PROJECT **: Development and Installation of MARINA System for the Issuance of Seafarer Identity Document (SID)**

DATE : 23 November 2015

Technical Specifications Checklist

Technical Specifications per TOR	Comply	Not comply
1. The bidder should propose an end-to-end process consisting of the following modules and functions/features:		
a. Application Capturing & Biometric Enrollment System		
▪ Ensures that seafarer's image and fingerprints are successfully verified before the enrolment is considered complete		
▪ Support most industry popular fingerprint scanners, flatbed scanners, and digital/web cameras		
▪ User friendly fingerprint and photo capturing unit		
▪ Auto and manual capture modes		
▪ Auto and manual verification modes		
▪ Automated Image quality Check		
▪ Automated finger sequence check		
▪ Support enrolment of flat fingerprints		
▪ Automated facial image tokenization to meet ICAO Standard Specification		
▪ Conforms to ILO, ISO and ICAO standards for biometric data format.		
▪ Data check with look-out-list (LOL)		
▪ Can function as both enrollment and releasing		
▪ Manage secure data transmission		
▪ Should support both desktop and laptop platforms and can both coexist in a networked environment or in isolation.		
b. Application Processing, Verification and Automated Biometric Identification System (ABIS) Overview		
• Performs data processing and verification against data collected from applicant. All collected data should be shown on a screen which is visible to the seafarer and the errors recognized by the seafarer shall be corrected before the enrolment is complete.		
▪ Ensures that seafarer's image and fingerprints are successfully verified before the enrolment is considered complete		
• Produces a clean seafarer database, free from duplicates or double registration.		

• Allows concerned MARINA official to review on screen all the data collected from seafarers and determine whether or not to issue the SID		
c. Data Preparation & Personalization System		
• Provision of a Self Signed Public Key Infrastructure System. The system should be ready for future registration with the Public Key Directory (PKD) system if so decided by MARINA.		
• Performs data grouping and formatting according to the data structure specified for ILO C185 compliance		
• Generates personalized chip loading scripts and ready for SID card personalization		
• Supports personalization and printing of the SID cards done in a VISA or Mastercard Certified Card Manufacturing and Personalization facility.		
d. Quality Control and Issuance		
• The SID should be issued to the applicants after a successful personalization, printing and quality checking.		
e. Reporting and Verification System		
• Includes generation of reports, query and verification module for issued SIDs/SIRBs.		
2. System Technical Requirements		
a. Creation of a National Electronic Database that contains the information of all national seafarers, . fully compliant to all the requirements as stated in Article 4 and Annex 2 of the Convention		
b. Provision of a web-based query system to allow authorized users to access the details contained in the National Electronic Database for SIDs and a separate web-based query for the SIRBs.		
c. Inclusion of terminals with verification system to allow seafarers to verify their biometrics contained in the issued SID and view all the other information in the national database		
d. Flexible information systems responsive to operation changes		
e. Sustainability and system maintainability		
f. Seafarer Data Capture Application requirements		
▪ Data Capture System shall have plug-and-play support for commercially available data capture peripherals (e.g. Digital Cameras, Fingerprint Scanners, Signature Pads). ▪ Provision of the list of detailed peripheral/hardware		

which are supported by the system. It shall ensure that the data capture application shall be updated regularly to support new peripherals.		
▪ Photograph ➢ Data capture application should support commercially available digital camera for photo capturing. ➢ It should provide functions such as: to crop the desired photo area and return the photo image to the calling program, automatic cropping of photo image compliant with ICAO standards, automated image enhancements; support multiple output file formats including JPEG, Windows BMP, TIFF, etc, and configurable JPEG compression quality		
▪ Seafarer's Signature - The data capture application should be able to display and save the signature written by the applicant on the signature pad and should crop out white space around the rectangular border of the signature		
▪ Fingerprints - The data capture application: ➢ should identify and pinpoint the core and details of the fingerprint image taken ➢ Incorporate a quality indicator ➢ Incorporate a date stamp on the fingerprint images taken ➢ Facilitate the capture of the fingerprint with the correct orientation and ensure that the ridges and core position are clearly visible on the display ➢ Have the ability to capture images from different fingerprint sizes ➢ Support image enhancement ➢ Capture fingerprint images at a resolution of at least 500 dpi ➢ Capture fingerprints as uncompressed raw images of 512x512 size and 256 grayscales; ➢ Have the ability to capture fingerprint images clearly and not be affected by defects of the epidermis (outer skin); ➢ Allow for real-time on-screen preview of the fingerprint images while performing the fingerprint capture ➢ The data capturing application shall be able to produce output fingerprint images stored in an open format and the image format shall not be		

