do so. During the training the Amadeus consultant clearly explains the customer this part and adds that this right should be granted to a very limited number of users.

7.11.1. Generate an Encryption Key

The Encryption Key is generated by the application and a user *must* have rights inside the application to do so. The process cannot be influenced in any way, since it is part of the application.

7.11.2. Distribution

The Encryption Key does not need to be distributed. The generated Encryption Key is automatically updated in the application data, and where needed the data is encrypted against the new key.

7.11.3. Encryption Key Protection

The Encryption Key is protected with a Key Encryption Key. A 10MB data stream is the core for the key and this data stream can be saved to an USB memory Stick and then stored in a vault.

7.11.4. Key renewal

There is no access to any key material by the customer. When a new key is generated, all encrypted data in IDPMS is decrypted against the old key and then encrypted against the new generated key. This process is done per credit card entry, first a decryption with the old key and then an encryption with the new key. Once all records are encrypted with the new key, the old key is destroyed.

7.12. Centralized Logging

The PCI specific logging of user actions can be exported in any desired format. To do so, the standard exporting tools of Amadeus PM PRO are used.

7.12.1. Export the Logging

Export of the logging can be performed at any time by selecting the specific export/report. It is possible to export the information during the so-called night audit, since the export is embedded in the standard workflow in Amadeus IDPMS.

7.13. Use of necessary and secure services and protocols

PA-DSS states that the payment application must only use necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties. Amadeus does not transport any information over the internet, so no recommendation for protocols in this area are necessary.

Communications to a so-called Gateway of the Credit Card Merchant (like SIX Cards) is over the LAN using a direct TCP/IP socket, or in most cases over Https.

7.14. Never store cardholder data on internet-accessible systems

Never store cardholder data on Internet-accessible systems (e.g., web server and database server must not be on same server.)

Please see article 4 for the recommended setup.

7.15. PCI-Compliant Delivery of Updates

The development process for updates and patches is described in the "Product Lifecycle Manual"

As a development company, we keep abreast of the relevant security concerns and vulnerabilities in our area of development and expertise.

Once we identify a relevant vulnerability, we work to develop & test a patch that helps protect IDPMS against the specific, new vulnerability. We attempt to publish a patch within days of the identification of the vulnerability. Typically, merchants are expected to respond quickly to and install available patches within 30 days.

Updates are downloaded automatically by the Clients by requesting these on our On-premise Update server

In accordance with the PCI "chain of trust" the client will verify the downloaded update package of IDPMS with the published Hash on the Amadeus Intranet. A mismatch between the published and the calculated Hash will stop the update process.

Updates are announced through the IDPMS mail system for selected IDPMS users.

7.16. **PCI-Compliant Remote Access**

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism (username/ password and an additional authentication item such as a token or certificate).

In the case of vendor remote access accounts, in addition to the standard access controls, vendor accounts should only be active while access is required to provide service. Access rights should include only the access rights required for the service rendered, and should be robustly audited.

If users and hosts within the payment application environment may need to use third-party remote access software such as RDP, Terminal Server, etc. to access other hosts within the payment processing environment, special care must be taken.

In order to be compliant, every such session must be encrypted with at least 128-bit encryption (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment). For RDP/Terminal Services this means using the high encryption setting on the server, and for FastViewer it means using symmetric or public key options for encryption. Additionally, the PCI user account and password requirements will apply to these access methods as well.

When requesting support from a vendor, reseller, or integrator, customers are advised to take the following precautions:

- Change default settings (such as usernames and passwords) on remote access software (e.g. VNC)
- Allow connections only from specific IP and/or MAC addresses
- Use strong authentication and complex passwords for logins according to PCI DSS 8.1, 8.3, and 8.5.8-8.5.15
- Enable encrypted data transmission according to PCI DSS 4.1
- Enable account lockouts after a certain number of failed login attempts according to PCI DSS 8.5.13
- Require that remote access take place over a VPN via a firewall as opposed to allowing connections directly from the internet
- Enable logging for auditing purposes
- Restrict access to customer passwords to authorized reseller/integrator personnel.
- Establish customer passwords according to PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.

7.17. **Data Transport Encryption**

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128 bit encryption strength (either at the transport layer with SSL or IPSEC; or at the data layer with algorithms such as RSA or Triple-DES) to safeguard cardholder data during transmission over public networks (this includes the Internet and Internet accessible DMZ network segments).

