Hacking the International RFQ Process - #KillTheBuzzWords

Dino Covotsos − Telspace Systems
@telspacesystems

TEL SPACE
Hackers for Hire

Whoami?

Work mostly in the Penetration Testing space

Approximately 20 years in…

Trying to keep some sort of work/life balance! ;)

4000 RFQ's in…

IEL SPACE
Hackers for Hire

What the cyber?

APT
NEXT-GEN
CYBERWAR
ZERO-ACCESS
KILLCHAIN
DEEP-WEB
CYBER

IEL SPACE
Hackers for Hire

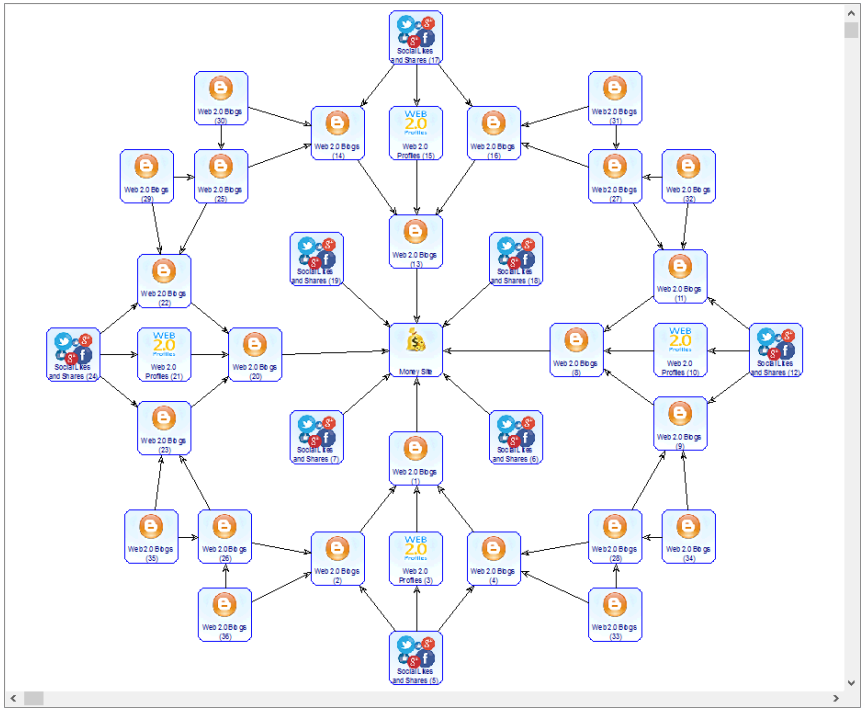
RFQ Process, we’re doing it wrong.

Let’s invite the attackers?

What about resellers?

POC, please?!

How do we exploit this RFQ process?



IEL SPACE
Hackers for Hire

Not really…

Personal examples, please!

So what can we get for enum?

Network Diagrams
Internal incident response procedures
Internal / hosts / ip's / ranges
External hosts / ip's / ranges
Core server operating systems, software versions etc
Firewall types, security technologies in use
Web Application information (in detail)
Patch levels
QA (Answers to vendors questions!)
and more..

IEL SPACE
Hackers for Hire

Annex A : SCOPE OF TESTING REQUIREMENTS

A 0.1 (I) Most tests in this ITQ involve DfE's back-office / core infrastructure systems, to support (retrospective) accreditation of the core ICT infrastructure, and likely requirements for connection to the 3-3-4 tier of the Public Sector Network.

A 0.2 (D) Tenders should indicate what additional information, not provided in this ITQ, the Department should provide soon after award of contract.

A 0.3 (D) At least **4** itemised prices are required covering these 10 areas of test (these are bulleted in the same order as sections A1 to A10 of this Annex)

- 'ROAM' SSL VPN : CESG Manual T validation, and Laptops
- Blackberry Enterprise Server, Microsoft Exchange & Outlook
- Back-office servers e.g. AD DHCP DNS Patch AV Proxy BDC
- Thin-client desktop implementation at Sheffield site
- General-purpose file servers and SAN
- Multi-Function Devices (printer-scanner-copiers) and Safecom application
- Firewalls and network devices
- S2S internet-facing system hosted by EduServ
- complex tests exploiting vulnerabilities found earlier

A2 Blackberry Enterprise Server, Microsoft Exchange & Outlook

A2.1 (I) Blackberry handsets are out of scope.

