Payment Card Industry
3-D Secure (PCI 3DS)

Attestation of Compliance

For use with PCI 3DS Core Security Standard v1.0

Revision 1.0

December 2017

Section 1: 3DS Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the 3DS entity's assessment with the *PCI 3DS Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server* (PCI 3DS Core Security Standard). Complete all sections. The 3DS entity is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the payment brands for PCI 3DS reporting and submission procedures.

Part 1. 3DS Entity and 3DS Assessor Information

Part 1a. 3DS Entity Organization Information

Company Name:	iServeU Technology Pvt. Ltd.	DBA (doing business as):	iServeU
Contact Name:	Ramesh Chandra Rana	Title:	Deputy CISO
Telephone:	9004513098	E-mail:	ramesh.rana@iserveu.in
Business Address:	Plot No. E-12, SRB Tower, 11th Floor Infocity, Chandaka Industrial Estate, I E, Area	City:	Bhubaneswar
State/Province:	Odisha	Country:	India	Zip:	751024
URL:	https://iserveu.in		

Part 1b. 3DS Assessor Company Information

Company Name:	CyberCube Services Pvt. Ltd.		
Lead 3DS Assessor Contact Name:	Anil Kumar	Title:	Principal Consultant
Telephone:	+91-9891675123	E-mail:	anil@cybercube.co.in
Business Address:	Plot 880, Third Floor, Udyog Vihar Phase 5, Sector 18	City:	Gurugram
State/Province:	Haryana	Country:	India	Zip:	122016
URL:	www.cybercube.co		

Part 2. Executive Summary

Part 2a. 3DS Functions

Identify the 3DS Function(s) covered by this 3DS assessment (Check all that apply)	Details of EMVCo Letter of Approval (LOA):
☒ 3DS Server (3DSS)	LOA reference number: 3DS_LOA_SER_ISTP_020301_01094 Date of LOA issued by EMVCo: August 25, 2025 Name of product LOA issued for: iServeU 3ds
☒ Access Control Server (ACS)	LOA reference number: 3DS_LOA_ACS_ISTP_020301_01178 Date of LOA issued by EMVCo: December 23, 2025

	Name of product LOA issued for: iServeU ACS
☐ Directory Server (DS)	LOA reference number:
	Date of LOA issued by EMVCo:
	Name of product LOA issued for:
☐ Other *(As defined by a payment brand)*	

Note: *If your organization performs 3DS functions that are not covered by this assessment, consult the applicable payment brand about validation for the other functions.*

PCI Security Standards Council _____

Part 2b. Description of 3DS Business

How and in what capacity does your business provide/manage 3DS functions?	iServeU Technology Private Limited provides and manages 3D Secure (3DS) functions in the capacity of an issuer processor, 3DS Server (3DSS) operator, and Access Control Server (ACS) operator as part of its Banking-as-a-Service (BaaS), card issuance, and payment processing platform.

iServeU operates an EMV 3DS version 2.X–certified ACS, which is used to authenticate card-not-present (CNP) transactions, including e-commerce (ECOM) and MOTO transactions, in accordance with the latest EMV 3DS specifications. The ACS supports issuer-side authentication for cards issued by iServeU and performs both frictionless and challenge-based authentication using issuer-defined strong customer authentication methods such as OTPs, login-based verification, and risk-based decisioning.

In addition to ACS operations, iServeU performs issuer processing functions, including card issuance, transaction authorization, reconciliation, settlement, chargeback handling, fraud management, card re-issuance, and delivery of internet and mobile banking services. These services integrate with the 3DS authentication flow to ensure transactions are authenticated prior to authorization.

As part of 3DS processing:

- The ACS receives Authentication Requests (AReq) from the payment network (Directory Server) containing card and transaction details required for authentication.

- The ACS validates the cardholder and returns Authentication Responses (ARes), indicating authentication status and whether a challenge is required.

- Where applicable, the ACS supports browser-based, application-based, and out-of-band authentication flows, including the exchange of challenge and result messages (CReq, CRes, RReq, RRes) in accordance with EMV 3DS protocols.

