Conceptual Architecture Design Specifications for an Electronic Signature Solution

---

SUMMARY: THIS DOCUMENT OUTLINES THE CONCEPTUAL ARCHITECTURE DESIGN OF AN ELECTRONIC SIGNATURE SOLUTION

DATE OF APPROVAL OF THIS ISSUE:

Abbreviations and Definitions

AeSign	Advanced electronic signature
CA	Certificate Authority
DMZ	De-Militarized Zone
ECM	Enterprise Content Management
EXCO	Executive Committee
ICT	Information and Communications Technologies
ISO	International Standards Organisation
PAN	Processor Area Network
PDF	Portable Document Format
RMS	Records Management System
SCM	Supply Chain Management
SLA	Service Level Agreement
VM	Virtual Machine
XML	Extensible Markup Language

Index of Architecturally Relevant Documents

Document Name	Document Link
Business Requirements Specification for Electronic and Digital Signature	http://intranet.net0.ad/sites/ict/eaim/BA/Business%20Requirements%20Specs/Business%20Requirements%20Specification%20for%2

Document Name	Document Link
	0an%20Electronic%20Signature%20Solution.doc
ARMSCOR ENTERPRISE ARCHITECTURE STANDARDS	http://intranet.net0.ad/sites/documents/Management%20Documents/A-DOC-5016.pdf#search=EA%20standards

Document Revision History

Version	Date	Comments
v0.01	2021-04-12	First Draft
v0.02	2022-02-14	Second Draft (updated Figure 2)
V0.03	2022-05-23	Third draft (update of Table 1 and Figure 3)
V0.1	2022-05-25	Final draft

Table of Contents

1. PROJECT INFORMATION

Armscor is a state-owned entity that exists in terms of Act 51 of 2003. Its core function is to acquire military equipment on behalf of the Department of Defence (DOD), including rendering other support functions. In its day-to-day operations, the organisation produces several document artefacts, most of which require official approval. The document approval process is currently facilitated by storing documents on Microsoft SharePoint from where they can either be electronically signed using Adobe Acrobat reader or printed out for manual signature. Email voting functionality is sometimes used as a form of electronic signature. Creating an electronic signature for use within Adobe Acrobat is a manual process prone to quality errors and security non-compliance. Email voting lacks a full audit trail, and manual signatures are inefficient, resulting in delays in the approval process.

As part of the corporate objectives to improve internal efficiencies, the organisation has acknowledged the value to be realised by endorsing the procurement of the digital and advanced electronic signature solution.

2. PROJECT SCOPE

The business requirement is for the Service Provider to implement, configure and maintain the digital and advanced electronic signature solution to enable Armscor to realise its corporate objectives.

2.1 Inclusions

The service provider to provide the following;

- An end-to-end solution to enable digital and advanced electronic signatures for document approval.
- Integrate the solution to identified business applications outlined in the interface map.
- All Armscor document types requiring signature-based sign-off; these documents must have a security classification below "Secret".

The service provider is also expected to provide support and maintenance of the solution post-implementation. Training of Armscor technical users must also be provided during the development of the solution. This is to ensure the solution is handed over properly and Armscor is able to support it internally in the long run.

The solution needs to operate as outlined in the Business Requirements Specifications document.

2.2 Exclusions

The following is excluded from the scope of this solution:

- All documents artefacts with a security classification level of "Secret" and "Top Secret".

3. ARCHITECTURAL SUBMISSION

3.1 Business Architecture

3.1.1 Business Strategies and Plans

In line with Armscor corporate objectives of improving internal efficiencies, the sourcing of a signature solution will help mitigate risks associated with long turn-around times in the approval of business documents. Below are some of the benefits of having a centralised electronic, digital and advanced electronic signature solution:

- Signatories do not need to be office-bound to be able to sign documents.
- Better alignment to legal and regulatory requirements governing the use of electronic signatures.
- Non-repudiation and audit trail of signed documents.
- A centralised system that ensures consistency and quality management of document approval procedures

3.1.2 Business Organisation Design

The solution's final implementation will impact all Armscor business areas and their respective departments.