PCI DSS requirement 4.1: Use strong cryptography and security protocols such as secure transport layer security (TLS 1.2) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

- Refer to the Dataflow diagram for an understanding of the flow of encrypted data associated with IDPMS.

IDPMS does not recommend the usage of their application over Public Networks.
If used over a WIFI network a VPN must be used at all times

IDPMS does not require nor permit the use of any insecure service or protocol. Here are those that IDPMS does use:

- TLS1.2
- HTTPS

7.18. PCI-Compliant Use of End User Messaging Technologies

IDPMS does not allow or facilitate the sending of PANs via any end user messaging technology (for example, e-mail, instant messaging, and chat).

7.19. Non-console administration

Although IDPMS does not support non-console administration and we do not recommend using non-console administration, should you ever choose to do this, must use SSH, VPN, or TLS1.2 for encryption of this non-console administrative access.

7.20. Network Segmentation

The PCI DSS requires that firewall services be used (with NAT or PAT) to segment network segments into logical security domains based on the environmental needs for internet access. Traditionally, this corresponds to the creation of at least a DMZ and a trusted network segment where only authorized, business-justified traffic from the DMZ is allowed to connect to the trusted segment. No direct incoming internet traffic to the trusted application environment can be allowed. Additionally, outbound internet access from the trusted segment must be limited to required and justified ports and services.

Refer to the standardized Network diagram for an understanding of the flow of encrypted data associated with IDPMS.

7.21. Maintain an Information Security Program

In addition to the preceding security recommendations, a comprehensive approach to assessing and maintaining the security compliance of the payment application environment is necessary to protect the organization and sensitive cardholder data.

The following is a very basic plan every merchant/service provider should adopt in developing and implementing a security policy and program:

- Read the PCI DSS in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
- Once the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.
- Create an action plan for on-going compliance and assessment.
- Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI Self-Assessment Questionnaire.
- Call in outside experts as needed.

7.22. Application System Configuration

Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PCI DSS compliance.

- Windows 7, Windows 8 &8.1 Windows 10
- Windows server 2008, 2008r2, 2012
  All latest updates and hot-fixes should be tested and applied, and vendors security recommendations should be followed.
- 2GB or higher recommended for Payment Application
- TCP/IP network connectivity
- SQL Server 2008R2 , 2012, 2014 or 2016
  All latest service packs, updates and hot-fixes should be tested and applied

7.22.1 System services required for workstation installation

- SQL Native client
- Microsoft Eventlog (optional)

7.22.2 Protocols required for client – server communication

- TCP/IP communication between client and server
- HTTPS communication between client and 3rd party payment providers (optional)

