A2SECURE

PCI Security Standards Council

Payment Card Industry (PCI)
Data Security Standard

HITTGROUP

HITTGROUP•ES

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:	Hitt Tourism S.L.U.		DBA (doing business as):	Dingus Spain S.L.	
Contact Name:	Marta Monserrat		Title:	Responsable seguridad	
Telephone:	+34 654 533 780		E-mail:	marta.monserrat@hittgroup.es	
Business Address:	C/ Germans Lumiere, Edificio Closell 2º		City:	Palma de Mallorca	
State/Province:	Baleares	Country:	Spain	Zip:	07121
URL:	https://www.hittgroup.es/				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	A2 Secure Technologias Informatica, Sociedad Ltd.				
Lead QSA Contact Name:	Guillem Cuesta Basseda		Title:	QSA & IT Consultant	
Telephone:	933 94 56 00		E-mail:	guillem.cuesta@a2secure.com	
Business Address:	Av. de Francesc Cambó, 21, 10ª.		City:	Barcelona	
State/Province:	Barcelona	Country:	Spain	Zip:	08003
URL:	https://www.a2secure.com/				

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:	Book&Payment	
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): CRS-Central Reservation System		

***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:	All Hitt Tourism S.L.U. services not specifically listed above	
Type of service(s) not 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):		
Provide a brief explanation why any checked services were not included in the assessment:	Bookincenter is a solution that allows for of all aspects of online distribution and sales management owned by Hitt Tourism S.L.U. This environment does not store, processes or transmits CHD Roomonline is a comprehensive solution for direct sales through the hotel's corporate website. This environment does not store, processes or transmits CHD	

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Following find the detail of how Book&Payment environment (located in AWS) processes, and transmits cardholder data: 1. BAP-PROXY instance receives CHD from different channels (Booking, Expedia, etc.) 2. Then, BAP-API-BACKEND instance generates a TOKEN that it is stored in a MongoDB instance 3. BAP-API-BACKEND process the payment against a PSP (Addon Payment, PaynoPain, etc.) 4. BAP-API-BACKEND deletes any type of CHD located in the environment.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Book&Payment environments does not store CHD. However, some data (PAN and CVV) is received and processed by the solution.

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*
Hitt Tourism headquarters	1	Palma Mallorca, Spain
AWS environment	1	eu-west-1 Europe (Ireland)

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)
-	-	-	☐ 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.*	All PCI environment has been deployed on AWS (Amazon Web Services) by HITTGROUP. The PCI environment includes 2 VPC (Public Subnet & Private Subnet) where all required instances are allocated. While on the public subnet HITTGROUP has allocated the ELB and the BASTION (sysadmin access through SSH), the API servers, the main DB (Mongo DB), Wazuh and other management services has been deployed on the private network.

	The access to the environment is performed through a 2FA
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:**
Amazon WebServices (AWS)	On-demand cloud computing platform
Addon Payments	Payment processing
PAYCOMMET	Payment processing
PayNoPain	Payment processing
Redsys	Payment processing
UniversalPay	Payment processing
Banca March through Redsys	Payment processing
Abreu Online	OTA (Online travel Agency)
Agoda	OTA (Online travel Agency)
ATRAPALO	OTA (Online travel Agency)
BOOKING	Travel fare aggregator
CHECK24	OTA (Online travel Agency)
CTRIP	OTA (Online travel Agency)
DESPEGAR	OTA (Online travel Agency)
EDREAMS	OTA (Online travel Agency)
EXPEDIA	Travel fare aggregator
FASTPAY	OTA (Online travel Agency)
GNA Hotel Solutions	OTA (Online travel Agency)
HBSI	OTA (Online travel Agency)
HOTELBEDS	OTA (Online travel Agency)
Hotetec	OTA (Online travel Agency)
Hotusa	OTA (Online travel Agency)
IGM WEB	OTA (Online travel Agency)

Lastminute	OTA (Online travel Agency)
LIBGO TRAVEL/FLIGHT CENTRE	OTA (Online travel Agency)
Mirai	
Neobookings	OTA (Online travel Agency)
PARATY	OTA (Online travel Agency)
ROIBACK	OTA (Online travel Agency)
SEE USA TOURS	OTA (Online travel Agency)
TRAFFICS/CONNECTED DESTINATIONS	OTA (Online travel Agency)
TRAVELREPUBLIC/DNATA	OTA (Online travel Agency)
W2M/NT INCOMING	OTA (Online travel Agency)
Welcomebeds	OTA (Online travel Agency)
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:	Book&Payment			
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:	☐	☒	☐	• **Req. 1.2.3:** *Wireless connections are not allowed in the CDE.*
Requirement 2:	☐	☒	☐	• **Req. 2.1.1:** *Wireless connections are not allowed in the CDE.* • **Req. 2.2.3:** *Insecure services, daemons, or protocols are not allowed in the CDE.* • **Req. 2.6:** *The assessed entity is not a shared hosting provider.*
Requirement 3:	☐	☒	☐	• **Req. 3.2:** *Hittgroup is not an issuer or company that support issuing services and store sensitive authentication data.* • **Req. 3.3, 3.4, 3.4.1, 3.5, 3.5.1, 3.5.2, 3.5.3, 3.5.4, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7 and 3.6.8:** *No electronic storage of any cardholder data on the merchant's systems or premises.*
Requirement 4:	☐	☒	☐	• **Req. 4.1.1:** *Wireless connections are not allowed in the CDE.*
Requirement 5:	☒	☐	☐	-
Requirement 6:	☐	☒	☐	• **Req. 6.4.6:** *Significant changes did not occur within the past 12 months.*
Requirement 7:	☐	☒	☐	• **Req. 7.1.4:** *During this last year there have been no new incorporations.*

Requirement 8:	☐	☒	☐	• **Req. 8.1.3:** *According to Oscar Sanchez, there have been no user terminations during the last year.* • **Req. 8.5:** *CCW* • **Req. 8.7:** *No electronic storage of any cardholder data on the merchant's systems or premises.*
Requirement 9:	☐	☒	☐	• **Req. 9.5, 9.5.1, 9.6, 9.6.1, 9.6.2, 9.6.3, 9.7, 9.7.1, 9.8, 9.8.1, 9.8.2, 9.9, 9.9.1, 9.9.2 and 9.9.3:** *The entity does not use devices that capture payment card data via direct physical interaction with the card*
Requirement 10:	☐	☒	☐	• **Req. 10.2.1:** *No electronic storage of any cardholder data on the merchant's systems or premises.*
Requirement 11:	☐	☒	☐	• **Req. 11.2.3:** *The entity confirms that during the last year there have been no significant changes to the platform.*
Requirement 12:	☒	☐	☐	-
Appendix A1:	☐	☐	☒	-
Appendix A2:	☐	☐	☒	-

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:	*28/09/2022*	
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 *28/09/2022*

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 Hitt Tourism S.L. 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.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor Qualys Inc

Part 3b. Service Provider Attestation

MONSERRAT BALAGUER MARTA - 43193832Q

Firmado digitalmente por MONSERRAT BALAGUER MARTA - 43193832Q
Fecha: 2022.09.28 10:35:38 +02'00'

Signature of Service Provider Executive Officer ↗	*Date:* ***28/09/2022***
Service Provider Executive Officer Name: Marta Monserrat	*Title:* ***Responsable seguridad***

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	*FULL PCI QSA audit. The QSA has assisted with knowledge on PCI-DSS and consultancy on how to interpret the requirements*

CUESTA BASSEDA GUILLEM - 47870246R

Digitally signed by CUESTA BASSEDA GUILLEM - 47870246R
Date: 2022.09.28 09:36:58 +02'00'

Signature of Duly Authorized Officer of QSA Company ↗	*Date: 28/09/2022*
Duly Authorized Officer Name: Guillem Cuesta	*QSA Company: A2 Secure Technologias Informática, Sociedad Ltd.*

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	☐	☐	N/A
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	N/A