Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.0

February 2014

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:	Eczacıbaşı Bilişim Hizmetleri A.Ş.		DBA (doing business as):	EBİ	
Contact Name:	Atilay Yilmaz		Title:	Project and Quality Systems Manager	
ISA Name(s) (if applicable):			Title:		
Telephone:	+90-(212)-350 88 66		E-mail:	atilay.yilmaz@eczacibasi.com.tr	
Business Address:	Büyükdere Caddesi Ali Kaya Sokak No: 5 Levent		City:	ISTANBUL	
State/Province:		Country:	TURKEY	Zip:	34394
URL:	www.ebi.com.tr				

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

Company Name:	Biznet Bilisim Sistemleri A.S				
Lead QSA Contact Name:	Onur Arikan		Title:	Security Consultant	
Telephone:	+90 (532) 267 53 27		E-mail:	onur.arikan@biznet.com.tr	
Business Address:	ODTU Teknokent Ikizler Binasi Kat:1		City:	ANKARA	
State/Province:		Country:	TURKEY	Zip:	06800
URL:	www.biznet.com.tr				

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:	EBİ Datacenter and Hosting Services	
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.

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:	

Type of service(s) not assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POS / 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		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting 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:	

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Eczacibasi Bilişim A.Ş. (EBİ) aims to provide datacenter and hosting services to service providers, banks and merchants those are related to payment cards.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Since EBİ is providing datacenter and server hosting services there are no payment channels in the scope of PCI DSS assessment. The payments channels for EBİ's customers should be examined for each company's PCI DSS assessments.

Part 2c. Locations

List types of facilities and a summary of locations included in PCI DSS review (for example, retail outlets, corporate offices, data centers, call centers, etc.):

Type of facility:	**Location(s) of facility (city, country):**
Datacenter	Levent, Istanbul, TURKEY

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	
			☐ 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.*	EBİ does not provide acquiring, issuing, clearing or any payment services. Aim of EBİ is to provide datacenter and server hosting services to member banks, service providers and merchants who need to be PCI DSS compliant.
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 one or more third-party service providers (for example, 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:

Type of service provider:	Description of services provided:
Securitas	Physical security services

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:	EBİ Datacenter and Hosting Services			
	Details of Requirements Assessed			
PCI DSS Requirement	**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:	☐	☐	☒	**Not Tested. Firewall and network management is excluded from the scope of PCI DSS assessment.**
Requirement 2:	☐	☐	☒	**Not Tested. Since only physical security requirements are assessed, the systems configurations are excluded from the scope of PCI DSS assessment.**
Requirement 3:	☐	☐	☒	**Not Tested. Cardholder data storage in the systems is customers' own responsibility. No managed security and database services are included in the scope of PCI DSS assessment.**
Requirement 4:	☐	☐	☒	**Not Tested. Cardholder data transmission to and from the systems located in EBİ will be customers' own responsibility. No managed security and system configuration services are included in the scope of PCI DSS assessment.**
Requirement 5:	☐	☐	☒	**Not Tested. Malware protection for the systems is not included in the scope of PCI DSS assessment.**
Requirement 6:	☐	☐	☒	**Not Tested. No payment software development and patch management process is included in the scope of PCI DSS assessment.**
Requirement 7:	☐	☐	☒	**Not Tested. Only physical access controls are evaluated within the scope of the PCI DSS assessment. Other logical access control mechanisms are not included in the scope of assessment.**
Requirement 8:	☐	☐	☒	**Not Tested. Username, password and account management is not included in the scope of PCI DSS**

				assessment.
Requirement 9:	☐	☒	☐	**9.8.1 - Not applicable. There is not a process in the company to get hardcopy documents of cardholder data in the company.**
Requirement 10:	☐	☐	☒	**Not Tested. Audit trails and log management is not included in the scope of PCI DSS assessment.**
Requirement 11:	☐	☒	☐	**11.2-6 - Not Tested. Security tests, IPS and FIM are not included in the scope of PCI DSS assessment.**
Requirement 12:	☐	☒	☐	**12.10.5 - Not applicable. Alerts from security devices including IDS/IPS and centralized log servers are continuously monitored. But these services are not in the scope of the assignment.**
Appendix A:	☐	☐	☒	**N/A**

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:	*27.February.2015*	
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

Based on the results noted in the ROC dated *27.February.2015*, 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 as of *27.February.2015*: ***(check one):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Eczacıbaşı Bilişim Hizmetleri A.Ş. (EBİ)* 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 *3.0*, 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

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* **27.February.2015**
Service Provider Executive Officer Name: **Atilay Yilmaz**	*Title:* **Project and Quality Systems Manager**

Part 3c. QSA Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	*On-site assessment*

Signature of QSA ↑	*Date: 27.February.2015*
QSA Name: Onur Arikan	*QSA Company:* Biznet Bilisim

Part 3d. ISA Acknowledgement (if applicable)

If an ISA was involved or assisted with this assessment, describe the role performed:	

Signature of ISA ↑	*Date:*
ISA Name:	*Title:*

[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	☒	☐	Not Tested
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	Not Tested
3	Protect stored cardholder data	☒	☐	Not Tested
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	Not Tested
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	Not Tested
6	Develop and maintain secure systems and applications	☒	☐	Not Tested
7	Restrict access to cardholder data by business need to know	☒	☐	Not Tested
8	Identify and authenticate access to system components	☒	☐	Not Tested
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	Not Tested
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