

HLD – EXC

Excasso-Complex (VFV)

Version: 1.3

Date: 17 November 2023

Document purpose

This High Level Design (HLD) is used to:

* Validate the Application solution from a technical perspective through architectural review
* Plan and execute implementation of the solution
* Support Technical Application Management

The document outlines:

* An overview of the application and its architecture
* Functional and non-functional requirements
* Solution description
  + By default, the solution will use standard services from the DXC catalog for UWV. Where applicable required variances will be described.

Relation to Reference Architecture, ABB’s, HLD VI, SBB’s and SAD

The UWV Reference Architecture provides the context for the HLD VI. The HLD VI is focused on the architectures enabling the datacentre hosting services, its building blocks and the integrations.

* **Architectures Building Blocks (ABB)**, maintained by UWV, are built up from a collections of solution building blocks (SBB’s), so most building blocks will interoperate with other building blocks (integrations).
* **Solution Building Blocks (SBBs),** maintained by DXC, represent components that will be used to implement the required capability for the datacenter hosting service;

This HLD leverages the ABB’s and SBB’s as a foundation for the solution.

The following documents may be relevant as context to this HLD:

* The Software Architecture Document
* Technisch Beheer Handboek (TBH – technical management handbook)
* Technisch Koppelvlak Document (TKD – technical interface document)
* Procedure HandBoek (PHB – procedure handbook – part 1 = standard, 2 – exceptions)

Structure of the document

High level flow: first the application overview and architecture are described followed by the functional and non-functional requirements that ‘drive’ the solution as described in the final chapter. The appendices include any additional details or specifics for the application described in this HLD. See table of contents on next page for further details.

Content of the document

DXC has prepared this document in good faith and is partly based on the information made available to it by UWV and IBM (e.g. HLD document). The statements and content in this document should be qualified accordingly. For the same reason some references in this document might be ‘outdated’ (i.e. not in this document anymore nor in other related documents).

Table of Contents

[1 Application Overview 4](#_Toc118721244)

[1.1 Introduction 4](#_Toc118721245)

[1.2 Application use cases 4](#_Toc118721246)

[1.3 Out of Scope 4](#_Toc118721247)

[2 Architecture 5](#_Toc118721248)

[2.1 Conceptual 5](#_Toc118721249)

[2.2 Context diagram 6](#_Toc118721250)

[3 Functional Requirements 16](#_Toc118721251)

[4 Non-Functional Requirements 17](#_Toc118721252)

[4.1 Security & Compliance classifications 17](#_Toc118721253)

[4.2 System and Software requirements 17](#_Toc118721254)

[4.3 Availability 18](#_Toc118721255)

[4.4 Security requirements 18](#_Toc118721256)

[4.5 System management 18](#_Toc118721257)

[4.6 Backup and Recovery 18](#_Toc118721258)

[4.7 Storage replication 19](#_Toc118721259)

[4.8 Scalability 19](#_Toc118721260)

[4.9 Disaster Recovery 19](#_Toc118721261)

[4.10 Infrastructure Technical Constraints 19](#_Toc118721262)

[4.11 DXC TAB requirements 19](#_Toc118721263)

[5 Solution 20](#_Toc118721264)

[5.1 Architectural Decisions 20](#_Toc118721265)

[5.2 Node descriptions and zone-projections 21](#_Toc118721266)

[5.3 System diagram – Production 23](#_Toc118721267)

[5.4 System diagram Non-Production 24](#_Toc118721268)

[5.5 SBB’s 26](#_Toc118721269)

[5.6 Load balancers 26](#_Toc118721270)

[5.7 Deviations from standards (RAL / EtP) 27](#_Toc118721271)

[5.8 Service Management 27](#_Toc118721272)

[5.9 Security 27](#_Toc118721273)

[6 Potential future improvements 30](#_Toc118721274)

[Appendix A: Technology and Sizing (at design 31](#_Toc118721275)

[Appendix B: Network Protocol Matrix 36](#_Toc118721276)

[Appendix C: Users and Groups 39](#_Toc118721277)

[Appendix D: Security 41](#_Toc118721278)

[Appendix E: Glossary 43](#_Toc118721279)

[Appendix F: Legenda 44](#_Toc118721280)

[Legenda Context Diagram 44](#_Toc118721281)

[Legenda System Diagram 44](#_Toc118721282)

[Appendix G: Control 45](#_Toc118721283)

# Application Overview

## Introduction

VFV (Excasso); Excasso Complex consists of several subsystems that perform specific tasks, which can be found in paragraph 2.1.

Gross/Net systems: The excasso application processes all Gross and Net requests from several claiming systems into a ´rekening courant´ claim or payments. Built-in functionalities are able to handle the financial functionalities automatically.

Claims (´Invorderingen´ or INV): Registers internal and external claims (claims by third parties).

RPO (´Regio Personeel en Organisatie´): Records the organisation diagrams and officials.

GEM (´Gemeenschappelijke fiscale persoonsgegevens´): Stores fiscal details which are consulted and used for verification of each payment.

EBH (´Excasso Boekhouding´): Contains and maintains the definitions of journal entries. EBH receives booking rules from the various subsystems and translates these to journal entries which are transferred to the financial administration (PeopleSoft).

BSU (´Betaling Systeem UWV Bouwnijverheid´): Automated, daily payments to insured or third parties.

ALIS (´Algemeen Loonbelasting InformatieSysteem´): Performs the fiscal information provision to the tax company.

SBS & OBS (replacing the current FBS application). SBS is an application designed to mutate the control tables for Excasso in all domains (OTAP). OBS is an application designed to mutate the other tables for Excasso in their respected domain only.

## Application use cases

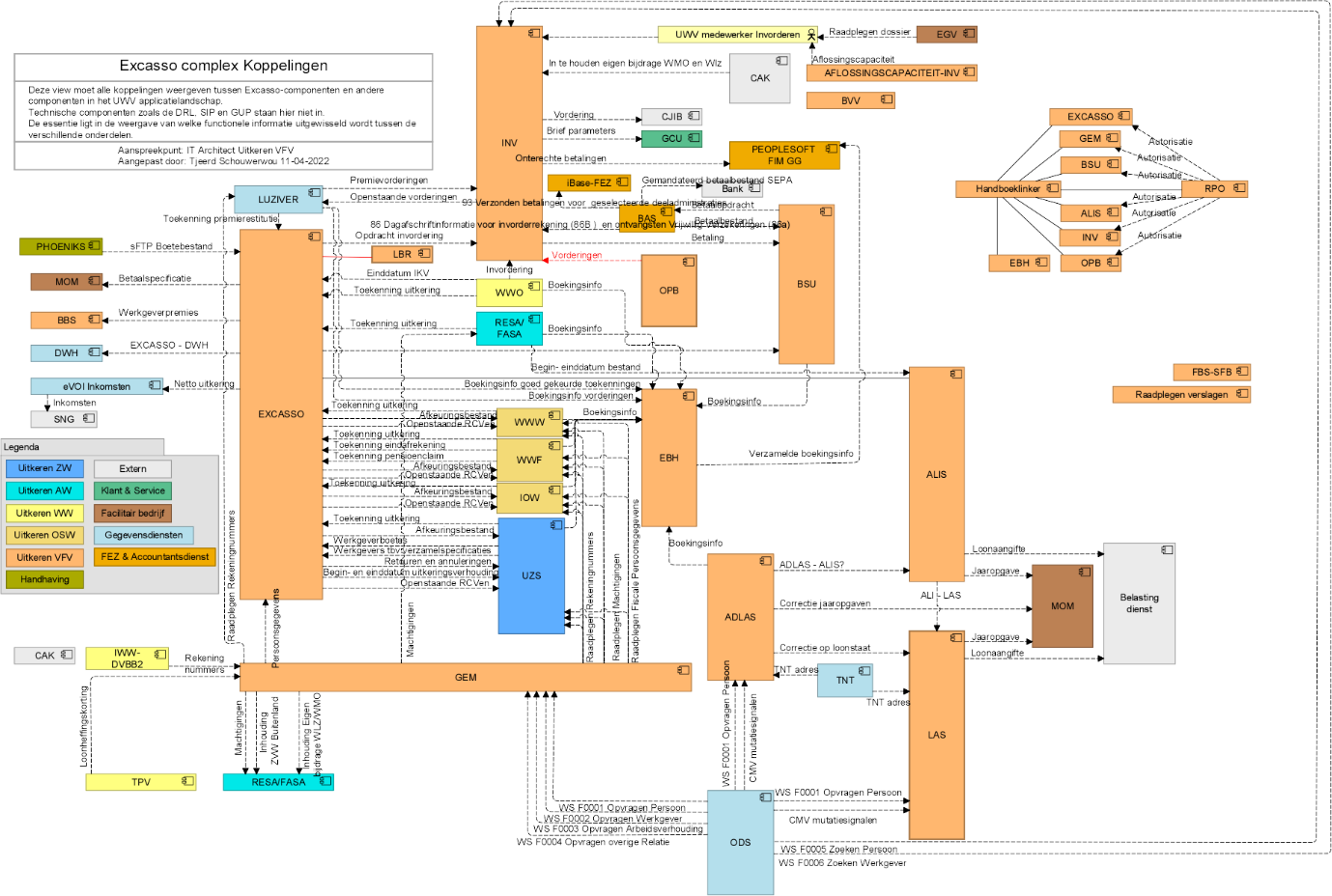
Application use cases are defined in 1.1.

