



Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments - Service Providers

A QSA led assessment of compliance validation according to the Payment Card Industry Data Security Standards and Security Assessment Procedures version 3.2.1.

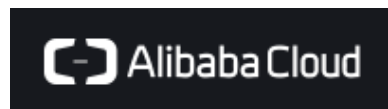
Level 1 Service Provider Validation: According to the service provider validation requirements defined by the payment brands (including VISA, MasterCard, JCB, American Express and Discover) in PCI industry, the annual onsite review by QSA for level 1 service provider could be compulsory.

Alibaba Cloud (Singapore) Private Limited

Report Date: August 17, 2022

Initial Compliance Date: October 25, 2017

Report Number: C131-87-2022-B



atsec (Beijing) Information Technology Co., Ltd
3/F, Block C, Bld.1, Boya C-Center, Life Science Park,
Changping District, Beijing, P.R. China, 102206
Tel: +86 10 53056679
Fax: +86 10 53056678
<https://www.atsec.com>

The attestation of compliance is based on the template (version 3.2.1, June 2018)
copyrighted by PCI Security Standards Council LLC



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: | Alibaba Cloud (Singapore) Private Limited (Branded as “Alibaba Cloud”) | | DBA (doing business as): | N/A | | |
| Contact Name: | Irene Wang | | Title: | Senior Security Compliance Manager | | |
| Telephone: | +65 87678528 | | E-mail: | irene.wang@alibaba-inc.com | | |
| Business Address: | 51 Bras Basah Road, #04-08 Lazada One, Singapore 189554 | | City: | - | | |
| State/Province: | - | Country: | Singapore | | Zip: | 189554 |
| URL: | https://www.alibabacloud.com | | | | | |

Part 1b. Qualified Security Assessor Company Information (if applicable)

| | | | | | |
|------------------------|--|----------|---------------------------|------|--------|
| Company Name: | atsec (Beijing) Information Technology Co., Ltd | | | | |
| Lead QSA Contact Name: | Jinyun Chen | Title: | QSA, Principal Consultant | | |
| Telephone: | +86 10 5305 6679 | E-mail: | jinyun@atsec.com | | |
| Business Address: | 3/F, Block C, Bld.1, Boya C-Center, Life Science Park, Changping District, Beijing, P.R. China, 102206 | City: | Beijing | | |
| State/Province: | - | Country: | P.R. China | Zip: | 102206 |
| URL: | https://www.atsec.com | | | | |

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:

Public Cloud International Services of Alibaba Cloud, including Alibaba Cloud DNS, AnalyticDB for MySQL, AnalyticDB for PostgreSQL, API Gateway, Application Configuration Management, Apsara File Storage NAS, ApsaraDB for MongoDB, ApsaraDB for PostgreSQL, ApsaraDB for Redis, ApsaraDB RDS for MySQL, ApsaraDB for POLARDB, ApsaraDB for SQL Server, Auto Scaling, Application Real-Time Monitoring Service (ARMS), Cloud Enterprise Network (CEN), Cloud Monitor, Cloud Storage Gateway, Container Registry, Container Service for Kubernetes, Data Management, Database Backup (DBS), DataV, DataWorks, Dedicated Host, ECS Bare Metal Instance, Elastic Compute Service (ECS), Elastic GPU Service, Elastic High Performance Computing (EHPC), Elastic IP Address, Elasticsearch, Enterprise Distributed Application Service (EDAS), Express Connect, Fraud Detection, Global Accelerator (GA), Cloud Governance Center, Hologres, Image Search, Intelligent Speech Interaction, Log Service (SLS), Machine Learning, MaxCompute, Message Queue (MQ), NAT Gateway, Object Storage Service (OSS), Operation Orchestration Service (OOS), PolarDB-X, Prometheus Service, Resource Management, Resource Orchestration Service (ROS), Server Load Balancer (SLB), Simple Application Server, Smart Access Gateway, Super Computing Cluster (SCC), Short message Service (dysms), Tablestore, Virtual Private Cloud (VPC), VPN Gateway, Alibaba Cloud Content Delivery Network (Alibaba Cloud CDN), Dynamic Content Delivery Network (DCDN), Secure Content Delivery Network (SCDN), ActionTrail, Anti-DDoS Basic, Anti-DDoS Premium, Bastionhost, Cloud Firewall, Cloud Config, Content Moderation, Data Encryption Service, IDaaS, Key Management Service (KMS), Resource Access Management (RAM), Security Center, Data Security Center, Web Application Firewall (WAF) service and Billing System.