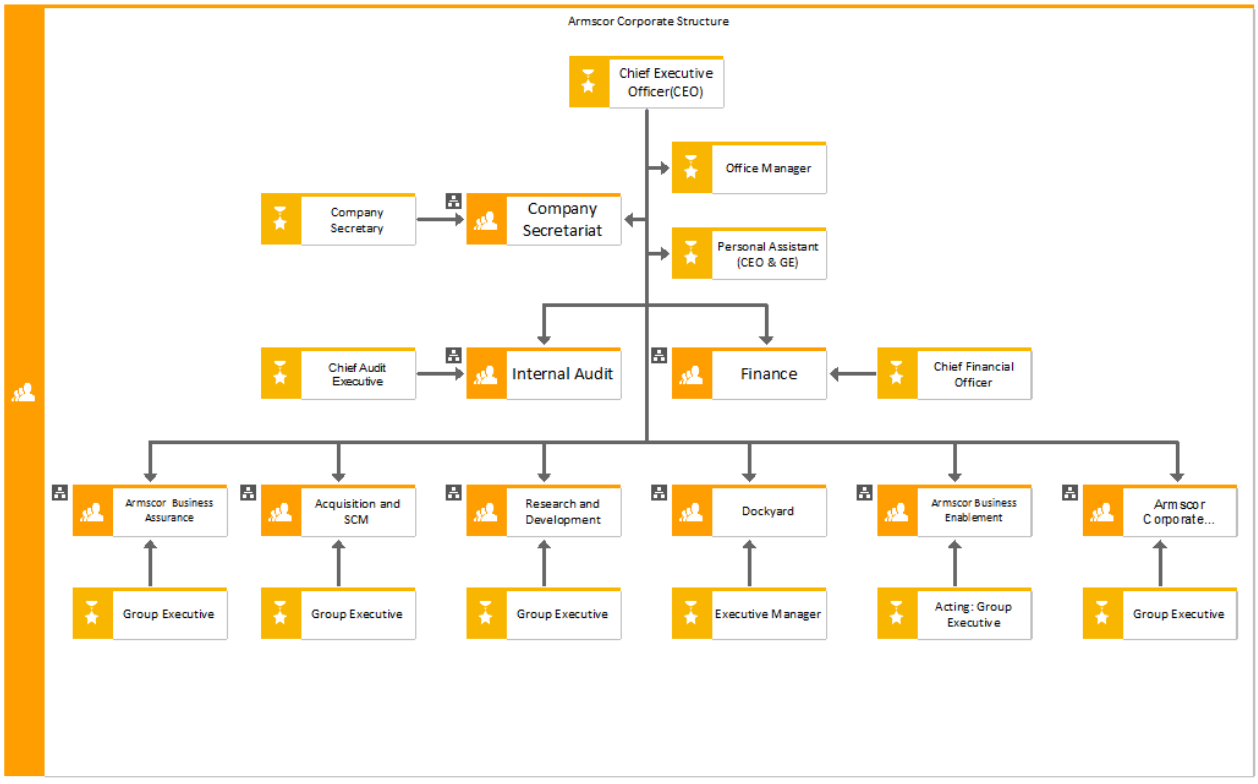

Figure 1: Armscor Organisational structure.

The solution must cater for 500 users broken down into the following signature types shown in the table below:

Signature Type	Total Number of Users
Digital signature	475
Advance electronic signature (AeSign)	25

Table 1: e-Signature allocation for Armscor staff

3.2 Application Architecture

3.2.1 Application Functional Decomposition

To support the requirement described in the business requirements document, the proposed solution will have the following key functionalities as depicted in the Application Capability model in Figure 2.