## Out of Scope

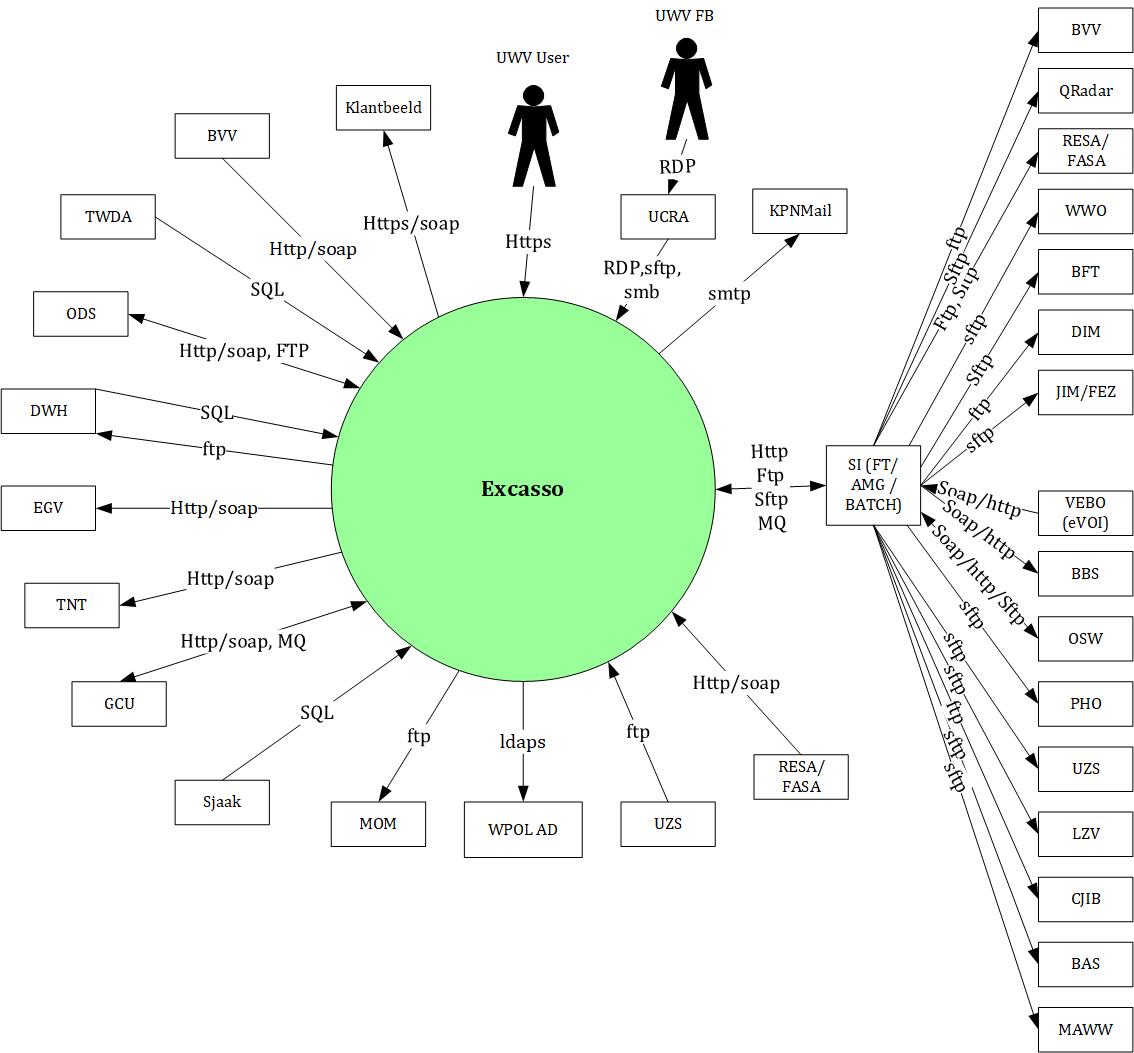
All components that belong to the UWV Office Infrastructure such as workstations, web browsers are out of scope.

# Architecture

## Conceptual



## Context diagram



### External entities

#### UWV User

|  |  |
| --- | --- |
| **Description** | End users of the Excasso Complex frontend application via KA Werkplek using Browser |
| **Protocol and Port** | HTTPS:443 |
| **DC (Datacenter) connection** | External |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method: RBAC (AD) & OAM  Use Certificates: yes (certificate type: Entrust /PKI overheid) |
| **Number of users** | 1000+ |
| **Number of transactions** | not specified |
| **Frequency of transactions** | not specified |
| **Volume of data** | not specified |

#### UWV FB

|  |  |
| --- | --- |
| **Description** | Functional maintenance of the Excasso Complex frontend application using the UCRA environment |
| **Protocol and Port** | RDP: 3389 | (s)FTP: port 20,21,22 | SMB:445 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method: RBAC (AD)  Uses Private/Public Keys for sftp connections |
| **Number of users** | 5+ |
| **Number of transactions** | not specified |
| **Frequency of transactions** | not specified |
| **Volume of data** | not specified |

#### AD / WPOL

|  |  |
| --- | --- |
| **Description** | Connection to the KPN AD Wpol for verification of users entered in the ABS |
| **Protocol and Port** | LDAPS:636 |
| **DC (Datacenter) connection** | External |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method: S2S  Uses Private/Public Keys for sftp connections |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### BAS

|  |  |
| --- | --- |
| **Description** | Betalingenbestand, retour betalingen |
| **Protocol and Port** | SFTP:22 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Via SI |
| **Security Controls** | Authorisation method: S2S  Other: public- en privatkey |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### MAWW

|  |  |
| --- | --- |
| **Description** | Ophalen/verwijderen machtigingen aangeleverd door MAWW |
| **Protocol and Port** | SFTP:22 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Via SI |
| **Security Controls** | Authorisation method: S2S  Other: public- en privatkey |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### BVV

|  |  |
| --- | --- |
| **Description** | Opsturen bestand, ophalen beslagvrije voet via XML, registreren modelmededeling |
| **Protocol and Port** | sFTP:22, Soap/Https:443 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound, Inbound |
| **Direct connection** | Yes for Soap (Inbound), via SI for SFTP (Outbound) |
| **Security Controls** | Authorisation method: S2S (Public/Private key) |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### CJIB

|  |  |
| --- | --- |
| **Description** | Sending and Receiving XML notices |
| **Protocol and Port** | FTP:21 |
| **DC (Datacenter) connection** | External |
| **Direction** | Outbound, Inbound |
| **Direct connection** | No, via SI |
| **Security Controls** | Authorisation method: S2S (Service Account) |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### DWH

|  |  |
| --- | --- |
| **Description** | DataWareHouse + DWH BO Business Objects |
| **Protocol and Port** | FTP:21, SQL\*Net:1526 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound and Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method: S2S (Service Account) |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### EGV

|  |  |
| --- | --- |
| **Description** | Raadplegen Dossier |
| **Protocol and Port** | SOAP/HTTPS:443 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method: S2S |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### JIM/FEZ

|  |  |
| --- | --- |
| **Description** | Leveren Boekhoudinformatie |
| **Protocol and Port** | SFTP:22 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | No via SI |
| **Security Controls** | Authorisation method: S2S (Public, Privatekey) |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### GCU

|  |  |
| --- | --- |
| **Description** | Brief Parameters |
| **Protocol and Port** | SOAP/HTTP:80, MQ:7501 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound, Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method: S2S |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### OSW

|  |  |
| --- | --- |
| **Description** | Combination of WWF, IOW, WWW |
| **Protocol and Port** | FTP:21, SFTP:22, SOAP/HTTPS:443 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound, Outbound |
| **Direct connection** | No, Outbound via SI (FTP, SFTP), Inbound via SI (SOAP). |
| **Security Controls** | Authorisation method: S2S (Private/Publickey, ServiceAccount) |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### WWO

|  |  |
| --- | --- |
| **Description** | WerkloosheidsWet Ontslag |
| **Protocol and Port** | SFTP:22 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | No, Outbound via SI (SFTP) |
| **Security Controls** | Authorisation method: S2S (Private/Publickey, ServiceAccount) |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### QRadar

|  |  |
| --- | --- |
| **Description** | Lomo, delivering data to QRadar. Storing Transactions. |
| **Protocol and Port** | SFTP:22 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | No, Outbound via SI |
| **Security Controls** | Authorisation method: S2S (Private/Publickey) |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### LZV

|  |  |
| --- | --- |
| **Description** | Luziver |
| **Protocol and Port** | SFTP:22 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | No, Outbound via SI |
| **Security Controls** | Authorisation method: S2S (Private/Publickey) |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### KPNMail

|  |  |
| --- | --- |
| **Description** | KPN Mail Relay |
| **Protocol and Port** | SMTP:25 |
| **DC (Datacenter) connection** | External |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method: S2S |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### ODS

|  |  |
| --- | --- |
| **Description** | Operational DataStore |
| **Protocol and Port** | SOAP/HTTP:80, FTP:21 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound, Inbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method: S2S |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### PHO

|  |  |
| --- | --- |
| **Description** | Phoeniks, Handhaving (Fraud) |
| **Protocol and Port** | SFTP:22 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | No via SI |
| **Security Controls** | Authorisation method: S2S (Public/Privatekey) |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### ResaFasa

|  |  |
| --- | --- |
| **Description** | ReSaFaSa opdrachten AOWP, afkeuringen, ophalen boekhoudingen |
| **Protocol and Port** | SOAP/HTTP:80, FTP:21, SFTP:22 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound, Inbound |
| **Direct connection** | Yes on inbound via WebServices, Outbound via SI |
| **Security Controls** | Authorisation method: S2S  Other: ServiceAccount with FTP and Privat/Publickey with SFTP |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### TNT

|  |  |
| --- | --- |
| **Description** | Postcode Tabel |
| **Protocol and Port** | SOAP/HTTP:80 |
| **DC (Datacenter) connection** | External |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method: S2S |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### UZS

|  |  |
| --- | --- |
| **Description** | Ziektewet Systeem |
| **Protocol and Port** | FTP:21, SFTP:22 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound, Inbound |
| **Direct connection** | Yes and No (via SI) |
| **Security Controls** | Authorisation method: S2S  Other: ServiceAccount with FTP and Privat/Publickey with SFTP |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### BFT

|  |  |
| --- | --- |
| **Description** | Belastingdienst FileTransfer; loonaangifteberichten (sftp), ophalen loonbelastingtabellen (ftp) |
| **Protocol and Port** | SFTP:22, FTP:21 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | No (via SI) |
| **Security Controls** | Authorisation method: S2S (Service Account and Private/Publickey) |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### DIM

|  |  |
| --- | --- |
| **Description** | Datafabriek, sending of a weekly/monthly manual created parfile by TAB |
| **Protocol and Port** | FTP:21 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | No (via SI) |
| **Security Controls** | Authorisation method: S2S (Service Account) |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### VEBO (eVOI)

|  |  |
| --- | --- |
| **Description** | VEBO (Uitkeringsbeslagen Personen) |
| **Protocol and Port** | SOAP/HTTP:80 |
| **DC (Datacenter) connection** | External |
| **Direction** | Inbound |
| **Direct connection** | No (via SI) |
| **Security Controls** | Authorisation method: S2S |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### Klantbeeld

|  |  |
| --- | --- |
| **Description** | GUP service EXC KB V0100 http: aanvragen klantbeeld |
| **Protocol and Port** | https:443 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Authorisation method: S2S |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### BBS

|  |  |
| --- | --- |
| **Description** | BBS, Opvragen Werkgeverspremie |
| **Protocol and Port** | SOAP/HTTP:80 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | No (via SI) |
| **Security Controls** | Authorisation method: S2S |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### MOM

|  |  |
| --- | --- |
| **Description** | Printing Jaaropgave and correctie Jaaropgave |
| **Protocol and Port** | FTP:21 |
| **DC (Datacenter) connection** | External |
| **Direction** | Outbound |
| **Direct connection** | YES |
| **Security Controls** | Authorisation method: S2S |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### TWDA

|  |  |
| --- | --- |
| **Description** | TWDA access to Query Database, for reporting purposes |
| **Protocol and Port** | SQL\*Net: 1526 |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | YES |
| **Security Controls** | Authorisation method: Local database user / password |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

#### Sjaak

|  |  |
| --- | --- |
| **Description** | Monitoring of timedifference between database and logical standby database (querydatabase) |
| **Protocol and Port** | SQL\*Net: 1526 |
| **DC (Datacenter) connection** | External |
| **Direction** | Inbound |
| **Direct connection** | YES |
| **Security Controls** | Authorisation method: Local database user / password |
| **Number of users** | Not specified |
| **Number of transactions** | Not specified |
| **Frequency of transactions** | Not specified |
| **Volume of data** | Not specified |

# Functional Requirements

No functional requirements specified.