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):

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 services provided by Alibaba Cloud in Public Cloud International Services environment are not included in the scope of PCI DSS assessment (except Alibaba Cloud DNS, AnalyticDB for MySQL, AnalyticDB for PostgreSQL, API Gateway, Application Configuration Management, Apsara File Storage NAS, ApsaraDB for MongoDB, ApsaraDB for PostgreSQL, ApsaraDB for Redis, ApsaraDB RDS for MySQL, ApsaraDB for POLARDB, ApsaraDB for SQL Server, Auto Scaling, ARMS, CEN, Cloud Monitor, Cloud Storage Gateway, Container Registry, Container Service for Kubernetes, Data Management, DBS, DataV, DataWorks, Dedicated Host, ECS Bare Metal Instance, ECS, Elastic GPU Service, EHPC, Elastic IP Address, Elasticsearch, EDAS, Express Connect, Fraud Detection, GA, Cloud Governance Center, Hologres, Image Search, Intelligent Speech Interaction, SLS, Machine Learning, MaxCompute, MQ, NAT Gateway, OSS, OOS, PolarDB-X, Prometheus Service, Resource Management, ROS, SLB, Simple Application Server, Smart Access Gateway, SCC, dysms, Tablestore, VPC, VPN Gateway, Alibaba Cloud CDN, DCDN, SCDN, ActionTrail, Anti-DDoS Basic, Anti-DDoS Premium, Bastionhost, Cloud Firewall, Cloud Config, Content Moderation, Data Encryption Service, IDaaS, KMS, RAM, Security Center, Data Security Center, WAF service and Billing System) |
|----------------------------------|--|

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):

Provide a brief explanation why any checked services were not included in the assessment:

Alibaba Cloud's Public Cloud International Services provides the capability for its clients utilizing Public Cloud International Services' process, storage, networks, and other fundamental computing resources, and the clients can deploy and run operating systems, applications and other software on the cloud infrastructure. Its Alibaba Cloud's business decisions to choose which services were included in the scope of this PCI DSS assessment.

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.

Public Cloud International Services offers computing resources for various clients (including merchants, payment service provider, payment processor, etc.). The security of cloud infrastructure and related administration security mechanisms are covered in this PCI DSS assessment. Based on business decision from Alibaba Cloud, other cloud environments (such as Public Cloud China Services, Fincloud, etc.) are not covered in this PCI DSS assessment.

Public Cloud International Services of Alibaba Cloud provides card-not-present payment method for its clients to purchase service on Alibaba Cloud webpage. Once the purchasing order has been created, the cardholder data (PAN, Cardholder Name and Expiration date) and sensitive authentication data (CAV2/CVV2/CVC2/CID) are input via the web page of Alibaba Cloud Billing System, then these information are transmitted to Alibaba Cloud Billing System by using strong cryptography over Internet. Once Alibaba Cloud Billing System complete internal processing, the cardholder data and sensitive authentication data are then forwarded to payment processor (Alipay Labs (Singapore) Pte. Ltd.) over Internet with strong cryptography. Cardholder data (PAN, Cardholder Name and Expiration date) and sensitive authentication data (CAV2/CVV2/CVC2/CID) are held in the VRAM (Volatile Random Access Memory) and purged immediately after authorization. No cardholder data and sensitive authentication data are stored in the Alibaba Cloud environment.

