WHITE PAPER

TRAVELPORT GLOBALWARE V7.3

OUT-OF-SCOPE WHITEPAPER

NICK TRENC | CISSP, CISA, QSA, PA-QSA

COALFIRE℠

North America | Latin America | Europe
877.224.8077 | info@coalfire.com | coalfire.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Travelport engaged Coalfire Systems Inc. (Coalfire), as a respected Payment Card Industry (PCI) Payment Application – Qualified Security Assessor (PA-QSA) company, to conduct an independent technical assessment of their GlobalWare application. Coalfire conducted assessment activities including technical testing, architectural assessment, and compliance assessment.

In this paper, Coalfire will describe that the GlobalWare application is not in scope of the Payment Application – Data Security Standard (PA-DSS).

Additionally, Coalfire has validated that if implemented in accordance to Travelport GlobalWare Implementation Guide, the GlobalWare application should not negatively impact an agency's PCI compliance.

ABOUT GLOBALWARE

Travelport GlobalWare 7.3 is a back-office system used by various travel agencies for the purposes of accounting and reporting as well as data backup management.

GlobalWare does not provide settlement or authorization functionality for the travel agencies; however, GlobalWare does store cardholder data in the application database solely for the purpose of account reconciliation and reporting. The cardholder data is fed into the application via GDS interface files, or via a file import. The data is then stored encrypted in a database and retained in accordance with business needs. Finally, when the data is no longer needed, the database records can be archived and all cardholder data is truncated to the first six and last four digits.

It is Coalfire's opinion, based on the fact that the application does not perform any authorization or settlement activities, that the Travelport GlobalWare application is out of scope of PA-DSS compliance requirements. In addition, there are no configuration options within the application that would bring GlobalWare into the scope of PA-DSS validaton.

GlobalWare's primary reason for storage of cardholder data is so that travel agencies can access this backup data in the event a payment or adjustment needs to occur. This data is also used for accounting and credit card charge reconciliation reporting.

AUDIENCE

This assessment white paper has two target audiences:

1. The first target audience includes travel agencies considering the impact of PCI DSS when using the GlobalWare application in their payment card environment;
2. The second target audience is the audit community (QSAs in particular) who need to understand the impact that the GlobalWare application may have on the individual travel agency environments.

ASSESSMENT SCOPE

The purpose of this assessment was to validate that GlobalWare 7.3 is out of scope of PA-DSS compliance requirements and to assess the impact of the implementation of the application in a agency's PCI environment.

The assessment testing focused on the following functional areas:

1. Implementation of GlobalWare 7.3 in a simulated network environment.

METHODOLOGY

Coalfire has implemented industry best practices in our assessment and testing methodologies. Coalfire completed a multi-faceted technical assessment process during the course of this project using these industry and audit best practices. Coalfire conducted technical lab testing in our Colorado lab 11/28/2016 – 12/9/2016

At a high level, testing consisted of the following tasks:

1. Technical review of the architecture and the full solution with all of its components
2. Implementation and testing of the application in a simulated network environment.
3. Validation that GlobalWare 7.3 does not negatively impact PCI DSS requirements.

TRAVEL AGENCY PCI COMPLIANCE SCOPE

There will always be certain controls for PCI compliance that must be independently assessed in any agency's environment and PCI compliance will always apply to an agency if cardholder data is transmitted, processed, or stored anywhere in their physical environment. Coalfire validated that the Travelport GlobalWare application would not negatively impact an agency's PCI compliance if implemented in accordance with the GlobalWare Implementation Guide.

TECHNICAL SECURITY ASSESSMENT

The modular design of the GlobalWare 7.3 application presented Coalfire with two deployment scenarios. Our assessment covered this deployment architecture and configuration options included with the application. The GlobalWare 7.3 application was reviewed following the Payment Application-Data Security Standard and following the format of the Report on Validation (ROV) normally completed by our PA-QSA team.