# Non-Functional Requirements

## Security & Compliance classifications

For the BIV Rating the advice of the “Coördinator informatiebeveiliging en privacy” is followed according to the latest ISRA (Information Security Risk Assessment).

|  |  |
| --- | --- |
| **Application** | Excasso Complex |
| **Owner** | Uitkeren |
| **Availability (Beschikbaarheid)** | 3 |
| **Integrity (Integriteit)** | 2 |
| **Confidentiality (Vertrouwelijkheid)** | 3 |
| **Type of information /Data Classification** | Financiële grote geldstromen |
| **Direct or Indirect part of the primary information chain** | Direct |

### Risk analysis UWV

No risk analysis provided by UWV

### Applicable security and compliance frameworks

|  |  |
| --- | --- |
| Security & Compliance Framework | Applicable |
| BIR 2017 | Yes |
| AVG / GDPR | Yes |
| DIGID | No |
| SUWI | No |
| Additional frameworks | No additional security or compliance Frameworks |

## System and Software requirements

### System (Operating system (OS))

| **Operating System** | **Version** |
| --- | --- |
| Windows | 2016 |
| RedHat Enterprise | 8.x |
| AIX | 7.2 |

### Software (Licenses)

| **Software product / component** | **Version** |
| --- | --- |
| IBM XL C FOR AIX | 16.1 |
| IBM JAVA SE | 8 |
| ORACLE DATABASE | 12cr2 |
| MICROFOCUS ACUCOBOL-GT EXTEND | 10.5 |

### Capacity and performance (volumetrics)

About 6000 users are registered in ABS to wpol group “BPB\_menu\_fa”, this means at most 6000 concurrent users will be able to use the Excasso application.

## Availability

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Environment** | **Application Target** | **Application Service Hours** | **Infra Target** | **Infra Service Hours** |
| Production | 99,8% | 7 x 24 | 99,8% | 7 x 24 |
| Acceptance | 98% | 5 x 12 (Mo-Fr, 7 - 19h) | 99,5% | 5 x 12 (Mo-Fr, 7 - 19h) |
| Education on Acceptance | 98% | 5 x 12 (Mo-Fr, 7 - 19h) | 98% | 5 x 12 (Mo-Fr, 7 - 19h) |
| Test | 98% | 5 x 12 (Mo-Fr, 7 - 19h) | 98% | 5 x 12 (Mo-Fr, 7 - 19h) |

## Security requirements

### System logging

No specific system logging requirements are applicable

* Testers and Functional Management will need RDP access to the application servers by using UCRA on the test environment. On acceptance and production access they will use UCRA and SMB to access shares on servers which is sufficient.
* Excasso Complex needs to comply to the UWV secure software development guidelines
* Excasso Complex application users must communicate in a secure way with the application server over the network.

Detailed Standard Security requirements are documented in Appendix D

## System management

No additional system management requirements have been provided.

### Additional application related infra requirements

|  |  |
| --- | --- |
| **Requirements** | **Status** |
| Use STARTTLS option for UWV mail | No |
| Is Microsoft DTC used for inflight transactions | No |
| Is HTTPS cookie stickiness required on the load balancer | No |

## Backup and Recovery

No specific Backup and Recovery requirements applicable

|  |  |  |
| --- | --- | --- |
|  | **Default** | **Deviation (when applicable)** |
| Backup | standard backup |  |
| Restore | no specific restore order |  |
| Dependency | no dependencies |  |

## Storage replication

|  |  |
| --- | --- |
| **Environment** | **Storage Replication** |
| Production | Replicated storage |
| Acceptance | Replicated storage |
| Education (Acceptance) | Non-replicated storage |
| Test | Non-replicated storage |

## Scalability

The design should allow for upscaling of resources in order to improve performance. The initial systems setup will be vertically and horizontally scalable.

Scalability limitations for the application are not defined, not applicable, or unknown to DXC.

## Disaster Recovery

No specific disaster recovery requirements applicable.

## Infrastructure Technical Constraints

No infrastructure technical constraints.

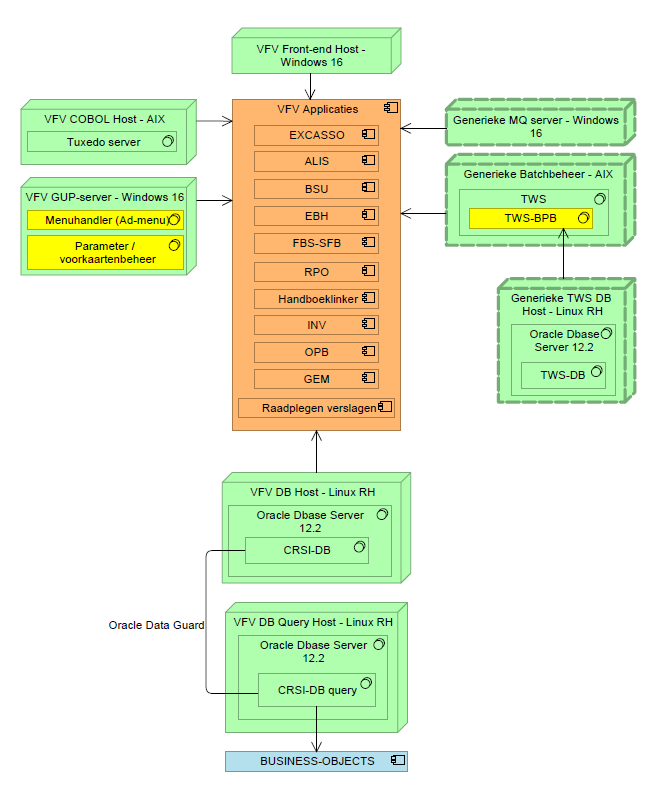
## DXC TAB requirements

|  |  |
| --- | --- |
| **Category** | **Description** |
| Deployment | XLdeploy in General,  Corsi-Basis and Corsi-FTP are deployed via Manual deploy by TAB using an Installation guide. |
| Other TAB applicable requirement | Specific application port for Sitescope for monitoring the websites on IISWeb servers, WebServices on GUP server |

# Solution

## Architectural Decisions

The SOLL has been determined to be as follows:



|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Decision** | **Comments** | **Status** |
| 1 | Some generic components like MiMas-Shared MQ and MiMas-Shared IWS are already in the HLD of Phoeniks. | High Level Design of Phoeniks. |  |
| 2 | Excasso will have the GUP server in the backoffice. This is different from the Phoeniks application that runs WebLogic, where the GUP server is also used as IISWeb server. |  |  |
| 3 | Based on the SOLL design there is an additional Query Database hosted in the Kluis that is connected via Dataguard with the production database. Only production will have a Query database, it will not be present in the Acceptance environment. |  |  |
| 4 | On the Acceptance infrastructure whe will host 2 different acceptance environments as Logical Separated Environments instead of having 1 infra per acceptance environment. | 1 infra for both logical environments. This is AS-IS and how the application and functional maintenance is designed in CMO. |  |
| 5 | The Excasso Query database is based on the current solution of an Oracle dataguard synchoronized standby database. | This means that the query database contains current Excasso data |  |
| 6 | FBS has been devided in OBS and SBS. The SBS part is going to be provided in the AM zone as it needs to connect to all OTAP Domains | OBS is going to installed on Windows server in every domain and SBS is going to be installed on windows server in AM zone |  |
| 7 | The Confidentiality of the application changed from 2 to 3 therefore we needed to change the place of the database servers in Acceptation and Production to the Kluis. |  |  |

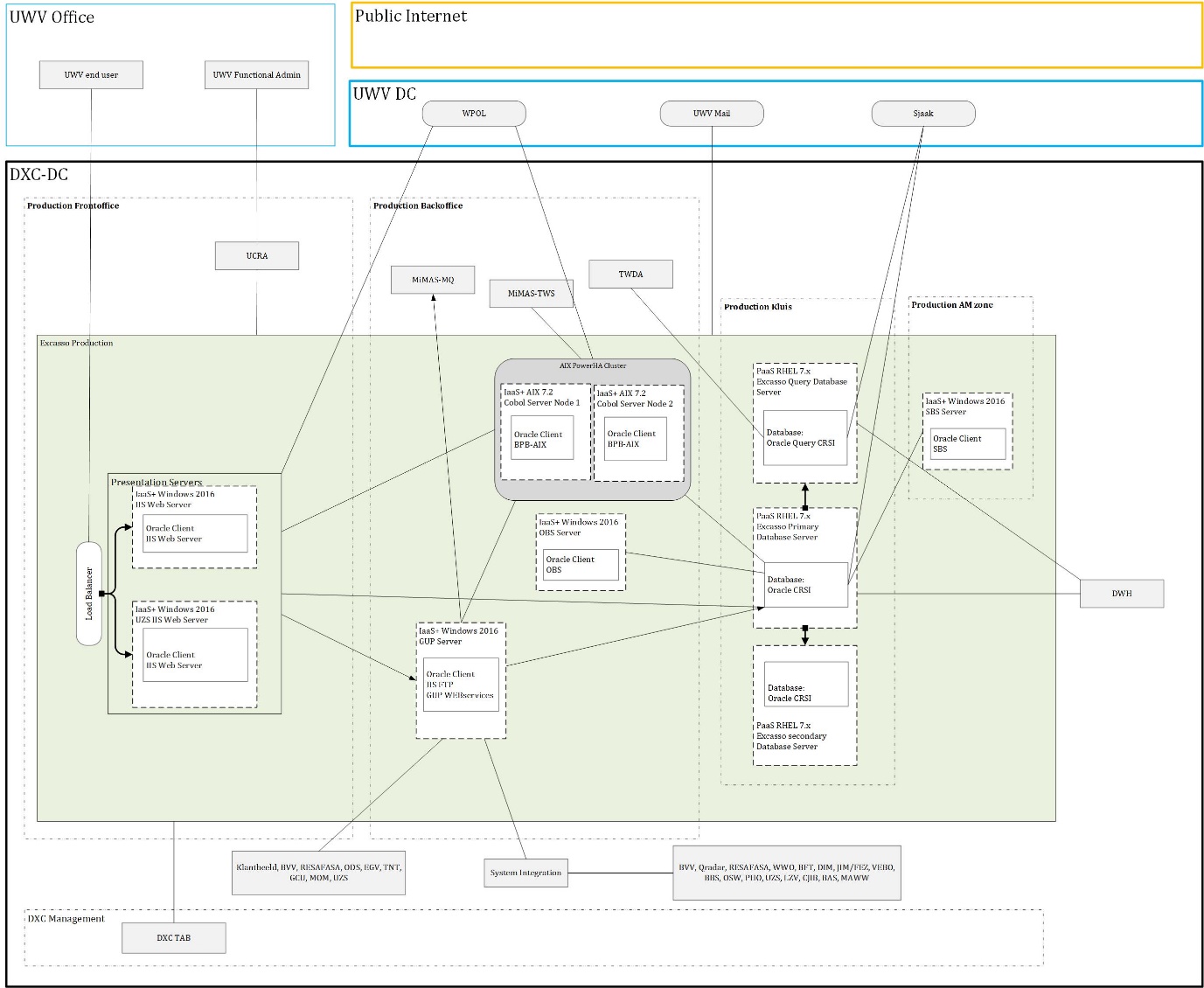
## Node descriptions and zone-projections

