Government High Level ICT Blueprint

Date: 18/07/2017
Version: 6.0
Department: Technology Direction and eGovernment

INVESTOR IN PEOPLE

Unclassified

Document Control Information

01. Document reference

CTO-REP-High Level ICT Blueprint-v6.0

02. Document type

Blueprint

03. Security classification

Unclassified

04. Synopsis

Government High Level ICT Blueprint

05. Document control

Author	Change controller	Distribution controller
Technology Direction and eGovernment Department	Technology Direction and eGovernment Department	Technology Direction and eGovernment Department

06. Authorisation

Issuing authority	Approval authority
Technology Direction and eGovernment Department	Technology Direction and eGovernment Department
Signature/Date	**Signature/Date**

07. Modification history

Version	Date	Comments
Version 1.0	03/03/2010	Release Version
Version 1.1	08/03/2010	Security Clearance Updates
Version 1.2	10/03/2010	Security Clearance Updates
Draft Ver 1.8	04/04/2011	Complete overhaul
Final Ver 2.0	14/04/2011	Release Version
Draft Ver 2.2	20/06/2011	Removed Reference to PRE
Final Ver 3.0	20/06/2011	Release Version
Draft Ver 4.0	06/06/2012	Updates related to MITA01
Draft Ver 4.1	27/09/2012	Data Sharing
Draft Ver 4.2	23/10/2012	Identity and authentication
Draft Ver 4.3	14/01/2014	Modified MITA portal URL references
Final Ver 5.0	06/07/2015	Release Version
Draft Ver 5.3	30/05/2017	Networks/Service/Security/Technology Updates
Draft Ver 5.4	12/07/2017	Include WSO2 Section
Final Ver 6.0	18/07/2017	Release Version

08. Acknowledgements

Technology Direction and eGovernment Department

09. References

Executive Summary

This document provides a High Level ICT Blueprint of Government's ICT managed by the Malta Information Technology Agency's (MITA). The document is structured in the following manner:

Section 1 – Overview outlines the purpose of the document.

Section 2 – A high level description of ICT assets.

Table of Contents

01. Overview

This blueprint presents a high-level view of Governments' ICT assets and can be used as a basis for more detailed/specific blueprints. The document will depict the following blocks:

- Magnet
- Govnet
- Object Directories
- Data Centres
- Clients
- Segregated Hosting Environment (SHE)
- ISP Services
- eGovernment Shared Services

01.1 High-level Technology Principles

Government of Malta strives to maximise investment and operational efficiency through the application of technology strategic principles.

The Technology Strategic principles include abstraction, interoperability, loose coupling, cohesiveness and generality.

In this context, and where applicable, Government will give preference to solutions that exhibit concrete evidence of a number of key attributes that enable these principles. These attributes are identified in constituents that clearly reflect engineering patterns based on discrete yet highly interoperable elements. All inter-connectivity and information exchange (at hardware, network and software levels etc.) between the solution constituents are to be built on the standards applicable in context. Software, Network and Hardware elements etc., as well as their intra-constituents should be independent of each other to the maximum extent possible. Amongst others, **Virtualization and Open Standards** are key enablers of the principles discussed herewith, as well as appropriate segregation at key layers of solution and component constituents. Specifically, with respect to solution stacks, irrespective of whether their implementation is physical, virtual or otherwise, access to resources outside any respective sandboxed environments that may already be in place (including databases, directory services, etc.) is to be governed by appropriate **adaptation ('adapters') schemes**.

The desktop element is considered critical in terms of the application of and adherence to these principles. To the maximum extent possible, dependencies on specific hardware and software stacks and respective configurations shall be avoided or appropriately mitigated.