The assessment included a comprehensive set of administration, technical, and physical control testing performed for the deployment architecture. Applicable compliance control requirement adherence to the PCI PA-DSS was validated within the scope of our security assessment. The assessment included the following components:

- **GlobalWare –** the client application that resides on a travel agent's Windows®-based desktop or laptop
- **Sybase SQL Anywhere database –** backend component for storage of all data related to the application. This database can be configured to store encrypted cardholder data depending on the business needs of the travel agency.

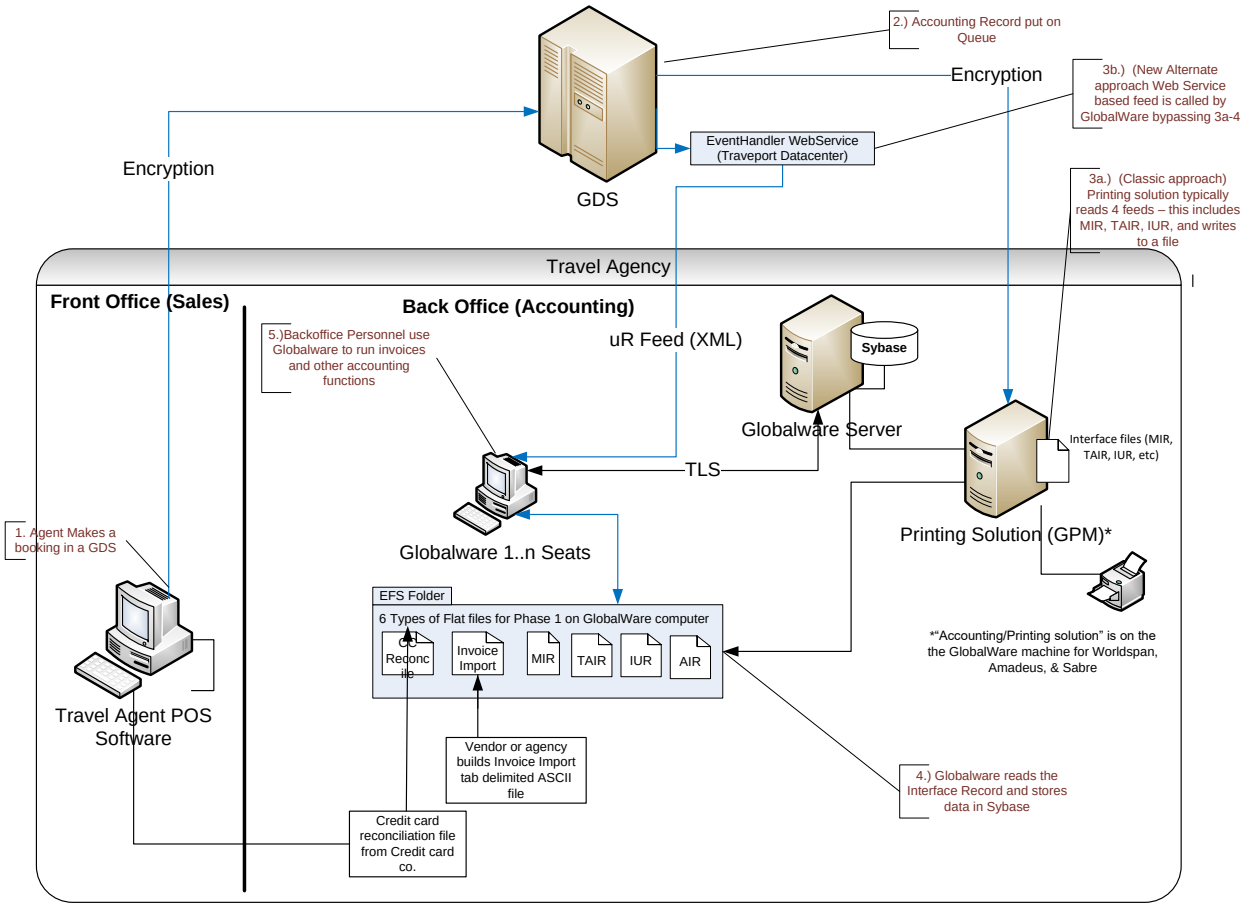
Deployment Scenarios

There are two deployment scenarios available for GlobalWare 7.3.

