



Government High-Level ICT Blueprint

Date: 18/09/2024

Version: 7.0

Department: CTO Office

Unclassified

Document Control Information

Document reference

CTO-REP-High Level ICT Blueprint-v7.0.docx

Document type

Blueprint

Security classification

Unclassified

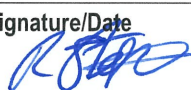
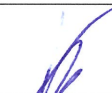
Synopsis

Government High-Level ICT Blueprint

Document control

Author	Change controller	Distribution controller
Roderick Stoner	CTO Office	CTO Office

Authorisation

Issuing authority	Approval authority
Roderick Stoner Enterprise Architect & Technical Fellow	Keith Aquilina CTO
Signature/Date  18/9/2024	Signature/Date  18/9/2024

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
Final Ver 7.0	18/09/2024	Updated version

Acknowledgements

Technology Direction and eGovernment Department

References

Executive Summary

This document provides a High-Level ICT Blueprint of the Government's ICT managed by the Malta Information Technology Agency (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

DOCUMENT CONTROL INFORMATION	2
EXECUTIVE SUMMARY	4
TABLE OF CONTENTS	5
01. OVERVIEW	6
01.1 HIGH-LEVEL TECHNOLOGY PRINCIPLES	6
01.2 DEFINITIONS	6
01.3 DATA SHARING	7
01.4 CORPORATE IDENTITY AND AUTHENTICATION	7
01.5 PROVISIONING OF LINE OF BUSINESS APPLICATIONS AND AUTHENTICATION	7
01.6 GOVERNANCE FRAMEWORK	8
02. NETWORK	9
02.1 MAGNET - GOVERNMENT'S NETWORK	9
02.2 GOVNET - GOVERNMENT'S INTERFACE TO THE OUTSIDE	10
02.2.1 Internet IP Connectivity	10
02.2.2 Remote access	10
02.3 CORE NETWORK ACROSS DATA CENTRES	11
03. DATA CENTRE FACILITIES	12
03.1 MONITORING & ALERTING - OPERATIONAL & SECURITY	12
04. CLIENTS (DESKTOPS/LAPTOPS)	13
04.1 DEPLOYMENT	13
04.2 SECURITY	13
04.3 OPERATING SYSTEM	14
05. CORE SERVICE	15
05.1 OBJECT DIRECTORIES	15
05.1.1 Corporate Active Directory	15
05.1.2 Segregated Hosting Environment Directories	15
05.2 DHCP	15
05.3 INTERNAL DNS	15
05.4 EMAIL	15
05.5 FILE SHARES	16
05.6 SHAREPOINT ONLINE	16
06. HOSTING PLATFORMS	17
06.1 ON-PREMISES HOSTING PLATFORM	17
06.2 OFF-PREMISES HOSTING PLATFORM	17
06.3 ADAPTERS	17
07. INTERNET SERVICE PROVIDER (ISP) SERVICES	18
07.1 INTERNET ACCESS	18
07.2 SERVICE HOSTING	18
07.2.1 Segregated Hosting Environments (SHE)	18
07.2.2 Public DNS	18
07.2.3 Reverse Proxies, Load balancers & WAF	18
07.2.3.1 Public IP Space	19
08. EGOVERNMENT SHARED SERVICES(EGSS)	20

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

The 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 several key attributes that enable these principles. These attributes are identified in constituents that 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 such 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 the solution and component constituents. Specifically, for 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, Web Services, 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 are 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, through 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 to be 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 on-premises physical servers or off-premises in the cloud. 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.
 - **Authentication:** Authentication is the process of verifying the identity of a user, system, or entity attempting to access a particular resource or service. It ensures that the claimed identity is legitimate before granting access, typically through the use of usernames and passwords, biometrics, or other secure methods. Federation Authentication refers to the establishment of trust relationships between various systems or applications to enable seamless and secure user access. Federation allows users to utilize a single set of credentials across a network of interconnected services, eliminating the need for multiple logins.

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 principles/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.

MITA's Interoperability Platform allows data sharing between systems in a standardised and secure manner. Data providers publish their respective data through APIs, and the platform allows consumers to request data that they are authorised to consume.

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. The use of legacy protocols such as LDAP and LDAPS is not allowed.