- Operational and notification messages (OReq/ORes) are exchanged between 3DS components to support configuration, status, and operational alerting.

All cryptographic operations related to 3DS and ACS processing, including message signing and cardholder

authentication, are performed using Hardware Security Modules (HSMs). Cryptographic keys are securely generated, stored, and managed within the HSMs. Any stored 3DS-related data is encrypted using AES-256, and all data transmitted between 3DS components is protected using secure communication protocols (TLS).

Through operation of both the 3DS Server and ACS, and by supporting issuer-side authentication and processing services, iServeU plays a central role in the end-to-end 3D Secure authentication lifecycle, directly managing and securing 3DS authentication flows and associated data.

Part 2c. Locations

List types of facilities (for example, corporate offices, data centers) and a summary of locations covered by the PCI 3DS assessment.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
Example: Data Center	*3*	*Boston, MA, USA*
Corporate Office	1	Bhubaneswar, Odisha
Data Center (AWS)	1	UAE
Disaster Recovery (AWS)	1	UAE

Part 2d.

Not used for this AOC

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 3DS environment (3DE).*
- *Critical system components within the 3DE, such as 3DS servers, databases, web servers, etc., and any other necessary 3DS components, as applicable.*

- 3DS Servers (3DSS)
- ACS Servers
- Databases
- Application Servers
- Data flows to/from the 3DE
- 3DS/ACS data storage, retention, and disposal
- Cryptographic key management & HSM
- Access control mechanisms
- Logical security controls

	System monitoring and logging
	Incident response processes
Does your business use network segmentation to affect the scope of your 3DS environment?	☐ Yes ☒ No

Part 2f. Third-Party Service Providers

| Does your company share 3DS data with any third-party service providers (for example, payment processors, gateways)? | ☐ Yes ☒ No |
| Does your company rely on any third party for any PCI 3DS requirements, or for support or maintenance of the 3DS environment? | ☒ Yes ☐ No |

If Yes:

Name of service provider:	Description of services provided:
AWS	Hosting Service Provider

Part 2g. Summary of requirements tested to the PCI 3DS Security Standard

| Did the 3DS entity leverage a PCI DSS assessment to meet the PCI 3DS Part 1: Baseline Security Requirements? | ☒ Yes ☐ No |

Identify the appropriate assessment result for each high-level PCI 3DS requirement. Complete the table as follows:

- *If the results of a PCI DSS assessment have been verified as meeting all the PCI 3DS Part 1 Requirements:*
  - o Select "In Place per PCI DSS" for the 3DS Part 1 Requirements.
  - o Select the appropriate finding for each PCI 3DS Part 2 Requirement.
- *If a PCI DSS assessment is not being leveraged to meet all the PCI 3DS Part 1 Requirements:*
  - o Select the appropriate finding for each 3DS Part 1 and Part 2 Requirement.

When determining the appropriate finding for each high-level 3DS requirement, the following principles apply:

1. If the finding for any requirement or sub-requirement is "Not in Place", select "Not in Place" for the high-level requirement.
2. If the finding for any requirement or sub-requirement is "N/A" and all other requirements are "In Place", select "In Place" for the high-level requirement.
3. If the finding for any requirement or sub-requirement is "In Place w/CCW" and all other requirements are "In Place", select "In Place w/CCW" for the high-level requirement.
4. If the findings include one or more requirements or sub-requirements as "N/A", and one or more as "In Place w/CCW", and all other requirements are "In Place", select "In Place w/CCW" for the high-level requirement.
5. If all requirements and sub-requirements are identified as "In Place", select "In Place" for the high-level requirement.