Scenario one is considered standalone mode wherein the application and database are located on a single system with no additional components required. Only simple transaction details such as invoice number, date, time, and amount are required by the Point of Sale software, keeping the POS application out of scope of PA-DSS compliance requirements.

Scenario two is a multi-user mode wherein the application is installed on multiple client machines and the database is installed on a single network server. This scenario is typical for larger travel agencies that have multiple users who operate in parallel with shared access to the centralized database

The diagram below provides a typical business context for the application and reflects how the Travelport GlobalWare application generally only operates with data that has already been settled and never initiates any transactions. Cardholder data is queried from the Issuing institution's database and a copy is stored locally for the purposes of accounting, reporting and backup data management.



SUMMARY FINDINGS

The following findings are relevant highlights from this assessment:

1. The GlobalWare application does not provide any capability or ability to facilitate authorization or settlement processes for credit card transactions.
2. Technical testing, architecture and documentation review all confirmed that the application does not transmit cardholder data to any external systems for authorization and settlement.
3. The GlobalWare application will not negatively impact agency's PCI compliance if implemented in accordance with the GlobalWare Implementation Guide

ASSESSOR COMMENTS

It is important to note that an 'Out of Scope' solution, as detailed in this whitepaper, does not alleviate an agency's responsibility to PCI DSS compliance requirements. Be aware that disregarding PCI requirements and security best practice controls for systems and networks outside of PCI DSS scope can introduce many other security or business continuity risks to the agency. Security and business risk mitigation should be any agency's goal and focus for selecting security controls

PCI PA-DSS COMPLIANCE SCOPE

The PCI PA-DSS applies to a payment application (as defined by PCI SSC) as follows: "The PA-DSS applies to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties (PCI PA-DSS Version 2.0, 2010, October: Page 5)."

The PCI Security Standards Council maintains a document entitled, "Applications Eligible for PA-DSS-Validation" which poses 13 questions for the purpose of determining if an application is eligible for assessment under the PA-DSS standard. As of the date of this writing, the document can be found at https://www.pcisecuritystandards.org/security_standards/documents.php?document=applications-eligible-for-padss-validation#applications-eligible-for-padss-validation

If the answer is YES to ANY of the following questions, the application is NOT eligible for validation under PA-DSS.

1. Is this a beta version of the application?
   a. **No**. This is a production ready application.
2. Does the application handle cardholder data, but the application itself does not facilitate authorization or settlement?
   b. Yes. The application does not facilitate authorization or settlement, however it does store cardholder data for the purposes of account reconciliation and reporting as well as occasional needs for chargeback or refunds (Travelport GlobalWare supplies cardholder data to travel agencies' payment applications, but doesn't perform any processing by itself).
3. Does the application facilitate authorization or settlement, but has no access to cardholder data or sensitive authentication data?
   a. **No**. This application has access to cardholder data but does not facilitate authorization or settlement.
4. Does the application require source code customization or significant configuration by the customer (as opposed to being sold and installed "off the shelf") such that the changes impact one or more PA-DSS requirements?
   a. **No**. The application is sold to customers and does not require source code customization.
5. Is the application a back-office system that stores cardholder data but does not facilitate authorization or settlement of credit card transactions? For example:
   1) Reporting and CRM
   2) Rewards or fraud scoring
   a. **Yes**. The application does not facilitate authorization or settlement, however it does store cardholder data for the purposes of account reconciliation and reporting as well as occasional needs for chargeback or refunds (GlobalWare supplies cardholder data to the travel agency's payment application, but doesn't perform any processing by itself).
6. Is the application developed in-house and only used by the company that developed the application?
   a. **No**. The application is sold to multiple customers.
7. Is the application developed and sold to a single customer for the sole use of that customer?
   a. **No**. There are multiple customers to which this application is sold.

