



Payment Card Industry Data Security Standard

Attestation of Compliance for Self-Assessment Questionnaire D for Service Providers

For use with PCI DSS Version 4.0.1

Revision 1

Publication Date: December 2024

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the entity's self-assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures*. Complete all sections: The entity is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which the Attestation of Compliance (AOC) will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Self-Assessment Questionnaire (SAQ).

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Self-Assessment Questionnaire.

Part 1. Contact Information

Part 1a. Assessed Entity

Company name:	Amoga Software Private Limited
DBA (doing business as):	Amoga
Company mailing address:	4th Floor, Krishna Tech Park, Kaverappa Layout, Kadubeesanahalli, Bengaluru, Karnataka 560103
Company main website:	amoga.io
Company contact name:	Mr. Bishal Lachhiramka
Company contact title:	CEO
Contact phone number:	
Contact e-mail address:	bishal@amoga.io

Part 1b. Assessor

Provide the following information for all assessors involved in the assessment. If there was no assessor for a given assessor type, enter Not Applicable.

PCI SSC Internal Security Assessor(s)

ISA name(s):	N/A
--------------	-----

Qualified Security Assessor

Company name:	Aegisra Assurance LLP
Company mailing address:	Office 125 Dwarka Sector 10 India
Company website:	www.aegisraassurance.com
Lead Assessor Name:	Arjun Walia
Assessor phone number:	+91 7838568637
Assessor e-mail address:	arjun@aegisraassurance.com
Assessor certificate number:	206-763

Part 2. Executive Summary

Part 2a. Scope Verification

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

Name of service(s) assessed: Amoga Application

Type of service(s) assessed:

Hosting Provider:

- ☒ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web-hosting services
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Multi-Tenant Service Provider
- ☐ Other Hosting (specify):

Managed Services:

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

Payment Processing:

- ☐ POI / 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 these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.

Part 2. Executive Summary *(continued)*

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 (select all that apply):

Name of service(s) not assessed: All the other services except mentioned above

Type of service(s) not assessed:

Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web-hosting services ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Multi-Tenant Service Provider ☐ Other Hosting (specify):	Managed Services: ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	Payment Processing: ☐ POI / 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:		Not Applicable

Part 2b. Description of Role with Payment Cards

Describe how the business stores, processes, and/or transmits account data.

Amoga Software Private Limited (hereafter referred to as "Amoga") is a B2B SaaS technology company providing enterprise-grade Low-Code/No-Code CRM and workflow automation solutions to businesses across multiple industries. Amoga's platform is hosted on Microsoft Azure cloud infrastructure and leverages modern web technologies, APIs, and microservice-based architecture for scalable enterprise deployments. The assessment covers Amoga's cloud-hosted SaaS platform and all supporting Azure infrastructure components required for its operation and client service delivery. Amoga does not store, process, or transmit cardholder data (CHD) in any form. Amoga's role is limited to providing the application platform and workflow

	automation capabilities through which its enterprise clients manage their business operations.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Although Amoga does not directly store, process, or transmit cardholder data, it has the ability to impact the security of its customers' account data in the following ways: • Application Platform Control: Amoga develops, manages, and supports the Low-Code/No-Code CRM and workflow automation platform used by enterprise clients who may process payment-related data within their own workflows. Any vulnerability or misconfiguration in Amoga's application layer could expose client data to unauthorized access or manipulation. • API and Integration Layer: Amoga's platform exposes APIs and integration endpoints used by client organizations for business operations. The security of these APIs — including authentication, authorization, and data handling — is under Amoga's management and could impact the integrity of client data flows. • Access Management: Amoga administers identity and access management through Keycloak IAM and Amoga RBAC access controls. Weaknesses in access controls could allow unauthorized parties to interact with client data within the platform. • Infrastructure Management: Amoga manages its Microsoft Azure cloud environment including application servers, PostgreSQL Flexible Server databases, and supporting services. Misconfigurations or vulnerabilities in the infrastructure layer could impact the availability and security of the hosted SaaS platform. • Data Protection: Amoga manages encrypted storage, retention, and disposal of client-submitted sensitive data. Any failure in encryption or data lifecycle controls could impact the confidentiality of client data stored within the platform. • Network Security: Amoga manages Cloudflare WAF and network security controls governing all inbound and outbound traffic flows. Any gaps in these controls could expose the platform and client data to unauthorized access.
Describe system components that could impact the security of account data.	1. Component Description Amoga SaaS Platform Low-code/no-code CRM and workflow automation platform. This is the core application through which enterprise clients manage business operations and data. 2. Microsoft Azure Cloud Infrastructure