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Security Zone** | **Domain** | **Server Type** | **Node ID** | **Infra Service Level** |
| FrontOffice | Production | Web server | IISWEB Server x2 | Gold |
| BackOffice | Production | Application server | GUP Server | Gold |
| BackOffice | Production | Application server | Cobol Server Power HA Cluster Nodes | Gold |
| Micro BackOffice | DXC Application Management | Application server | SBS Server | Gold |
| BackOffice | Production | Application server | OBS Server | Gold |
| Kluis | Production | Database server | Oracle RDBMS  Primary | Gold |
| Kluis | Production | Database server | Oracle RDBMS  Secondary | Gold |
| Kluis | Production | Database server | Oracle Query RDBMS | Gold |
| FrontOffice | Acceptance | Web server | IISWEB Server x2 | Silver |
| BackOffice | Acceptance | Application server | GUP Server | Silver |
| BackOffice | Acceptance | Application server | Cobol Server | Silver |
| BackOffice | Acceptance | Application server | OBS Server | Silver |
| Kluis | Acceptance | Database server | Oracle RDBMS | Silver |
| FrontOffice | Acceptance | Web server | EDU IISWEB Server | Bronze |
| BackOffice | Acceptance | Application server | EDU GUP Server | Bronze |
| BackOffice | Acceptance | Application server | EDU Cobol Server | Bronze |
| BackOffice | Acceptance | Database server | EDU Oracle RDBMS | Bronze |
| FrontOffice | Test | Web server | IISWEB Server | Bronze |
| BackOffice | Test | Application server | GUP Server | Bronze |
| BackOffice | Test | Application server | OBS Server | Bronze |
| BackOffice | Test | Application server | Cobol Server | Bronze |
| BackOffice | Test | Database server | Oracle RDBMS | Bronze |

### DNS (customer facing name)

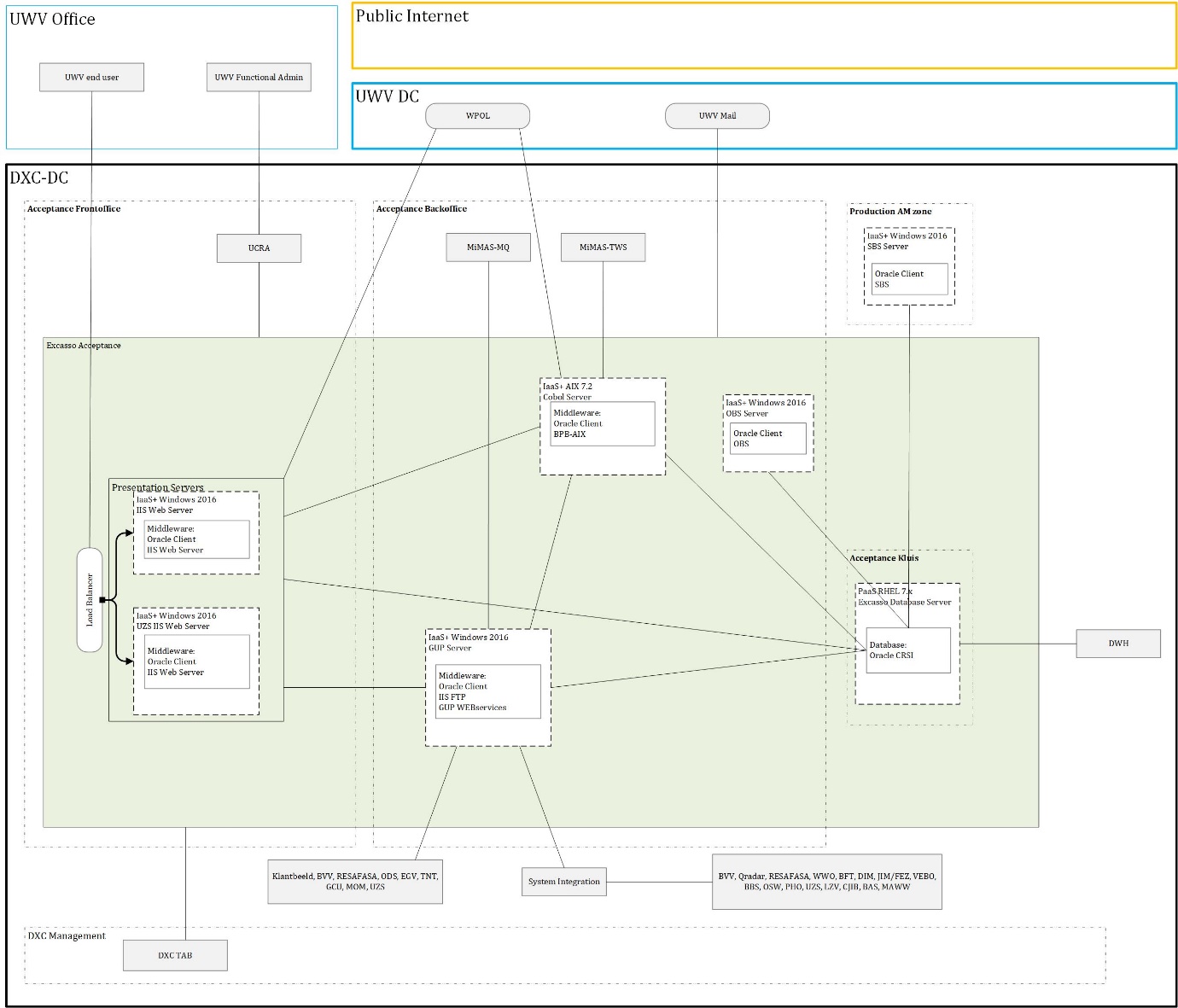
|  |  |  |
| --- | --- | --- |
| **Domain** | **Customer facing name** | **DNS suffix** |
| Production | Excasso | P-dc.ba.uwv.nl |
| Production | Exc | P-dc.ba.uwv.nl |
| Production | Exc-obs | P-dc.ba.uwv.nl |
| Production | Exc-sbs | P-dc.ba.uwv.nl |
| Production | Exc-gup | P-dc.ba.uwv.nl |
| Production | Exc-ftp | P-dc.ba.uwv.nl |
| Production | Exc-cbl | P-dc.ba.uwv.nl |
| Production | Exc-db | P-dc.ba.uwv.nl |
| Production | Exc-dbq | P-dc.ba.uwv.nl |
| Acceptance | Exc-A1 | A-dc.ba.uwv.nl |
| Acceptance | Exc-A1-obs | A-dc.ba.uwv.nl |
| Acceptance | Exc-A1-gup | A-dc.ba.uwv.nl |
| Acceptance | Exc-A1-ftp | A-dc.ba.uwv.nl |
| Acceptance | Exc-A1-cbl | A-dc.ba.uwv.nl |
| Acceptance | Exc-A1-db | A-dc.ba.uwv.nl |
| Acceptance | Exc-A2 | A-dc.ba.uwv.nl |
| Acceptance | Exc-A2-obs | A-dc.ba.uwv.nl |
| Acceptance | Exc-A2-gup | A-dc.ba.uwv.nl |
| Acceptance | Exc-A2-ftp | A-dc.ba.uwv.nl |
| Acceptance | Exc-A2-cbl | A-dc.ba.uwv.nl |
| Acceptance | Exc-A2-db | A-dc.ba.uwv.nl |
| Acceptance | Exc-E | A-dc.ba.uwv.nl |
| Acceptance | Exc-E-gup | A-dc.ba.uwv.nl |
| Acceptance | Exc-E-ftp | A-dc.ba.uwv.nl |
| Acceptance | Exc-E-cbl | A-dc.ba.uwv.nl |
| Acceptance | Exc-E-db | A-dc.ba.uwv.nl |
| Test | UWV-EXC-\* | T-dc.ba.uwv.nl |

