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: Monext

Date of Report as noted in the Report on Compliance: January 2nd, 2025

Date Assessment Ended: December 31st, 2024

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:	MONEXT
DBA (doing business as):	MONEXT
Company mailing address:	80 Chemin de la Faisanderie 13290, Aix en Provence
Company main website:	https://www.monext.eu/
Company contact name:	Grégoire MAUX
Company contact title:	Operational Security Manager – PCI Compliance Manager
Contact phone number:	+33 442 25 92 63
Contact e-mail address:	Gregoire.MAUX@monext.net

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):	NA
Qualified Security Assessor	
Company name:	DATAPROTECT
Company mailing address:	La Défense 1-7. Cours Valmy, Le Belvédère, 92800, Puteaux, France
Company website:	https://www.dataprotect.fr/
Lead Assessor name:	Yahya EL KOUHEN
Assessor phone number:	+33 7 55 48 12 97
Assessor e-mail address:	yelkouhen@dataprotect.fr
Assessor certificate number:	PCI QSA - 206-538

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:	- ACQUIRER SERVICES (ACE, MBA, PMC, RED2 and Back-office) - ISSUER SERVICES (ECC, ABP, MBE, ICI, IPF, CPU, SA, 3DS, FullCB Back-office) - MERCHANT SERVICES (Monext Online, GTAA, Monext In-Store) - FortKnox : Cardholder data wallet solution - SOCLE SERVICES (Tokenizer, PGFS)

Type of service(s) assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☒ Systems security services	☒ POI / card present
☒ Hardware	☐ IT support	☒ Internet / e-commerce
☒ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☒ Security services		
☒ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (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): Tokenization, Data preparation, Card Management System, Authorization, Dynamic Currency Conversion, Multi Channel Payment

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 Monext services not specifically listed above

Type of service(s) not assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POI / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (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:	NA

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.	Monext processes Account Data in order to provide issuing and acquiring services (authorization, clearing, CMS, Data preparation, etc.) on behalf of its customers (issuing and acquiring banks). Monext also processes Account Data in order to provide payment acceptance solutions for e-commerce and POS merchants. Account Data are processed using in-house software running on IBM Z/OS Mainframe, IBM AIX and Linux systems. Monext processes Account Data using an in-house merchant, acquiring and issuing programs (CMS (PowerCard), authorization servers (Clear2Pay)), and

	3DS ACS (Modirum MDPAY)) running on IBM Z/OS Mainframe, IBM AIX and Linux RedHat systems. Monext stores Account data to fulfill the customers legal, business and regulatory responsibilities to keep transactions and payment history details during at least 18 months (banking regulation), in the database (encrypted at column-level or at application-level). Monext transmits CHD to card schemes, card creators, acquirers and issuers using private links, IPSEC VPN and Internet. Monext stores Account Data in both PostgreSQL and Oracle databases (encrypted at column-level or at application-level, and using Thales Payshield HSM or Bull Crypt2Pay HSM). Monext transmits Account Data using card schemes private gateway, IPSEC VPN, private networks and Internet.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Monext activities could impact the security of account data in the context of infrastructure (network, system and applications) and human resources management since the CDE is within Monext infrastructure and Monext Operators process account Data in the context of their legitimate activities. This infrastructure supports the CDE and all security solutions in place to ensure that all restriction and protection controls are operational.
Describe system components that could impact the security of account data.	All components that could impact the security of account data include all systems providing management to the CDE, proxy servers, internal load balancers, FIM solution, Antivirus, deployment solutions and all Security solutions. All those compoents are included in the Scope of Assessment and the PCI Compliance program maintained by Monext

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.*	The assessed environment is composed of : - Inbound network connections: Internet, PSTN networks and private networks (MPLS, IPSEC VPN, etc.) - Private connections with Card shemes (Visa VEAS and MasterCard GMIP on premises gateway) - Outbound network connections with acquirers using various private networks and Internet VPN Critical Compontents that could impact the security of account data : - Front-end firewalls and back-end firewalls - In-house processing applications - Databases and web applications - Load balancers and SSL offloaders - Web servers (Appache Tomcat and Oracle Fusion middleware) N.B All activities providing management to the CDE, proxy servers Management, network components Administration, Security solutions administration (Fim solution, antivirus and access control tools). All concerned components are included in the Scope of Assessment and the PCI Compliance program maintained by Monext N.B The Data centers hosting the CDE are managed by ARKEA and covered by another assessment (AOC was collected)
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)
Example: Data centers	*3*	*Boston, MA, USA*

Monext Office	1	80 Chemin de la Faisanderie, 13290 Aix-en-Provence

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))	☒ Yes ☐ 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)	☒ 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 Services Provided:
Arkéa	Hosting Infrastructure System-level maintenance of the IBM Z/OS Mainframe Housing Physical security
Nextalk	Issuer and Acquirer Call Center
ACI PAYON Nepting Dejamobile	Payment Processing (Merchant acceptance)
Lyra Network TRIONIS REDSYS	E-business platform for e-commerce Payment gateway services Payment Processing
TNS	Connectivity services
CloudFlare	Transmission services (Content Delivery Nework/DDOS protection)
GEMALTO/THALES DIS IDEMIA	Card Manufactorers
PPRO	Transaction processing
Microsoft Corporation	Microsoft SharePoint Online and OneDrive for Business Microsoft Azure Microsoft 365 (M365)
SEA TPI Europ-Assistance	Supervision service & OPEN Exploitation Authentication Services (MFA)

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:

- ACQUIRER SERVICES (ACE, MBA, PMC, RED2 and Back-office)
- ISSUER SERVICES (ECC, ABP, MBE, ICI, IPF, CPU, SA, 3DS, FullCB Back-office)
- MERCHANT SERVICES (Monext Online, GTAA, Monext In-Store)
- FortKnox : Cardholder data wallet solution
- SOCLE SERVICES (Tokenizer, PGFS)

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:	☒	☐	☐	☐	☐
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 9 : All sub-requirements are not-applicable since they are covered by another assessment (Cf. AOC of ARKEA) - A1 (All sub-requirements are not-applicable since Payplug is not a shared hosting provider) - A2 (All sub-requirements are not applicable since Monext has no POS POI terminals)
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	NA

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	2024-02-05
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2024-12-30
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely?	☒ Yes ☐ 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 2024-12-31)*.

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)**:***

☒	**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 MONEXT has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**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 *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements. **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 before completing Part 4.
☐	**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 *(Service Provider Company Name)* 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. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

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)

☒	The ROC was completed according to *PCI DSS*, Version 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the 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

DocuSigned by:
Guillaume Prin
2B59C80590C0477...

Signature of Service Provider Executive Officer ↗	Date: 2025-01-02
Service Provider Executive Officer Name: Guillaume PRIN	Title: Président du Directoire

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: NA

Yahya EL KOUHEN

Signature of Lead QSA ↗	Date: 2025-01-02
Lead QSA Name: Yahya EL KOUHEN	

Signature of Duly Authorized Officer of QSA Company ↗	Date: 2025-01-02
Duly Authorized Officer Name: Ali EL AZZOUZI	QSA Company: DATAPROTECT

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: NA

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