01.2 Definitions

- Adapters: Logical segregators which vary from software, hardware or specialised devices / environments (including firewalls, VLANs, etc) to various operational procedures or contractual agreements.
- Abstraction: The mechanism and practice of abstraction is the reduction and factoring out of details so that focus and attention is given to a few concepts at a time.
- Interoperability: Within the context of Public services delivery, is the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems.
- Loose coupling: Loose coupling is the ability to reduce the degree to which programs/modules rely/depend on one another.
- Cohesiveness: Cohesiveness is the ability to combine different programs/modules which contribute to a single well-defined task/scope.

- Generality: Generality is the ability of being generic (applicable to all) in terms of business/technical implementation.
- Virtualisation: Virtualisation is the ability to create and run independent virtual ICT resources on one or more physical systems. ICT resources that can be considered for virtualisation include application, server, desktop, operating system, file, storage and network.
- Open Standards: Open specifications (informally referred to as Open Standards) are formalised specifications which within the context of public services delivery, are characterised by the following features:
    - All stakeholders have the same possibility of contributing to the development of the specification and public review is part of the decision-making process;
    - The specification is available for everybody to study;
    - Intellectual property rights related to the specification are licensed on FRAND terms or on a royalty-free basis in a way that allows implementation in both proprietary and open source software.

01.3 Data Sharing

The ability to share and process data beyond its source of origin is considered fundamental and expected. Any shareable data shall be exposed through appropriate machine readable mechanisms in an industry standard fashion, using open standards and interoperable engineering principle/practices.

Specifically, in the context of domain data, ownership of the data is considered to rest within the respective legally empowered authority/authorities, unless explicitly otherwise indicated. As a matter of preference, any machine to machine (solution to solution) interaction between data consumers and providers shall happen directly between the consumer and the specific information system storing and processing such domain data.

01.4 Corporate Identity and Authentication

In the Government context, the Core/Corporate Identity is considered to be the official identity. In the case of decentralised/federated identity and authentication management/provisioning, authentication exchange and/or sharing within and across domains (line of business, Corporate, etc.) should be abstracted and governed using the appropriate industry standard protocols.

01.5 Provisioning of Line of Business Applications and Authentication

Provisioning of line of business applications should be achieved in such a way that promotes maximum abstraction from the desktop stack in order to allow both the desktop and applications to evolve independently of each other. 'Webification[1]', Application virtualisation and Remote Desktop Services are three technologies that have been identified to promote such application abstraction.

From an authentication perspective, solutions should implement open and industry standard authentication schemes which promote loose coupling and abstraction from associated technology stacks.

01.6 Governance Framework

Relevant governance will be applied through the GMICT Policy Framework available online at http://ictpolicies.gov.mt. The same framework regulates the possibility and extent of compliance issues.

[1] The act of converting content from its original format into a format capable of being displayed on the World Wide Web.

02. Network

02.1 MAGNET - Government's Network

MAGNET is Government's network linking Data Centres to Ministries, Departments, Local Councils, district offices, schools and embassies. This seamless network allows Government employees to securely access information within Ministries and Department.

