



Payment Card Industry Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024

PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: CEDACRI INTERNATIONAL

Date of Report as noted in the Report on Compliance: 2025, November 15

Date Assessment Ended: 2025, November 15

Section 1: Assessment Information

Instructions for Submission

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

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

Part 1. Contact Information

Part 1a. Assessed Entity (ROC Section 1.1)

Company name:	Cedacri International
DBA (doing business as):	Cedacri International
Company mailing address:	bd. Stefan cel Mare 171/1, MD-2004 Chisinau, Moldova
Company main website:	https://www.cedacrinternational.md
Company contact name:	Elena Ciubara
Company contact title:	Certification Officer
Contact phone number:	+373 22 855610
Contact e-mail address:	elena.ciubara@iongroup.com

Part 1b. Assessor (ROC Section 1.1)

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):	Not applicable
--------------	----------------

Qualified Security Assessor

Company name:	366 Security and Compliance Srl
Company mailing address:	Via dell'Umiltà 49, 00187 Rome, Italy
Company website:	https://www.366secom.com
Lead Assessor name:	Amedeo Lupinelli
Assessor phone number:	+39 393 9100090
Assessor e-mail address:	amedeo.lupinelli@366secom.com
Assessor certificate number:	202-901

Part 2. Executive Summary

Part 2a. Scope Verification

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

Name of service(s) assessed:	Call Center support for C-Global customer for POI (Physical POS and ATM) Management (GEBA - POS Open - GEPO - Automa)
------------------------------	---

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): Call Center support for C-GLOBLA's customer Banks on ATM and POS, and Call Center support for fraud prevention for C-GLOBAL's principal member customers through Principal Member technological infrastructure and environment

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 Assessment (select all that apply):

Name of service(s) not assessed: All services provided by CEDACRI and C-GLOBAL and external Principal Member

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:

The services provided by Cedacri were not assessed in this report as those had been already assessed in Cedacri ROC dated 2025 November 15 and into C-GLOBAL ROC dated 2025 November 15 which are Service Providers Level 1 PCI DSS v4.0.1 compliant.

Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)

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

Cedacri International provides comprehensive support services to client banks of C-Global for managing technical anomalies and issues affecting ATMs and POS terminals. These services are delivered through dedicated applications, which are hosted and secured

	<p>by Cedacri in its capacity as a PCI DSS certified Service Provider (version 4.0.1).</p> <p>Additionally, Cedacri International offers fraud management support to C-Global's customers. This service line leverages specialized applications that are managed and provisioned directly by the customer banks themselves</p>
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Processes where Customer care operators are involved in antifraud operations
Describe system components that could impact the security of account data.	Systems owned and completely managed by CEDACRI and/or C-GLOBAL or third party customers

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.*

Cedacri International's ROC is fully integrated with Cedacri S.p.A. and C-Global's ROC.

His critical function is entirely overseen and governed by Cedacri S.p.A., which operates as a Level 1 Service Provider fully compliant with the PCI DSS v 4.0.1 standard.

To maintain the highest levels of data security and compliance, Cedacri International adheres to a strict, multi-layered access control policy managed by CEDACRI:

Principle of Least Privilege: Operators of Cedacri International can not access LIVE PANs (Primary Account Numbers) in any operational context; the only exception to this rule is for explicitly authorized fraud management activities. In these specific cases, Principal Members formally define and justify the business need, granting Cedacri International operators a temporary and strictly monitored mandate for fraud prevention practices.

Cedacri Network Access: All user accounts for accessing the internal Cedacri network are managed directly and exclusively by Cedacri S.p.A.'s own security team.

Principal Member System Access: When operators require access to the Principal Members' external fraud management systems, the credentials and permissions for these systems are granted, controlled, and audited solely by the Principal Members themselves.

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

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

☒ Yes ☐ No

Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this 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>
Head Quarter and offices	1	Chisinau- Moldova

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)

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
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				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 (ROC Section 4.4)

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))	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
• Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

If Yes:

Name of Service Provider:	Description of Services Provided:
CEDACRI S.p.A.	Network Security, System Security, Data Security, Connection Security, Antivirus Services, Application Security, Logical Access Security, Log Management, VA and PT, Policy and Procedures.