8. Does the application function as a shared library (such as a DLL) that must be implemented with another software component in order to function, but that is not bundled (that is, sold, licensed and/or distributed as a single package) with the supporting software components?
    a. **No**. The application does not function as a shared library..
9. Does the application depend on other software in order to meet one or more PA-DSS requirements, but is not bundled (that is, sold, licensed and/or distributed as a single package) with the supporting software?
    a. **No**. The application does not depend on other software to meet PA-DSS requirements.
10. Is the application a single module that is not submitted as part of a suite, and that does not facilitate authorization or settlement on its own?
    a. **No**. The payment application is not a single module that is not part of a suite and the application does not facilitate authorization and settlement on its own.
11. Is the application offered only as software as a service (SAAS) that is not sold, distributed, or licensed to third parties?
    a. **No**. The application is not offered only as software as a service.
12. Is the application an operating system, database or platform; even one that may store, process, or transmit cardholder data?
    a. **No**. GlobalWare is a standalone application which executes on a Windows® platform computer.
13. Does the application operate on any consumer electronic handheld device (e.g., smart phone, tablet or PDA) that is not solely dedicated to payment acceptance for transaction processing?
    a. **No.** The application resides on a Windows®-based server, desktop or laptop device.

Based upon the responses to the questions outlined in the application eligibility guidance provided by PCI, the GlobalWare application is not in scope of PA-DSS and is not considered a payment application as defined by the PCI Security Standards Council.

TECHNICAL ASSESSMENT

ASSESSMENT METHODS

The assessment used the following methods to assess the PCI PA-DSS scope-impact of the solution:

1. Analysis of the architecture and configuration of the solution.
2. Validation that card processing is not supported by the application in both deployment scenarios

ASSESSMENT ENVIRONMENT

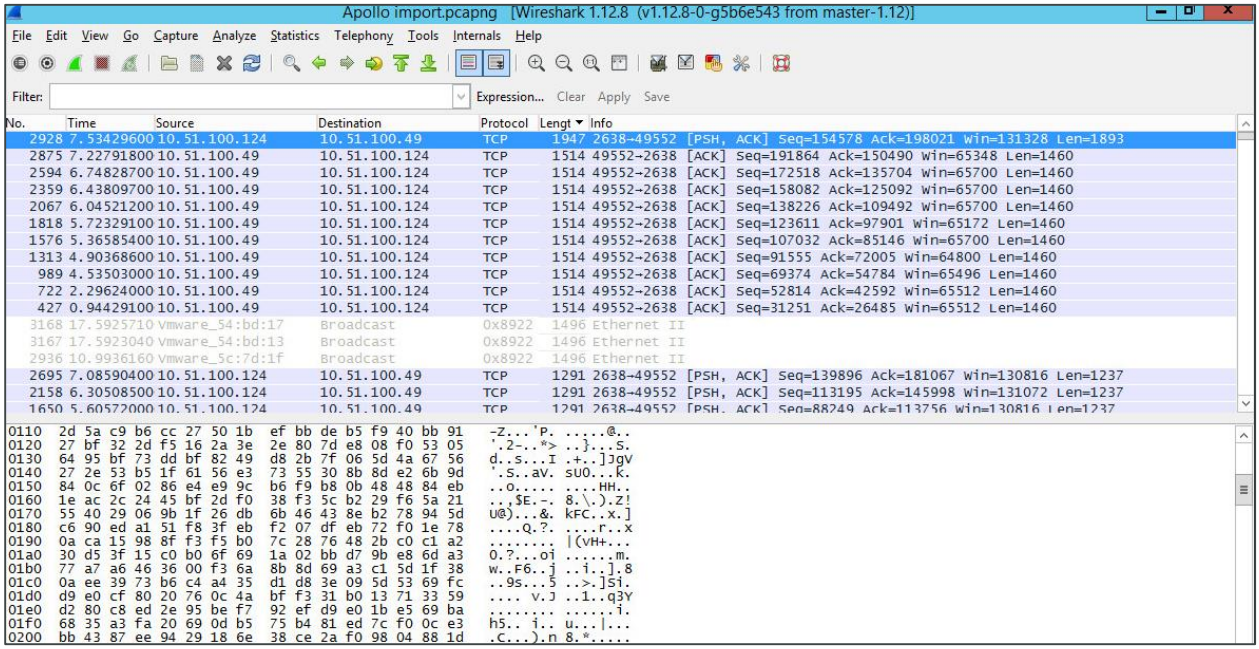
For the two possible deployment scenarios, the GlobalWare solution was installed in a segregated virtual environment utilizing VMware® ESXi 6.1 in the following manner:

