Security
Standards Council

Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

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:	KDDI France		DBA (doing business as):		
Contact Name:	Cécile Naton		Title:	Responsable Processus	
Telephone:	+33 6 42 20 70 67		E-mail:	cecile.naton@fr.kddi.eu	
Business Address:	65 rue Léon Frot		City:	Paris	
State/Province:		Country:	France	Zip:	75011
URL:	www.fra.kddi.com				

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

Company Name:	ECSC Group Plc				
Lead QSA Contact Name:	David Tattersall		Title:	Consultant	
Telephone:	+44 (0) 1274 736223		E-mail:	david.tattersall@ecsc.co.uk	
Business Address:	28 Campus Road		City:	Bradford	
State/Province:	W Yorkshire	Country:	United Kingdom	Zip:	BD7 1HR
URL:	www.ecsc.co.uk				

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:	Data centre co-location services – Léon Frot, Paris
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:	Any other services provided by KDDI and any sites not included in the scope of this assessment (i.e. rest of world).

Type of service(s) not assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
□ Applications / software □ Hardware □ Infrastructure / Network □ Physical space (co-location) □ Storage □ Web □ Security services □ 3-D Secure Hosting Provider □ Shared Hosting Provider □ Other Hosting (specify):	□ Systems security services □ IT support □ Physical security □ Terminal Management System □ Other services (specify):	□ 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:	

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Not applicable – KDDI France (KDDI) does not store, process or transmit cardholder data. This assessment only covers the physical security controls of the co-location environment provided by KDDI and does not include customers' systems or any associated card data.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	KDDI has one data centre within scope of this assessment providing co-location services to numerous clients. The services provided by KDDI could potentially impact clients' Cardholder Data Environments (CDEs). The scope of this assessment covers the physical security aspects of the facility at Rue Léon Frot, in Paris, France.

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):
Example: Retail outlets	*3*	*Boston, MA, USA*
Data Centre	1	Paris, France

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)
Not applicable			□ Yes ☒ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	

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.*	KDDI France (KDDI) has operates a data centre in Paris providing co-location physical hosting services and facilities for customers. KDDI requires that the facility be PCI DSS compliant as some of its clients, to be hosted within the KDDI facility, may be processing payment card transactions. The Léon Frot data centre is the only one of KDDI's facilities in scope for this assessment. The services provided include the provision of the physical environment, supporting environmental services (e.g. mains power, UPS, cooling, fire detection and suppression) and physical security for the environment. Customer equipment is supplied and owned by the customer and KDDI has no logical access to

	this equipment. KDDI offers two variants of this service in the Léon Frot data centre in Paris: 1. Dedicated Facilities Management (DFM) – computer suites dedicated to a single customer, where access is controlled with, as a minimum, proximity access control readers and in some cases additional measures as specified by the customer. 2. Shared Facilities Management (SFM) – either single or multiple full equipment racks within a computer suite where the suite is access controlled by proximity access control readers for a number of customers.

Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	□ Yes ☒ 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:	
QIR Individual Name:	
Description of services provided by QIR:	
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:**

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:	Data centre co-location services

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:	□	□	☒	All requirements – not applicable. *This requirement is not considered to be in scope for this assessment and therefore not tested. Neither KDDI or its customers' infrastructure are in scope; only data centre physical controls and security systems are in scope.*
Requirement 2:	□	□	☒	All requirements – not applicable. *This requirement is not considered to be in scope for this assessment and therefore not tested. Neither KDDI or its customers' infrastructure are in scope; only data centre physical controls and security systems are in scope.*
Requirement 3:	□	☒	□	*Only the following requirements are fulfilled by KDDI:* *- 3.1.x* *- 3.2.a, 3.2.b, 3.2.c, 3.2.d* *These requirements have been marked as in place to reflect that the assessor has confirmed that KDDI does not directly transmit, process or store cardholder data and has no access to cardholder or sensitive authentication data on their customers' systems.* *All other requirements not applicable. Neither KDDI or its customers' infrastructure are in scope; only data centre physical controls and security systems are in scope.*
Requirement 4:	□	□	☒	All requirements – not applicable. *This requirement is not considered to be in scope for this assessment and therefore not tested. Neither KDDI or its customers' infrastructure are in scope; only data centre physical controls and security systems are in scope.*
Requirement 5:	□	□	☒	*All requirements – not applicable.*