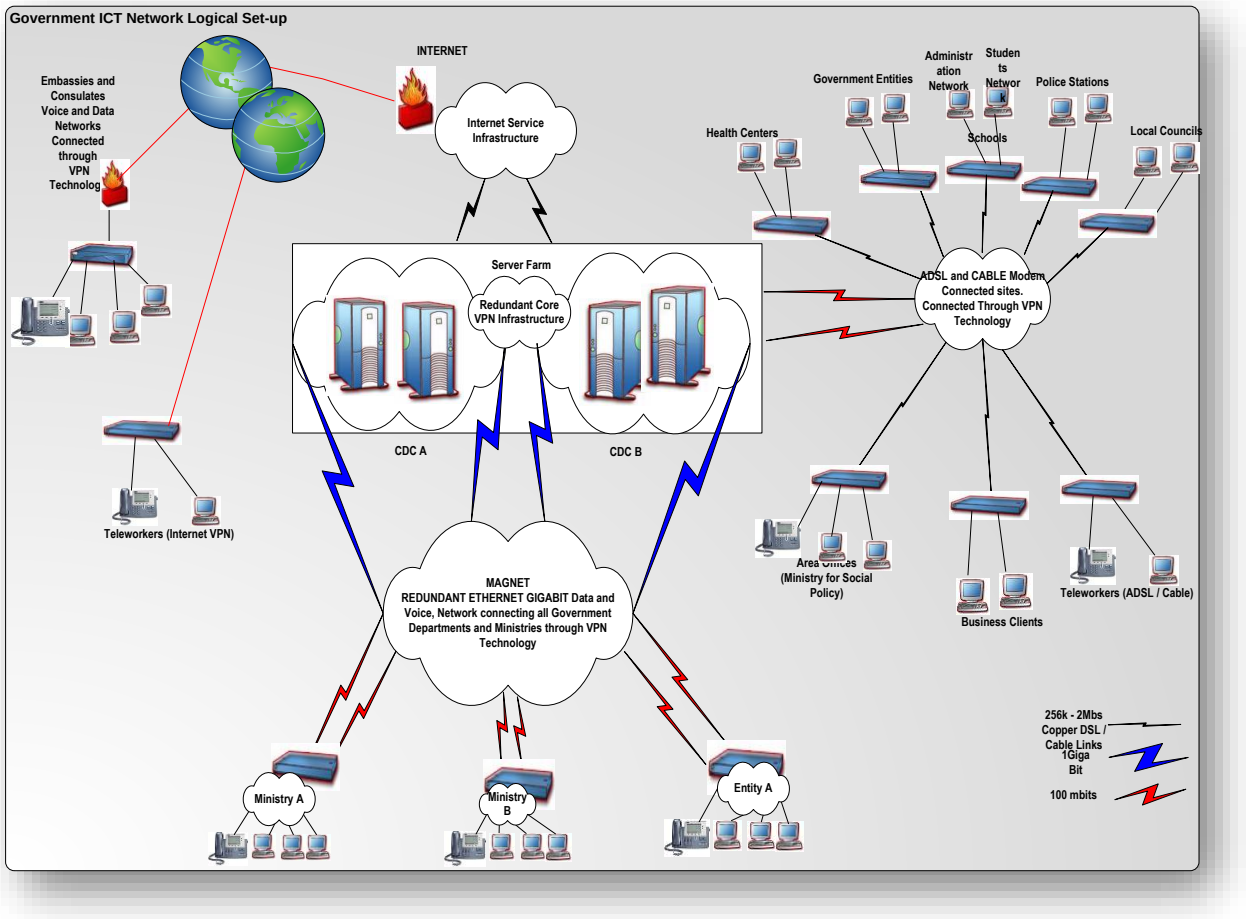

Figure 1 Government ICT Network Logical Set-up

The network architecture supports emerging applications such as voice, video, wireless data, storage network technologies, enhanced network management and security. MAGNET has been designed to meet both current applications and future ICT needs with the implementation of state-of-the-art equipment and advanced network technologies based on a high-speed fibre optic network that provides the required bandwidth, security, resilience, redundancy, flexibility and scalability.