A2.2 (M) The Department's two (2) Blackberry Enterprise Servers should be subjected to a configuration review and IT Health Check for compliance with the CESG specifications detailed in BlackBerry Enterprise Solution for Administrators Issue 2.2.

A2.3 (D) The interface between the BES's and DfE's two (2) MS Exchange servers should be tested for compliance with best practice (and any criteria in the CESG BES specification).

A2.4 (I) One BES and one Exchange server are located at each of the Westminster and Sheffield sites. Metrics for Firewalls protecting the BES installation are provided at A7.

A2.5 **(M)** Both (2) MS Exchange servers must be subject to an appropriate IT Health Check against best practice.

A2.5 (D) The interface between the MS Exchange servers and Microsoft Outlook shall be tested for compliance with best practice, on one (1) LAN-connected Laptop and one (1) ROAM-connected Laptop (see A1.3), and one (1) Thin-Client desktop at Sheffield (see A4).

A2.6 (I) DfE Laptops run Outlook 2003. Thin-client desktops run Outlook 2010.

A3 Back-office servers

A3.1 **(M)** All such servers shall be subject to IT Health Checks performed over the network, to identify gaps against best practice.

A3.2 (I) Configuration review is out of scope.

A3.3 (D) Numbers, types and locations of such servers to be tested are as follows -

- Domain Controller with primary role for all AD functions one (1) Sheffield
- Windows 2008 Domain Controllers (provide DNS) : eight (2 at each HQ site)
- Windows 2003 DHCP servers : eight (2 at each HQ site)
- Windows Update and Patch deployment server (1 – Runcorn)
- Anti-Virus deployment servers (2 - Runcorn & Sheffield)
- ISA web proxy server running SurfControl : two clusters (2) Westminster and Sheffield
- ISA web proxy server, pointing to the above SurfControl servers : 2 clusters (Darlington and Runcorn)

and if enough servers exist and are not already tested in the above :

- Windows 2000 Server build : not more than 2 at each HQ site. These may well be business/application servers, because DfE has upgraded most back-office systems to win2003 or win2008. Only the Windows 2000 build should be assessed, not software or web applications.

A3.4 (I) Generic Windows 2003 Server build is covered off by DHCP servers above, and generic Windows 2008 Server build is covered by Domain Controller / DNS servers above.

A7.2 (I) Out of scope : vulnerability and application testing of web servers and other computers located in the DfE extranet. There are approximately 35 live servers in the extranets, of which a small proportion are in the GSI-facing extranet rather than Internet-facing.

There are 16 Firewalls surrounding the DfE Extranet (4), ROAM & Blackberry DMZ (8), and the Collect DMZ (4), of which eight (8) can be deemed Internet-facing (though some may be inside others) and the other 8 will be downstream providing connection to the DfE internal network. Some Firewall pairs operate in failover mode and others load-sharing / resilience.

A7.3 **(M)** Subject to confirmation by the configuration review, all Firewalls should be tested for the soundness against best practice of their configuration, both for ingress and egress, including to DMZs for any Firewalls with 3 or more network interfaces.

A7.4 **(M)** Metrics and Locations. All Firewalls operated by DfE must be tested.

The Department operates 9 Cisco (PIX or ASA) Firewalls and 18 NOKIA (IP 260 to IP390) Firewalls. One PIX is located at Darlington, two Nokias at Runcorn, 7 Firewalls in Sheffield, and the remaining 17 in London.

A8.1 (I) Background information

S2S comprises 2 IIS and 2 SQL servers, and shared Firewalls protecting and separating the systems, operating on virtualised infrastructure hosted by EduServ in the TeleHouse Docklands data centre.

S2S is a system to facilitate schools to transfer pupil records in a defined XML format known as CTF (Common Transfer File) when pupils change schools. Each school has its own access-controlled upload/download repository. Local Authorities also have access to S2S.