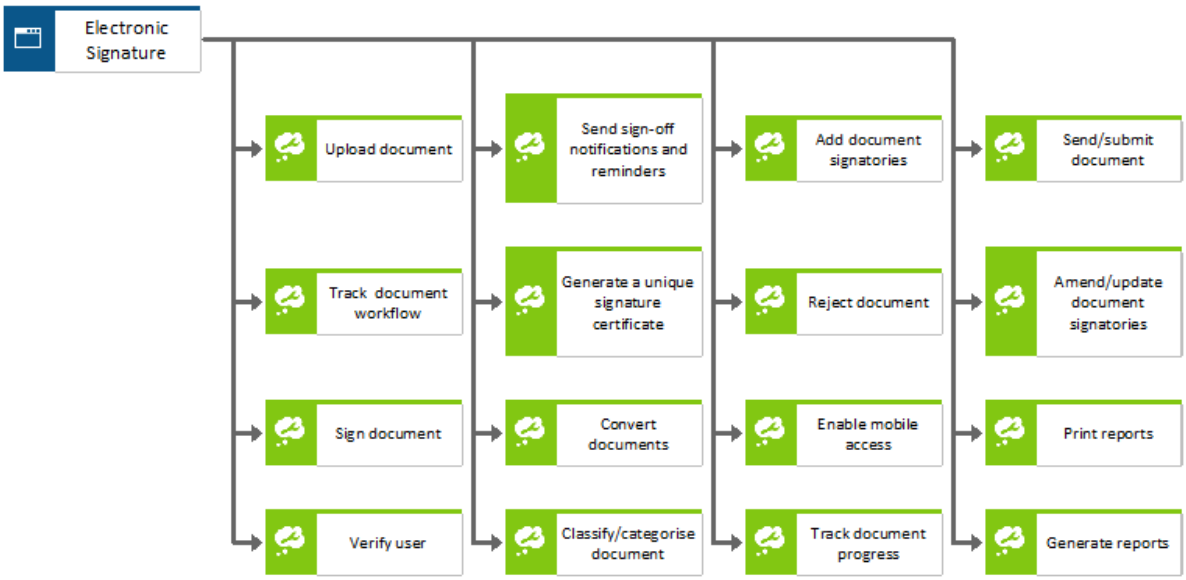

Figure 2: Application Capability model

3.2.2 Application Development

The solution comprises several hardware and software components that make up the complete system. Solution deployment will consist of all the individual hardware/software components that function as one fully integrated solution. An in-depth description of all the system's features will be outlined in the detailed architecture design document upon selecting the preferred solution.

3.3 Data Architecture

3.3.1 Data Models

The solution shall include a centralised, configurable data dictionary describing table structure, relationships, and appropriate metadata levels. All the relevant data models will be identified and defined during the detailed architecture design phase.

3.3.2 Object/Application Service Models

To be addressed in the detailed architecture design document.

3.3.3 Information Flow

The information flow is depicted in Figure 2.