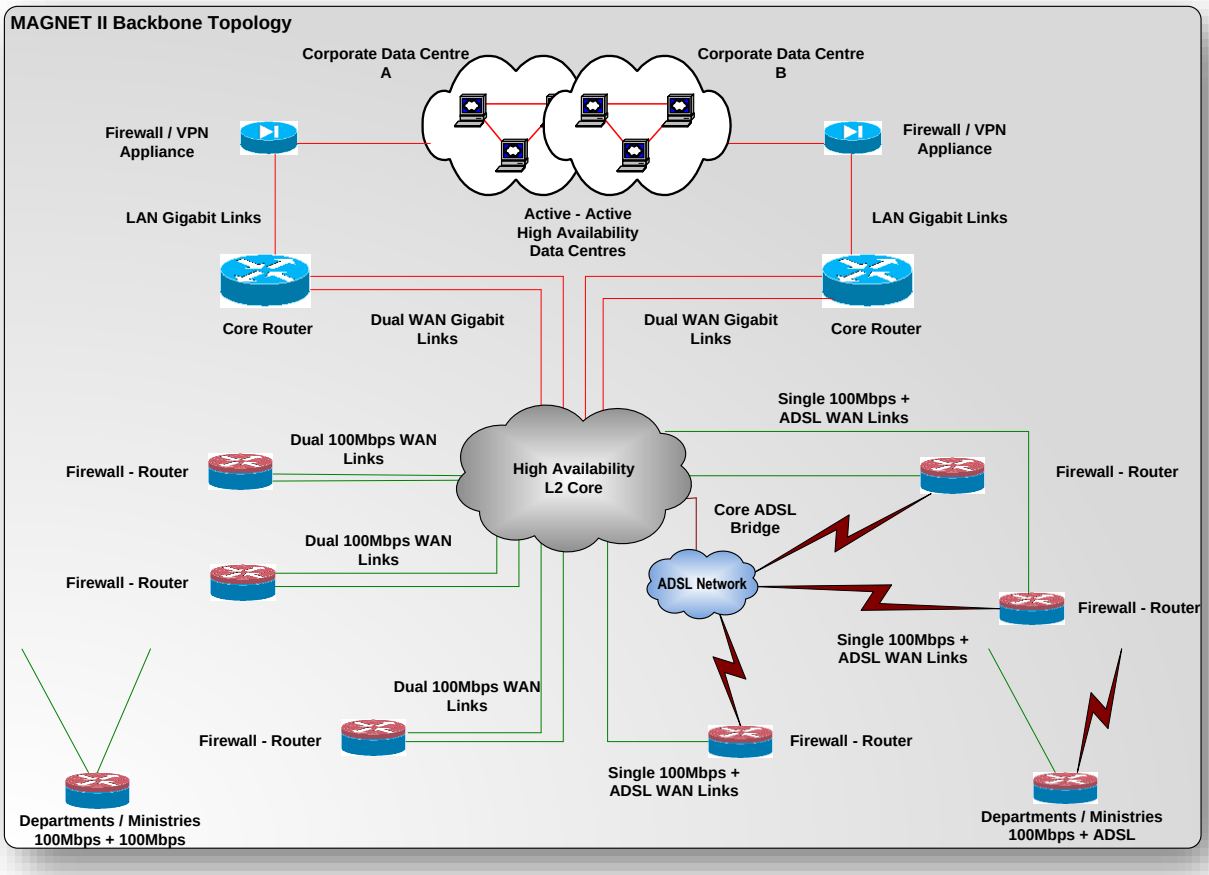

Figure 2 MAGNET II Backbone Topology

The core of MAGNET is concentrated within the Valletta – Floriana –Santa Venera geographical region connecting the 'core' to 'access' routers, via fibre links, which in turn are connected to the Local Area Networks (LAN) at the Ministries and Departments. These are VPN encrypted links providing 80Mbps (VPN overhead factored in) full duplex with a low latency (2ms at 85% utilisation). Most of the critical sites have dual fibre connections passing through physically separate routes with each link of the dual connection terminating on different switches at the 'core'. The remaining sites are connected with one fibre link and an ADSL backup link.

Sites not within this geographical area are connected to the core either via ADSL, cable or via fibre technology. These connections are also secured using VPN technology. Government embassies and Foreign Offices are connected via a VPN tunnel over the Internet.

02.2 GOVNET - Government's Interface to the outside

The GOVNET infrastructure is designed to offer internet connectivity, web and email services to MITA and its clients. The infrastructure is spread across two Data Centres having each component replicated on each site providing high availability. The underlying Layer 2 networks are extended across both Data Centres (MDC & MDH) allowing services to be provided across sites.

02.2.1 Internet IP Connectivity

This section details Government's IP connectivity to the outside world. Govnet currently provides internet connectivity via several links with a local ISPs.