	Underlying IaaS/PaaS platform hosting all in-scope application components, databases, and supporting services. 3. Azure Application Servers Compute instances hosting the Amoga SaaS platform and microservice-based application components. PostgreSQL Flexible Server (v17.9) Managed database service on Azure storing application and client-submitted data. 4. Keycloak IAM Identity and access management platform governing authentication and authorization across the Amoga environment. 5. Amoga RBAC Role-Based Access Control (RBAC) framework enforcing least-privilege access to application and data components. 6. ELK Stack (Elasticsearch, Logstash, Kibana) Centralized log aggregation, monitoring, audit trail analysis, and security event visibility platform deployed on Azure. 7. Cloudflare & WAF Network security, DDoS protection, and web application firewall controlling all inbound traffic to the platform. Encrypted Storage 8. Azure-managed encrypted storage for client-submitted sensitive data with defined retention and disposal controls. 9. Microsoft Defender Endpoint Protection Antivirus and endpoint security solution protecting in-scope infrastructure components. 10. Microsoft Intune Device management platform governing endpoint compliance and security policy enforcement. 11. Cloudflare WARP Secure network access solution protecting connectivity between authorized personnel and the Amoga environment.
--	---

Part 2. Executive Summary *(continued)*

Part 2c. Description of Payment Card 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 POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.*
- *System components that could impact the security of account data.*

Amoga Software Private Limited operates a fully cloud-based environment hosted on Microsoft Azure. The assessed environment encompasses Amoga's B2B SaaS Low-Code/No-Code CRM and workflow automation platform and all supporting Azure-hosted components. Amoga does not store, process, or transmit cardholder data directly.

Connections into and out of the environment:

- Enterprise client users connect inbound to the Amoga SaaS platform via HTTPS (TLS encrypted) over the public internet, protected by Cloudflare WAF and DDoS mitigation before reaching the application layer.
- API connections are made between the Amoga platform and client systems via secured, authenticated API endpoints.
- Administrative access to the Azure infrastructure and application components is restricted to authorized Amoga personnel, enforced through Keycloak IAM, MFA, and RBAC controls.
- Outbound connectivity is provided through Cloudflare WARP for secure access by authorized personnel.

Critical system components within the environment:

- Amoga SaaS Platform — core Low-Code/No-Code CRM and workflow automation application.
- Azure Application Servers — microservice-based compute layer hosting the platform.
- PostgreSQL Flexible Server (v17.9) — managed database storing application and client data.
- Keycloak IAM and Amoga RBAC — identity, authentication, and access control layer.
- ELK Stack — centralized security monitoring and audit logging.

System components that could impact the security of account data:

- Microsoft Azure Cloud Infrastructure — underlying platform hosting all in-scope components.
- Cloudflare and WAF — perimeter security for all inbound traffic flows.

Indicate whether the environment includes segmentation to reduce the scope of the assessment.

(Refer to "Segmentation" section of PCI DSS for guidance on segmentation.)

☐ Yes ☒ No

Part 2d. In-Scope Locations/Facilities

List all types of physical locations/facilities—for example, corporate offices, data centers, call centers, and mail rooms—in scope for the PCI DSS assessment.

Facility Type	Total number of locations (How many locations of this type are in scope)	Location(s) of facility (city, country)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>
Corporate Office	1	Bengaluru, Karnataka, India
Cloud Infrastructure	1	Azure Cloud Infra: Pune; DR: Hyderabad

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions*?

☐ Yes ☒ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions.

Name of PCI SSC validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which product or solution was validated	PCI SSC listing reference number	Expiry date of listing (YYYY-MM-DD)

-
- * For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website (www.pcisecuritystandards.org)—for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions, and Mobile Payments on COTS (MPoC) products.

