Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information					
Part 1a. Service Provider Organization Information					
Company Name:	SAP Ariba		DBA (doing business as):	-	
Contact Name:	Ermias Desta		Title:	Interim Business Information Security Officer	
Telephone:	+44 792002 1110		E-mail:	ermias.desta@sap.com	
Business Address:	3420 Hillview Ave		City:	Palo Alto	
State/Province:	CA	Country:	USA	Zip:	94304
URL:	https://www.ariba.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	usd AG				
Lead QSA Contact Name:	Torsten Schlotmann		Title:	QSA	
Telephone:	+49 6102 8631 330		E-mail:	torsten.schlotmann@usd.de	
Business Address:	Frankfurter Str. 233, Haus C1		City:	Neu-Isenburg	
State/Province:	-	Country:	Germany	Zip:	63263
URL:	https://www.usd.de				

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed:	Ariba	
Type of service(s) assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☒ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☒ Others (specify): Supplier management		

***Note**: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.*

Part 2a. Scope Verification *(continued)*		
Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):		
Name of service(s) not assessed:	All other SAP offerings (see "Others (specify)" below)	
Type of service(s) not assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☒ Others (specify): All other offerings of SAP not directly related to Ariba, e.g. application development or other cloud services, were not part of this assessment.		
Provide a brief explanation why any checked services were not included in the assessment:	All other offerings of SAP not directly related to Ariba, e.g. application development or other cloud services, were not part of this assessment. The assessment scope includes only the SAP Ariba related services.	

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	SAP Ariba (Ariba) is subsidiary of SAP SE (SAP). SAP is a German-based software corporation that focuses on B2B software that acquired Ariba in 2012. Ariba is the leading B2B solution for procurement that helps their clients managing their supply chain more efficiently. Ariba provides their customers with access to the Ariba's cloud applications, where they are able to interact with millions of suppliers for direct or indirect expense categories. All buyers and suppliers that are part of the Ariba Network are able to facilitate the procurement process including invoicing on the cloud-based platform of Ariba. Payment can include the transmission of cardholder data between the buyer and the seller. In order to improve and streamline the procurement process for their customers, Ariba enables the invoicing between buyers and suppliers. Further, the Spot Buy application allows users to search for and buy non-sourced goods from their Buying solutions. Payment can be facilitated via a deposited corporate procurement card. Spot Buy helps buying non-sourced goods (e.g. goods that have not been put under contract) without the need to source the supplier, provide the supplier with any payment method and so on. For that process, storing, processing and transmission of cardholder data is necessary.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	-

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility:	Number of facilities of this type	Location(s) of facility (city, country):
Example: Retail outlets	*3*	*Boston, MA, USA*
Corporate Offices	1	Palo Alto, CA, USA
Data Center	1	San Jose, CA, USA
Data Center	1	Sterling, VA, USA
Data Center	1	Santa Clara, CA, USA
Data Center	1	St. Leon-Rot, Germany
Data Center	1	Amsterdam, Netherlands
Data Centers	2	Moscow, Russia
Data Center	1	Shanghai, China
Data Center	1	Beijing, China

Data Center	1	Dubai, United Arab Emirates
Data Center	1	Riyadh, Saudi Arabia
Data Center	1	Dammam, Saudi Arabia
Data Center	1	Tokyo, Japan
Data Center	1	Osaka, Japan
Data Centers	2	Sydney, Australia

Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☐ Yes ☒ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
-			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	

Part 2e. Description of Environment

Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	The following regions hosting Core Stack applications were part of this assessment: US, EU, RU, CN, MENA, JP, AU. In general, there are two data centers per region (US, EU, RU CN, JP, AU). However, the MENA region consists of three and the US region of three data centers. In each data center, a similar, layered network approach is implemented. The various networks contain CDE components such as databases, web and application servers. Other critical systems are management components (NTP, SIEM, IDS, remote access, monitoring) and network devices (firewall, load balancer, router, switches).
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☒ Yes ☐ No

Part 2f. Third-Party Service Providers	
Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?	☐ Yes ☒ No

If Yes:	
Name of QIR Company:	-
QIR Individual Name:	-
Description of services provided by QIR:	-

Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?	☒ Yes ☐ No

If Yes:	
Name of service provider:	**Description of services provided:**
Equinix Inc.	Housing / co-location services
Cyxtera Technologies, Inc.	Housing / co-location services
vXchnge	Housing / co-location services
Equinix EMEA	Housing / co-location services
SAP SE	Housing / co-location services, Central IT services
Centr Hraneniya Dannih LLC (Rostelecom Data Centers)	Housing / co-location services
DataLine LLC (Rostelecom Data Centers)	Housing / co-location services
Detecon Al Saudia Co. Ltd. (DETASAD)	Housing / co-location services
Etihad Etisalat Co. (Mobily)	Housing / co-location services
GDS Services Ltd.	Housing / co-location services
CyberSource	Payment Processing & Fraud Management
Google LLC	Infrastructure as a Service

Note: *Requirement 12.8 applies to all entities in this list.*

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.
- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

Note: *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

Name of Service Assessed:	Ariba

PCI DSS Requirement	Details of Requirements Assessed			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☒	☐	☐	-
Requirement 2:	☒	☐	☐	-
Requirement 3:	☒	☐	☐	-
Requirement 4:	☐	☒	☐	4.1.1: N/A. No wireless networks in scope of this assessment.
Requirement 5:	☐	☒	☐	5.1, 5.1.1, 5.2, 5.3: N/A. No systems commonly affected by malicious software in scope of this assessment.
Requirement 6:	☒	☐	☐	-
Requirement 7:	☒	☐	☐	-
Requirement 8:	☐	☒	☐	8.1.5: N/A. No third-parties with remote access. 8.5.1: N/A. SAP Ariba has no access to customer premises.
Requirement 9:	☐	☒	☐	9.6, 9.6.1 – 9.6.3: N/A. No media containing cardholder data are distributed. 9.8.1: N/A. There are no hard-copy materials in scope of this assessment. 9.9, 9.9.1 – 9.9.3: N/A. No POS devices in scope of this assessment.
Requirement 10:	☒	☐	☐	-

Requirement 11:	☒	☐	☐	-
Requirement 12:	☐	☒	☐	12.3.9: N/A. No vendors or business partners with remote access in scope of this assessment.
Appendix A1:	☐	☐	☒	A1, A1.1 – A1.4: N/A. The assessed entity is no shared hosting provider.
Appendix A2:	☐	☐	☒	A2, A2.1 – A2.3: N/A. No POS devices in scope of this assessment.

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	*19 Sep 2021*	
Have compensating controls been used to meet any requirement in the ROC?	☒ Yes	☐ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements not tested?	☐ Yes	☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes	☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated *19 Sep 2021.*

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (***check one):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *SAP Ariba* has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provider Company 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.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.2.1*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Part 3a. Acknowledgement of Status (continued)	
☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *Tenable Network Security, Inc.*

Part 3b. Service Provider Attestation

DocuSigned by: John Wookey 2268F5FF7FB44C8...

DocuSigned by: Ermias Desta 5A5939BCD161443...

Signature of Service Provider Executive Officer ↑	*Date:* **19 Sep 2021**
Service Provider Executive Officer Name: **John Wookey / Ermias Desta**	*Title:* **President – Intelligent Spend and Business Network / Interim Business Information Security Officer**

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	The QSAs (Torsten Schlotmann / Jan Kemper) assessed all relevant PCI DSS requirements.

DocuSigned by: Torsten Schlotmann 9366AA034EE04CE...

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* **19 Sep 2021**
Duly Authorized Officer Name: **Torsten Schlotmann**	*QSA Company:* **usd AG**

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	-

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] 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 Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements *(Select One)*		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	☐	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☐	☐	
3	Protect stored cardholder data	☐	☐	
4	Encrypt transmission of cardholder data across open, public networks	☐	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☐	☐	
6	Develop and maintain secure systems and applications	☐	☐	
7	Restrict access to cardholder data by business need to know	☐	☐	
8	Identify and authenticate access to system components	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
10	Track and monitor all access to network resources and cardholder data	☐	☐	
11	Regularly test security systems and processes	☐	☐	
12	Maintain a policy that addresses information security for all personnel	☐	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☐	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