REF URL: http://oaklawn-il.gov/Home/ShowDocument?id=10952

Oak Lawn Library

External Network Vulnerability Assessment

- Number of IP addresses in target space: 38
- Number of live hosts: 15

Internal Network Vulnerability Assessment

- Number of servers in target space: 18
- Number of network devices in target space: 27
- Number of workstations in target space: 127

Server Configuration Reviews

Number and type (operating system and function) of servers to be reviewed:

- 2 domain controllers 1 Server 2012R2, 1 server 2016
- 2 File servers 1 Server 2012R2, 1 Server 2016
- Web Server- Server 2012R2
- 3 Maintenance servers (System Center) all server 2016
- Exchange server (Management for Office 365) server 2012 r2
- 3 Virtualization Platform servers (Proxmox) 12
- Voice Mail server - Server 2012R2
- 2 MSSQl Servers 1 Sever 2012R2, 1 Server 2016
- 1 SharePoint Server – Server 2012R2
- 2 Federations Servers, 2 Server 2012R2

Firewall Reviews

- Number of type of firewalls to be reviewed: 2
- Number of rules in each firewall rule set: 50

Web Application Assessment

- Name and description of each application to be assessed: 1 -- Symphony (Credit Card)
- Number of user input pages for each application: 30
- Number of user roles / privilege levels for each application: 3

Application Code Review

- Name and description of each application to be assessed: 0
- Number of lines of code in the application:0
- Language(s) the application is written in: 0

http://www.kirklandwa.gov/Assets/Finance+Admin/Finance+Admin+PDFs/Purchasing/Q$!26A+Network+Security+Assessment.pdf

Are the City's utility operations (electric, water, and sewer) in scope for penetration testing? Answer: Yes
10. When was the last time penetration testing or a vulnerability assessment was done? Answer: 2011
11. What types of devices and operating systems will be reviewed for the Critical Systems Configuration Analysis? How many unique devices will be reviewed?

Answer: Detailed information on these devices will only be available to finalists for security reasons.
- ?Routers, Switches, Firewalls, wireless (all CISCO)
- ?Servers, All Windows
- ?Some VM Appliances (CISCO, McAfee, Linux)

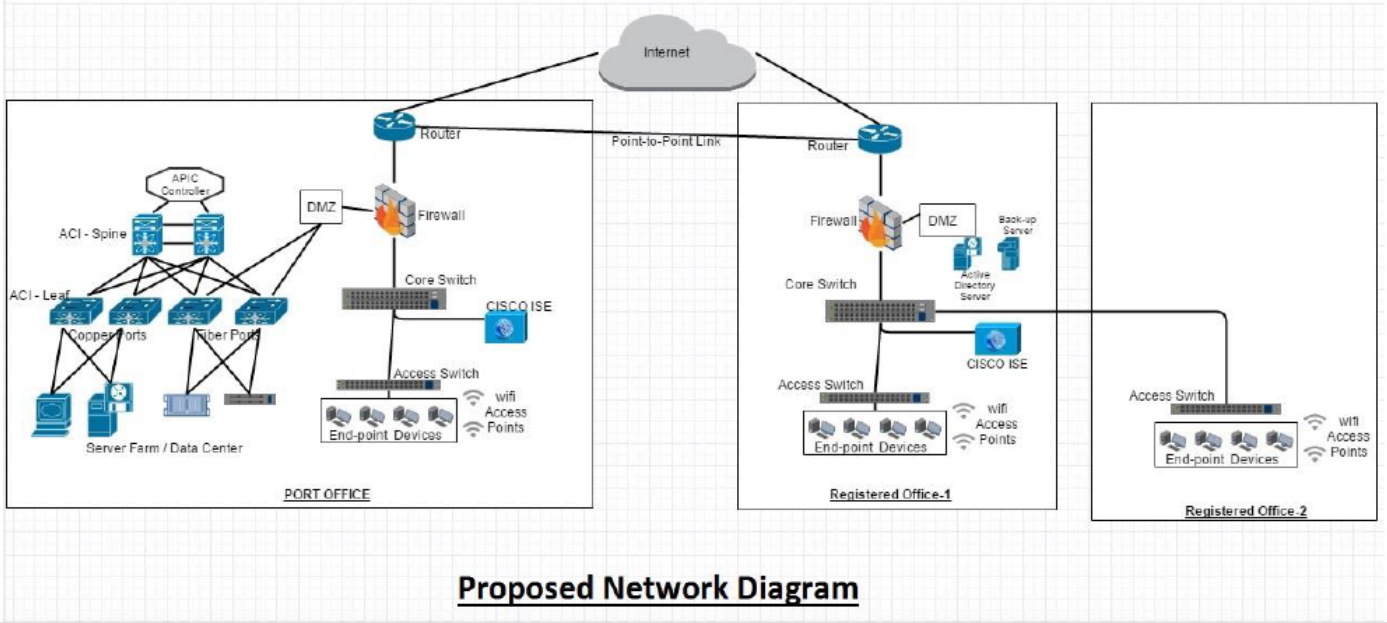
Is there a standard operating system involved? Answer: we currently standardize on Windows 7 and Windows 10.