## System diagram – Production



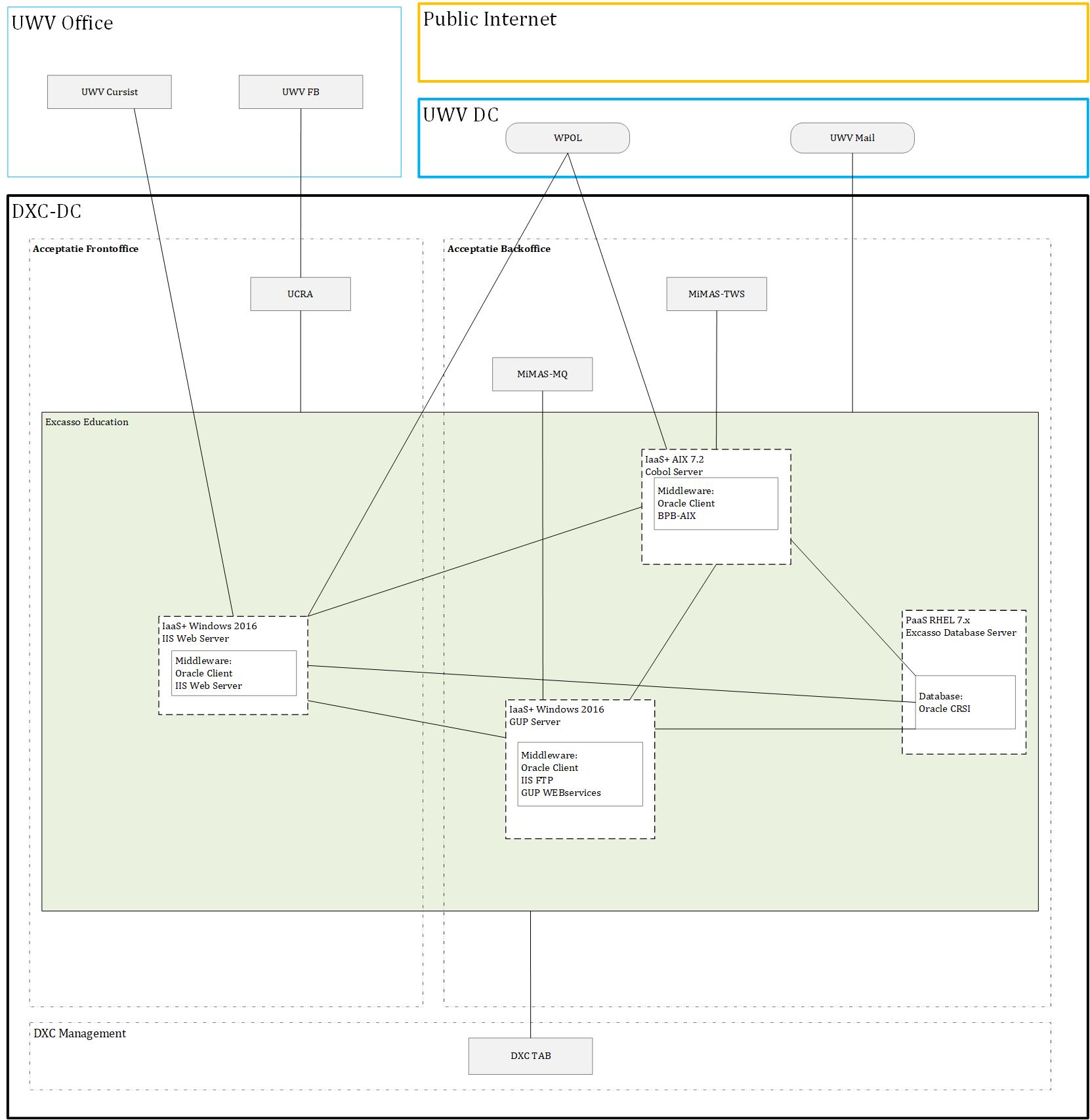
## System diagram Non-Production

### System Diagram Acceptation



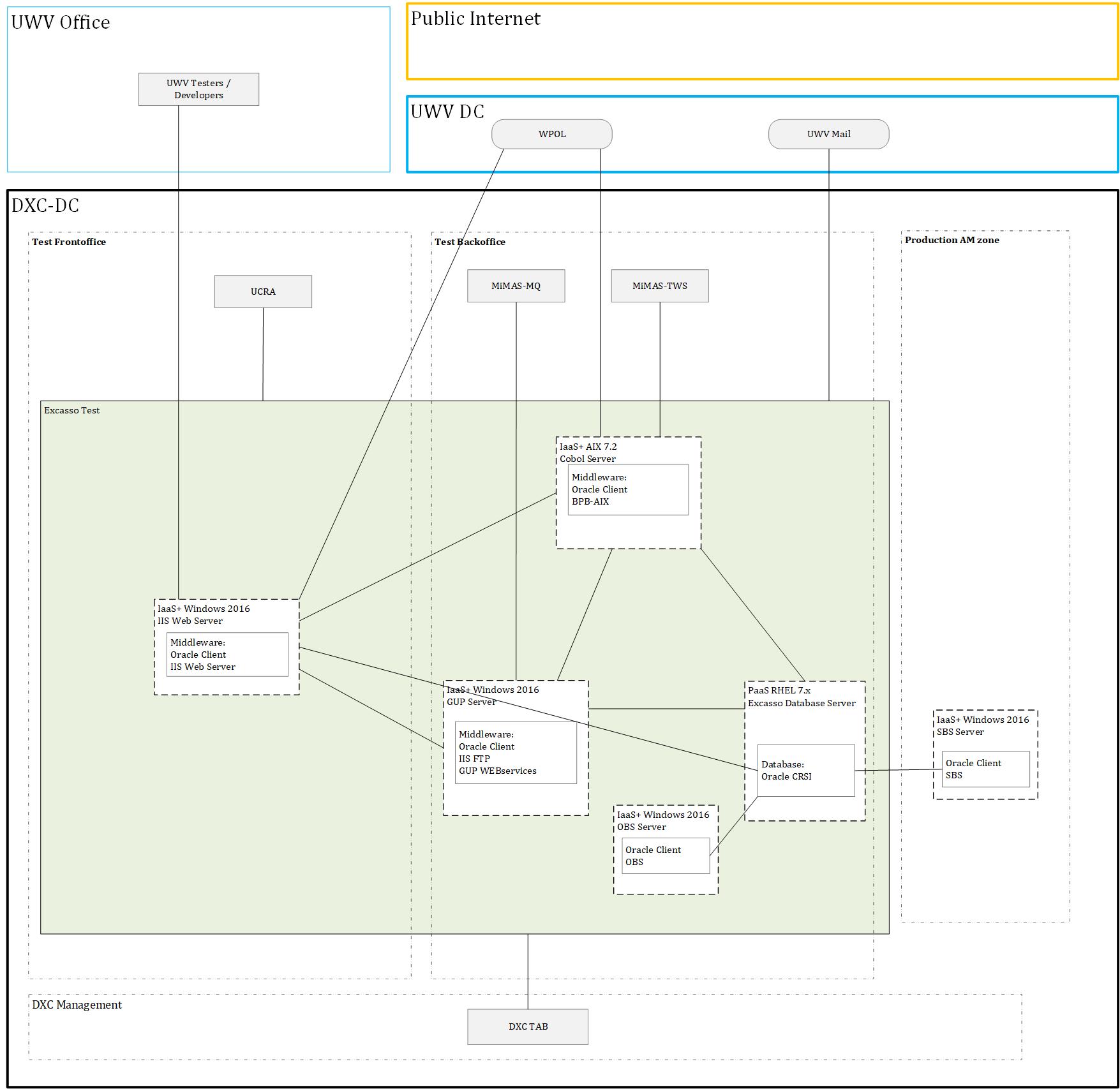
There is no query database in the acceptation environment. A1 and A2 reside on the same servers AS-IS CMO.

### System Diagram Education



The education environment is in the Acceptation domain and is similar to the Test environment therefor the database will be in the backoffice.

### System Diagram Test



The Test environment does not have load balanced IISWeb servers or a Query Database

## SBB’s

|  |
| --- |
| **Standard Building Block Type** |
| IaaS+ - VM- DXC Managed |
| PaaS - Virtual Oracle database - DXC Managed |
| Legacy hosting - AIX LPAR - DXC Managed |

## Load balancers

|  |  |  |  |
| --- | --- | --- | --- |
| **Domain** | **Load balancer** | **Load balancer type** | **Description** |
| Production | Yes | NSX-T (Private Cloud) | LB for App webservices |
| Acceptance | Yes | NSX-T (Private Cloud) | LB for App webservices |

Details can be found in Appendix A – Load balancers

## Deviations from standards (RAL / EtP)

RAL (Risk Acceptance Letter) / EtP (Exception to Policy)

| **Nr** | **Short description of the deviation** | **RAL / EtP required** | **Risk ID** |
| --- | --- | --- | --- |
| 1 | Connection from FrontOffice servers (IISWeb / WebLogic) to database in Vault | Yes | Tbd |
| 2 | Connection from Test domain to Accept Domain (TNT, ODS) | Yes | 20210412-004-  -MIMAs-CrossZoneConnections.docx |
| 3 | UWV accesses the Query database in Kluis/Vault from the UCRA  in FO environment.  This database is used for queries/processing that cannot take place in production itself due to performance issues. | Yes | 20221103-001-A |
| 4 | Connection needed between IBM BO server and Vault.  UWV accesses the Query database from the Business Object server.  This database is used for data reporting that cannot take place in production itself due to performance issues. | Yes | 20221103-002-A |
| 5 | Cross Zone: GCU in FO SEC to Kluis The UWV has an obligation to inform clients of a claim. The claim letters are created in day processing INVDAGRAP and offered to GCU via this link. If this link is not realised, the UWV will not be able to meet its legal obligation in this respect | Yes | 20221108-003-A |
| 6 | HTTP Security Header Not Detected. | Yes | 20230322-001-A |
| 7 | IBM MQ Denial of Service (DoS) Vulnerability (6833806) not remediated | Yes | 20230405-003-A |
| 8 | Using obsolete software Microsoft Visual C++ 2010 Redistributable Package. | Yes | 20230412-002-A |
|  |  |  |  |

## Service Management

|  |  |  |  |
| --- | --- | --- | --- |
| **Environment** | **Infra Hosting** | **Database / Middleware Management** | **Technical Application Management** |
| Production | Gold | TAB Plus | TAB Plus |
| Acceptance | Silver | TAB Basis | TAB Basis |
| Education | Bronze | TAB Basis | TAB Basis |
| Test | Bronze | TAB Basis | TAB Basis |

## Security

Security details can be found in Appendix D, any deviations are document in chapter ‘Deviations from standards’.

### User Authentication and Authorization

Specify below per user type: UWV FB (RDP and Fileshare)

Variation 1 (LDAP- UWV AD group nested in DXC AD group - using the trust): User Authentication and Authorization will be performed against the UWV AD using nested groups, as per standard design.

Specify below per user type: UWV Users/Cursisten and UWV FB (Access to IWS application on AIX)

Variation 2 (LDAP – UWV AD group - using nested groups is not possible): User Authentication and Authorization will be performed against the UWV AD using a direct LDAP connection, for applications that cannot use nested groups.

Specify below per user type: UWV FB (Access to AIX)

Variation 4 (Local - local login using local account): User Authentication and Authorization will be performed localy using a local user account, Middleware or AIX access for UWV users requested through the ABS IAM system and changes in PDXC.

Details are specified in Appendix C

### Firewalls

The data center network offers multiple logical network compartments and has security zones and OTAP domains within it kept separate through a combination of dedicated physical firewall clusters and distributed software defined firewall functions.

* Connections, like interfaces, coming from outside the network security zone do cross one or more firewalls.
* Node to node communication inside the FrontOffice security zone and the same domain do not need to cross a firewall
  + Exception: Node to loadbalancer communication (inside the FrontOffice security zone and the same domain) do need to cross a firewall
* Node to node communication inside the BackOffice security zone and the same domain do not not need to cross a firewall
  + Exception: Node to loadbalancer communication (inside the BackOffice security zone and the same domain) do do need to cross a firewall

For the application we distinguish the following connection categories:

* *Internal:* Connection within the application. For example, ODBC connection between the application- and the database server, if they are in different security zones a firewall is required and the Internal connection is document in the table below
* *External (inside DXC):* Connection external for the application but inside the DXC data center. For example, FTP connection between Application server and SI-File Transfer. To determine if these connections require a Firewall request the security zones must be known, this level of detail is not available in the HLD. The external (inside DXC) connections are not documented in the HLD but can be found in the application connectivity overview sheet.
* *External (outside DXC):* Connection external for the application and outside the DXC data center. For example, HTTPS connection between Application server and the UWV Citrix KA farm. All external (outside DXC) connections are documented in the table below

For Excasso Complex the following is applicable:

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Connection Type** | **Between (component 1)** | **And (component 2)** |
| Internal | SQL\*NET | IISWeb Server | Database Server |
| Internal | SQL\*NET | GUP Server | Database Server |
| Internal | SQL\*NET | Cobol Cluster | Database Server |
| Internal | SQL\*NET | SBS Server | Database Server |
| Internal | SQL\*NET | OBS Server | Database Server |
| External (outside DXC) | HTTPS | UWV KA Office | IISWeb Loadbalancer |
| External (outside DXC) | LDAPS | IISWeb Server | WPOL |
| External (outside DXC) | LDAPS | Cobol Server | WPOL |
| External (outside DXC) | LDAPS | GUP Server | WPOL |
| External (outside DXC) | SMTP | GUP Server | KPN Mail Relay |
| External (outside DXC) | SMTP | IISWeb Server | KPN Mail Relay |
| External (outside DXC) | SMTP | COBOL Server | KPN Mail Relay |
| External (Outside DXC) | SQL\*Net | UWV KA Office | Query Database server |