The links are terminated at MDC and at MDH thus providing failover in case of DC failure.

02.2.2 Remote access

Teleworkers remote access is securely provisioned via SSL VPN and two factor authentication, whilst network to network VPN is offered via IPSec in tunnel model with Encapsulating Security Payload (ESP) using authentication and encryption services.

All backend operations on any part of the Government network from outside is carried out over VPN.

02.3 Core Network across Data Centres

Connectivity across sites is via multiple pairs of dark fibre passing through two separate routes.

The core Ethernet network across data centres is composed of four switches (2 per site) virtualized into 3 logical switches. 80Gbps of bandwidth is available across sites and this is split between various L2 networks. Due to this extreme high bandwidth both data centres, though physically separate, can be seen logically as one large data centre. Redundancy is achieved at Layer 2 via LACP or via Layer 3 routing protocols.

The Storage Area Network is based on a star network topology and is made up of four FC Switches at its core. Each pair of switches at either site interconnect with via FC links over the Optical Transport Network and form two separate merged switch fabrics. All switches are partitioned into several Virtual SANs (VSANs), where each VSAN is managed as an independent logical fabric, while still maintaining end-to-end visibility and management services across the entire storage network.

02.4 Virtualization stack

The virtualization stack is based on VMware 6.5 and is stretched across both DCs offering flexible availability options for VMs.

The platform does not support the use on Microsoft network load balancing or the use of RDMs.

03. Data Centre Facilities

MITA operates two Data Centres on behalf of Government. The Data Centre in Santa Venera(MDC) is certified as TIER III by the Uptime Institute and hence provides facility availability of 99.987% per annum. Solutions requiring high-availability levels should be implemented in a redundant fashion across both data centres.

03.1 Monitoring & Alerting - Operational & Security

Government owns a Monitoring and Alerting Platform which handles both operational and security related events.

03.2 SAN - Government's Storage Area Network

Introduced by the consolidation project, Government owns a Storage Area Network (SAN) extended across the two Corporate Data Centres (CDCs). The two CDCs are installed with storage facilities that interconnect across the optical transport network. Both CDCs are individually equipped with storage units supporting different tiers of storage and an array of FC switches which form two independent fabrics that extend between CDCs.

03.2.1 Storage Units

The disk array component of the consolidation solution is based on a several arrays, catering for different storage tiers (performance/cost) hosted across data centres.

03.2.2 Remote Data Mirroring

Data volumes on the storage arrays can be mirrored across data centres.

04. Clients (Desktops/Laptops)

This section details information related to clients managed by MITA.

All desktops managed by MITA are configured to ensure that users are logged-in and authenticated with a corporate Active Directory service. Moreover, each PC is being provided with a standard desktop profile.

04.1 Deployment

This section details the mechanisms used to deploy the initial desktop images and updates thereafter.

MITA is responsible for the creation, maintenance, versioning and archiving of desktop images which are passed on to the Desktop Supplier for the necessary installation and configuration of the desktop.

Typically, the Desktop Image contains the operating system and includes the following:

- Standard Software (such as Office, Anti-Virus etc.);
- MITA Software (Development Run-Time Components and Line of Business Applications developed/supported by MITA);
- 3rd Party Software (Development Run-Time Components and Line of Business Applications developed/supported by 3rd Parties);
- Client Software (Non-Standards Software as per CIO requirements).

04.2 Security

This section details desktop restrictions, AV, network segregation etc.

