Abstract

This document includes the statement of Georgian Card JSC about the proposals to purchase the product (including services). Document includes procurement’s procedure, where the requirements may be described in terms of conceptual principle (in general), but also with functional and result-oriented specifications – without mentioning a specific way (detailed technical specifications) to achieve the desired result

Details

Tender #19 Announcement Date: 6/20/2023

End Date: 6/28/2023

Security assessment against pci DSS and PCI PIN standards’ requirements

Request for Proposal

Contact Information

Mariam Tabatadze

tenders@gc.ge

+995 577 331197

Contents

[INTRODUCTION 2](#_Toc130831590)

[Purpose 2](#_Toc130831591)

[Briefly about our Georgian Card JSC 2](#_Toc130831592)

[Scope of Work 2](#_Toc130831593)

[REQUIREMENTS 3](#_Toc130831594)

[DELIVERABLES 3](#_Toc130831595)

[INFORMATION REQUEST 3](#_Toc130831596)

[DISCLAIMER 4](#_Toc130831597)

[EVALUATION CRITERIA 4](#_Toc130831598)

[PROPOSAL SUBMISSION 4](#_Toc130831599)

[Assignments description 5](#_Toc130831600)

[Attached documentation 5](#_Toc130831601)

[Appendix 1: – Price List 6](#_Toc130831602)

[Appendix 2: Bank Details 7](#_Toc130831603)

[Appendix 3: Solution/Service characteristics 8](#_Toc130831604)

# INTRODUCTION

Purpose of this document and therefore tender, is to select service provider for Georgian Card JSC (one of the biggest card payment processing center in Georgia), which will provide assessment services against PCI DSS and PCI PIN security standards’ requirements.

## Purpose

As a Level 1 Service Provider and VISANET Processor, Georgian Card JSC is willing to perform onsite or remote security assessment against PCI DSS and PCI PIN security standard requirements. As a result, we have decided to conduct market research in order to evaluate possible partnership in the scope of PCI DSS and PCI PIN security standards requirements assessment.

In this regards, we are looking for the interested VISA Approved Security Assessor (SA), 3DS Assessor (3DS), Qualified PIN Assessor and Qualified Security Assessor (QSA) companies. We are free to discuss the details regarding PCI DSS, PCI PIN and other PCI family standards (in specific PCI 3DS, PCI CP) for possibility of future cooperation.

## Briefly about our Georgian Card JSC

Georgian Card JSC is the leading service operator of the payment business, providing the service to the companies in Georgia since 1997. Until today, Georgian Card retains its position of the market leader: processing up to 200 operations per second for 1000 ATM-s, more than 10000 POS terminals and more than 3000 Self-Service terminals.

## Scope of Work

The bidder shall conduct an assessment of Georgian Card JSC’s Cardholder Data (CDE) and PIN/KEY Management environments against the PCI DSS and PCI PIN security standards.

Furthermore, The Bidders shall be able to provide internal/external Vulnerability Scanning and internal/external Penetration Testing services, Vulnerability Assessment and Manual Risk Ranking services/tools.

Vulnerability Assessment and Manual Risk Ranking must be compliant with PCI DSS Requirement - 6.3.1, and must provide ability to: manually assign criteria for ranking vulnerabilities that may include criticality of a vulnerability identified in an alert from Forum of Incident Response and Security Teams (FIRST) or a CERT, consideration of the CVSS score, the classification by the vendor, and/or type of systems affected.

The assessment and other security services or tools shall include the following:

**PCI DSS**

* Review of the Cardholder Data environment architecture, configuration, and documentation.
* Assessment of the Cardholder Data environment against the PCI DSS requirements.
* Identification of any gaps or deficiencies in the Cardholder Data security controls implementation.
* Remediation guidance to address any identified gaps or deficiencies.
* Comprehensive and user friendly compliance management portal, that allows:
  + Upload Business as Usual (BAU) security action items needed for compliance;
  + Ability to export previously uploaded action items with associated files and comments;
  + Dashboard based compliance status monitoring;
  + Retrieve remediation advisory documents associated with services provided;
  + Submit disputes for results of services provided;
  + Retrieve certificates of completion for services provided.

**PCI PIN**

* Review of the PIN/KEY Management environment architecture, configuration, and documentation.
* Assessment of the PIN/KEY Management environment against the PCI PIN requirements.
* Identification of any gaps or deficiencies in the PIN/KEY Management security controls implementation.
* Remediation guidance to address any identified gaps or deficiencies.
* Comprehensive and user friendly compliance management portal, that allows:
  + Upload Business as Usual (BAU) security action items needed for compliance;
  + Ability to export previously uploaded action items with associated files and comments;
  + Dashboard based compliance status monitoring;
  + Retrieve remediation advisory documents associated with services provided;
  + Submit disputes for results of services provided;
  + Retrieve certificates of completion for services provided.