Alibaba Cloud IaaS, PaaS and SaaS Service (including Alibaba Cloud DNS, AnalyticDB for MySQL, AnalyticDB for PostgreSQL, API Gateway, Application Configuration Management, Apsara File Storage NAS, ApsaraDB for MongoDB, ApsaraDB for PostgreSQL, ApsaraDB for Redis, ApsaraDB RDS for MySQL, ApsaraDB for POLARDB, ApsaraDB for SQL Server, Auto Scaling, ARMS, CEN, Cloud Monitor, Cloud Storage Gateway, Container Registry, Container Service for Kubernetes, Data Management, DBS, DataV, DataWorks, Dedicated Host, ECS Bare Metal Instance, ECS, Elastic GPU Service, EHPC, Elastic IP Address, Elasticsearch, EDAS, Express Connect, Fraud Detection, GA, Cloud Governance

| | |
|--|---|
| | <p>Center, Hologres, Image Search, Intelligent Speech Interaction, SLS, Machine Learning, MaxCompute, MQ, NAT Gateway, OSS, OOS, PolarDB-X, Prometheus Service, Resource Management, ROS, SLB, Simple Application Server, Smart Access Gateway, SCC, dysms, Tablestore, VPC, VPN Gateway, Alibaba Cloud CDN, DCDN, SCDN, ActionTrail, Anti-DDoS Basic, Anti-DDoS Premium, Bastionhost, Cloud Firewall, Cloud Config, Content Moderation, Data Encryption Service, IDaaS, KMS, RAM, Security Center, Data Security Center, WAF service) do not directly transmit, process, or store cardholder data, and the PCI compliant environment facilitates its clients' PCI DSS compliance (i.e. that the products or systems do not enforce implementation or configuration settings that violates a PCI DSS requirement). Please note that the cardholder data environments of Alibaba Cloud's clients and their system components are not covered in this PCI DSS assessment.</p> <p>Here are some services provided by Public Cloud International Services and clients may implement these security services for their PCI DSS compliance. These are:</p> <ul style="list-style-type: none"> ■ HTTPS application program interface with strong cryptography provide by Server Load Balancer service is available for clients to transfer cardholder data between Merchant/cardholder and the application implemented on Public Cloud International Services or service provided by Public Cloud International Services. ■ KMS provided encryption mechanism for clients' cardholder data protection. ■ SLS provides centralized log management service for clients to meet PCI DSS 10.7 requirement. ■ RAM provides centralized identity and access control service as well as password policy for clients to manage Alibaba Cloud User Console and resource. ■ Public Cloud International Services securely disposes the metadata (including cardholder data, etc) according to the clients' deletion request or service expiration period. However, it is client's responsibility to define |
|--|---|

| | |
|--|--|
| | their own data retention period in Public Cloud International Services virtual network segmentation. |
| Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data. | All Public Cloud International Services system components are hardened according to the same security baseline and managed by the same vulnerability and patch management policies. The cloud services which are not included in the scope of this QSA assessment are put in different zone of the clusters and separated via strict access controls. The access controls are enforced by the core switch within Public Cloud International Services production environment. |

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): |
|--------------------------------|-----------------------------------|--|
| <i>Example: Retail Outlets</i> | 3 | <i>Boston, MA, USA</i> |
| Office Network | 2 | <ul style="list-style-type: none"> ■ Hangzhou Office is located in Apsara Park, Shilongshan Road, Xihu District, Hangzhou City, Zhejiang Province, P.R.China, 310024 ■ Singapore Office is located in 51 Bras Basah Road, #04-08 Lazada One, Singapore 189554 |
| Datacenter | 132 | Cloud DataCenters of Public Cloud International Services: <ul style="list-style-type: none"> ■ Hong Kong Zone B ■ Hong Kong Zone C ■ Asia Pacific SE 1 (Singapore) Zone A ■ Asia Pacific SE 1 (Singapore) Zone B ■ Asia Pacific SE 1 (Singapore) Zone C ■ Asia Pacific SE 2 (Sydney) Zone A ■ Asia Pacific SE 2 (Sydney) Zone B ■ Asia Pacific SE 3 (Kuala Lumpur) Zone A ■ Asia Pacific SE 3 (Kuala Lumpur) Zone B ■ Asia Pacific SE 5 (Jakarta) Zone A ■ Asia Pacific SE5 (Jakarta) Zone B ■ Asia Pacific SE5 (Jakarta) Zone C ■ Asia Pacific SE 6 (Manila) Zone A ■ Asia Pacific SE 7 (Bangkok) Zone A ■ Asia Pacific SOU 1 (Mumbai) Zone A ■ Asia Pacific SOU1 (Mumbai) Zone B ■ Asia Pacific NE1 (Tokyo) Zone A ■ Asia Pacific NE1 (Tokyo) Zone B ■ Asia Pacific NE 2 (Seoul) Zone A ■ EU Central 1 (Frankfurt) Zone A |