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers

For the services being validated, does the entity have relationships with one or more third-party service providers that:

Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs), and off-site storage)	☐ Yes ☒ No
Manage system components included in the scope of the entity's PCI DSS assessment—for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, and IaaS, PaaS, SaaS, and FaaS cloud providers.	☒ Yes ☐ No
Could impact the security of the entity's CDE—for example, vendors providing support via remote access, and/or bespoke software developers.	☒ Yes ☐ No

If Yes:

Name of service provider:	Description of service(s) provided:
Microsoft Azure	IaaS/PaaS cloud infrastructure provider hosting all in-scope application components, databases, networking, and security services.
Cloudflare	CDN, WAF, and DDoS protection for all inbound traffic; also provides Cloudflare WARP for secure administrative access..
Microsoft Defender / Intune	Endpoint security and device management services protecting in-scope infrastructure and personnel endpoints.
KeyCloak	Centralized Identity & Access Management Platform (Keycloak)
GitHub	Source Code Repository & Version Control Platform (GitHub)
ELK	Centralized Log Management Platform (ELK Stack)

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

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment

(SAQ Section 2 and related appendices)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either “Not Applicable” or “Not Tested,” complete the “Justification for Approach” table below.

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: Amoga Application

PCI DSS Requirement	Requirement Responses				
	<i>More than one response may be selected for a given requirement. Indicate all responses that apply.</i>				
	In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
Requirement 1:	☒	☐	☒	☐	☐
Requirement 2:	☒	☐	☒	☐	☐
Requirement 3:	☐	☐	☒	☐	☐
Requirement 4:	☐	☐	☒	☐	☐
Requirement 5:	☒	☐	☒	☐	☐
Requirement 6:	☒	☐	☒	☐	☐
Requirement 7:	☒	☐	☐	☐	☐
Requirement 8:	☒	☐	☒	☐	☐
Requirement 9:	☐	☐	☒	☐	☐
Requirement 10:	☒	☐	☒	☐	☐
Requirement 11:	☒	☐	☒	☐	☐
Requirement 12:	☒	☐	☒	☐	☐
Appendix A1:	☐	☐	☒	☐	☐
Appendix A2:	☐	☐	☒	☐	☐

Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.

Requirement 1:

- 1.2.6 – Not Applicable as Amoga Software Private Limited does not utilize any insecure services, protocols, or ports within the scoped environment.
- 1.3.3 – Not Applicable as no wireless networks are present or in use within Amoga's scoped environment.

Requirement 2:

- 2.2.5 – Not Applicable as Amoga Software Private Limited does not utilize any insecure services across the scoped environment.
- 2.3.1 & 2.3.2 – Not Applicable as no wireless networks are present or in use within Amoga's scoped environment.

Requirement 3:

- Requirement 3 in its entirety – Not Applicable. Amoga Software Private Limited does not store cardholder data (CHD) in any form. Amoga's platform is a B2B SaaS CRM and workflow automation solution; it does not handle payment card data at any stage. As no CHD is stored in any form, all sub-requirements under Requirement 3 are not applicable to Amoga's environment.

Requirement 4:

- Requirement 4 in its entirety – Not Applicable. Amoga Software Private Limited does not transmit cardholder data (CHD) in any form. The platform does not handle, route, or transmit payment card data at any point in its operations. As no CHD is transmitted, all sub-requirements under Requirement 4 are not applicable to Amoga's environment.

Requirement 5:

- 5.2.3 – Not Applicable as there are no system components within Amoga's scoped environment that are considered to be not commonly affected by malicious software.
 - 5.2.3.1 – Not Applicable as there are no system components within Amoga's scoped environment that are considered to be not commonly affected by malicious software.
 - 5.3.2.1 – Not Applicable as there are no system components within Amoga's scoped environment that require periodic evaluations for malicious software risk.
- 5.3.3 – Not Applicable as removable electronic media is not permitted or present within Amoga's cloud-based Azure environment.

Requirement 6:

- 6.4.3 – Not Applicable as Amoga Software Private Limited does not operate a customer-facing payment page. The platform is a CRM and workflow automation solution with no browser-based payment page in scope.
- 6.5.2 – Not Applicable as no significant changes have occurred within the scoped environment during the assessment period.

Requirement 8:

- 8.2.3 – Not Applicable as Amoga Software Private Limited does not have access to any customer environment; all interactions are conducted via secured API integrations only.
 - 8.2.7 – Not Applicable as no third parties have direct privileged access to Amoga's scoped cardholder data environment.
 - 8.4.3 – Not Applicable as there are no non-employee users accessing Amoga's environment from outside the entity's network boundary.
 - 8.6.1 & 8.6.2 – Not Applicable as interactive logins to system accounts are not in scope within Amoga's environment; all system access is governed through Keycloak IAM, Amoga RBAC, and MFA mechanisms.
- Requirement 9:
- Requirement 9 in its entirety – Not Applicable. Amoga Software Private Limited operates a fully cloud-based environment hosted on Microsoft Azure with no physical data centers, no on-premises infrastructure, no point-of-interaction (POI) devices, no physical media, and no wireless networks within the scoped environment. Physical security of the underlying data center infrastructure is the responsibility of Microsoft Azure under the shared responsibility model. As such, all sub-requirements under Requirement 9 are not applicable to Amoga's environment.
- Requirement 11:
- 11.2.2 – Not Applicable as no wireless networks are present within Amoga's scoped environment.
 - 11.3.1.3 – Not Applicable as no significant changes have occurred within the scoped environment during the assessment period.
 - 11.3.2.1 – Not Applicable as no significant changes have occurred within the scoped environment during the assessment period.
 - 11.4.7 – Not Applicable as Amoga Software Private Limited is not a multi-tenant service provider.
 - 11.6.1 – Not Applicable as Amoga Software Private Limited does not operate a browser-based payment page within the scoped environment.
- Requirement 12:
- 12.3.2 – Not Applicable as Amoga Software Private Limited has not utilized the customized approach for any PCI DSS requirements within this assessment.
- Appendix A1:
- Not Applicable as Amoga Software Private Limited is not a multi-tenant service provider and does not offer shared hosting services to other entities.
- Appendix A2:
- Not Applicable as Amoga Software Private Limited does not use SSL or early TLS anywhere within the scoped environment. All communications are protected using TLS 1.2 or higher across the Microsoft Azure hosted environment.

For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable

Section 2: Self-Assessment Questionnaire D for Service Providers

Self-assessment completion date:	2026-06-18
Were any requirements in the SAQ 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 SAQ D (Section 2), dated (Self-assessment completion date 2026-06-18).

Indicate below whether a full or partial PCI DSS assessment was completed:

- ☒ **Full** – All requirements have been assessed therefore no requirements were marked as Not Tested in the SAQ.
- ☐ **Partial** – One or more requirements have not been assessed and were therefore marked as Not Tested in the SAQ. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the SAQ D noted above, each signatory identified in any of Parts 3b–3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document.

Select one:

☒	Compliant: All sections of the PCI DSS SAQ are complete, and all assessed requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall COMPLIANT rating; thereby <i>Amoga Software Private Limited</i> has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above.								
☐	Non-Compliant: Not all sections of the PCI DSS SAQ are complete, or one or more requirements are marked as Not in Place, resulting in an overall NON-COMPLIANT rating, thereby (<i>Service Provider Company Name</i>) has not demonstrated compliance with the PCI DSS requirements included in this SAQ. Target Date for Compliance: YYYY-MM-DD An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted <i>before completing Part 4</i>.								
☐	Compliant but with Legal exception: One or more assessed requirements in the PCI DSS SAQ are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall COMPLIANT BUT WITH LEGAL EXCEPTION rating; thereby (<i>Service Provider Company Name</i>) has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above or as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. <i>If selected, complete the following:</i> <table border="1"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met						
Affected Requirement	Details of how legal constraint prevents requirement from being met								

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

☒	PCI DSS Self-Assessment Questionnaire D, Version 4.0.1, was completed according to the instructions therein.
☒	All information within the above-referenced SAQ and in this attestation fairly represents the results of the entity's assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	Date: 2026-06-18
Service Provider Executive Officer Name: Bishal Lachhiramka	Title: CEO

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this assessment, indicate the role performed:	☒ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:

Arjun Walia

Signature of Lead QSA ↑	Date: 2026-06-18
Lead QSA Name: Arjun Walia	

Arjun Walia

Signature of Duly Authorized Officer of QSA Company ↑	Date: 2026-06-18
Duly Authorized Officer Name: Arjun Walia	QSA Company: Aegisra Assurance LLP

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has a Non-Compliant status noted in Section 3.

If asked to complete this section, select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement below. For any “No” responses, include the date the entity expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

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 network security controls	☒	☐	
2	Apply secure configurations to all system components	☒	☐	
3	Protect stored account data	☒	☐	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☒	☐	
5	Protect all systems and networks from malicious software	☒	☐	
6	Develop and maintain secure systems and software	☒	☐	
7	Restrict access to system components and cardholder data by business need to know	☒	☐	
8	Identify users and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Log and monitor all access to system components and cardholder data	☒	☐	
11	Test security systems and networks regularly	☒	☐	
12	Support information security with organizational policies and programs	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections	☒	☐	

Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance-accepting organization to ensure that this form is acceptable in its program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/.