AMIR E-government IQC

- Statement of Work -

Task Order 7: E-Government Architecture & Design for the SGN, email, & Web Environment

Vendor: STS

Client Agency: Ministry of Information and Communications Technology, e-Government Programme Management Office (MoICT/PMO)

Client Project Manager: Mr. Fadi Mari, Egov Project Manager and Mr. Nour Bani, Egov Consultant

Background

The AMIR program has committed to assisting the Government of Jordan (GoJ) in creating an e-government portal. The primary purpose of the GoJ portal is to create a central point of access to information and services that the GoJ makes available on-line, either via the Internet, or on the government's Secure Government Network (SGN). The reader is strongly urged to read the "E-Government Portal Web Site Scope and Vision Document" for background. The detailed analysis in that document will not be repeated here.

The AMIR 2.0 program has contracted EDS to source and install the SGN and E-mail hardware and software, EDS is cooperating with STS in order to accomplish this task, AMIR also contracted with five technology firms under its E-Government Indefinite Quantity Contract (IQC). Given the size of the overall E-Government Portal Web Site project, the wide variety of tasks, and the deadline under which the work must be completed, all five IQC firms are assigned an important piece of the portal work. Estarta is assigned the portal coordination role, Information architecture design and search engine, STS is assigned the enterprise directory, personnel and organization directories, CNS is assigned the G2G site, ITG is assigned the G2B site and Alliedsoft is assigned the G2C site. AMIR is counting on all five firms to adopt a cooperative approach, which is critical to the success of the overall project.

Introduction

This task order has been issued by the AMIR program to acquire Architecture & Design services for the E-Government SGN, email, & Portal web environment. The Vendor is to perform on the activities, and produce the deliverables, as detailed in this Task Order. Yet, the Vendor is also expected to utilize, & expand on, whatever Designs/Architectures & Documentation already created by the previous Architecture Owners & those of which are available to AMIR & at MoICT.

This Task Order describes these tasks:

Phase A: Architecture & Design (First 2 months)

- Overall E-Government Data Center (SGN, email, Portal) architecture & design.
- Coordinate with the Portal coordinator to Configuration & infrastructure implementation of the Data Center environment as per the requirements of the design.

- Prepare the Operations Center environment for applications deployment.
- The overall architecture & design of the E-government Web Portal environment, including determining the best method for hosting the CMS & its Web/Production & Staging/Development Environments.
- Liaise with Portal Coordinator the CMS configuration & implementation, Including High-level Architectural & Design concepts & constraints.

Phase B: Maintain & Operate the Data Center & Change Management

- Supervise the overall E-Government Portal system implementation.
- Maintain the Data Center
- Operate & Manage the Data Center
- Change Control & Quality Control Management.
- Hand-Over & Training to eventual Team in Charge
- Recommend the first iteration of a new or enhanced architecture designed to meet requirements

The two phases encompassed will take place over a combined period of 5 months with Phase A and B overlapping during the third month.

Overall SGN, email,& Portal Architecture & Design ownership

The task order requires the Vendor to analyze key inputs including current data center strategies, architecture, requirements, performance, operations and procedures, costs, constraints and risks. Based on an understanding of these areas, the Vendor will work with AMIR to develop relevant options for the network design. These designs will take into consideration appropriate technologies and standards, Enterprise portal Architecture Scope, recognized E-Government applications needs, today and future, as referred to in Roadmap & Blueprint.

The overall objective is to develop an architecture & design that meets the e-government applications and technology requirements as specified today, and which can adapt to meet future requirements as recognized from provided references.

The vendor is also responsible for filling the role of the web environment Architecture Owner, insuring that the Architecture as a whole fits within the Guidelines & Plans of the immediate needs and longer-term E-Government infrastructure & directives. The Vendor should also provide guidance to harmonize architectural approaches of those firms when necessary, and reporting to Client Agency Project Management and to AMIR staff if integration or compatibility problems arise.