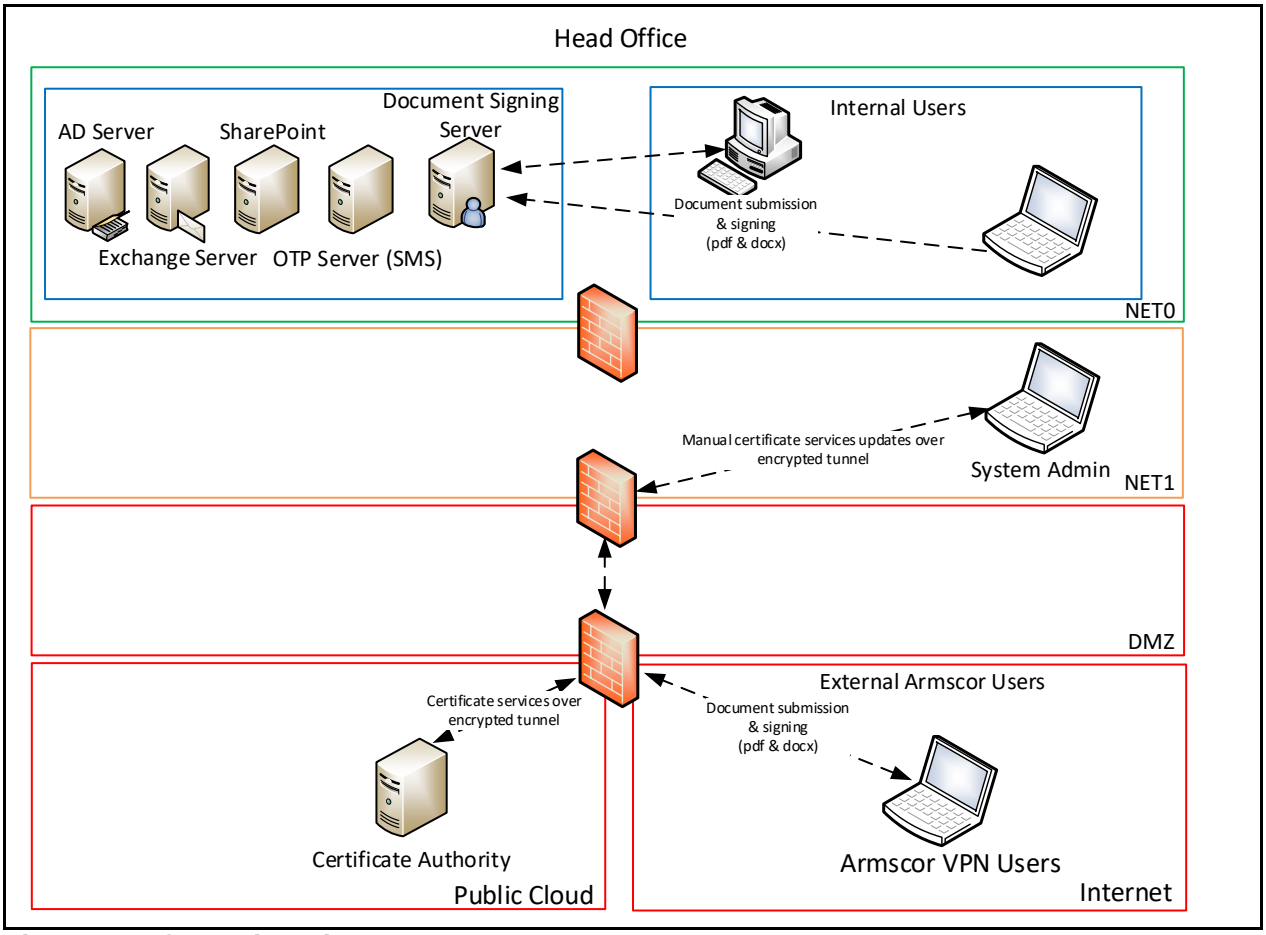

Figure 3: Information Flow

3.3.4 Information Integrity and Custodianship

The solution will remain the property of the service provider, with Armscor paying a perpetual annual license fee. The service provider will also be responsible for the support and maintenance of the solution, including the support and maintenance of the certificate authority infrastructure hosted on the public cloud. The system admin/user will be responsible for entering

and configuring users and services on the system. Custodianship of the signed and unsigned documents will rest with the business owners of those specific documents stored on the system.

3.3.5 Information Access and Confidentiality

Once the system is rolled out to the rest of the organisation, user access to the system will be aligned with their defined roles and responsibilities within their respective departments. The access roles and rights of users will be defined in the detailed architecture design phase.

3.3.6 Information Related Business Continuity

The solution will be classified in line with current ad hoc tools/processes used within the ICT DevOps division. The following table serves as a guideline for the different system classification levels:

System Importance to Business	Tier 0	Tier 1	Tier 2	Tier 3
Maximum Downtime / RTO	0 Hours	12 Hours	24 Hours	48 Hours
Maximum Data Loss / RPO	0 Hours	12 Hours	24 Hours	48 Hours

Table 2: System criticality classification levels.

Armscor's current, existing and approved business continuity mechanisms will be adopted. An SLA will be entered between Armscor and the service provider of the solution regarding all services offered via a public cloud.