For details see Appendix B

# Potential future improvements

|  |  |  |
| --- | --- | --- |
| **ID** | **Proposed improvement** | **Reason** |
| 1 | Migrate Cobol application to RHeL platform | AIX is Legacy and should where possible be replaced with Linux solutions |
| 2 | Upgrade Database and OS to newer version in keeping with Technology Roadmap | GOH should take place right after go live to replace the possible EoS situations of several software Items |
| 3 | Instead of using a MiMas-shared IWS environment we could TWS-Generiek if possible to align with enterprise wide solution | We have a separated solution for all mimas application which also needs a license and it could be possible to use a generic enterprise wide solution. |
| 4 |  |  |

Appendix A: Technology and Sizing (at design **verification)**

***Node details***

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Landing Zone** | **Security Zone** | **Location** | **Domain** | **Node ID** | **vCPU** | **RAM (GB)** | **OS** | **Infra SLA** | **SBB Type** | **Replication** |
| Private Cloud Oracle DB | Kluis | AM2 | Production | Excasso Primary Database Server | 12 | 192 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Silver | PaaS | yes |
| Private Cloud Oracle DB | Kluis | AM3 | Production | Excasso Secondary Database Server | 12 | 192 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Silver | PaaS | yes |
| Private Cloud Oracle DB | Kluis | AM2 | Production | Excasso Query Database Server | 8 | 192 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Silver | PaaS | yes |
| Legacy Hosting AIX | BackOffice | AM2 | Production | Cobol Server  Active Node | 8 | 128 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | AIX 7.2 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Gold | Legacy | yes |
| Legacy Hosting AIX | BackOffice | AM3 | Production | Cobol Server  Passive Node | 8 | 128 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | AIX 7.2 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Gold | Legacy | yes |
| Private Cloud | BackOffice | AM2 | Production | GUP Server | 2 | 16 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Windows 2016 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Gold | IaaS+ | yes |
| Private Cloud | FrontOffice | AM2 | Production | IISWeb Server 1 | 2 | 16 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Windows 2016 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Gold | PaaS | yes |
| Private Cloud | FrontOffice | AM3 | Production | IISWeb Server 2 | 2 | 16 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Windows 2016 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Gold | PaaS | yes |
| Private Cloud | Micro BackOffice | AM3 | Production | SBS Server | 2 | 8 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Windows 2016 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Gold | IaaS+ | yes |
| Private Cloud | BackOffice | AM2 | Production | OBS Server | 2 | 8 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Windows 2016 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Gold | IaaS+ | yes |
| Private Cloud Oracle DB | Kluis | AM3 | Acceptance | Excasso Database Server | 12 | 192 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Silver | PaaS | yes |
| Legacy Hosting AIX | BackOffice | AM3 | Acceptance | Cobol Server | 8 | 128 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | AIX 7.2 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Silver | Legacy | yes |
| Private Cloud | BackOffice | AM3 | Acceptance | GUP Server | 2 | 16 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Windows 2016 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Silver | IaaS+ | yes |
| Private Cloud | FrontOffice | AM3 | Acceptance | IISWeb Server 1 | 2 | 16 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Windows 2016 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Silver | PaaS | yes |
| Private Cloud | FrontOffice | AM2 | Acceptance | IISWeb Server 2 | 2 | 16 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Windows 2016 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Silver | PaaS | yes |
| Private Cloud | BackOffice | AM3 | Acceptance | OBS Server | 2 | 8 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Windows 2016 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Silver | IaaS+ | yes |
| Private Cloud Oracle DB | BackOffice | AM2 | Acceptance | Excasso EDU Database Server | 2 | 16 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | PaaS | no |
| Legacy Hosting AIX | BackOffice | AM2 | Acceptance | Cobol EDU Server | 4 | 64 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | AIX 7.2 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | Legacy | no |
| Private Cloud | BackOffice | AM2 | Acceptance | GUP EDU Server | 2 | 8 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Windows 2016 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | no |
| Private Cloud | FrontOffice | AM2 | Acceptance | IISWeb EDU Server | 2 | 8 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Windows 2016 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | PaaS | no |
| Private Cloud Oracle DB | BackOffice | AM2 | Test | Excasso Database Server | 2 | 16 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | RHEL 7.9 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | PaaS | no |
| Legacy Hosting AIX | BackOffice | AM2 | Test | Cobol Server | 4 | 32 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | AIX 7.2 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | Legacy | no |
| Private Cloud | BackOffice | AM2 | Test | GUP Server | 2 | 8 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Windows 2016 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | no |
| Private Cloud | FrontOffice | AM2 | Test | IISWeb Server | 2 | 8 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Windows 2016 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | PaaS | no |
| Private Cloud | BackOffice | AM2 | Test | OBS Server | 1 | 4 | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Windows 2016 | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | Bronze | IaaS+ | no |

*Dependency:*

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Landing Zone** | **Security Zone** | **Location** | **Domain** | **Node ID** | **vCPU** | **RAM (GB)** | **OS** | **Infra SLA** | **SBB Type** | **Replication** |
| Select | Select | Select | Select |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Select | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Select | Select | | |  |  | | --- | --- | | Windows 2016 | Select | | | | Select | Select | Select |

***Storage***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Node ID** | **Domain** | **C-drive OS (Fixed)** | **D-drive App (mandatory)** | **E-drive (optional)** | **F-drive (optional)** | **…-drive (optional)** |
| IISWEB Servers | Production | 100 GB | 100 GB | n/a | n/a | n/a |
| GUP Server | Production | 100 GB | 200 GB | n/a | n/a | n/a |
| SBS Server | Production | 100 GB | 50 GB | n/a | n/a | n/a |
| OBS Server | Production | 100 GB | 50 GB | n/a | n/a | n/a |
| IISWEB Servers & EDU | Acceptance | 100 GB | 100 GB | n/a | n/a | n/a |
| OBS Server | Acceptance | 100 GB | 50 GB | n/a | n/a | n/a |
| GUP Server & EDU | Acceptance | 100 GB | 100 GB | n/a | n/a | n/a |
| IISWEB Server | Test | 100 GB | 200 GB | n/a | n/a | n/a |
| OBS Server | Test | 100 GB | 50 GB | n/a | n/a | n/a |
| GUP Server | Test | 100 GB | 200 GB | n/a | n/a | n/a |
|  |  |  |  |  |  |  |

*Windows Application server(s)*

*AIX Application server(s)*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Node ID** | **Domain** | **Disk 0 – Mountpoint 1 OS (Fixed)** | **Disk 1 – Mountpoint 1 App (mandatory)** | **Disk 1 – Mountpoint 2 (optional)** | **Disk 1 – Mountpoint 3 (optional)** | **Disk 2 – Mountpoint 1 (optional)** |
| Cobol Server EDU | Acceptance | 100 GB | 500 GB | 100 GB | n/a | n/a |
| Cobol Server ACC | Acceptance | 100 GB | 500 GB | 50 GB | 500 GB | 5 x 1 TB |
| Cobol Server | Test | 100 GB | 500 GB | 500 GB | n/a | n/a |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Node ID** | **Cluster node Type**  **(active / passive)** | **Domain** | **Disk 0 – Mountpoint 1 OS (Fixed)** | **SHARED Disk 1 – Mountpoint 1 Cluster (fixed)** | **SHARED Disk 2 – Mountpoint 1 Qourum (fixed)** | **SHARED Disk 3 – Mountpoint 1 (Mandatory)** | **SHARED Disk 3 – Mountpoint 2 (optional)** |
| Node 1 | Active | Production | 100 GB | 10 GB | 1 GB | 6 x 1 TB |  |
| Node 2 | Passive | Production | 100 GB |

*AIX GOLD – PowerHA Cluster*

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Node ID** | **Domain** | **Disk0 OS (Fixed)** | **Disk1 Oracle Binaries (Fixed)** | **Disk2 ASM Binaries (Fixed)** | **ASM DATA1 DiskGroup1 Data Files, Control Files** | **ASM DATA2 DiskGroup1 Data Files, Control Files** | **ASM FRA1 DiskGroup2 Archive and Flashback Logs** | **ASM FRA2 DiskGroup2 Archive and Flashback Logs** | **Additional App Drives** |
| Excasso Primary Database | Production | 100 GB | 100 GB | 100 GB | 4 TB | 4 TB | 1 TB | 1 TB | 250 GB |
| Excasso Secondary Database | Production | 100 GB | 100 GB | 100 GB | 4 TB | 4 TB | 1 TB | 1 TB |  |
| Excasso Query Database | Production | 100 GB | 100 GB | 100 GB | 4 TB | 4 TB | 1 TB | 1 TB |  |
| Excasso Database | Acceptance | 100 GB | 100 GB | 100 GB | 6 TB | 6 TB | 3 TB | 3 TB | 250 GB |
| Excasso EDU Database | Acceptance | 100 GB | 100 GB | 100 GB | 500 GB | 500 GB | 500 GB | 500 GB |  |
| Excasso Database | Test | 100 GB | 100 GB | 100 GB | 1 TB | 1 TB | 1 TB | 1 TB | 7 x 1 TB |

*Oracle Database server(s)*

The production databases will need to have the max of 7 TB of disk space to hold the Excasso Database. The acceptation database has A1 and A2 both 3,4 TB large at discovery time the 1st of February 2021.

***Software***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Node Description** | **Suite** | **Software** | **Version** | **Supported by vendor** |
| Cobol Server | 1-OS | AIX | 7.2 | Y |
| GUP Server  OSB Server  SBS Server  IISWeb Server | 1-OS | Windows | 2016 | Y |
| Cobol Server | 2-Library | Java SE | 8 | Y |
| Cobol Server | 2-Library | AcuCobol Extend | 10.5 | Y |
| IISWeb Server | 4-Middleware | IISWeb | 10 | Y |

*Database:*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Node Description** | **Suite** | **Software** | **Version** | **Supported by vendor** |
| Database Server | 1-OS | RHEL | 7.9 | Y |
| Database Server | 3-Database | Oracle Database | 12cR2 | Y |
|  |  |  |  |  |

***Load Balancers***

***Private Cloud***

|  |  |  |
| --- | --- | --- |
| **Application Shortname** | Excasso | Excasso |
| **FQDN** | LB-EXC-P-WEB-VIP.p-dc.ba.uwv.nl | LB-EXC-A-WEB-VIP.a-dc.ba.uwv.nl |
| **FQDN alias** | Exc.p-dc.ba.uwv.nl | Exc.a-dc.ba.uwv.nl |
| **FROM: Security zone**  **(client side)** | Internal en External to Data Center | Internal en External to Data Center |
| **TO: Security zone**  **(load balancer server side)** | FrontOffice | FrontOffice |
| **Domain** | Production | Acceptance |
| **Pool Members (Node ID)** | IISWeb Server 1  IISWeb Server 2 | IISWeb Server 1  IISWeb Server 2 |
| **Application Layer Protocol** | TCP (L4) | TCP (L4) |
| **Application Port(s)** | 443 | 443 |
| **Expected concurrent connections** | < 5000 | < 5000 |
| **Load balancing Algorithm** | Least Connections | Least Connections |
| **Stickiness/Persistance** | System-Persistence-Client-IP | System-Persistence-Client-IP |
| **Health monitor type** | System-HTTPS | System-HTTPS |
| **Port / Ports for use with Health Monitor** | 443 | 443 |
| **HTTP Get request (optional)** |  |  |
| **HTTP Response string / code (optional)** |  |  |
| **Additional Comments** | Excasso Production load balancer | Excasso Acceptance load balancer |

# Appendix B: Network Protocol Matrix

*The following ports must be allowed on the firewalls (Only Internal and External (outside DXC) connections are mentioned, External (inside DXC) are specified in the connectivity sheet).*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| KA Werkplek | Excasso | HTTPS | 443 | LB |

**KA Werkplek to Excasso**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| UCRA | Excasso | FTP | 20,21 |  |
|  |  | SFTP | 22 |  |
|  |  | SMB | 445 |  |
|  |  | RDP | 3389 |  |

**UCRA to Excasso**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Excasso | WPOL | LDAPS | 636 |  |

**Excasso to WPOL (KPN)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| BAS | Excasso | SFTP | 22 | GUP |

**BAS to Excasso**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| MAWW | Excasso | SFTP | 22 | GUP |

**MAWW to Excasso**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| BVV | Excasso | SOAP/HTTPS | 443 | GUP |
|  |  | SFTP | 22 | SI |

**BVV to Excasso**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| CJIB | Excasso | FTP | 21 | SI |

**CJIB to Excasso**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Excasso | DWH | FTP | 21 | GUP |

**Excasso to DWH**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| DWH-BO | Excasso | SQL\*Net | 1526 | Query DB |

**DWH to Excasso**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Excasso | EGV | SOAP/HTTPS | 443 | GUP |

**Excasso to EGV**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Excasso | FEZ/JIM | SFTP | 22 | GUP |

**Excasso to FEZ/JIM**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| GCU | Excasso | SOAP/HTTP | 80 | GUP |
|  |  | MQ | 7501 |  |

**GCU to Excasso**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| OSW | Excasso | SOAP/HTTPS | 443 | GUP |
|  |  | SFTP | 22 | SI |
|  |  | FTP | 21 | SI |

**OSW to Excasso**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Excasso | QRadar | SFTP | 22 | GUP |

**Excasso to QRadar**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Excasso | LZV | SFTP | 22 | GUP |

**Excasso to Luziver**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Excasso | KPN Mail Relay | SMTP | 25 | KPN |

**Excasso to KPN Mail Relay**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| ODS | Excasso | SOAP/HTTP | 80 | GUP |
|  |  | FTP | 21 | GUP |

**ODS to Excasso**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Excasso | PHO | SFTP | 22 | SI |

**Excasso to Phoeniks**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Resa/Fasa | Excasso | SOAP/HTTP | 80 | GUP |
|  |  | SFTP | 22 | SI |
|  |  | FTP | 21 | SI |

**Resa/Fasa to Excasso**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Excasso | TNT | SOAP/HTTP | 80 |  |

**Excasso to TNT**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Excasso | UZS | SFTP | 22 | SI |
|  |  | FTP | 21 | GUP |

**Excasso to UZS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Excasso | BFT | SFTP | 22 | SI |

**Excasso to BFT**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Excasso | DIM | FTP | 21 | SI |

**Excasso to DIM**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| VEBO | Excasso | SOAP/HTTP | 80 | SI |

**VEBO to Excasso**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| TPV | Excasso | FTP | 21 |  |

**TPV to Excasso**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Excasso | BBS | SOAP/HTTP | 80 | SI |

**Excasso to BBS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Excasso | MOM | FTP | 21 |  |

**Excasso to MOM**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| Sjaak | Excasso | SQL\*Net | 1526 | Query DB |
|  |  | SQL\*Net | 1526 | DB |

**Sjaak to Excasso**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| TWDA | Excasso | SQL\*Net | 1526 | Query DB |

**TWDA to Excasso**

# Appendix C: Users and Groups

DXC Managed Users and groups are documented by DXC TAB in the TBH / TMM (Technisch Beheer Handboek / Technical Maintenance Manual) or by the Lead Engineer during the realization phase

**Variation 1: LDAP - nested groups**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **UWV** | | **DXC** | |  |
| **Environment** | **Domain** | **Group** | **Domain** | **Group** | **Description** |
| Production | Uwv.wpol.nl | UWV SP G-UG-UWV-P-EXCASSO-FB | P-dc.ba.uwv.nl | L-RG-UWV-P-EXCASSO-FB | Access to Exc P logfiles and Fileshares |
| Acceptance | Uwv.wpol.nl | UWV SP G-UG-UWV-A-EXCASSO-FB | A-dc.ba.uwv.nl | L-RG-UWV-A-EXCASSO-FB | Access to Exc A logfiles and Fileshares |
| TEST | Uwv.wpol.nl | UWV SP G-UG-UWV-T-EXCASSO-TOEGANG-DXC-TESTERS | t-dc.ba.uwv.nl | L-RG- UWV-T-EXCASSO-TOEGANG-DXC-TESTERS | Access to Excasso T servers |
| TEST | Uwv.wpol.nl | UWV SP G-UG-UWV-T-EXCASSO-TOEGANG-DXC-ONTWIKKELAARS | t-dc.ba.uwv.nl | L-RG- UWV-T-EXCASSO-TOEGANG-DXC-ONTWIKKELAARS | Access to Excasso T servers |
| Acceptance | Uwv.wpol.nl | G-UG-UWV-A-FBS-SFB-USERS\_uwv | A-dc.ba.uwv.nl | L-RG-UWV-A-SBS-OBS-USERS | Users of the acceptance SBS\OBS application |
| Acceptance | Uwv.wpol.nl | G-UG-UWV-A-FBS-SFB-AUDIT\_uwv | A-dc.ba.uwv.nl | L-RG-UWV-A-SBS-OBS-AUDIT | Auditors of the acceptance SBS\OBS application |

**Variation 2: LDAP - nested groups are not possible**

|  |  |  |  |
| --- | --- | --- | --- |
| **Environment** | **Domain** | **Group** | **Description** |
| Production | Uwv.wpol.nl | UWV SP G-UG-UWV-P-EXCASSO-Users | Access to P\_EXC Web Application |
| Acceptance | Uwv.wpol.nl | UWV SP G-UG-UWV-A-EXCASSO-Users | Access to A\_EXC Web Application |

**Variation 3: Local - local logon using DXC AD account**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Domain** | **User Permissions** | **ABS role** | **Server** | **DXC Solution Group** | **Group** | **Description** |
|  |  |  |  |  |  |  |

**Variation 4: Local - local logon using local account**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **User role** | **User permissions** | **ABS Role** | **Application /Server** | **DXC Solution Group** | **Description** |
| **Functional Beheer** | **AIX user** | G-UG-UWV-P-EXCASSO-FB | **Cobol AIX server** |  | **As AIX is not part of AD we need to create local users for access** |

***Service Accounts:***

The following accounts are not compliant to the default settings, will be added in version 1.1

|  |  |  |  |
| --- | --- | --- | --- |
| **Account** | **Domain / local location** | **Noncompliant setting** | **Description** |
| Svc\_exc\_A\_MQ\_connect | A-dc.ba.uwv.nl | MQ | MQ User |
| Svc\_exc\_P\_MQ\_connect | P-dc.ba.uwv.nl | MQ | MQ User |
| SVC\_EXC\_T\_OBS | T-DC.BA.UWV.NL | Create and write reports on fileshare | Application account for OBS and SBS |
| SVC\_EXC\_A\_OBS | A-DC.BA.UWV.NL | Create and write reports on fileshare | Application account for OBS and SBS |
| SVC\_EXC\_OBS\_RPT | T-DC.BA.UWV.NL | Create and write reports on fileshare | Application account for OBS for accessing a remote share (where reports are stored) |
| SVC\_EXC\_P\_OBS | P-DC.BA.UWV.NL | Create and write reports on fileshare | Application account for OBS and SBS |
| SVC\_GUP\_INSTALLER\_T | T-DC.BA.UWV.NL | Installing en running services, Local Admin | Account for GUP |
| SVC\_GUP\_INSTALLER\_A | A-dc.ba.uwv.nl | Installing en running services, Local Admin | Account for GUP |
| SVC\_GUP\_INSTALLER\_P | P-dc.ba.uwv.nl | Installing en running services, Local Admin | Account for GUP |
| SVC\_EXC\_FTP\_WEB\_A | A-dc.ba.uwv.nl | FTP full control | (s)FTP User |
| SVC\_EXC\_FTP\_BPB\_A1 | A-dc.ba.uwv.nl | FTP full control | (s)FTP User |
| SVC\_EXC\_FTP\_BPB\_A2 | A-dc.ba.uwv.nl | FTP full control | (s)FTP User |
| SVC\_EXC\_FTP\_INV\_A1 | A-dc.ba.uwv.nl | FTP full control | (s)FTP User |
| SVC\_EXC\_FTP\_INV\_A2 | A-dc.ba.uwv.nl | FTP full control | (s)FTP User |
| SVC\_EXC\_FTP\_OPB\_A1 | A-dc.ba.uwv.nl | FTP full control | (s)FTP User |
| SVC\_EXC\_FTP\_OPB\_A2 | A-dc.ba.uwv.nl | FTP full control | (s)FTP User |
| SVC\_EXC\_FTP\_ODS\_A2 | A-dc.ba.uwv.nl | FTP full control | (s)FTP User |
| SVC\_EXC\_FTP\_UZS\_A1 | A-dc.ba.uwv.nl | FTP full control | (s)FTP User |
| SVC\_EXC\_FTP\_UZS\_A2 | A-dc.ba.uwv.nl | FTP full control | (s)FTP User |
| SVC\_EXC\_FTP\_WRINT\_A1 | A-dc.ba.uwv.nl | FTP full control | (s)FTP User |
| SVC\_EXC\_FTP\_WRINT\_A2 | A-dc.ba.uwv.nl | FTP full control | (s)FTP User |
| SVC\_EXC\_FTP\_WEB\_P | P-dc.ba.uwv.nl | FTP full control | (s)FTP User |
| SVC\_EXC\_FTP\_BPB\_P | P-dc.ba.uwv.nl | FTP full control | (s)FTP User |
| SVC\_EXC\_FTP\_INV\_P | P-dc.ba.uwv.nl | FTP full control | (s)FTP User |
| SVC\_EXC\_FTP\_OPB\_P | P-dc.ba.uwv.nl | FTP full control | (s)FTP User |
| SVC\_EXC\_FTP\_ODS\_P | P-dc.ba.uwv.nl | FTP full control | (s)FTP User |
| SVC\_EXC\_FTP\_UZS\_P | P-dc.ba.uwv.nl | FTP full control | (s)FTP User |
| SVC\_EXC\_FTP\_WRINT\_P | P-dc.ba.uwv.nl | FTP full control | (s)FTP User |