Critical Systems Configuration Analysis - **Do they want policy review or assessment texting? What types of and how many firewalls?** Answer: Both and
1 HA Pair of CISCO ASA

kind of physical security systems implemented like CCTV, Guards, Dogs, Fire Extinguishers etc Answer: We are interested in the physical security of IT systems. We do have video security in some buildings. We do not use dogs, or guards.

http://www.ennoreport.gov.in/upload/uploadfiles/files/EOI_Document.pdf &
http://www.ennoreport.gov.in/upload/uploadfiles/files/RFP-Cyber-Security-Audit-for%20NIT.pdf

The IT network diagram (high-level) covered under the audit is provided below :



Proposed Network Diagram

IT-Infra in Scope:

Description	Type / No of Servers	Platforms
Application	Internet Banking	Infosys Product
Application Server	2 Servers	WAS ND 8.5 / Network Deployment Cluster Setup
HTTP Server	2 Servers	IHS 7 (Only one active at a time)
Database Servers	1 Server	Oracle 11G (1 Server)
Public IP	One	

D. SCOPE OF WORK :

1.Project Name :- CCC Payment Portal

Brief Introduction:- This is a web portal developed for online payment relate every month examination activities of CCC and BCC courses.

URL :- http://14.139.251.168/cccpayment_revised/ **[Temp]**

Project Details:

S. No.	Information About the Application	Version and Count
1.	Database	MySQL 4.0.10.14
2.	Development platform for application	PHP 5.6.20 and JavaScript
3.	How many application roles/privilege levels of users?	5
4.	Does the application provide a file download feature (Yes / No)?	YES
5.	Does the application use Client-side certificate (Yes / No)?	NO
6.	Is there a CMS (Content Management System) present to maintain the public portal/login module?	NO
7.	Tentative Testing environment (Development / Staging / Production Box)?	Staging
8.	Does the application has SMS integration (Yes/No)?	NO
9.	Does the application has E-Mail integration (Yes/No)?	NO
10.	Does the application has Payment Gateway integration (Yes/No)?	NO

2. Project Name :- ISEA GOT E-Learning Portal

Brief Introduction:- Web Portal has been developed for providing Technology Enhanced Learning to the Government Officials as well as I.T Security Professionals. This portal is used for facilitating E-Learning Platform for the officers of Central / State government, I.T Security Professionals as well as IT Security students also.

URL:- http://14.139.251.163/iseagot/ **[Temp]**

Project Details:

S. No.	Information About the Application	Version and Count
1.	Database	MySQL Ver 15.1 Distrib 5.5.52 -Maria DB
2.	Development platform for application	PHP 7.0.18 and JavaScript
3.	How many application roles/privilege levels of users?	7
4.	Does the application provide a file download feature (Yes / No)?	YES
5.	Does the application use Client-side certificate (Yes / No)?	NO
6.	Is there a CMS (Content Management System) present to maintain the public portal/login module?	YES (Moodle 3.3.2 +)
7.	Tentative Testing environment (Development / Staging / Production Box)?	Staging
8.	Does the application has SMS integration (Yes/No)?	NO
9.	Does the application has E-Mail integration (Yes/No)?	YES
10.	Does the application has Payment Gateway integration (Yes/No)?	NO
11.	Does the application provide a file upload feature (Yes / No)?	Yes

3. Project Name:- **BigBlueButton Web Portal**

Brief Introduction :- This is a web application being used for Online classes , assessments and interaction of Audio and video with teacher or students ,slides and chat.

URL :- http://14.139.251.171/bigbluebutton/ **[Temp]**

Project Details:

S. No.	Information About the Application	Version and Count
1.	Database	NO
2.	Development platform for application	JSP and HTML
3.	How many application roles/privilege levels of users?	2
4.	Does the application provide a file download feature (Yes / No)?	NO
5.	Does the application use Client-side certificate (Yes / No)?	NO
6.	Is there a CMS (Content Management System) present to maintain the public portal/login module?	YES
7.	Tentative Testing environment (Development / Staging / Production Box)?	Staging
8.	Does the application has SMS integration (Yes/No)?	NO
9.	Does the application has E-Mail integration (Yes/No)?	NO
10.	Does the application has Payment Gateway integration (Yes/No)?	NO
11.	Does the application provide a file upload feature (Yes / No)?	YES

ICT SECURITY PENETRATION TESTING SERVICES

Successful bidder

Bidder name	Tender Description	Tender No.	B-BBEE Points	Points Awarded
Deloitte and Touché	ICT SECURITY PENETRATION TESTING SERVICES	FSB2016/17-T005	---------	90.00

Participants

Participant name	Participants contact details
As per details.	Name of unsuccessful bidder (s) Points claimed Contract price (if applicable) Directors names Sensepost (Pty) Ltd 49.47 R2 270 492.58 Charl van der Walt Jaco van Graan Etinne Greeff Ernst and Young Advisory Services (Pty) Ltd 7.45 R3 041 295.00 Refer to the attached list. KPMG Services (Pty) Ltd -84.95 R4 522 326.00 Refer to the attached list. PricewaterhouseCoopers Incorporated -95.76 R4 770 270.00 Refer to the attached list. Ironsky (Pty) Ltd Did not pass the functionality evaluation stage. R2 878 651.08 Sibusiso Teboho Sishi Robert Danio Beney Computer Security and Forensic Solutions (Pty) Ltd Did not pass the functionality evaluation stage. R1 024 632.00 Willem Cornelius Britz Craig Retief Johannes Roux Athena IT Consulting cc Did not pass the functionality evaluation stage. R1 155 100.00 Matsobane Rabalao PUBLICATION OF AWARD FORM Name of unsuccessful bidder (s) Points claimed Contract price (if applicable) Directors names Phakamo Holdings (Pty) Ltd Did not pass the functionality evaluation stage.

As per details.	Points claimed
	Contract price (if applicable)
	Directors names
	Phakamo Holdings (Pty) Ltd
	Did not pass the functionality evaluation stage.
	R3 500 000.00
	Lucas Lefeta Ledwaba
	Odirile It Holdings (Pty) Ltd
	Did not pass the functionality evaluation stage.
	R2 620 683.07
	Solomon Mathews
	Daniel Mametse
	Nambiti Technologies (Pty) Ltd
	Did not pass the functionality evaluation stage.
	R31 792 320.00
	Kevin Paul
	Theresa Paul

*REFERENCE URL: https://www.raf.co.za/Procurement/Documents/Network%20and%20Devices%20Clarification_ICT%20SECURITY%20SERVICES.pdf

RAF/2014/00014: ICT SECURITY SERVICES - ADDITIONAL CLARIFICATION REGARDING NETWORKS AND DEVICES

No.	Short Description of enquiry/request	Response
1	Please provide high level network architecture diagram depicting connectivity from head office to branch offices.	Not required as all events are from a centralised data centre location.
2	Please provide breakup of 3000 IP devices such as how many desktops, servers, switches, routers, firewalls and others.	Approximately 300 Servers, 700 Endpoints, 1600 thin clients, remaining IPs are routers, switches, IP phones.
3	Are you using any monitoring tool and/or security incident reporting tool in existing setup, if yes please provide details.	Splunk
4	Please provide average number of firewall related change requests received per month.	10
5	Provide detail list of Operating systems and databases used on desktops/servers.	MS Windows Server 2003 to Server 2012. Windows 7/8, Linux, IIS, AIX, HP-UX

Question 4: What model of Cisco ASA Firewall is used by RAF
Answer 4: Cisco ASA 5540 with ASA-SSM-40 Module (There are 2 of these Firewalls in a High Availability setup)
Question 5: What are the current AMC details?
Answer 5: SMARTNET 24x7x4 valid till March 2016
Question 6: Are you using the integrated IPS in the firewall device or a separate device? If separate device what are model and AMC details?
Answer 6: ASA-SSM-40 which is licenced
Question 7: What is the expected SLA response window for intrusion detection?

*REFERENCE URL: https://www.resbank.co.za/AboutUs/Departments/FinancialServices/Procurement1/Documents/GVDW%2002-2013.pdf

Section 3: Scope of work

3.1 Background

The Business Systems and Technology department, in conjunction with the National Payment Systems Department within the Bank are seeking the services of a company to provide web-based security and penetration testing and security assessment, on the web-based user interface (SAMEXWeb) for the Bank's current Real Time Gross Settlement System (SAMOS).