**VULNERABILITY ASSESSMENT**

* Ability to conduct Authenticated Vulnerability Scanning, Vulnerability Scoping, Vulnerability Assessment, Risk Assessment (ID, Rank), Prioritization, Remediation Advisory and Reporting Services of internal network.
* Ability to conduct Authenticated Vulnerability Scanning, Vulnerability Scoping, Vulnerability Assessment, Risk Assessment (ID, Rank), Prioritization, Remediation Advisory and Reporting Services of external network.
* Ability to conduct Authenticated Vulnerability Scanning, Vulnerability Scoping, Vulnerability Assessment, Risk Assessment (ID, Rank), Prioritization, Remediation Advisory and Reporting Services of web applications.
* Ability to conduct Network Segmentation Testing, Gap Assessment and Remediation Advisory Services of network segregation.
* Ability to provide and maintain comprehensive Vulnerability Assessment and Management tool, which supports manual risk ranking.
* Must be listed as an ASV (Approved Scanning Vendor) for external vulnerability scanning service, to validate adherence with the external scanning requirements of PCI DSS Requirement 11.2.2.
* Ability to provide reporting on any of the above services necessary to meet applicable PCI DSS vulnerability identification, assessment, manual risk ranking and general management reporting requirements.
* Ability to provide an online portal that allows user access to:
  + Initiate internal and external scans on demand;
  + Schedule internal and external network scans;
  + Retrieve internal and external network scan results;
  + Retrieve remediation advisory documents associated with services provided;
  + Submit disputes for results of services provided;
  + Retrieve certificates of completion for services provided.

**PENETRATION TESTING**

* Ability to conduct Penetration Testing, Finding Assessment and Remediation Advisory Services of internal network.
* Ability to conduct Penetration Testing, Finding Assessment and Remediation Advisory Services of external network.
* Ability to conduct Penetration Testing, Finding Assessment and Remediation Advisory Services of web applications.
* Preferable, if service provider is listed as a crest-certified (crest-approved) penetration testing service provider.
* Ability to provide reporting on any of the above services necessary to meet applicable PCI DSS penetration testing and finding assessment reporting requirements.
* Ability to provide an online portal that allows user access to:
  + Book internal and external penetration testing on demand;
  + Schedule internal and external penetration testing on demand;
  + Retrieve internal and external penetration testing results;
  + Retrieve remediation advisory documents associated with services provided;
  + Submit disputes for results of services provided;
  + Retrieve certificates of completion for services provided.

# REQUIREMENTS

In order to qualify for the review, the bidder must meet all the requirements listed below:

* Must be listed as a PCI DSS and PCI PIN Assessor (in the corresponding online listing).
* Must be able to conduct onsite or remote (if pre-agreed and pre-approved) PCI DSS and PCI PIN assessment against latest versions of the standards mandated by PCI SSC.
* Must be able to conduct onsite or remote (if pre-agreed and pre-approved) PCI DSS assessment 5 (five) times in a raw starting from year 2023.
* Must be able to conduct onsite or remote (if pre-agreed and pre-approved) PCI PIN assessment 2 (two) times in a raw starting from year 2024.
* Must be able to provide consulting in the scope of PCI DSS, PCI PIN and other PCI standards family (in specific PCI 3DS, PCI CP).
* Must be able to issue RoC and AoC that are acceptable by all brands, included but not limited to VISA, MASTERCARD and AMERICAN EXPRESS.
* Must be able to negotiate compliance confirmation with payment brands, included but not limited to VISA, MASTERCARD and AMERICAN EXPRESS.
* Must be able to conduct assessments in region of Georgia.
* Must be able to start assessment within 14 (calendar days) from the formal written notice from Georgian Card JSC.
* Must not face insolvency proceedings and must not be in the process of liquidation / reorganization.
* Must have at least **5** (**five**) years of experience in providing similar services.

# DELIVERABLES

The bidder shall provide the following deliverables:

* PCI DSS Assessment report detailing the results of the assessment and any identified gaps or deficiencies.
* PCI PIN Assessment report detailing the results of the assessment and any identified gaps or deficiencies.
* Vulnerability Assessment report detailing the results of the assessment and any identified gaps or deficiencies.
* Penetration Testing report detailing the results of the assessment and any identified gaps or deficiencies.
* Segmentation Testing report detailing the results of the assessment and any identified gaps or deficiencies.
* Remediation guidance report detailing the actions required to address any identified gaps or deficiencies.
* Final report detailing the results of the remediation efforts.

# INFORMATION REQUEST

In order to qualify for the review, the bidder must provide following information:

* General overview of the company:
  + Short history of the company (presentation).
  + Number of clients.
  + Experience (list of verifiable projects in the scope of PCI DSS, PCI PIN and other PCI standards family).
  + Number of successful assessment.
  + Number of clients that are currently using or previously used vulnerability assessment and penetration testing services.
  + Contact information for three references from previous PCI DSS and PCI PIN assessment clients.
  + Contact information for three references from previous Vulnerability Assessment and Penetration Testing clients.
  + CV of assessor(s).
  + Regional presence for Georgia (or country from which account manager will be assigned to Georgian Card JSC).
* Description of onsite and remote assessment process:
  + PCI DSS Assessment methodology.
  + PCI PIN Assessment methodology.
  + Penetration testing methodology.
  + Vulnerability assessment methodology.
  + Service portal demo.
  + Assessment timeline.
  + Information about pre-engagement work (that must be completed by Georgian Card JSC).
* Budgeting:
  + Assessment service price for PCI DSS.
  + Assessment service price for PCI PIN.
  + Assessment service price for internal and external Network vulnerability.
  + Assessment service price for internal and external Web Application vulnerability.
  + Segmentation testing service price for internal and public facing Networks.
  + Penetration testing service price for internal and external Networks.
  + Penetration testing service price for internal and external Web Applications.
  + Price of any additional services, included but not limited to assessment services of PCI family standards (PCI 3DS and PCI CP), incident response, security operations center or any other managed security services that can be related to the proposed scope.
  + Any additional costs, included but not limited to travel, accommodation.

# DISCLAIMER

The announcement of the tender does not oblige Georgian Card JSC to sign a contract with any of the participants and at any stage of the tender Georgian Card JSC reserves the right to terminate the tender without disclosing reason to any of the bidders.

# EVALUATION CRITERIA

Proposals will be evaluated based on the following criteria:

* Experience and qualifications of the bidder and its personnel.
* Proposed approach to conducting the assessment.
* Cost of the service.
* References from previous clients.

# PROPOSAL SUBMISSION

Bidders must submit a proposal that includes the following:

* Bidders are obliged to provide the documents required by the tender requirements – to the contact person, indicated in this document;
* Additional information – if needed, should be obtained or clarified by contacting to the person – via e-mail or telephone, indicated on the cover page of this document;
* After the completion is over, the tender commission will review the bids and select the supplier with the best conditions;
* The bidder should submit the total price of the service;
* The bidder should submit a presentation of the proposed product (or service) and datasheet files;
* Proposal currency should be indicated in USD excluding VAT;
* All documents and information that should be submitted by the bidder must be certified with the signature and seal of the authorized representative;
* In order to participate in the tender, it is necessary for the organization to submit the following mandatory documents:
* Suggested price list (**Appendix 1**);
* Bank details (**Appendix 2**);
* Decision characteristics (**Appendix 3**) (only when needed and if not pre-filled);
* Extract from the Entrepreneurial Register;
* MAF [Manufacturer Authorization Form] that is given to resellers from manufacturer to prove that they are indeed partners accredited by the manufacturer (if applicable for the tender type);
* During the tender, bidder is obliged to submit an additional legal or financial document upon the request;
* The proposal must be valid at least for 90 calendar days.

# Assignments description

A detailed description of the subject solution/service characteristics is given in **Appendix 3** (only when needed and if not pre-filled).

# Attached documentation

* Appendix 1: Price list;
* Appendix 2: Bank details;
* Appendix 3: Product/Service characteristics.

### Appendix 1: Price List

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Quantity | Price | Service Delivery Date |
| Mandatory: Five Years (Five engagement) PCI DSS Security Assessment Service | 1 |  |  |
| Mandatory: Four Years (Two engagement) PCI PIN Security Assessment Service | 1 |  |  |
| Mandatory: Internal Network and Web Application Vulnerability Assessment Service | 1 |  |  |
| Mandatory: External Network and Web Application Vulnerability Assessment Service | 1 |  |  |
| Mandatory: Internal Network and Web Application Penetration Testing Service | 1 |  |  |
| Mandatory: External Network and Web Application Penetration Testing Service | 1 |  |  |
| Mandatory: Internal and Public Facing Network Segmentation Testing Service |  |  |  |
| Optional: Any other managed security service offered by bidder that can relate to proposed scope (such as Incident Response, Security Operations Center, etc…) | 1 |  |  |
| Optional: Any other managed security service offered by bidder that can relate to proposed scope (such as Incident Response, Security Operations Center, etc…) | 1 |  |  |

### Appendix 2: Bank Details

|  |  |
| --- | --- |
| Information about bidder organization | |
| Company Name: |  |
| Company Identification Number: |  |
| Company Business Address: |  |
| Address 2: (if different from above) |  |
| Manager Name and Surname: |  |
| Manager Identification Number (local bidders only): |  |
| Manager Phone Number: |  |
| Name and Surname of the contact person: |  |
| Contact Person Identification Number (local bidders only): |  |
| Phone: |  |
| E-mail: |  |
| Web-page: |  |
| Bank Name: |  |
| Bank Code: |  |
| Bank Account Number: |  |

### Appendix 3: Solution/Service characteristics

|  |  |  |
| --- | --- | --- |
| N | Solution (Service) Name/Description | Quantity |
| 1 | N/A | 1 |
| 2 | N/A | 1 |
| 3 | N/A | 1 |
| 4 | N/A | 1 |