Following is a highlight of the tasks to be performed to produce the new architecture:

- Identify service level requirements

- Assess Current Architecture capability to meet those requirements, including people, processes, and technology
- Examine any recommended architecture
- Refine the architectural approach that will best meet needs, addressing service level requirements across system layers and tiers
- Enumerate gaps
- Review best practices
- Provide recommendations
- Provide a high-level plan for realization of the infrastructure

Key activities of Architecture & Design Ownership include, but may not be limited to:

The following baseline activities will be performed for the overall Data Centre infrastructure, which may include, and may not be limited to, the following:

- Assessment of Current Design and Needs Analysis.
- Gathering the requirements and capacity planning
- Planning for high availability, load balancing, scalability and failover
- Architecting & Designing the New Data Center & SGN (Network & Servers).
- Architecting a tiered architecture for adding capacity on demand
- Site Preparation Recommendations, Considerations, & Review.
- Configure, and Deploy the Data Center and SGN including, & not Limited to:
    - Physical & Logical Architecture,
    - Network Addressing (IP schema and planning).
    - VLAN configuration & implementation
    - Network Management configuration,
    - Routing/Switching,
    - Firewalls,
    - VPN (Zoning),
    - RAS
    - Load Balancing
    - Hardware Systems & Operating Environment
    - Hardened / Operating System
    - Databases
    - Web & Application Servers
    - IDS
    - Backup & Storage
    - Disaster Recovery strategy

  - Integrating with existing design
  - Backup and Restore strategy
  - Constant tuning and screening of problems in system
  - Monitor Performance of Architecture
  - Routine maintenance plans
- Architecture & Design Of Enterprise Portal Web Environment (Hardware, Software Platform licenses, Databases, WebServers, AppServers, … etc.)
- Define & Document Portal Web Environment Platform (Hardware/Software) Requirements
- Recommendation on Production Application Design & Development Best Practices & Standards, forming a guideline for any future expansion & development.
- Develop a Security Policy
- An interoperability plan that describes how the infrastructure sub-systems meet the interoperability requirements of the portal web sites; the government-wide email system; authentication for the CMS, G2G site and other GoJ on-line applications; the Personnel Directory, and the Organization Directory.
- Post implementation assessment & Security Policy Review.
- Post implementation Backup Policy Review
- Overall Data Center & SGN Maintenance Services.
- Overall Data Center & SGN Operation & Management Services.

Key Deliverables of Architecture & Design Ownership include, but may not be limited to:

The following lists Key deliverables that are expected to be the product of all the activities detailed in this task order. Such deliverables may include, and may not be limited to, the following:

- Overall SGN Implementation Plan.
- Overall Architecture & Design Documentation.
- Overall Configuration Document customized to reflect GoJ SGN Configuration (H/W & S/W)
- Define & Document Overall Test Plan and Acceptance Procedures & Criteria.
- An acceptance test form, representing results of the functional tests.
- Define & Document Overall Reliability/Availability Considerations & Measures
- Define & Document Overall Security Policy.
- Define & Document Overall Security/Privacy Considerations, & Measures.
- Define & Document Overall Naming/Password Standards & Policies.
- Define & Document overall Authentication/Authorization Standards & Policies.
- Define & Document Capacity Planning & Storage Sizing for current phase and future phases needs.

- Define & Document overall Administration & Operational Procedures & Guidelines
- Define & Document Overall Backup Policy.
- Define & Document overall Maintenance Plan & Guidelines
- Define & Document Hand-over (& Training) Plan
- Define & Document Change Control/Management Procedures
- Define & Document Quality Control/Management Procedures.

Implementation Services Activities in Detail - Architecture & Design Ownership:

The following baseline categories, & its relevant procedures, will be performed for the overall SGN, email & Portal environments. These categories include, but may not be limited to:

- Network Implementation Service
- Intrusion Detection System Implementation Service
- Hardware & Operating System installation Service
- Database Cluster Implementation Service
- Security Policy & Firewall Implementation Service
- Web/Application Server Implementation Service
- CMS Implementation Service in coordination with the portal coordinator
- Backup implementation Service

Network Implementation Service

The following baseline procedures & activities will be performed for the production site network infrastructure, which may include, and may not be limited to, the following Components:

- Load balancing switches (Production systems) if needed
- Load balancing switches (CMS systems) if needed
- VPN/RAS/RADUIS
- 2nd-Level/Back-end Firewalls
- Backend Core switches
- Management System
- Cards & Fabrics for existing environment

Installation and Configuration - STS will perform the following installation and configuration tasks:

- Implement the VLANs as per the requirements of the design.
- Implement security policy & firewall rules in load balancing equipment.
- Implement Virtual IP Addresses and Server Load Balancing groups, as specified by the design.
- Implement Network Address Translation, if required and as specified by the design.
- Configuration of Servers supplied with this solution, to enable NIC failover as required by the design.
- Configuration of Trunk Ports as required by the design.
- Re-configuring the existing hardware supplied by first stage, if needed by the data center expansion design.