01.5 Provisioning of Line of Business Applications and Authentication

The strategic provisioning of line-of-business applications demands a meticulous approach geared towards fostering maximum abstraction from the desktop stack. This strategic manoeuvre not only facilitates the autonomous evolution of both desktop environments and applications but also enhances operational agility. Recognizing the pivotal role of abstraction in this context, it has been discerned that web applications and containerized solutions stand out as prime candidates to deliver the requisite level of abstraction.

Furthermore, in the realm of authentication, it is imperative to adopt robust, open, and industry-standard authentication protocols, adopting a federated-approach for authentication. Such a proactive stance not only ensures heightened security measures but also promotes loose coupling and abstraction from the

intricacies of underlying technology stacks. Federated Authentication is considered a key element in the solutions design and can be facilitated by integrating with MITA's authentication services provisioned through Azure Active Directory B2C.

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.

02. Network

02.1 MAGNET - Government's Network

MAGNET is the Government's network linking the MITA Data Centres to Ministries, Departments, Local Councils, district offices, hospitals, entities, embassies, and the off-premises cloud infrastructure. This seamless network allows Government employees to securely access information hosted at the MITA Data Centres, Cloud Based systems and also provide Internet Connectivity.

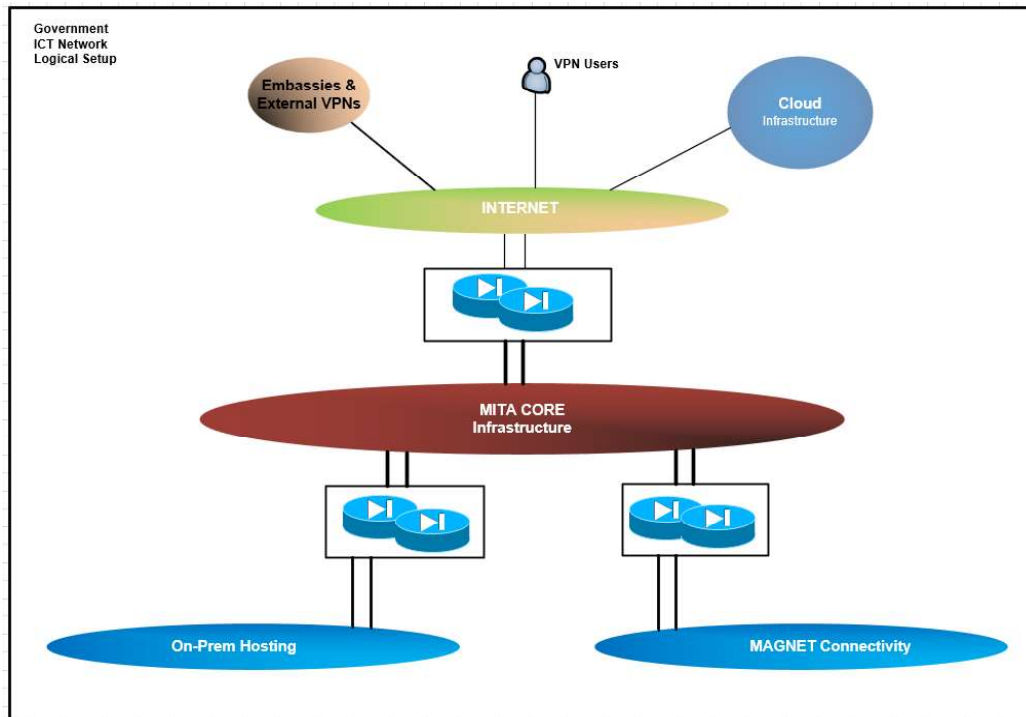


Figure 1 Government ICT Network Logical Set-up

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.