| | | |
|--|--|--|
| | | <ul style="list-style-type: none"> ■ EU Central 1 (Frankfurt) Zone B ■ EU Central 1 (Frankfurt) Zone C ■ UK London Zone A ■ UK London Zone B ■ US West 1 (Silicon Valley) Zone A ■ US West 1 (Silicon Valley) Zone B ■ US East 1 (Virginia) Zone A ■ US East 1 (Virginia) Zone B ■ Middle East 1 (Dubai) Zone A <p>Datacenters related to Alibaba Cloud CDN, SCDN and DCDN Services:</p> <ul style="list-style-type: none"> ■ CDN data centers in following P.R. China regions <ul style="list-style-type: none"> ■ 7 CDN data centers in Hong Kong Special Administrative Region ■ 2 CDN data centers in Macau Special Administrative Region ■ 4 CDN data centers in Taiwan Province of China ■ 2 CDN data centers in Australia region ■ 2 CDN data centers in Germany region ■ 5 CDN data centers in Malaysia region ■ 9 CDN data centers in Indonesia region ■ 9 CDN data centers in India region ■ 1 CDN data center in United Kingdom region ■ 3 CDN data centers in Japan region ■ 3 CDN data centers in Republic of Korea region ■ 6 CDN data centers in Thailand region ■ 3 CDN data centers in Philippines region ■ 4 CDN data centers in Vietnam region ■ 1 CDN data center in Kuwait region ■ 1 CDN data center in State of Qatar region ■ 1 CDN data center in Sultanate of Oman region ■ 4 CDN data centers in Russian Federation region ■ 1 CDN data center in Ukraine region ■ 1 CDN data center in France region ■ 1 CDN data center in Netherlands region ■ 2 CDN data centers in Spain region ■ 1 CDN data center in Italy region ■ 1 CDN data center in Sweden region ■ 1 CDN data center in South Africa region ■ 1 CDN data center in Brazil region ■ 6 CDN data centers in Singapore region ■ 11 CDN data centers in USA region <p>WAF Datacenters:</p> <ul style="list-style-type: none"> ■ Asia Pacific SE 1 (Singapore) Zone A ■ Asia Pacific SE 1 (Singapore) Zone B ■ Asia Pacific SE 2 (Sydney) Zone A |
|--|--|--|

| | | |
|--|--|--|
| | | <ul style="list-style-type: none"> ■ Asia Pacific SE 3 (Kuala Lumpur) Zone A ■ Asia Pacific SE5 (Jakarta) Zone A ■ Asia Pacific SOU1 (Mumbai) Zone A ■ China East 2 Zone A ■ China East 2 Zone B ■ EU Central 1 (Frankfurt) Zone A ■ EU Central 1 (Frankfurt) Zone B ■ Hong Kong Zone B ■ Hong Kong Zone C ■ UK London Zone A ■ US East 1 (Virginia) Zone A ■ US West 1 (Silicon Valley) Zone A ■ US West 1 (Silicon Valley) Zone B <p>Anti-DDoS Datacenters:</p> <ul style="list-style-type: none"> ■ JP141 Site-Data Processing Zone ■ MY86 Site-Data Processing Zone ■ OE24 Site-Data Processing Zone ■ OE26 Site-Data Processing Zone ■ OE28 Site-Data Processing Zone ■ OI39 Site-Data Processing Zone ■ US50 Site-Data Processing Zone ■ GB145 Site-Data Processing Zone ■ ID165 Site-Data Processing Zone <p><i>Note: The detail location of above datacentres is removed based on Alibaba Cloud's confidential requirement. The detail addresses of those datacentres are recorded in the ROC which release by atsec (Beijing) information Technology Co., Ltd at August 17, 2022</i></p> |
| | | |