Desktop restrictions on machines managed by MITA are controlled via Group Policies which are implemented via Active Directory. Over and above each PC is being provided with a standard desktop profile to ensure that each PC:

- Adheres to a standard desktop configuration governed through the Active Directory service and related tools;
- Applies the group policy objects for the purposes of 'locking' to minimise user tampering and experimentation with the desktop's configuration, thus minimising the amount of desktop incidents;
- Have applicable endpoint security which is active and always up to date.
- Is managed via SCCM.
- User accounts are set up such that users have local user rights on their workstations. The default security settings will prevent end users compromising the integrity of the operating system and installed programs. Users cannot modify system wide registry settings, operating system files, or program files. Users can run certified Windows programs that have been installed or deployed by administrators. Users have Full Control over all of their own data files (%userprofile%) and their own portion of the registry (HKEY_CURRENT_USER);

04.3 Operating system

Most of the desktops and notebooks managed by MITA are installed with Windows 10 Enterprise. The operating system is centrally managed via GPOs/GPPs and updated through a patch management function within MITA which makes sure to keep all machines up to date with the latest patches and updates.

05. Core Service

05.1 Object Directories

MITA operates a logical directory based on Microsoft Active Directory on behalf of Government. This directory:

- Stores the recognised Core/Corporate Identity of Government employees;
- Is used to manage Government Workstations which are managed by MITA.

In the context of Government, the Core/Corporate Identity is considered to be the official identity of public officer/s. MITA's corporate identity persistence and provisioning schemes are currently exposed through identity federation services provisioned through the Microsoft Active Directory Federation Services (ADFS) 3.0 via a Federated Authentication approach using industry standards WS-Federation, WS-Trust or SAML 2.0 supported by Microsoft Active Directory Federation Services 3.0 (ADFS 3.0).

Any implementation profile using SAML 2.0 Tokens is acceptable as long as the SAML 2.0 Token security controls (sign, validate and encrypt) are in line with the guidelines found by following this link[1].

05.1.1 Corporate Active Directory

This section contains information related to the Corporate Active Directory (AD).

Government's AD forest is made up of a root domain which acts as an 'empty container' to 'link' a child domain which is used as a container for users within Government.

05.1.2 Segregated Hosting Environment Directories

Segregated hosting environment (SHE) Directories are directory services solely managed by the SHE system administrators to serve dedicated solutions that require a totally sandboxed environment.

05.2 DHCP

Workstations over the MAGNET are allocated IP addresses via DHCP.

05.3 Internal DNS

Internal DNS zones are currently integrated within Active Directory and each domain is authoritative for its own namespace. All other queries are forwarded to a central DNS service which knows about all authoritative DNS servers and can forward queries accordingly.

05.4 Email

Corporate mail services are provided throughout MAGNET and the internet. Users are provided with access to the central mailboxes on MS Exchange through the use of Outlook Web Access, RPC over HTTPS and ActiveSync for mobile services.

Email coming from the internet is received by the Mail Exchangers via SMTP. Email is passed through a number of security layer filters for malicious content and solicitation, amongst others, prior to delivering to the user mailbox.

05.5 File Shares

The Government allocates an amount of storage space for central storage of user data and project related information. These file shares are available on the Government consolidated office automation resources through Windows File Sharing.

05.6 Document Collaboration Service

MITA document collaboration platform is based on MS SharePoint 2013 and is available as a core service throughout government. Team sites are configured for clients who manage most components of the site, including authorisation. Users are stored within the corporate active directory and authentication is carried out through ADFS. No users are stored in the directory supporting the platform operations. Rights Management System services may be introduced.

06. Segregated Hosting Environment

A Segregated Hosting Environment (SHE) is an environment which enables Contractors to locate their resources in a segregated environment within the Government's network. Access from the SHE environment to any external resources (including databases, directory services etc.) shall be governed by 'adapters'.

Solutions targeting the SHE should include the provisioning and support of all infrastructure equipment to fully service in a self-sufficient manner the solution therefore including servers (physical and/or virtual), storage, backups, switches, firewalls, software etc. MITA will only provide connectivity to Government's network.

06.1 Adapters

Adapters are used to expose ICT systems/services to external and/or un-trusted systems. Several adapters already exist such as Corporate Identity, email, DNS, etc. while other adapters are being introduced gradually.

07. Internet Service Provider (ISP) Services

07.1 Internet Access

Internet browsing functionality is provided via a web filter.