Summary of Findings		In Place per PCI DSS		In Place	In Place w/CCW	N/A	Not in Place
Part 1: Baseline Security Requirements							
P1-1	Maintain security policies for all personnel			☐	☐	☐	☐
P1-2	Secure network connectivity			☐	☐	☐	☐
P1-3	Develop and maintain secure systems			☐	☐	☐	☐
P1-4	Vulnerability management	☒	OR	☐	☐	☐	☐
P1-5	Manage access			☐	☐	☐	☐
P1-6	Physical security			☐	☐	☐	☐
P1-7	Incident response preparedness			☐	☐	☐	☐
Part 2: 3DS Security Requirements							
P2-1	Validate scope			☒	☐	☐	☐
P2-2	Security governance			☒	☐	☐	☐
P2-3	Protect 3DS systems and applications			☒	☐	☐	☐
P2-4	Secure logical access to 3DS systems			☒	☐	☐	☐
P2-5	Protect 3DS data			☒	☐	☐	☐
P2-6	Cryptography and key management			☒	☐	☐	☐
P2-7	Physically secure 3DS systems			☒	☐	☐	☐

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite PCI 3DS assessment, which is documented in an accompanying 3DS Report on Compliance (ROC).

The assessment documented in this attestation and in the 3DS ROC was completed on:	*24-12-2025*
Was PCI DSS used to meet PCI 3DS Part 1: Baseline Security Requirements?	☒ Yes ☐ No
Have compensating controls been used to meet any PCI 3DS requirement?	☐ Yes ☒ No
Were any PCI 3DS requirements identified as being not applicable (N/A)?	☐ Yes ☒ No
Were any PCI 3DS requirements unable to be met due to a legal constraint?	☐ Yes ☒ No

Section 3: Validation and Attestation Details

Part 3. PCI 3DS Validation

This AOC is based on results noted in the 3DS ROC dated *(24-12-2025).*

Based on the results documented in the 3DS 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 3DS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *(iServeU Technology Pvt. Ltd.)* has demonstrated full compliance with the PCI 3DS Core Security Standard.
☐	**Non-Compliant:** Not all sections of the PCI 3DS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(3DS Entity Company Name)* has not demonstrated full compliance with the PCI 3DS Core Security Standard. **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 applicable 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 the applicable payment brand(s). *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 3DS ROC was completed according to the PCI 3DS Core Security Standard, Version *1.0*, and was completed according to the instructions therein.
☒	All information within the above-referenced 3DS ROC and in this attestation fairly represents the results of my assessment in all material respects.
☒	I have read the PCI 3DS Core Security Standard and I recognize that I must maintain 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 3DS requirements that apply.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *Clone Systems*

Part 3b. 3DS Entity Attestation

Ramesh Chandra Rana
Date: Dec 26 2025 16:01:22 IST
Aadhaar eSign by:
ramesh.rana@iserveu.in
sign.zoho.in

Signature of 3DS Entity Executive Officer ↑	*Date:* **24-12-2025**
3DS Entity Executive Officer Name: **Ramesh Chandra Rana**	*Title:* **Deputy CISO**

Part 3c. 3DS Assessor Acknowledgement

Anil Kumar

Digitally signed by
Anil Kumar
Date: 2025.12.24
22:33:24 +05'30'

Signature of Duly Authorized Officer of 3DS Assessor Company ↑	*Date:* **24-12-2025**
Duly Authorized Officer Name: **Anil Kumar**	*Title:* **Principal Consultant**
3DS Assessor Company: **CyberCube Services Pvt Ltd**	

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI 3DS 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 3DS Requirement	Compliant to PCI 3DS Requirements *(Select One)*		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
P1	Maintain security policies for all personnel	☒	☐	
	Secure network connectivity	☒	☐	
	Develop and maintain secure systems	☒	☐	
	Vulnerability management	☒	☐	
	Manage access	☒	☐	
	Physical security	☒	☐	
	Incident response preparedness	☒	☐	
P2	Validate scope	☒	☐	
	Security governance	☒	☐	
	Protect 3DS systems and applications	☒	☐	
	Secure logical access to 3DS systems	☒	☐	
	Protect 3DS data	☒	☐	
	Cryptography and key management	☒	☐	
	Physically secure 3DS systems	☒	☐	