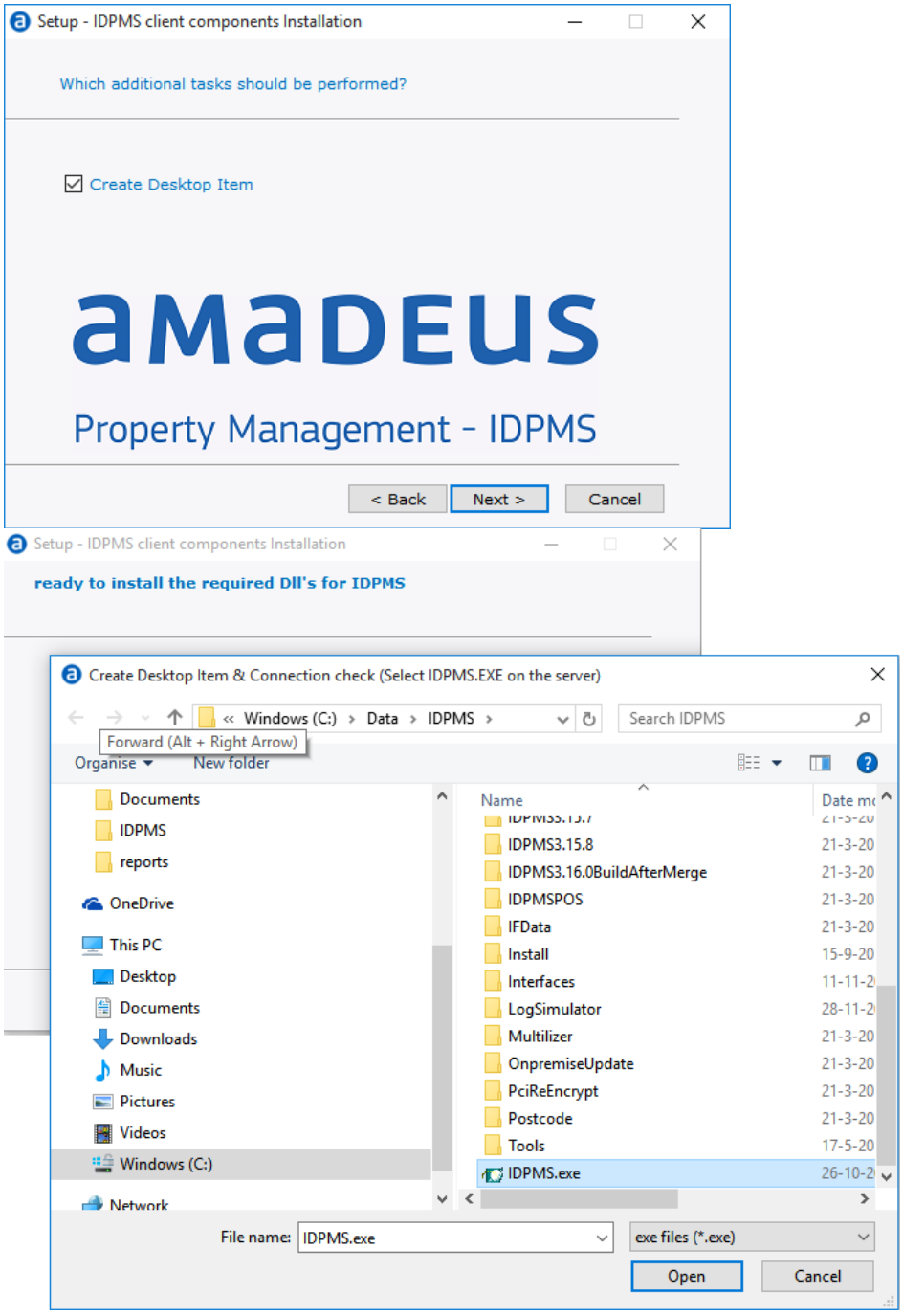
7.23. Payment Application Initial Setup & Configuration

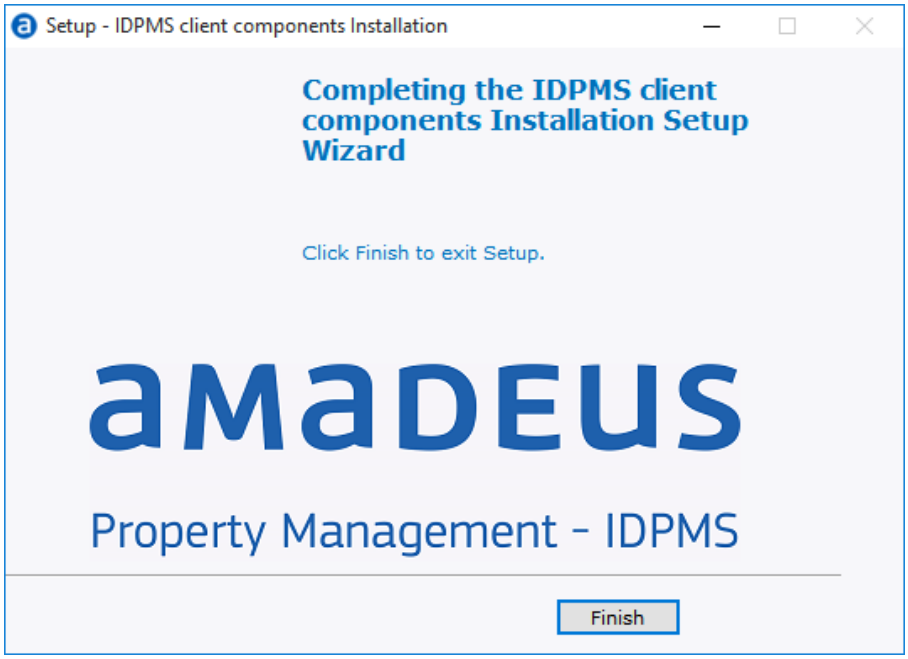
The initial setup is always performed by an Amadeus Installer.

7.24. New Installation of Clients

The following configuration will be performed by Amadeus representatives at installation, oftentimes in close conjunction with the customers' System Administrator and is listed here for installation of additional clients or replacements.

- From the Client browse to the File servers IDPMS folder and start the Client_Install.exe





7.25. **Defining the Payment Gateway**

The payment gateway is installed by payment processor; this is not within the scope of an IDPMS installation.

Tests of the payment gateway will be done in joint effort.