Implementation Testing - STS will setup and conduct functional testing to verify the following:

- VLAN configurations are correct.
- Inter-VLAN communication is working as required by the design.
- Server Load balancing is working as required by the design.
- Secure separation of VLANs, Back-end, Internal Customer Network & Operations Centre has been achieved.
- Correct operation for each fail-over scenario identified in the detailed design. i.e. where protection against a single point of failure is to be provided, it will be tested to demonstrate it works correctly.
- Correct operation of each service that is delivered through the VSDN infrastructure.

Hardware and Operating System Installation Service

The following baseline procedures & activities will be performed for the production site hardware infrastructure, which may include, and may not be limited to, the following Components:

- Backup Solution Components
- Storage Solution Components
- Web Environment Components
- CMS Staging/Development Components in coordination with the portal coordinator
- OpSys for Microsoft/Solaris/Linux Servers

Installation and Configuration - STS will perform the following installation and configuration tasks:

1. Rack mount all computer systems included in the scope of this phase.
2. Integration of the new hardware and storage with the existing setup and network infrastructure
3. Scaling up the exiting storage hardware and reconfigure the storage to fit the new requirement
4. Power up and run hardware diagnostics on all computer systems included in the scope of this phase. Successful completion of this step demonstrates that there are no hardware failures in the configuration.
5. Install operating system on all computer systems included in the scope of this phase. Then bring the hardware and operating system up to the latest engineering revision by the application of all required software patches and firmware revisions.
6. Backup software installation and testing.
7. Performance Tuning and Optimisation of the operating environment
8. Applying required Patches to the operating environment
9. Hardware and Software implementation services
10. Storage Implementation Services
11. Integration & Collaboration Services
12. Security and Backup services

Implementation Testing

1. Run testing on all computer systems to demonstrate that all hardware is working under operating system control.
2. Perform backup/restore procedure to authenticate the process
3. Testing connectivity within the LAN and Storage box

Security Policy and Firewall Implementation Service

This includes the design and delivery of a security policy document, detailing the traffic rules for the firewalls and load balancers within the solution, including the rule set for the operations centre and development environment. After completion of the document, firewall and load balancers packet filtering will be implemented for the production system, operations and development environment security implementation.

Security Policy Creation – The following Tasks will need to be conducted before devising a Security Policy;

- Construct a data flow analysis that develops the threat profile and trust model
- Review existing server configuration
- Identifying security requirements which may include, and may not be limited to :
  - access control
  - authentication and authorization
  - privacy
- Capture needs and uses for the application and services intended for the server

Installation and Configuration - STS will perform the following installation and configuration tasks:

1. Develop a security policy document for the production, operations centre and development sites, including rules and policies for:
   – Firewalls
   – Load Balancers
   – Operating system hardening for the desired servers
   – Authentication & Access Control
2. Install firewall on requisite servers;
3. Add the Firewalls to the CSPM management station and apply related rules
4. Configure security policy on the firewalls and load balancers;
5. Implement OS hardening for the desired servers, as per the security policy document.
6. Configure Authentication and Access control settings on the OS

Implementation Testing - STS will setup and conduct functional testing to verify the following:

1. Verify the functionality of the firewall rule set;
2. Resiliency provided by the load balancers;
3. Failover for the firewalls.