3.2 Scope of SAMEXWeb

3.2.1 SAMEXWeb General Architecture Design Overview

The purpose of this section is to provide an overview of the SAMEXWeb solution architecture design. In the interest of positioning the SAMEXWeb solution in relation to the rest of the SAMOS business system, the SAMOS business application and database server is shown as well.

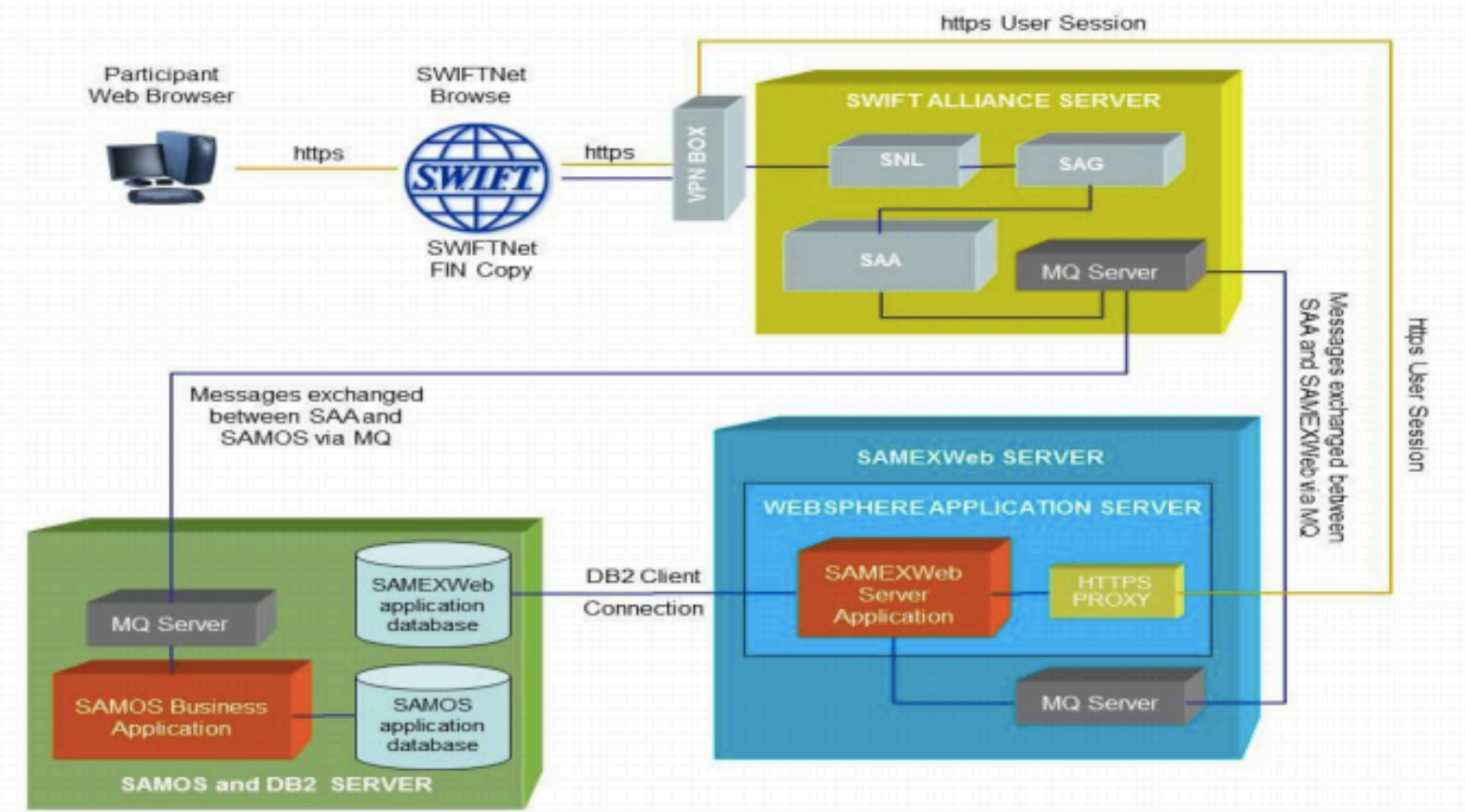


Figure 1 – SAMEXWeb Architecture Logical View

3.2.2 SAMOS Application and Database Server

The SAMOS application and database server hosts the SAMOS core business application and the DB2 database management system on a z/OS mainframe partition.