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) |
|--------------------------|----------------|--------------------|---|--|
| Billing System | 20210521 | Alibaba Cloud | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No | Not applicable |

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.*

All system components of this PCI DSS QSA assessment are located in above DataCenters. Alibaba Cloud provides the capability for clients utilizing Public Cloud International Services' processing, storage, networks, and other fundamental computing resources, and the clients can deploy and run operating systems, applications and other software on its cloud infrastructure. Public Cloud

International Services provides secure application program interface (API) for the client to transfer cardholder data information between the clients and the application implemented on Public Cloud International Services or service provided by Public Cloud International Services. Public Cloud International Services also provides Security Service (ActionTrail, Anti-DDoS Basic, Anti-DDoS Premium, Bastionhost, Cloud Firewall, Cloud Config, Content Moderation, Data Encryption Service, IDaaS, KMS, RAM, Security Center, Data Security Center and WAF service) for the clients to protect their virtual environment.

The critical system components involved in this QSA scope include Alibaba Cloud DNS, AnalyticDB for MySQL, AnalyticDB for PostgreSQL, API Gateway, Application Configuration Management, Apsara File Storage NAS, ApsaraDB for MongoDB, ApsaraDB for PostgreSQL, ApsaraDB for Redis, ApsaraDB RDS for MySQL, ApsaraDB for POLARDB, ApsaraDB for SQL Server, Auto Scaling, ARMS, CEN, Cloud Monitor, Cloud Storage Gateway, Container Registry, Container Service for Kubernetes, Data Management, DBS, DataV, DataWorks, Dedicated Host, ECS Bare Metal Instance, ECS, Elastic GPU Service, EHPC, Elastic IP Address, Elasticsearch, EDAS, Express Connect, Fraud Detection, GA, Cloud Governance Center, Hologres, Image Search, Intelligent Speech Interaction, SLS, Machine Learning, MaxCompute, MQ, NAT Gateway, OSS, OOS, PolarDB-X, Prometheus Service, Resource Management, ROS, SLB, Simple Application Server, Smart Access Gateway, SCC, dysms, Tablestore, VPC, VPN Gateway, Alibaba Cloud CDN, DCDN, SCDN, ActionTrail, Anti-DDoS Basic, Anti-DDoS Premium, Bastionhost, Cloud Firewall, Cloud Config, Content Moderation, Data Encryption Service, IDaaS, KMS, RAM, Security Center, Data Security Center, WAF, bastion machine, and NTP server. Only the security of cloud infrastructure and related administration security mechanisms are covered in this PCI DSS assessment. Please note that clients' cardholder data flow and the compliance of their own cloud components are not covered in this PCI DSS assessment, and it is the responsibility of

| | | |
|--|---|---|
| | Alibaba Cloud's clients to have their own cardholder data environment fully compliant with PCI DSS based on the services provided by Public Cloud International Services. | |
| Does your business use network segmentation to affect the scope of your PCI DSS environment? <i>(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)</i> | | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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: Not applicable.

QIR Individual Name: Not applicable.

Description of services provided by QIR: Not applicable.