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

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment (ROC Section 1.8.1)

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: Call Center support for C-Global customer for POI (Physical POS and ATM) Management

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
Requirement 1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Justification for Approach

<p>For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.</p>	<p>2.3.1 - No Wireless network connected to CDE</p> <p>2.3.2 - No Wireless network connected to the CDE9 CEDACRI INTERNATIONAL</p> <p>4.2.2 – CEDACRI INTERNATIONAL personnel cannot send the real PAN as they have no access to it. This is both a technical and policy enforcement.</p> <p>4.2.1.2 - wireless networks were isolated from the CDE and did not handle PAN</p> <p>6 (all Requirements) CEDACRI INTERNATIONAL never develops software for PCI DSS environment, but it used commercial applications running on technological environment supplied and completely managed by CEDACRI.</p> <p>9.4 - No PAN in any format is stored within Cedacri International environment</p> <p>9.4.1 - No PAN in any format is stored within Cedacri International environment</p> <p>9.4.1.1 - No PAN in any format is stored within Cedacri International environment</p> <p>9.4.1.2 - No PAN in any format is stored within Cedacri International environment</p> <p>9.4.2 - No PAN in any format is stored within Cedacri International environment</p> <p>9.4.3 - No PAN in any format is stored within Cedacri International environment</p> <p>9.4.4 - No PAN in any format is stored within Cedacri International environment</p> <p>9.4.5 - No PAN in any format is stored within Cedacri International environment</p> <p>9.4.5.1 - No PAN in any format is stored within Cedacri International environment</p> <p>9.4.6 - No PAN in any format is stored within Cedacri International environment</p> <p>9.4.7 - No PAN in any format is stored within Cedacri International environment</p> <p>9.5 - No POI is managed by Cedacri International</p> <p>9.5.1 - No POI is managed by Cedacri International</p> <p>9.5.1.1 - No POI is managed by Cedacri International</p> <p>9.5.1.2 - No POI is managed by Cedacri International</p> <p>9.5.1.2.1 - No POI is managed by Cedacri International</p> <p>9.5.1.3 - No POI is managed by Cedacri International</p> <p>APPENDIX A1 – CEDACRI INTERNATIONAL is not a multi-tenant service providers</p> <p>APPENDIX A2 – CEDACRI INTERNATIONAL does not use SSL/Early TLS for Card-Present POS POI Terminal Connections</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>Not applicable</p>

Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3)

Date Assessment began: Note: <i>This is the first date that evidence was gathered, or observations were made.</i>	2025-09-03
Date Assessment ended: Note: <i>This is the last date that evidence was gathered, or observations were made.</i>	2025-11-15
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated *(Date of Report as noted in the ROC 2025-11-15)*.

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

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

Based on the results documented in the ROC 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)*:

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall COMPLIANT rating; thereby CEDACRI INTERNATIONAL has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.</p>								
<input type="checkbox"/>	<p>Non-Compliant: Not all sections of the PCI DSS ROC 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 PCI DSS requirements.</p> <p>Target Date for Compliance: YYYY-MM-DD</p> <p>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 before completing Part 4.</p>								
<input type="checkbox"/>	<p>Compliant but with Legal exception: One or more assessed requirements in the ROC 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 In Place or 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 except those noted as Not Tested above or as Not in Place due to a legal restriction.</p> <p>This option requires additional review from the entity to which this AOC will be submitted.</p> <p><i>If selected, complete the following:</i></p> <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 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0.1 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 the Assessment in all material respects.
<input checked="" type="checkbox"/>	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: 2025-11-15
Service Provider Executive Officer Name: Francesco Pipio	Title: Chief executive officer

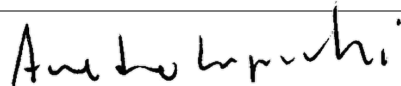
Part 3c. Qualified Security Assessor (QSA) Acknowledgement

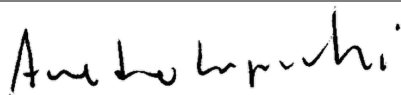
If a QSA was involved or assisted with this Assessment, indicate the role performed:

☒ QSA performed testing procedures.

☐ QSA provided other assistance.

If selected, describe all role(s) performed:

	
Signature of Lead QSA ↗	Date: 2025-11-15
Lead QSA Name: Amedeo Lupinelli	

	
Signature of Duly Authorized Officer of QSA Company ↗	Date: 2025-11-15
Duly Authorized Officer Name: Amedeo Lupinelli	QSA Company: 366 Security and Compliance

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 Non-Compliant results 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 provide 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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<input 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 type="checkbox"/>	<input type="checkbox"/>	

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 their program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/