The DB2 DBMS provides managed access via DB2 client connections to separate database images for the SAMOS application as well as the SAMEXWeb application. The databases and the application binaries are physically located on the Storage Area Network (SAN).

Transactional messages are sent and received by the SAMOS application via MQ and Swift Alliance Access.

3.2.3 SAMEXWeb Application Server

The SAMEXWeb Application Server hosts the SAMEXWeb WAS internet server and J2EE application components on an AIX partition.

The core functions of the SAMEXWeb server is to:

- Integrate with SWIFTNet Evolution in order to authenticate users during the logon process;
- Manage the browser-based sessions with participant users (HTTPS over the SWIFTNet Secure IP Network);
- Provide user authentication and authorisation services;
- Provide the presentation layer and transform business data between the user Web pages and SAMOS message structures; and
- Send and receive business messages to and from the SAMOS application via MQ and Swift Alliance Access.

3.2.4 SWIFT Infrastructure and Alliance Server

The purpose of the SWIFT server is to host the SWIFT software components required to connect to the SWIFTNet SIPN (SWIFT Internet Protocol Network) and send and receive messages to and from SWIFT service offerings.

In the context of the SAMEXWeb sub-system, SAA provides message management and routing services between SAMOS and the SAMEXWeb server application via MQ.

The HTTPS connectivity form the SAMEXWeb user browser is routed via the SWIFTNet VPN box to the HTTPS proxy provided by the WAS environment on the SAMEXWeb application server.

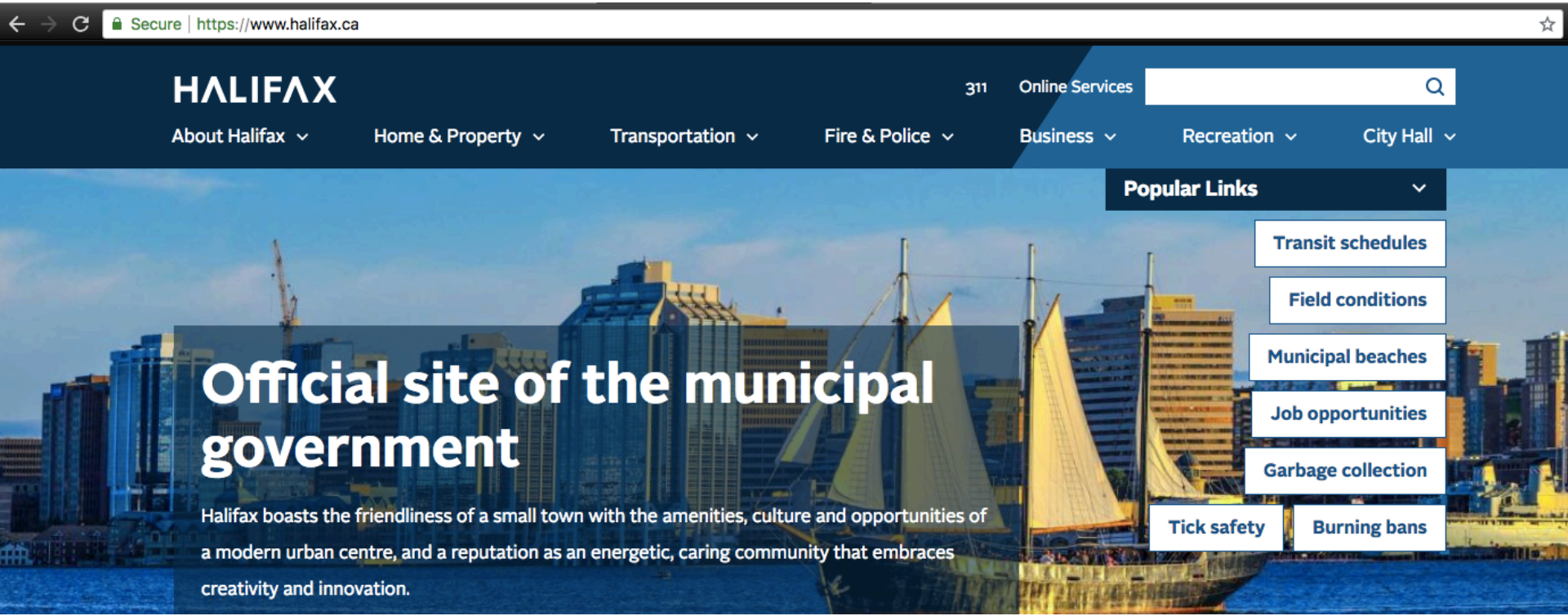
3.2.5 User Authentication and Authorisation

