Term of References
For
Acquisition of PCI DSS Certification for the National Switch
Payment switch at APS

Particular	Description
Position	Consultant services (Firm)
Selecting Organisation Name	Da Afghanistan Bank – Central Bank of Afghanistan
Address	Pashtoonistan Watt, Kabul, Afghanistan
Website	www.dab.gov.af
Telephone	+93 202510654
Fax	+93 202100305
Funding Agency	Payments Automation and Integration of Salaries in Afghanistan (PAISA) Project ID P168266 Grant No D4530AF
Contact Person	Abdul Qahir Sahak Deputy DG Financial Sector Strengthening Project Phone: +93744331010 E-mail: qahir.sahak@dab.gov.af

September 2020

INTRODUCTION

The objective of the Payments Automation and Integration of Salaries in Afghanistan (PAISA) Project is to support the development of digital government-to-person payments in Afghanistan. There are four components to the project:

- The first component being Biometric identification system for civil servants and pensioners. This component will support the biometric registration and issuance of a unique registration number (URN) to recipients of government salaries and transfers, which will be managed by NSIA.
- The second component is the integration of the identification, verification and payment systems. The component will focus on the integration of various systems playing different roles in the salary payments, process to achieve full-fledged straight-through processing (STP). This component includes two subcomponents: integration of public financial management infrastructure with digital ID and payments ecosystems, and integration of the national payment's infrastructure with digital ID Infrastructure.
- The third component is the expansion of financial services and access points. This component aims to ensure that, with the shift to electronic payments, civil servants, including those hither to paid by 'bonded trustees', and pensioners can either: (i) withdraw cash from their account from safe and convenient locations; or (ii) use their account balance to make cashless payments for goods and services.
- Finally, the fourth component is the project management. This component will be implemented by MoF and support the provision of resources to carry out the coordination, administrative, social and fiduciary aspects of the project. In line with new requirements at MoF, staffing needs have been estimated for the project life. This component will also finance the undertaking of surveys and other activities related to the monitoring of project outcomes.

The Payment systems play a critical role in supporting the financial and real economies. From a broader perspective, a less than optimal use of payment instruments and inefficient or poorly designated system to process these instruments may ultimately have an impact on systemic stability, economic development and growth. The Payment systems are moving from being a narrow channel for transferring funds to a much wider integrated network for transferring additional forms of value. The creation of networks and systems for retail payments can have a substantial role in supporting financial access in developing countries; and modern retail payment technologies an innovative program to channel recurrent payments efficiently can, and are already being used to, integrate the previously underserved an non-served population into the formal financial sector. A well-functioning infrastructure to efficiently and safely process modern payment instruments is necessary to adopt widespread use of modern payment systems.

A modernized national payments system is the cornerstone of the overall financial infrastructure in Afghanistan. Hence, in 2013 Da Afghanistan Bank procured and signeda contract for supply and installation of national card and mobile payment switch dated August 18, 2013 with Banking Production Centre (BPC of the Netherlands under the World Bank

funded Financial Sector Rapid Response Project (FSRRP) in Kabul and as per to the contract the national card and mobile payment switch was supplied, installed and implemented by BPC firm and APS office by end of 2015. Subsequently, the Service Level Agreement (SLA) for warranty services period was signed with BPC for support and maintenance of the national payment switch for three years (2017-2019) under FSRRP which has recently been completed by end of 31st December 2019; it is worth mentioning that in accordance to the technical requirements in original contract the APS payment switch need additional support and maintenance services during post-warranty period as well, which is part of the PAISA project procurement plan approved by the World Bank group for further process.

CURRENT STATUS OF APS

Afghanistan Payments System (APS) was initially inaugurated and found by Pashtany Bank, BMA and Ghazanfar Bank in 2011, which subsequently other banks such as Azizi and Islamic Bank of Afghanistan also received its full membership. In 2013, APS as the National e-Payment Switch of Afghanistan, received funds from World Bank (WB) through Da Afghanistan Bank (DAB).

APS is now operating under the umbrella of DAB and is playing a leading role in developing and modernizing the retail banking market in Afghanistan by providing innovative electronic and mobile payment services that help in enhancing the retail banking offerings in the country.