3.4 Integration Architecture

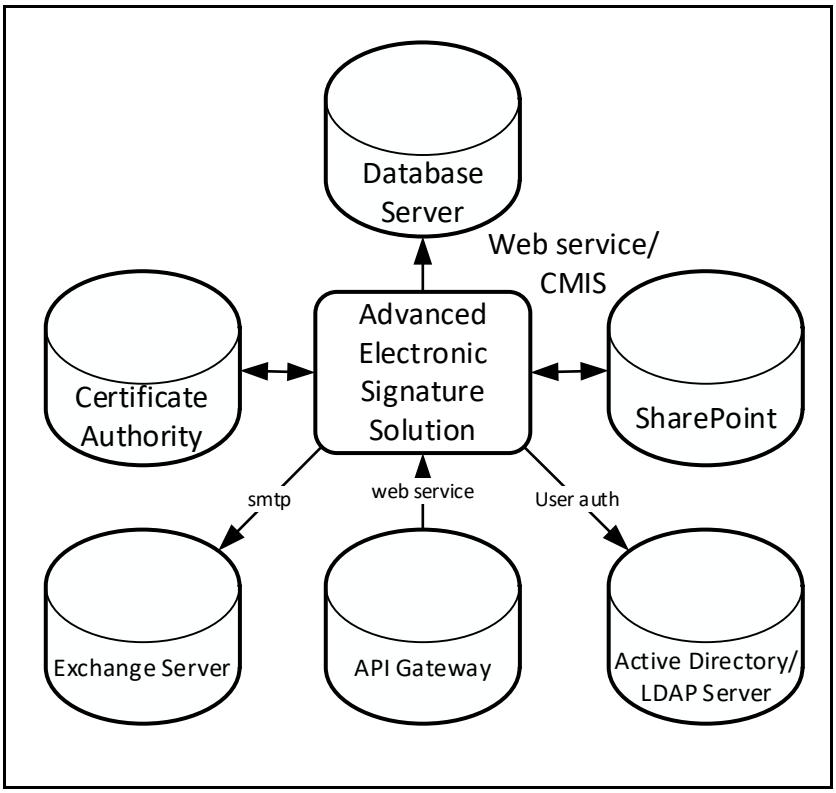

Figure 4: Interface Map

Please note that there will not be a direct integration between the on-premise document signing portal and the certificate authority infrastructure hosted on the internet. The updating, revocation of root certificates and updating of user certificates/information will be done manually through a secure connection from Net1 to the PKI infrastructure hosted on the internet.

3.5 Technical Architecture

3.5.1 Applied Technologies

The Digital and Advanced Electronic Signature solution is required to conform to the following technologies:

Database	**Support Relational SQL-based databases**
Operating System	Support all of these client operating systems: • Windows 7 or later Support at least one of these server operating systems: • SUSE Linux Enterprise Server 12 (SLES) • Ubuntu 18.04 LTS or later • Microsoft Windows Server 2012 R2 or later
User Authentication	• Active Directory and LDAP
Reporting	Export content in, at a minimum:

	• PDF • MS Word compatible formats (DOC, DOCX, RTF, ODF) • HTML (web-based) • Image formats as stipulated in the BRS document
Interoperability	The system should be able to interface with various third-party solutions using standard API technologies • Rest, JSON API or XML
Integration	Internal systems to integrate with: • MS Exchange 2010 • MS SharePoint 2013

3.5.2 Basic Infrastructure

The hardware, software, and network infrastructure needed to support the solution's deployment will be outlined in the detailed architecture design document to be supplied by the service provider. However, Figure 4 illustrates a high-level implementation of the proposed solution at Armscor Head Office including how Armscor users at remote sites and via VPN will connect to the solution.