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: |
|---------------------------|-----------------------------------|
|---------------------------|-----------------------------------|

| | |
|-----------------------------------|--------------------------------|
| Alipay Labs (Singapore) Pte. Ltd. | Payment authorization 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: | Public Cloud International Services of Alibaba Cloud, including Alibaba Cloud DNS, AnalyticDB for MySQL, AnalyticDB for PostgreSQL, API Gateway, Application Configuration Management, Apsara File Storage NAS, ApsaraDB for MongoDB, ApsaraDB for PostgreSQL, ApsaraDB for Redis, ApsaraDB RDS for MySQL, ApsaraDB for POLARDB, ApsaraDB for SQL Server, Auto Scaling, ARMS, CEN, Cloud Monitor, Cloud Storage Gateway, Container Registry, Container Service for Kubernetes, Data Management, DBS, DataV, DataWorks, Dedicated Host, ECS Bare Metal Instance, ECS, Elastic GPU Service, EHPC, Elastic IP Address, Elasticsearch, EDAS, Express Connect, Fraud Detection, GA, Cloud Governance Center, Hologres, Image Search, Intelligent Speech Interaction, SLS, Machine Learning, MaxCompute, MQ, NAT Gateway, OSS, OOS, PolarDB-X, Prometheus Service, Resource Management, ROS, SLB, Simple Application Server, Smart Access Gateway, SCC, dysms, Tablestore, VPC, VPN Gateway, Alibaba Cloud CDN, DCDN, SCDN, ActionTrail, Anti-DDoS Basic, Anti-DDoS Premium, Bastionhost, Cloud Firewall, Cloud Config, Content Moderation, Data Encryption Service, IDaaS, KMS, RAM, Security Center, Data Security Center, WAF service and Billing System. | | | |
|----------------------------------|--|-------------------------------------|--------------------------|--|
| 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: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Requirement 1.2.3 was marked as not applicable. Because wireless networks are not enabled in the scope of this PCI DSS assessment. Requirement 1.3.6 was marked as not applicable. Because cardholder data are not stored in cardholder data environment. |
| Requirement 2: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Requirement 2.1.1 was marked as not applicable. Because wireless networks are not enabled in the scope of this PCI DSS assessment. Requirement 2.6 was marked as not applicable. Because the in-scope Alibaba Cloud services are not shared hosting service and no shared hosting service are involved in this PCI DSS assessment |
| Requirement 3: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Requirements 3.1 and 3.4 were marked as not |

| | | | | |
|-----------------|-------------------------------------|-------------------------------------|--------------------------|---|
| | | | | <p>applicable. Because cardholder data are not stored in the cardholder data environment.</p> <p>Requirement 3.3 was marked as not applicable. Because full PANs or mask PANs are not visible to internal personnel.</p> <p>Requirement 3.4.1 was marked as not applicable. Because disk level encryption mechanisms are not engaged for the cardholder data protection.</p> <p>Requirements 3.5, 3.5.1, 3.5.2, 3.5.3, 3.5.4, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7 and 3.6.8 were marked as not applicable. Because cardholder data are not stored in the cardholder data environment and thus encryption keys are not used to protect cardholder data.</p> |
| Requirement 4: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <p>Requirement 4.1.1 was marked as not applicable. Because wireless networks are not enabled in the scope of this PCI DSS assessment.</p> <p>Requirement 4.2 was marked as not applicable. Because PANs are not transmitted via end-user messaging technologies.</p> |
| Requirement 5: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | All requirements in this section were marked as applicable. |
| Requirement 6: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | All requirements in this section were marked as applicable. |
| Requirement 7: | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | All requirements in this section were marked as applicable. |
| Requirement 8: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <p>Requirement 8.1.5 was marked as not applicable. Because vendor accounts are not enabled in the cardholder data environment.</p> <p>Requirement 8.7 was marked as not applicable. Because cardholder data are not stored in database servers of Billing System.</p> |
| Requirement 9: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <p>Requirements 9.5, 9.5.1, 9.6, 9.6.1, 9.6.2, 9.6.3, 9.7, 9.7.1, 9.8, 9.8.1 and 9.8.2 were marked as not applicable. Because media is not engaged in the storage of cardholder data.</p> <p>Requirements 9.9, 9.9.1, 9.9.2 and 9.9.3 were marked as not applicable. Because card-present services are not supported in the cardholder data environment.</p> |
| Requirement 10: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Requirement 10.2.1 was marked as not applicable. Because cardholder data are not accessible in the cardholder data environment. |
| Requirement 11: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Requirement 11.1.1 was marked as not applicable. Because wireless access points are not enabled in the cardholder data environment. |
| Requirement 12: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Requirement 12.8.5 was marked as not applicable. Because PCI DSS requirements are not managed by external entities. |