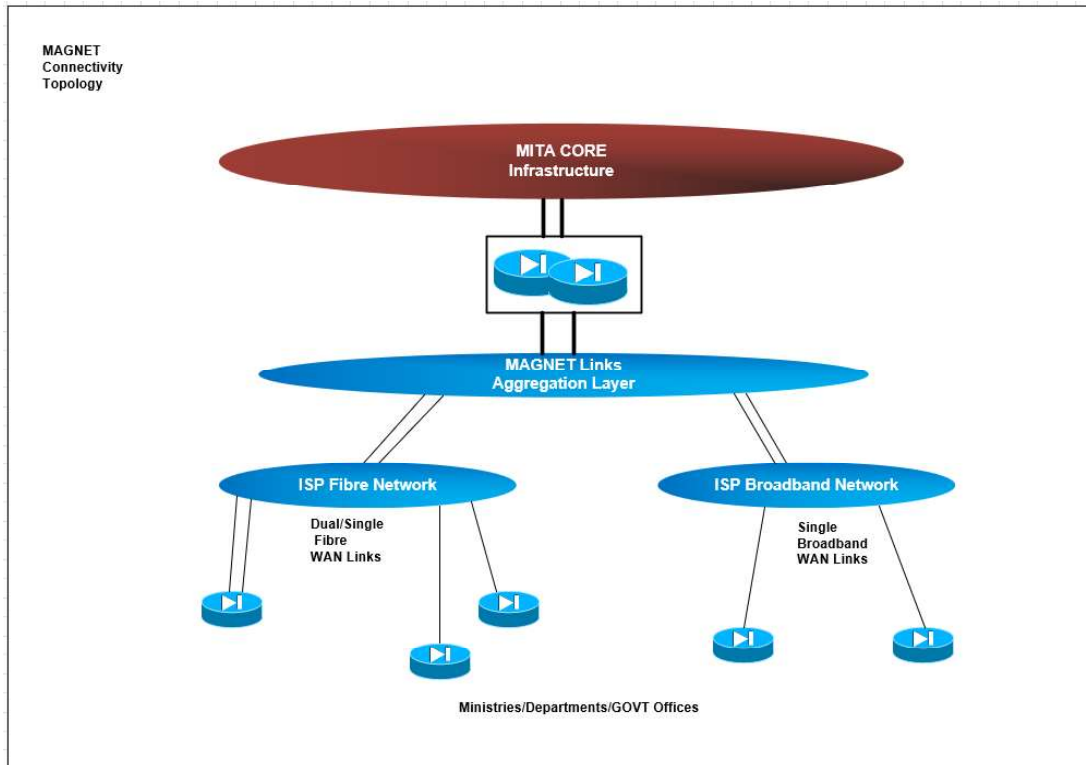


Figure 2 MAGNET Backbone Topology

The MAGNET connectivity is geographically present across Malta and Gozo, connecting all MITA services to the Government sites via fibre and broadband links. These are VPN encrypted links providing low latency, and high bandwidth connectivity. Most of the critical sites have dual fibre connections passing through physically separate routes. The remaining sites are connected via one fibre link or a broadband link.

Government embassies and Foreign Offices are connected via VPN Technology 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 local ISPs.

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

02.2.2 Remote access

Teleworkers and Remote Users access is securely provisioned via SSL VPN and multi-factor authentication, whilst network to network VPN is offered via IPSec in tunnel 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 2 logical environments. 80Gbps and 40 Gbps of bandwidth is available across sites and 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 Layer 3 routing protocols.

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 should be implemented redundantly, preferably at the application level, across both data centres.

03.1 Monitoring & Alerting - Operational & Security

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

The Network Operations Centre (NOC) ensures 24x7 monitoring of the entire Government ICT infrastructure, including servers, services, networking equipment, websites, backups, and Data Centre facilities, to maximize service availability and meet target availability figures. This is accomplished through a comprehensive Network Management System (NMS) equipped with various service availability monitoring tools, providing full visibility, and enabling the NOC to respond to alerts effectively. Additionally, NOC serves as the gatekeepers for the two corporate Data Centres, handling any related physical interventions or hosting requests.

The Security Operations Centre (SOC) within MITA continuously monitors the Malta Government Network (MAGNET), connected assets and consumed identities. The SOC maintains active security monitoring through various tools, including an Endpoint Detection & Response (EDR) agent which is installed on devices connected to MAGNET. The tool is used to scan, detect, and respond to security threats on endpoints based on several characteristics such as software signer, file hash, detected activity, and user behaviour analytics.

04. Clients (Desktops/Laptops)

This section details information related to clients managed by MITA.

All desktops managed by MITA are hybrid joined to Microsoft Entra ID and the local Active Directory. Moreover, each PC is being provided with a standard desktop profile. Devices are managed using both Microsoft Configuration Manager (SCCM) and Microsoft Intune.