				This requirement is not considered to be in scope for this assessment and therefore not tested. Neither KDDI or its customers' infrastructure are in scope; only data centre physical controls and security systems are in scope.
Requirement 6:	☐	☐	☒	All requirements – not applicable. *This requirement is not considered to be in scope for this assessment and therefore not tested. Neither KDDI or its customers' infrastructure are in scope; only data centre physical controls and security systems are in scope.*
Requirement 7:	☐	☐	☒	All requirements – not applicable. *This requirement is not considered to be in scope for this assessment and therefore not tested. Neither KDDI or its customers' infrastructure are in scope; only data centre physical controls and security systems are in scope.*
Requirement 8:	☐	☐	☒	*All requirements – not applicable.* *This requirement is not considered to be in scope for this assessment and therefore not tested. Neither KDDI or its customers' infrastructure are in scope; only data centre physical controls and security systems are in scope.*
Requirement 9:	☐	☒	☐	*The following requirements were not applicable as KDDI does not store any cardholder data on any media:* *- 9.5, 9.6-9.8.1, 9.8.2.* *The requirements within 9.9 were not applicable as KDDI does not have any card-reading devices in scope of this assessment.* *Neither TIE or its customers' infrastructure are in scope; only data centre physical controls and security systems are in scope.*
Requirement 10:	☐	☒	☐	*Only the following requirements are fulfilled by KDDI:* *- 10.8.x* *The remainder were marked as not applicable; neither KDDI or its customers' infrastructure are in scope; only data centre physical controls and security systems are in scope.*
Requirement 11:	☐	☐	☒	*All requirements – not applicable.* *This requirement is not considered to be in scope for this assessment and therefore not tested. Neither KDDI or its customers' infrastructure are in scope; only data centre physical controls and security systems are in scope.*
Requirement 12:	☐	☒	☐	The following requirements are not applicable as they are not considered to be in scope for this assessment: *- 12.3.x – KDDI does not have access to any critical technologies in relation to cardholder data.* *- 12.5.4, 12.5.5 – KDDI does not have any logical access to cardholder data.*

				- 12.8.x – KDDI does not have any service providers with whom cardholder data is shared, or that could directly affect the security of cardholder data. *Neither KDDI or its customers' infrastructure are in scope; only data centre physical controls and security systems are in scope.* *With respect to the services within scope of this assessment, KDDI are responsible for all activities and none are outsourced (i.e. where any 3rd party companies are involved, they are regarded as either KDDI personnel or contractors).*
Appendix A1:	□	□	☒	*Entity is not a shared hosting provider*
Appendix A2:	□	□	☒	*Assessment based on SAQ A outsourced payment process.*

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:	*24 May 2022*	
Have compensating controls been used to meet any requirement in the ROC?	□ Yes	☒ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	□ No
Were any requirements not tested?	□ Yes	☒ No
Were any requirements in the ROC 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 the ROC dated 24 May 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)*:**

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby KDDI France has demonstrated full compliance with the PCI DSS.
☐	**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 *(Service Provider Company Name)* has not demonstrated full compliance with the PCI DSS. **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 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 acquirer or payment brand. *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 ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version 3.2.1, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS 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 DSS requirements that apply.

Part 3a. Acknowledgement of Status (continued)	
□	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. **Not applicable – the scope of this assessment was limited to physical co-location services.**
□	ASV scans are being completed by the PCI SSC Approved Scanning Vendor **Not applicable – the scope of this assessment was limited to physical co-location services.**

Part 3b. Service Provider Attestation	
太田 誠	
Signature of Service Provider Executive Officer ↑	*Date:*
Service Provider Executive Officer Name: Makoto Ota	*Title:* President, KDDI France

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)	
If a QSA was involved or assisted with this assessment, describe the role performed:	*Assessor*
Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 24 May 2022
Duly Authorized Officer Name: Robert (David) Tattersall	*QSA Company: ECSC Group Plc*

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:	

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