| | | | | |
|--------------|--------------------------|-------------------------------------|-------------------------------------|---|
| Appendix A1: | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | All requirements were marked as not applicable. Because the in-scope Alibaba Cloud services are not shared hosting service and no shared hosting service are involved in this PCI DSS assessment. |
| Appendix A2: | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Requirement A2.1 was marked as not applicable. Because POS POI terminals are not supported in the scope of this PCI DSS 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: | August 17, 2022 |
| Have compensating controls been used to meet any requirement in the ROC? | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| Were any requirements in the ROC identified as being not applicable (N/A)? | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| Were any requirements not tested? | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No |
| Were any requirements in the ROC unable to be met due to a legal constraint? | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No |

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated *August 17, 2022*

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**):

| <input checked="" type="checkbox"/> | <p>Compliant: All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>Alibaba Cloud (Singapore) Private Limited</i> has demonstrated full compliance with the PCI DSS.</p> | | | | | | |
|-------------------------------------|--|----------------------|--|--|--|--|--|
| <input type="checkbox"/> | <p>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 <i>Alibaba Cloud (Singapore) Private Limited</i> has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date for Compliance:</p> <p>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. <i>Check with the payment brand(s) before completing Part 4.</i></p> | | | | | | |
| <input type="checkbox"/> | <p>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.</p> <p><i>If checked, complete the following:</i></p> <table border="1"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table> | Affected Requirement | Details of how legal constraint prevents requirement being met | | | | |
| Affected Requirement | Details of how legal constraint prevents requirement being met | | | | | | |
| | | | | | | | |
| | | | | | | | |

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

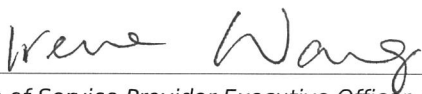
(Check all that apply)

| | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2.1, and was completed according to the instructions therein. |
| <input checked="" type="checkbox"/> | All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects. |
| <input checked="" type="checkbox"/> | I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization. |
| <input checked="" type="checkbox"/> | I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times. |
| <input checked="" type="checkbox"/> | 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)

| | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | 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. |
| <input checked="" type="checkbox"/> | ASV scans are being completed by the PCI SSC Approved Scanning Vendor <i>atsec (Beijing) Information Technology Co., Ltd</i> |

Part 3b. Service Provider Attestation

| | |
|---|---|
|  | |
| Signature of Service Provider Executive Officer ↑ | Date: August 17, 2022 |
| Service Provider Executive Officer Name: Irene Wang | Title: Senior Security Compliance Manager |

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

| | |
|--|---|
| If a QSA was involved or assisted with this assessment, describe the role performed: | QSA assessment and evidence validation. |
|--|---|

| | |
|---|---|
|  | |
| Signature of Duly Authorized Officer of QSA Company ↑ | Date: August 17, 2022 |
| Duly Authorized Officer Name: Jinyun Chen (陈谨运) | QSA Company: <i>atsec (Beijing) Information Technology Co., Ltd</i> |

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: | Not applicable. Because ISA is not involved in this PCI DSS assessment. |
|---|---|

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 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 2 | Do not use vendor-supplied defaults for system passwords and other security parameters | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 3 | Protect stored cardholder data | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 4 | Encrypt transmission of cardholder data across open, public networks | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 5 | Protect all systems against malware and regularly update anti-virus software or programs | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 6 | Develop and maintain secure systems and applications | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 7 | Restrict access to cardholder data by business need to know | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 8 | Identify and authenticate access to system components | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 9 | Restrict physical access to cardholder data | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 10 | Track and monitor all access to network resources and cardholder data | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 11 | Regularly test security systems and processes | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 12 | Maintain a policy that addresses information security for all personnel | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| Appendix A1 | Additional PCI DSS Requirements for Shared Hosting Providers | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| Appendix A2 | Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |