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 joins the device to the local Active Directory and includes the following:

- Standard Software (Such as; Office Productivity Tools and Antimalware, etc.);
- SCCM agent

Microsoft Entra ID joined Windows workstations can also be deployed using Autopilot. This requires the hardware hash of the machine to be collected beforehand and sent to MITA for enrolment.

04.2 Security

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

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

- Adheres to a standard desktop configuration.
- Applies the group policy objects and Intune policies for the purposes of 'locking' to minimise user tampering and experimentation with the desktop's configuration, thus minimising the number of desktop incidents;
- Have applicable endpoint security which is active and always up to date.
- Is managed via SCCM / Intune.
- User accounts are set up such that users have local user rights on their workstations. The default security settings will prevent end-users from compromising the integrity of the operating system and installed programs.
- Users cannot modify system-wide registry settings, operating system files, or program files and do not have the necessary permissions to install applications.
- Users can run certified Windows programs that have been installed or deployed by administrators. Users have Full Control over all their data files (%userprofile%) and their portion of the registry (HKEY_CURRENT_USER).
- OneDrive has been setup to automatically backup the users profile, namely Desktop, Documents and Pictures
- BitLocker, secure boot and TPM are enabled.

04.3 Operating system

Most of the desktops and notebooks managed by MITA are installed with either Windows 10 Enterprise or Windows 11 Enterprise. The operating system is centrally managed via GPOs/GPPs/Intune 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 MITA's B2C. Federated Authentication approach must use industry standards such as OpenID and SAML 2.0 and must follow the industry's best practices

05.1.1 Corporate Active Directory

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

The Government's AD Forest is made up of a root domain that acts as an 'empty container' to 'link' a child domain which is used as a container for users, groups and computer/server objects within Government.

The directory is synchronised with Microsoft Entra ID (formerly known as Azure AD) via Entra ID Connect. User logins, Groups and Computer objects are synchronised.

Microsoft Entra Domain Services (formerly known as Azure AD DS) is available to connect legacy workload hosted on the cloud.

A separate Active Directory domain for Health is also available, which has a forest trust with the root domain mentioned earlier. This domain contains server objects, service (application) accounts and groups related to Health systems. This domain is not synchronised with Entra ID

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 fully sandboxed environment.

05.2 DHCP

Workstations over the MAGNET are allocated IP addresses and other related settings such as DNS via DHCP. Servers on On-Premises platforms should be allocated static IPs.

05.3 Internal DNS

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

05.4 Email

MITA provides an Electronic Mail (email) Service, with mailboxes hosted on MITA's infrastructure and also on the cloud, as a store and forward method of composing, sending, receiving, and storing messages over electronic communication systems.

Email coming from / to the internet is filtered through several security filters for malicious content and solicitation, amongst others, before delivering to the user mailbox.

On-premises solutions requiring email sending services may use MITA's on-premises SMTP servers, whilst solutions in the off-premises cloud may use MITA's off-premises SMTP offering which requires SMTPAuth for authentication.

05.5 File Shares

MITA allocates an amount of storage space for the storage of user data via OneDrive. Project data related shares are provided through a mapped drive from the Government consolidated File Share Service resources through Windows File Sharing (SMB). Such file shares are mapped using DFS Namespace and can also be accessible through an online portal upon request.

05.6 SharePoint Online

Microsoft SharePoint Online is a Cloud Storage Service assigned with Office 365 subscription licences. This service is intended to facilitate collaboration and sharing by means of a platform where users can create, edit, and share data with other users within the Government Tenant.

The service is divided into two streams:

MITA managed sites – For MITA managed sites, permissions, and design falls under the responsibility of MITA. These sites are to adopt the same concept as that of the current FSS shares and will be used to host data from such location.

Client managed sites – For Client managed sites, it is the responsibility of client to nominate an administrator to manage permissions and design. Client managed sites include sites which are created when users create a team in MS Teams, Hub sites and any other sites which users request to be created.

06. Hosting Platforms

MITA operates the notion of a Segregated Hosting Environment (SHE) principle. A SHE is an environment that 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, in the case of physical servers, this includes; servers, storage, backups, switches, firewalls, software etc. In the case of virtual servers hosted on the on-premises hosting platform, the platform servers, storage, switches, and firewalls will be managed by MITA whilst VMs and their contents are to be managed by 3rd parties. Whilst, when a solution is being hosted in the off-premises hosting platform, MITA is responsible till the Resource Group and the 3rd party will be responsible for any resource within the Resource Group. In all cases, MITA will only provide connectivity to Government's network.

06.1 On-Premises Hosting Platform

The on-premises hosting platform is based on an HCI VMware implementation that is stretched across both DCs offering flexible availability options for VMs. Storage is implemented via VMware's vSAN all-flash storage. Storage / VMs can be hosted on a single-site or dual-site.

The platform does not support the use of Microsoft NLB (Network Load Balancing) or the use of RDMS. The use of physical bus sharing is also discouraged.

06.2 Off-Premises Hosting Platform

The off-premises hosting platform is based on Microsoft's Azure Cloud and is available in the following regions; Italy North, West Europe and North Europe. Italy North and West Europe are the primary regions for all workloads, with Italy North being preferred due to its proximity to Malta. West Europe is used when a required service is not available at Italy North. West Europe is also used in conjunction with North Europe for those solutions that require regional disaster recovery. Other regions within the EU may be offered in the future as MITA deems fit.

06.3 Adapters

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

07. Internet Service Provider (ISP) Services

07.1 Internet Access

Internet browsing functionality is provided via multiple redundant fibre links from two separate ISP's. These are ultimately aggregated on a redundant firewall cluster.

The Firewall 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 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).

07.2.2 Public DNS

Public DNS service is hosted in the off-premises cloud.

07.2.3 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.

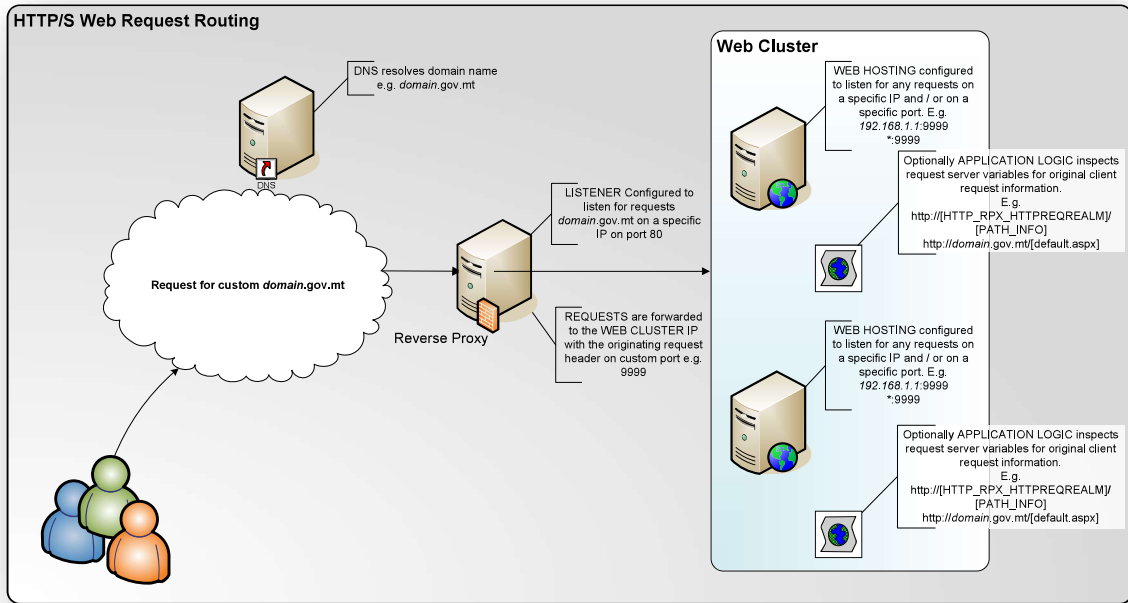


Figure 3 HTTP/S Web Requesting Routing

07.2.3.1 Public IP Space

MITA can provide Segregated Environment with public IPs although discouraged. Solutions requiring external access should ideally use internal IPs and be exposed via an adapter.

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 on the investments carried out.

Several services such as; Workflow Automation Solution, Government Payment Gateway, Notifications Platform, and the WordPress Hosting Platform are available horizontally within Government to complement various IT systems.

Technical information related to established eGSS is available through the MITA Portal at <https://mita.gov.mt/portfolio/information-systems/>