proprietary ➢ The fingerprint images for storage shall be compressed using FBI's Wavelet Scalar Quantization (WSQ) fingerprint compression algorithm of at least 15:1 compression ratio.		
• Personal Informaton		
• Scan Supporting Documentary Requirements		
• The Biometric Data Capture Machines should be equipped with the following:		
➢ field proven data capture application which has enrolled at least 1M persons used by any government agencies / entities.		
➢ field proven identity management system which has managed over 1M records used by any government agencies / entities.		
➢ a complete matching solution based on field proven matching technologies used by any government agencies / entities.		
• Biometric Identification Requirements		
➢ Facial Recognition ❖ Should be compliant with ISO/IEC19794-5 ❖ 1:N and 1:1 Matching of Photos for Enrollment and Verification ❖ Proven track record on matching accuracy based on NIST Face Recognition Vendor Test (FRVT) using at least 1M records ❖ False Negative Identification Rate (FNIR) shall be less than or equal to 0.45 based on NIST's FRVT of 2013.		
➢ Fingerprint Recognition		
❖ Should be compliant with ISO/IEC19794-4 ❖ 1:1 Matching of Fingerprints for Verification. The verification application shall allow the user to set threshold value for performing 1:1 matching. The bidder shall advise on the threshold value to be set.		
g. System Architecture and Application		
• The System should have an open architecture to ascertain the following:		
➢ Open system – the System should be based on open standards preferably on a Service Oriented Architecture (SOA) with no proprietary hardware in order to prevent vendor lock-in.		
➢ Modular design – software must be built-up in a modular fashion. Such that, if there are upgrades or fixes, only the affected module		

needs to be addressed.		
➢ Alterations to the workflow should be configurable without the need to rewrite major portions of the applications or services		
➢ International open standard format for biometrics – Biometrics information should be stored according to international standards		
➢ Flexible Architecture – Architecture should allow biometrics matching vendors to be changed without having the need to recapture existing biometric data		
➢ Upgradeable Architecture – Architecture should allow addition of new biometrics matching system without major impact on both front-end data capture and backend processing		
➢ The system data schema for biometric and biographic data fields should be fully configurable on startup and during subsequent operation.		
➢ Data management capabilities for archiving of data should be provided.		
➢ An event records of all business events should be provided		
➢ A tamper environment audit trail of all transactions should be provided.		
h. The Bidder shall supply and configure a Commercial off the Shelf (COTS) product based on the identity management system with a proven track record and published product roadmap.		
i. Should not be based on a proprietary hardware platform		
j. The proposed System should:		
• Achieve high matching speeds using an array of servers as matching engine processors. Matching performance should increase when hardware performance is increased		
• Ability to scale-up the System by simply adding additional processors. The newly added processor can be a different model from the existing processors, thus allowing the System to leverage on the more powerful processors that will be available in the future.		
• Advanced load balancing technique to ensure even distribution of matching operation to all available matching processors, to achieve shortest search time.		