The web filter cluster provides the following functionality:

- Address translation converting the internal (private) IPs to public IPs;
- Authentication against the corporate user;
- Filtering of websites based on categories;
- A degree of traffic prioritisation.

07.2 Service Hosting

MITA acting as Government's ISP provides internet hosting services, these are located within the Internet Block.

07.2.1 eGovernment Services Hosting Platform

The eGovernment Services Platform consists of two distinct hosting environments each satisfying a diverse set of requirements:

07.2.1.1 SharePoint based Gov 2.0 Enterprise Content Management System

This environment is based on Microsoft SharePoint 2013. Some site collections are configured with Microsoft SharePoint 2010 experience[2]. SharePoint 2013 rest interfaces are exposed as adapters.

07.2.1.2 Web Framework This environment is a Microsoft based, multi-tenant web hosting platform based on:

- Windows Server 2016;
- SQL 2016.

Applications are currently published via a TMG reverse proxy.

07.2.2 Segregated Hosting Environments (SHE)

SHEs can be used to host applications entirely managed by third parties.

Such environments could be virtual environments or in the case of large solutions requiring the computational power of multiple physical servers working simultaneously to provide the required service. The contractor/service owner will procure the necessary servers, data storage, network equipment, security appliances, etc. which can then be installed in MITA's Data Centre(s).

07.2.3 Public DNS

Three public DNS servers are present that serve DNS requests for the zones delegated to them (namely gov.mt) and resolve internet queries for MAGNET clients. The DNS servers are split across separate subnets to minimize the risk of denial of service attacks.

[2] https://mita.gov.mt/en/eGov/eGovServices/Pages/Gov-mt-.aspx

07.2.4 SMTP

The SMTP layer in Govnet consists of:

- a number of incoming sendmail servers acting as a first line of defence against spam and viruses thus dropping or tagging the majority of spam/malicious emails at this layer;
- a number of outgoing sendmail servers used to send email to internet recipients.

07.2.5 Reverse Proxies, Load balancers & WAF

The Reverse Proxy layer consists of an array of Reverse Proxies. Client connections terminate at the reverse proxy which in turn opens a new request to the appropriate web server. External listeners on http (port 80) https (port 443) communicate internally with websites on a random port.

Any internet originating requests for http and https are handled via reverse proxies. The diagram below depicts the typical HTTP web request routing.