1) Standalone installation where the GlobalWare software and the SAP® SQL Anywhere database are running on a single computer running Windows Server 2012 R2.
2) Multiple computer installation where GlobalWare software and the SAP® SQL Anywhere are installed on separate computers. One computer was Windows Server 2012 R2 and two client machines; one running Windows 10 and one running Windows 7 SP1. S

Both systems had the latest Windows updates applied and auto-update feature enabled. Additionally Windows Defender anti-virus software was installed on each computer. The entire solution was contained in a PCI DSS compliant environment segregated from other network traffic using a Fortinet virtual firewall.

NETWORK TRAFFIC ASSESSMENT

A Wireshark Ethernet port sniffer was used to monitor traffic coming out of the system with GlobalWare installed. The captures indicate that no cardholder data is being transmitted over the network in the clear.



FORENSIC ANALYSIS

The technical assessment included a forensic examination of the hard drive of the system running the GlobalWare solution.

The process for examining the hard drive was as follows:

1. The GlobalWare solution installation disks were captured for forensic analysis.
2. FTK was used to search the forensic images for key criteria, including cardholder and sensitive authentication data.

No findings were identified with the image when searched using FTK. The following represents the conclusions from performing forensic analysis:

1. The forensic analysis demonstrates that there is no residual cardholder or sensitive authentication data on the system running GlobalWare.

After conducting several transactions, the disk image of the testing system was taken and scanned for the evidence of any credit card data or sensitive authentication data. FTK software was used for this forensic analysis and it showed no findings. The interview with the developers and review of the Arrival Manager software confirmed that the application never stores cardholder data in the clear.

TOOLS AND TECHNIQUES

Standard tools Coalfire utilizes for its application security reviews can include:

TOOL NAME	DESCRIPTION
FTK	*Forensic tool for digital data and media analysis.
Wireshark	Wireshark Ethernet port sniffer was used to observe the traffic coming in and out of the system.
Additional tools	FTK Imager, Process Explorer

*Forensic tool: A tool or method for uncovering, analyzing and presenting forensic data, which provides robust ways to authenticate, search, and recover computer evidence rapidly and thoroughly.

ABOUT THE AUTHOR

Nick Trenc | Practice Director

Nick Trenc (ntrenc@coalfire.com) is an Application Security Specialist with Coalfire. Nick has many years of experience working as a QSA and PA-QSA helping clients develop systems and software for use in PCI DSS environments. He has authored and spoken on multiple security topics including mobile security, application security, virtualization, cyber risk management, secure software development, and PCI DSS and PA-DSS compliance. He holds a CISSP, CISA, QSA, and PA-QSA.

Published Dec 2016.

ABOUT COALFIRE

As a trusted advisor and leader in cybersecurity, Coalfire has more than 15 years in IT security services. We empower organizations to reduce risk and simplify compliance, while minimizing business disruptions. Our professionals are renowned for their technical expertise and unbiased assessments and advice. We recommend solutions to meet each client's specific challenges and build long-term strategies that can help them identify, prevent, respond, and recover from security breaches and data theft. Coalfire has offices throughout the United States and Europe. www.coalfire.com