• Automated search tasks scheduling with priority control and on-line monitoring facilities		
• The System should include a hit list management component for the processing of duplicate records.		
• The System should be fully compliant with BioAPI 2.0 (ISO 19784-1:2006)		
k. High Availability: • Provision of adequate hardware equipment for backup purposes at key steps in the workflow in order to guarantee required output volumes and smooth operation of the system.		
• A clear and detailed proposal on risk management and business continuity plan should be included. • The critical servers should be designed with high availability to ensure public services will not be disrupted due to single server failure.		
l. The proposed System should have a flexible and scalable system configuration		
• Flexible System Configuration – support many hardware and software options, such as database options, fingerprint livescan devices, network printer, etc. Client can choose the appropriate servers and workstation products to best meet the project requirements at multiple production sites, from time to time.		
• Allow scaling of system both vertically and horizontally to cater for future system growth.		
• Options for phased hardware deployment to minimize initial investment on hardware.		
m. The proposed System should be highly secured and reliable through implementation various security features and strict compliance to relevant security guidelines:		
• End to end security of data transmitted over WAN with encryption and digital signatures		
• Application level data encryption is possible for data transfer over network and sensitive databases. All Encryption support functions including key revocation, key change and key length should be configurable.		
3. Good and Services		
a. Hardware Products		
Supply of hardware per Annex “1” and specifications in Item 5.6 of the TOR		
b. Software Products		

• Advanced Server Operation System compatible with network and domain management functions, database server applications, web server, active directory services, messaging system and multi-protocol routing capabilities.		
• Database system developed specifically for large enterprise databases. Offer replication in a number of models: snapshot, transactional and merge. Must have adequate security for government applications.		
• Professional edition/full product version operating system license bundle of the latest operating system platform, compatible with database applications and software packages for workstations.		
• All software components required for a system of data capture, facial recognition and fingerprint matching and production and issuance of SID and SIRB which is fully compliant with all the requirements of ILO Convention No. 185 and ICAO Document 9303 and its Supplements.		
• Data capture application software which is based on the Commercial Off the Shelf (COTS) product with a proven track record and published product road map and should have the following capabilities:		
➢ Support device for biometric modality (facial and fingerprint) ➢ Able to perform fingerprint quality check ➢ Capture Signature ➢ Able to capture a pre-defined number of documents via a scanner. ➢ This proof of identity documents which should be scanned and the combination of documents should be configurable as a scanning business rules. ➢ End to end security with encryption when transferring captured data to central server for storage ➢ Able to perform 1:1 fingerprint matching		
c. Networking Products		
• Switches • Routers • Firewall/VPN • One (1) year internet connectivity (at least 20 Mbps) for MARINA Central Office and (at least 3 Mbps) for		

the 11 Regional Offices sufficient to provide real time connectivity for SID and SIRB issuance		
d. Physical set up and commissioning of an ICT and ICT-related infrastructure • setting up of a server room • structured cabling • network installation • ISP connection facility		
4. SID SPECIFICATIONS		
a. Card manufacturing and personalization facility per detailed specifications in Item 6.1 of the TOR		
• Visa or Mastercard certified manufacturing plant in the Philippines • In the business of card manufacturing for at least 5 years • Centralized personalization with minimum capacity of 7,000 cards per day • No net loss in the last 3 years to ensure that they are financially capable to deliver the SID cards on the required duration of the project. • No recorded significant delay in the implemention of any government project for the last 5 years.		
• 400,000 MARINA SID Cards with contactless chip with detailed specifications and requirements under Item 6.2 of the TOR including the Track Record of satisfactory performance or delivery on at least 2 national ID or electronic passport projects with at least 1 M documents issued per project for the last 3 years.		
b. Physical Card Security Features specified in the TOR		
c. ID design and printing of variable information		
d. Chip encoding of ICAO compliant data		
e. No export of sovereign data outside of the Philippines		
5. MARINA's ownership of the system after the completion of the project		
6. Maintenance and support should be included (in the duration of the proposal) until five (5) after acceptance		
7. Commitment for Future System Expansion and Technology Upgrade		
8. The Bidder shall provide the following deliverables: • Project Plan • Monthly Progress reports • Final Requirements Specifications (after confirmation) • Final design document • Acceptance test specification and procedures		

• System Software Source Code • Hardware devices • Training materials • System Software Documentation		
9. User’s Training		
10. Full Documentation (soft and hard copies)		