APS is offering e-Payment services by establishing interoperability and interconnectivity in the banking and payments ecosystems for all the state banks, private/commercial banks, microfinance institutions, mobile money operators and payment institutions across the country. APS launched a Domestic Card Scheme named AfPay with debit, credit and prepaid functionalities, and DAB mandated all financial institutions in Afghanistan to integrate with APS for establishing interoperable payment eco-system in or outside the country.

APS functions as a coordinating body bringing together all the member participants, adapting an industry collaborative approach to define payment services, common operating procedures, service levels and standards, as well as representing its member banks and partners in the international card associations and networks, principally in relation to the national payments matters.

Besides being the National e-Payments Switch of Afghanistan, APS is the first and only institution in the country that provides shared platform for electronic fund transfers within the boundaries for all the financial institutions (including banks and mobile money operators), as well as the retail businesses and general public.

APS Vision

“To deliver a shared interoperable retail e-Payment infrastructure, which provides a low cost, multi-channel switch for e-Payment processing & switching, merchant acquiring, card services and Mobile Financial Services for mutual benefits of all consortium members toward a cashless society”.

APS Mission

"To proactively encourage e-Payment systems for ushering in a cashless society in Afghanistan and to ensure e-Payment systems in the country are safe, efficient, interoperable, authorized, accessible, inclusive and compliant with international standards".

OBJECTIVE OF THE ASSIGNMENT

The overall objective of this TOR is to select a service provider to assist the APS for PCI QSA Compliance & PCI ASV Services, and PA DSS & PCI QIR Evaluation Services, as to maintaining high standards of quality and service.

All solutions must adhere to prevailing payment cards rules and regulations especially with the PCI DSS. So that to protect the cardholder data wherever it is processed, stored or transmitted. APS will achieve the following goals by implement PCI DSS:

- Boosting consumer confidence on card-based payments,
- Building and maintaining a secure network,
- Protecting cardholder data,
- Complying with and maintaining the most updated standards of PCI DSS and security policy,
- Implementing strong access control measures,
- Regularly monitoring and testing the networks,

SCOPE OF SERVICES

The provider will be required to provide all of the services listed in section A and B of this TOR that are requested by APS.

A. PCI ASV & PCI QSA Compliance Services

1. Provide PCI DSS validated internal network scanning, vulnerability assessments, and associated remediation advisory services.
2. Provide PCI DSS validated internal network penetration testing and associated remediation advisory services.
3. Provide PCI DSS validated external network scanning, vulnerability assessments, and associated remediation advisory services.
4. Provide PCI DSS validated external network penetration testing and associated remediation advisory services.
5. Provide PCI DSS validated web application vulnerability assessments and associated remediation advisory services.
6. Provide PCI DSS validated web application penetration testing and associated advisory services.
7. Provide PCI DSS validated network segmentation testing, vulnerability assessments, and associated advisory services.
8. Provide reporting on any of the above services necessary to meet applicable PCI DSS ASV reporting requirements.

9. Provide review of security policies related to PCI DSS Compliance.
10. Provide risk assessment advisory services.
11. Provide consulting and advisory services for the development and implementation of PCI environments, applications, and services.
12. Provide onsite and/or remote PCI training.
13. Provide any other QSA services necessary to conform to PCI standards and approved by the APS that are not specifically mentioned in this TOR.
14. Submit ROVs to the PCI Security Standards Council ("PCI SSC") for approval.
15. 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.

B. PCI QIR Evaluation & PA DSS Services

1. Provide PA DSS gap analysis.
2. Provide PA DSS onsite compliance audits to ensure sensitive data is secure as it is stored, processed, and transmitted by payment applications.
3. As part of PA DSS onsite compliance audits, create a formal PA DSS Report on Validation (ROV) including an Attestation of Validation.
4. Provide sufficient and adequate documentation within the Report on Validation (ROV) to demonstrate the payment application's compliance with PA-DSS.
5. Review security policies to ensure compliance with PA DSS standards and requirements.
6. Conduct formal PA DSS assessments that verify the PA-DSS payment application is properly configured and securely implemented, in accordance with PA DSS requirements.

SELECTION CRITERIA

- Provider must be certified by the appropriate governing body to provide PCI DSS ASV services, PCI DSS QSA services, PA DSS services, P2PE Encryption Assessment services, and/or PCI QIR Evaluation services, as applicable.
- All PCI-related services provided by provider must adhere to the most current version of the relevant PCI standard

End