



Appendix E: Attestation of Compliance – Service Providers Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Atos Worldline SIPS

Version 1.2

September 2009

Instructions for Submission

The Qualified Security Assessor (QSA) and Service Provider must complete this document as a declaration of the Service Provider's compliance status with the Payment Card Industry Data Security Standard (PCI DSS). Complete all applicable sections and submit to the requesting payment brand.

Part 1. Qualified Security Assessor Company Information

Company Name:	Verizon Business		
Lead QSA Contact Name:	Abdelbaset LATRECHE	Title:	Principal Consultant
Telephone:	+ 33 1 41 62 42 32	E-mail:	abdelbaset.latreche@verizonbusiness.com
Business Address:	14, rue de la Montjoie	City:	Saint-Denis
State/Province:		Country:	France
		ZIP:	93210
URL:	http://www.verizonbusiness.com		

Part 2. Service Provider Organization Information

Company Name:	Atos Worldline	DBA(s):	PSP
Contact Name:	Jean-Michel LAVAUD	Title:	Audit Manager
Telephone:	+33 3 88 14 85 43	E-mail:	jean-michel.lavaud@atosorigin.com
Business Address:	19, rue de la Vallée Maillard	City:	Blois
State/Province:		Country:	France
		ZIP:	67905
URL:	http://www.atosworldline.com		

Part 2a. Services Provided (check all that apply)

<input checked="" type="checkbox"/> Authorization	<input type="checkbox"/> Loyalty Programs	<input checked="" type="checkbox"/> 3-D Secure Access Control Server
<input type="checkbox"/> Switching	<input checked="" type="checkbox"/> IPSP (E-commerce)	<input type="checkbox"/> Process Magnetic-Stripe Transactions
<input checked="" type="checkbox"/> Payment Gateway	<input checked="" type="checkbox"/> Clearing & Settlement	<input checked="" type="checkbox"/> Process MO/TO Transactions
<input type="checkbox"/> Hosting	<input checked="" type="checkbox"/> Issuing Processing	<input type="checkbox"/> Others (please specify):

List facilities and locations included in PCI DSS review: Blois, Seclin and Vendôme

Part 2b. Relationships

- o Does your company have a relationship with one or more third-party service providers (for example, gateways, web-hosting companies, airline booking agents, loyalty program agents, etc)? Yes No

Part 2c. Transaction Processing

How and in what capacity does your business store, process and/or transmit cardholder data?
 Atos Worldline is dedicated to services and solutions covering the whole process of payment and information flows through Payment and Card Processing services, CRM services and Multi Channel Contact (Internet and Voice services), Atos Worldline process more than 30 millions transactions.

Payment Application in use: N/A

Payment Application Version: N/A

JPD

Part 3. PCI DSS Validation

Based on the results noted in the Report on Compliance ("ROC") dated 09/14/2009, *Abdelbaset LATRECHE* asserts the following compliance status for the entity identified in Part 2 of this document as of 09/14/2009 (check one):

- Compliant:** All requirements in the ROC are marked "in place¹," and a passing scan has been completed by the PCI SSC Approved Scanning Vendor *Verizon Business* thereby *Afos Worldline* has demonstrated full compliance with the PCI DSS 1.2 for the SIPS environment.
- Non-Compliant:** Some requirements in the ROC are marked "not in place," resulting in an overall **NON-COMPLIANT** rating, or a passing scan has not been completed by a PCI SSC Approved Scanning Vendor, thereby (*Service Provider Name*) has not demonstrated full compliance with the PCI DSS.
Target Date for Compliance:
 An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4, since not all payment brands require this section.*

Part 3a. Confirmation of Compliant Status

QSA and Service Provider confirm:

- The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures, Version 1.2*, and was completed according to the instructions therein.
- All information within the above-referenced ROC and in this attestation fairly represents the results of the assessment in all material respects.
- The Service Provider has read the PCI DSS and recognizes that they must maintain full PCI DSS compliance at all times.
- No evidence of magnetic stripe (i.e., track) data², CAV2, CVC2, CID, or CVV2 data³, or PIN data⁴ storage after transaction authorization was found on ANY systems reviewed during this assessment.

Part 3b. QSA and Service Provider Acknowledgments

<i>Abdelbaset</i> Signature of Lead QSA ↑	Date: 09/14/2009
Lead QSA Name: Abdelbaset LATRECHE	Title: Principal Consultant
<i>J. Duvet</i> Signature of Service Provider Executive Officer ↑	Date: 09/14/2009
Service Provider Executive Officer Name: Jean Pascal Duvet	Title: SIPS Business Unit Manager

¹ "In place" results should include compensating controls reviewed by the QSA. If compensating controls are determined to sufficiently mitigate the risk associated with the requirement, the QSA should mark the requirement as "in place".
² Data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic stripe data after transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.
³ The three- or four-digit value printed on the signature panel or face of a payment card used to verify card-not-present transactions.
⁴ Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 4. Action Plan for Non-Compliant Status

Please select the appropriate "Compliance Status" for each requirement. If you answer "No" to any of the requirements, you are required to provide the date Company will be compliant with the requirement and a brief description of the actions being taken to meet the requirement. *Check with the payment brand(s) before completing Part 4 since not all payment brands require this section.*

PCI Requirement	Description	Compliance Status (Select One)	Remediation Date and Actions (If Compliance Status is "No")
1	Install and maintain a firewall configuration to protect cardholder data.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
3	Protect stored cardholder data.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
4	Encrypt transmission of cardholder data across open, public networks.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
6	Use and regularly update anti-virus software.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
6	Develop and maintain secure systems and applications.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
7	Restrict access to cardholder data by business need to know.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
8	Assign a unique ID to each person with computer access.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
9	Restrict physical access to cardholder data.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
10	Track and monitor all access to network resources and cardholder data.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
11	Regularly test security systems and processes.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
12	Maintain a policy that addresses information security.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	