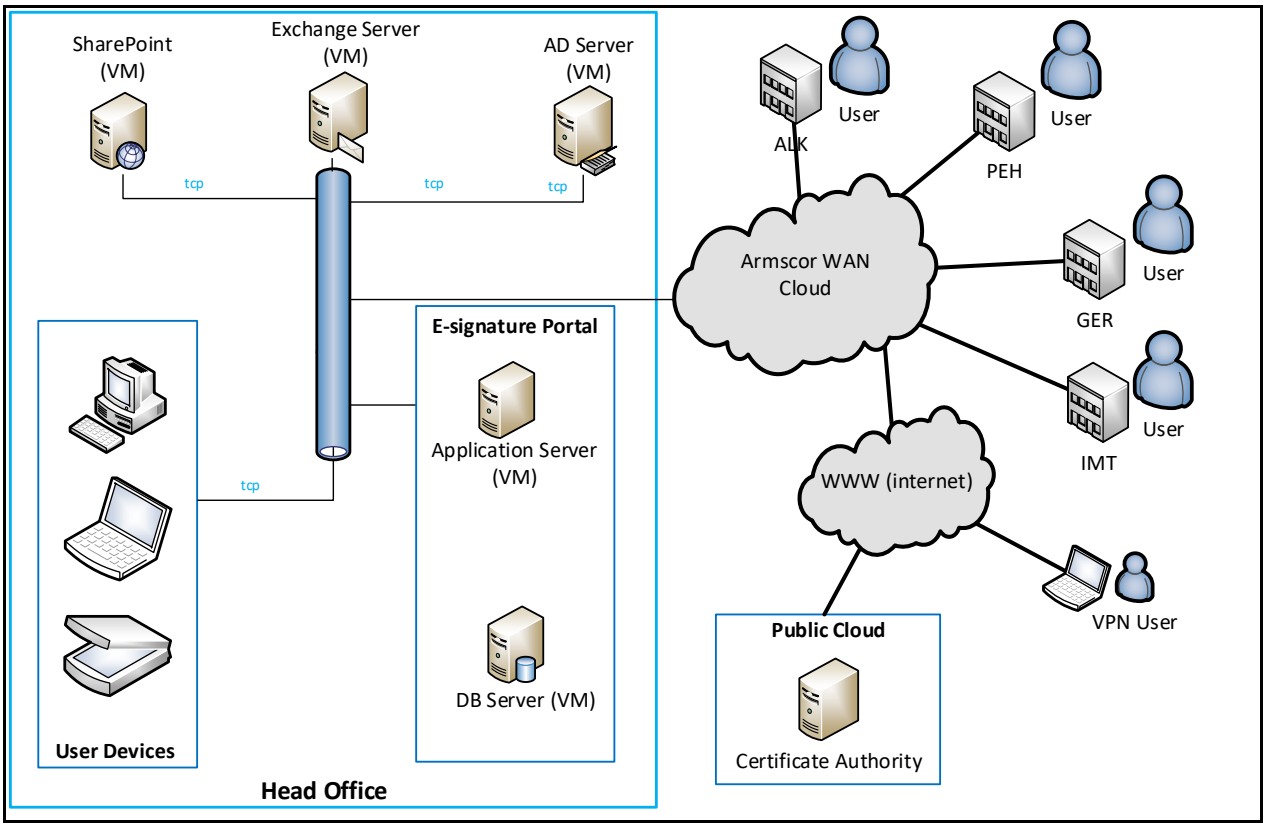

Figure 5: Basic technical architecture for the digital and advanced electronic signature solution

3.5.3 Deployment Considerations

The client-facing document submission and signing application server will be deployed on-premise at Armscor head office in a virtualised server environment running on Microsoft Hyper-V platform. This environment comprises a Processor Area Network (PAN) that utilises a Storage Area Network back-end. The PAN is housed on Cisco Unified Computing System hardware platform. The detailed layout of the physical infrastructure will be outlined in the detailed architecture specification document.

Figure 5 shows the Armscor Metro Ethernet (ME) WAN network layout for all the sites.