User authentication is implemented using a personalised 2-factor USB token / PKI certificate combination provided by SWIFT under its internal SWIFTNet Certification Authority service, using a SAML Identity Provider service also provided by SWIFT. The SAMEXWeb application integrates with this security infrastructure provided by SWIFT as part of the SWIFTNet Browse Evolution product offering.

User authorisation is based on a proprietary application-level user repository integrated into the SAMEXWeb server application, with distributed management based on segregation of duties and multiple levels of authorisation.

The successful vendor will be provided with additional details and a copy of the SAMEXWeb trust model once the NDA is in place.

This is not just for pentesting…



IEL SPACE
Hackers for Hire

Specifications:

To supply Symantec Endpoint Protection support renewals
to the Halifax Regional Municipality - Public Library.

HRM contact: Tracy Leblanc (902) 490-5764.

Required renewals:

Symantec Endpoint Protection v. 12.1 - Essential Support (Renewal)
1 User Academic - Symantec Buying Program:
Academic - 1 Year - Price Level H
Academic - Symantec Buying Program:
Academic - 1 Year - Price Level H End Date March 24, 2016
672 units required

Symantec #0E7IOZZ0ER1AH

Symantec Endpoint Protection v. 12.1 - Essential Support (Renewal)
1 User Academic - Symantec Buying Program:
Academic - 1 Year - Price Level H
Academic - Symantec Buying Program:
Academic - 1 Year - Price Level H:CoTermStart:5-Nov-2015
CoTermEnd:24-Mar-2016
250 units required

Symantec #0E7IOZZ0ER1A

Symantec Endpoint Protection v. 12.1 - License
1 User Academic - Symantec Buying Program:

www.oman-gas.com.om

شركة الغاز العمانية ش.م.ع.م.
OMAN GAS COMPANY S.A.O.C

EN عربي

ABOUT US SUSTAINABILITY QHSE CAREERS MEDIA CENTRE TENDER CONTACT US

About Us

Oman Gas Company S.A.O.C (OGC) is a midstream natural gas transportation company established in the year 2000 in the Sultanate.

Our Achievements

High Omanisation percentage more than 90% representing the highest rate in Oil & Gas Industry in the Sultanate.
Received the GCC Award for the localization of jobs 2015.
Fully-Omanised management.

QHSE

Oman Gas Company has a stringent Quality policy in place and ascertains its implementation across the organisation.

Oman Gas Company & Contractors have worked for

154

days without lost time injury.

IEL SPACE
Hackers for Hire

SL	Item Number	Item Description	Delivery Date	QTY	UOM	Unit Rate	Total Amount
10		McAfee Licenses 2017		1	AU		
						Total Amount	

The Item covers the following services:

10		UPGRADE Suite (from ETP to CTP)-EXISTING LICENSES (endpoint protection) - Grant Number: 9566142-NAI,Account Number: 856894 (MFE Complete EP Protect Bus 1Yr GL -CEBYFM-AA-EA - QTY 302) ========== UPGRADE Suite (migration from ETP to CTP > from Endpoint ThreatProtection (ETP) to Complete Endpoint Threat Protection (CTP) for 302licenses + maintenance\support for 1 year (April 2017 to April 2018).		1	LOT		
20		NEW PRODUCT : ETD for existing customer-NEW PRODUCT : End Point Threat defense (ETD for existing customers) for302 licenses. Maintenance\Support for 1 year (April 2017 to April 2018).		1	LOT		
30		EXISTING LICENSES RENEWAL (dlp)-EXISTING LICENSES (dlp) - Grant Number: 9566142-NAI, Account Number:856894 . (MFE Data Loss Prvtn Endpoint 1YR G[P+] - DLPYFM-AA-EA - QTY302) ========== RENEWAL of exiting DLP (302 licenses). Maintenance\Support for 1 year(April 2017 to April 2018).		1	LOT		

Transparency vs x(y)

Solving this issue is hard.

Q and A

@telspacesystems

www.telspace.co.za