Post Implementation Assessment & Security Policy Review– The following Tasks will need to be conducted after Deployment to re-assess Security Practices:

- Review Firewall/DMZ environment and how it relates to line of business

- Gather appropriate security data/information
- Review existing security policies, procedures, and practices
- Comprehensive analysis of the following:
  - Current architecture of Firewall/DMZ environment
  - Audit logs and accountability checks
  - Review of firewall rule-base
  - Assess IT staff technical security knowledge and training

Backup Implementation service

Installation and Configuration - STS will perform the following installation and configuration tasks:

1. Install the backup software on relevant server/s and on any required clients, as per the design document;
2. Configure the backup software with backup server and associated devices (e.g. L20);

Implementation Testing - STS will setup and conduct functional testing to verify the following:

1. Standard operation of all tape drives in the tape library;
2. Backup and restore operation of a server;
3. Backup and Restore operation of a client data.

Post Implementation Backup Policy Review– The following Tasks will need to be conducted after Deployment to re-assess Backup Practices:

- Review Backup configuration and environment including the existing network infrastructure and clients services.
- Review Backup Solution Design
- Design a strategy for backup to meet the allowed backup window
- Design a strategy for restoring the backup server
- Optional Performance testing of backup and restore

Intrusion Detection System Implementation Service

Installation and Configuration - STS will perform the following installation and configuration tasks:

1. Install IDS network engines, IDS host engines and IDS monitor/s, as per the design document
2. Add the IDS system to CSPM-I and configure its ID's
3. Configure reporting from engines to the monitor

Implementation Testing - STS will setup and conduct functional testing to verify the following:

1. Standard operation of network engines in each segment and host engines on the selected

servers, as per design document;

2. Verify alarm functionality on the monitor
3. Verify IDS response on attacks, these responses include TCP reset and IP blocking

Cluster Implementation Service

The following tasks will be performed for all cluster implementations resultant from the design.

Installation and Configuration

1. Plan and document the detailed configuration design of the cluster environment to ensure it meets the availability levels required by the customer business
2. Basic hardware and OS platform installation followed by testing of the platform hardware for at least x hrs, storage hardware testing will be done separately depending on the storage hardware chosen.
3. Storage installation and disk layout as defined by the customer and discussed in the planning meeting,
4. Cluster software installation and configuration,
5. Volume manager installation and configuration,
6. Integration of any required application into the cluster environment
7. Installation of database binaries, creation of database instance(s) based on application requirements provided by the customer. This **will not** include architecting the database nor any other database related consultancy.

Implementation Testing

1. Testing of the completed platform focusing on its RAS (reliability, availability and serviceability) features to ensure that the cluster and any integrated applications behave according to specification,

Web/Application Server Implementation Service

The following baseline procedures & activities will be performed for the production site Web infrastructure, which may include, and may not be limited to, the following Components:

- Web Server
- Enterprise Application Server
- OS Hardening

Installation and Configuration - STS will perform the following installation and configuration tasks:

1. Install web server/s
2. Install the Enterprise Application Server on machine/s, and configure for load balancing and high availability;
3. Configure High Availability on Application Servers (Product Dependant)
4. Install OS hardening

Implementation Testing - STS will setup and conduct functional testing to verify the following:

1. Standard operation of HTTP;
2. Standard operation of the Enterprise Application server, using a "Hello World" basic Java program;
3. Validating the OS hardening

CMS & Search Engine Implementation Service

The following tasks will be performed as part of the CMS implementation service and will be in close coordination with the portal coordinator. This task requires that a CMS and search engine have been selected and procured and that the CMS and Search Engine are both compliant in the Enterprise Architecture. If not, this task may be postponed and reassigned in a later task order:

Installation and Configuration - STS will perform the following installation and configuration tasks:

1. Install the Content Management System, as per the design document;
2. Install the Search Engine, as per the design document;
3. Install and configure any required servlet engine;
4. Install and configure any Deployment Server;
5. Configure load balancing on the CMS & Search Engine, if required by the design;
6. Install any CMS & Search engine plugins on the Web Server, if available.

Implementation Testing - STS will setup and conduct functional testing to verify the following:

1. Standard HTML services from the CMS & Search system;
2. Standard delivery of a simple HTML form through the web server/s;
3. Verify load balancing and fail-over on CMS & Search Engine components, if required by design.

Note: STS needs to agree with the portal coordinator on the required installation and configuration details before commencing the work described above in this section.

----- End of document ------