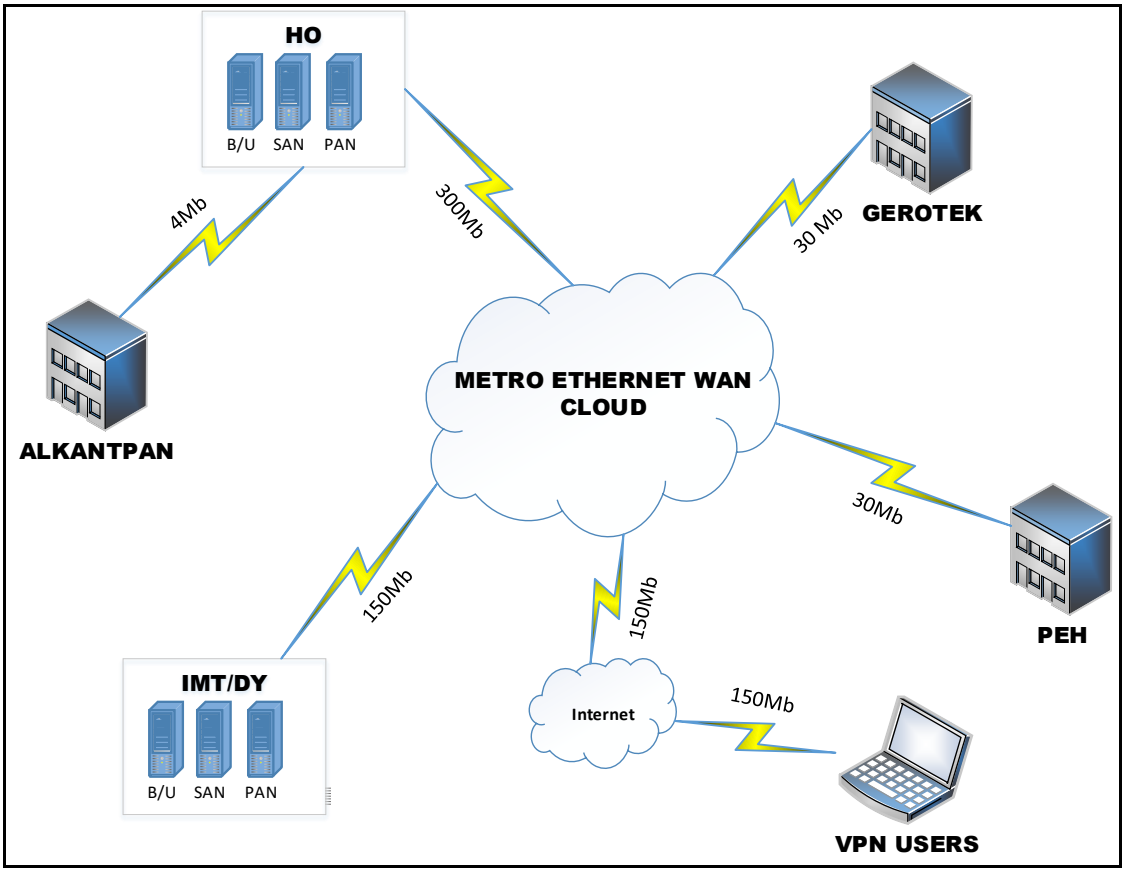

Figure 6: High-level Armscor network topology

3.5.4 Solution Development Environment

The solution development environments shall include:

- Development;
- Testing;
- Production.

Hardware requirements for each environment shall be detailed as part of the response.

3.6 Security Requirements

Security is the ability of a system to protect information and system resources with respect to availability, confidentiality and integrity. The security requirements, including formulation and enforcement of adherence to the agreed security architecture, as defined by Cyber, will be used to define and design the processes and data access controls during the System Delivery Specification and Technical System Design.

The solution will operate in an existing secure environment but will require in addition, its internal application security to be controlled by an Application System Administrator. The security capability will be required to conform to the relevant Armscor security policies and practices.

Within the context of the broader Armscor security architecture, the following considerations need to be taken into account:

- There should be a formal user registration and de-registration procedure for granting access to all multi-user information systems, resources and services;
- Message authentication should be used for applications where there is a security requirement to protect the integrity of the message content;
- Sensitive or Confidential data/information across the networks, or to copy to other media, when Confidentiality and Integrity of the data needs to be assured;
- Non-repudiation services should be used to resolve disputes about the occurrence or non-occurrence of an event or action;
    - Access control at the data and functionality level must be according to roles. Partitioning of data access must always be based on a need to know approach. In essence, a hierarchical structure where various parties have organisational and role-based access to the system and its data and functionality must be provided along with tools for simple and easy User Administration thereof.
- Audit Trail;
    - The design and implementation shall ensure audit trails to track user access and behaviour to ensure system integrity through verification.
- The solution should have an open and extensible security platform.