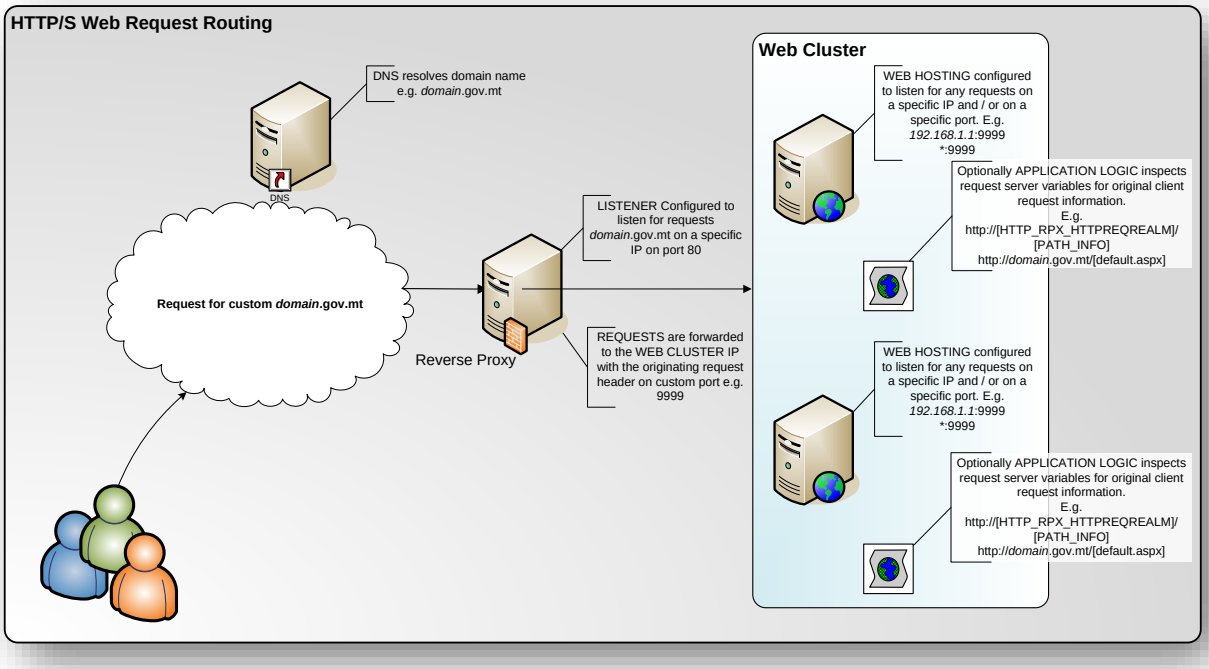

Figure 3 HTTP/S Web Requesting Routing

The reverse proxy does not provide WAF functionality. In this regard, the service owners, may opt to implement a WAF such as mod security under his/her responsibility. In the case of SHE, solution providers may implement own WAF and Load Balancing components and may be subject to auditing by MITA.

07.2.5.1 Public IP Space

GOM can provide Segregated Environment with public IPs

08. eGovernment Shared Services(eGSS)

The eGovernment shared Services (eGSS) aim is to create a services framework for use in citizen related applications, as well as for other bespoke systems to capitalise the investments carried out.

Several services such as mGovernment, myAlerts, eID, Hosted Payment Page and eForms have been developed and new services are being introduced gradually.

Technical information related to established eGSS is available through the MITA Portal at https://mita.gov.mt/en/eGov/Pages/eGovernment.aspx

09. Shared Middleware Platform

MITA operates a multi-tenant shared middleware platform based on WSO2 components. An enterprise support plan is in place to cover the 3rd line support on the platform.
The shared middleware platform enables clients (tenants) to:

1. become more agile with the development of web and mobile applications using shared building blocks;
2. explore alternatives to building and supporting common platforms, such as multi-tenancy, reducing cost and effort;
3. reduce the need for tightly coupled custom code through configuration;

The test and production platforms are made up of the following building blocks.

09.1 WSO2 Identity Server

An Enterprise Identity Bus (EIB) to connect and manage multiple identities across applications, enable alternative authentication methods, manage entitlement/authorization and access control, provision identities and manage API keys.

WSO2 Identity Servers is responsible for the identity and access management across the enterprise applications, services and APIs. The Identity Server uses most widely used standards and allows enterprise architects to implement a security layer upon their own existing assets across their own business. The main capabilities of this building block are: Self-service, Applications catalogue, API calls, Social Login, Broker trust with external IdPs, Account management, SSO and Identity federation (including SSO protocols such as OpenID Connect, SAML 2.0 and WS -Federation to provide a single SSO experience) and the opportunity to manage user and groups with automated user provisioning.

09.2 WSO2 API Manager

Design and publish APIs.

The API Manager building block allows tenants to create APIs and publish them through the API publisher portal. It gives the administrator access control to clearly separate the API developers (The Creators) from the API Publishers (Who are responsible to make the API publicly available). This building block gives tenants the opportunity to secure APIs with different OAUTH2 grant types such as credentials, token and SAML allowing users to consume APIs from different types of applications.

09.3 WSO2 Data Services Server

Integrates data stores, create composite data views and host data services.

The Data Services Server building block allows tenants to make data accessible from anywhere across different formats and transports. This building block provides the capability to combine data from multiple data sources into a single resource, secure data through encryption, create a collection of REST resources for CRUD operations, validate data with built-in validators for standard data types and manage large chunks of data using streaming.