# Appendix D: Security

| Security & Compliance requirement | Deviations from the standard | Implementation of the requirements |
| --- | --- | --- |
| Authorization | No deviations | See Appendix C |
| OS hardening | No deviations |  |
| Additional Middleware / database security configuration settings | No deviations |  |
| Firewall ports (GRIP SSD-1) | Applicable | See Appendix B |
| UWV Admin / console interface  (GRIP SSD-17) | Not Applicable | Admin console available: No |
| Limit HTTP header information  (GRIP SSD-24) | Applicable | HTTP header information must be limited to the bare minimum to limit the impact of fingerprinting.  A review of header information must be held and approved by UWV.  The HTTP header information is not allowed to show:   1. webserver software 2. webserver version 3. http protocol   detailed error messages |
| Limit HTTP methods  (GRIP SSD-26) | Applicable | All non-relevant http method information must be removed. By default, only GET and POST are allowed |
| Disable Directory Listing  (GRIP SSD-29) | Applicable |  |
| TLS/SSL Certificates | Applicable | New SSL certificates must be created. Specify the details on all SSL certificates necessary for this application |
| Session Encryption - HTTPS  (GRIP SSD-4) | Applicable | If applicable specify: HTTP / HTTPS |
| Session Encryption – SFTP  (GRIP SSD-4) | Applicable | If applicable specify: FTP / SFTP / FTP-S |
| Session Encryption – TLS version (GRIP SSD-4) | Applicable | If applicable specify TLS version (1.2 is required)  Only allowed cyphers are implemented. 1) |
| Security of Data in Transit External | No deviations |  |
| Security of Data in Transit Internal | No deviations |  |
| Segregation in security zones for Production | No deviations | See Appendix A |
| Segregation of Development, Test, Acceptance and Production environment | No deviations | See Appendix A |
| All software used must be supported by the vendor | No deviations | See Appendix A |
| Malware protection | No deviations | Standard scanning |
| Security Logging and -Monitoring retention  (default=1 year) | No deviations | 1 year |

1) *Based upon the latest NCSC recommendations and the used technologies within UWV*

*At design verification the allowed* *Cyphers are:*

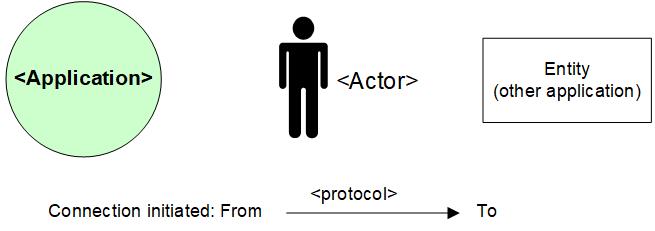
* *TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384*
* *TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256*
* *TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384*
* *TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256*
* *TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384*
* *TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA*
* *TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256*
* *TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA*
* *TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384*
* *TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA*
* *TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256*
* *TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA*
* *TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384*
* *TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256*
* *TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA*
* *TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA*

# Appendix E: Glossary

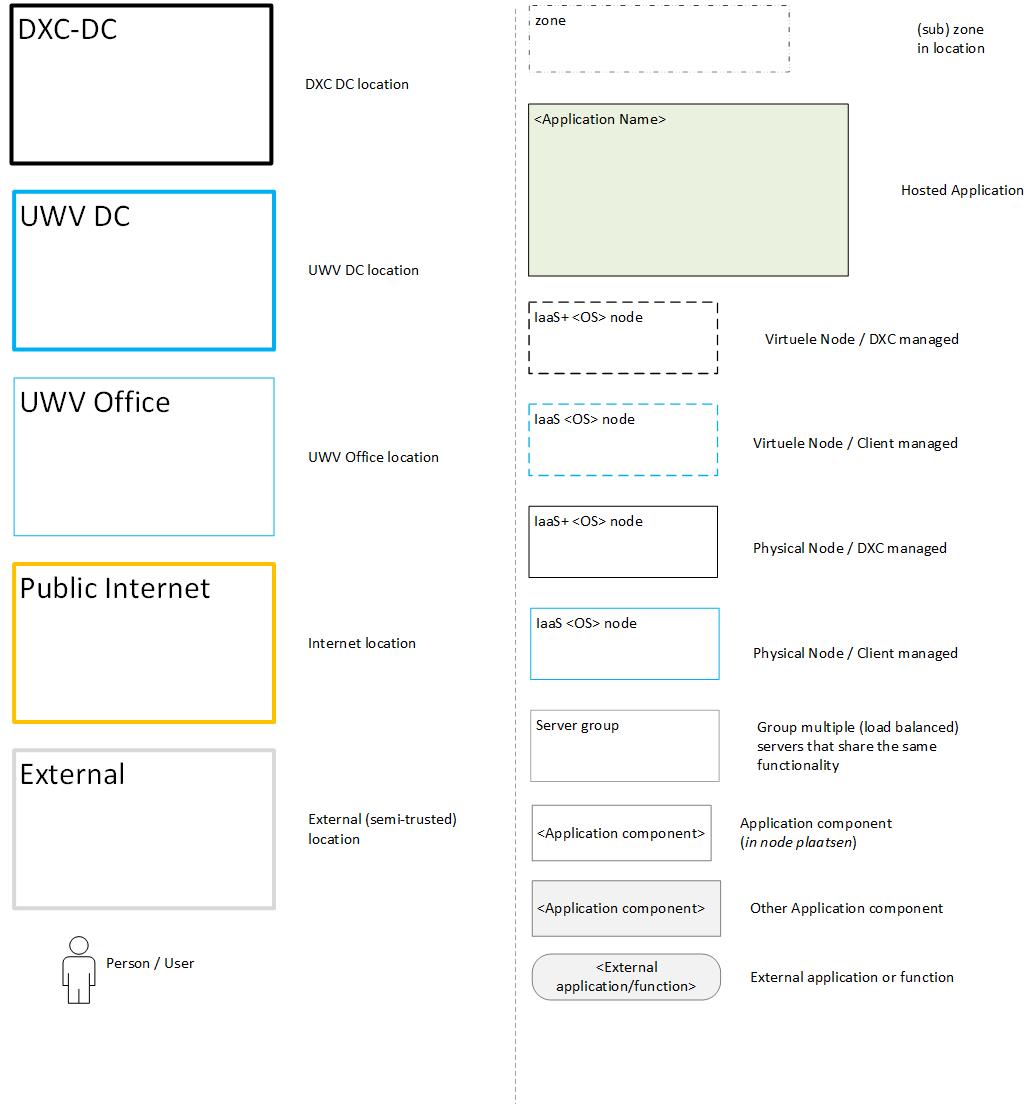
| **Acronym** | **Description** | **Notes** |
| --- | --- | --- |
| **ASO** | Account Security Officer |  |
| **CMO** | Current Mode of Operation refers to the old situation at IBM |  |
| **DXC managed systems** | All systems in the datacenters where DXC is responsible for |  |
| **EoS** | End of Support |  |
| **MSS** | DXC’s portfolio of Managed Security Services |  |
| **SBB** | Solution Building Block |  |
| **PDXC** | Platform DXC |  |
| **CVA** | Customer Virtual Appliance |  |
| **GRC** | Governance risk and compliance |  |
| **SPCM** | Server policy and compliance monitoring |  |
| **TCM** | Technical compliance monitoring |  |
| **SECMON** | Security monitoring |  |
| **MEP** | Managed Endpoint Protection |  |
| **PAM** | Privilege Account Management |  |
| **IBP** | Informatie Beveiligings Plan |  |
| **ASP** | Account Security Plan |  |
| **ISMS** | Information Security management System |  |
| **WEC** | Windows Event Collector |  |
| **DXC management REALM** | Management network of DXC dedicated for UWV in Amsterdam DC’s |  |
| **CI** | Configuration Item |  |
| **CIs** | Configuration Items |  |
| **SME** | Subject matter expert |  |
| **TCM** | Technology compliance management |  |
| **IBP** | Informatie beveiligings plan |  |
| **SIEM** | Security Incidents and Event management |  |
| **(s)FTP** | Secure File Transfer Protocol - SSH |  |
| **FTPs** | File Transfer Protocol - SSL |  |

# Appendix F: Legenda

## Legenda Context Diagram



## Legenda System Diagram



# Appendix G: Control

**USED TEMPLATE**

|  |
| --- |
| Based on HLD Template: UWV HLD - TEMPLATE 1.84.docx |

**DOCUMENT AUTHORISATION**

| Name | Role | Date |
| --- | --- | --- |
| Hans Kreisel | DXC Account Architect (verification) |  |
| Raymond Groenewoud | UWV Lead Architect (verification) |  |
| Rick van Diemen, delegated to Hans Kreisel | DXC Account Delivery Lead (acceptance) |  |

**DOCUMENT DISTRIBUTION**

| Name | Role | Date |
| --- | --- | --- |
| As per agreed PMO process |  |  |
| UWV Design Office | Design authority |  |

**CHANGE HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Summary of Changes |
| SharePoint version 0.1 | 17-11-2021 | DXC architecture team | First iteration of the HLD   * First iteration of HLD with partially filled in chapters 1 to 3. To be addressed by UWV architect. |
| SharePoint version 0.3 | 06-01-2022 | DXC architecture team | Second iteration of the HLD   * Populated chapter 1 * Populated paragraph 2.1 with conceptual diagram * Delivered content for 2.2.x * Chapter 3 is default remark. * Chapter 4 still empty, send example of some content to UWV Functional application management. |
| SharePoint version 0.4 | 17-01-2022 | DXC architecture team | Third iteration of the HLD   * Populated chapter 2.2 * Draft version chapter 4 and 5 * Appendixes Filled based on available knowledge of 5. |
| Verification version 0.5 | 24-01-2022 | DXC architecture team | 4th iteration of the HLD   * Appendixes filled, prepped for Peer Review and UWV architects review * Added Decision based on query database. Dataguard can on replicate what is in the original database. |
| Verification version 0.8 | 28-01-2022 | DXC architecture team | 5th iteration of the HLD   * Removed Comments * Added Review content on Education and Primary/Secondary database server * Prepped for Lead Architect review |
| Verification version 0.9 | 18-02-2022 | DXC architecture team | Design Office verification |
| Verification version 0.9.1 | 07-03-2022 | DXC architecture team | Design Office verification  Slight addition in Appendix C, |
| Version 1.0 | 22-03-2022 | DXC architecture team | Positive verified HLD |
| Version 1.1 | 03-08-2022 | DXC architecture team | Post implementation HLD  Changes base on changed BIV classification to 3, placing database in vault and additional servers for OBS/SBS solution  Implemented newer template 1.84   * + Additional 4.2.1 paragraph stating Operating systems   + moving of License to 4.2.2 from chapter 5   + Added 4.5.1 ‘Additional application related infra requirements’   + Changed 4.6 with additional table   + Appendix A, additional PowerHA table, changed LB private cloud Table new format   Chapter 4.1, BIV has changed so Confidentiality has become 3.  Chapter 5.1 Architectural Decision added point 7 about Confidentiality change from 2 to 3 meaning database had to be in Vault.  Chapter 5.2 Database for Prod and Acceptance now in Security Zone ‘Kluis’ also added missing infrastructure components for Functional Beheer servers SBS and OBS.  Chapter 5.3 Introduced servers for SBS and OBS and moved database in KLUIS.  Chapter 5.4.1 Introduced servers for SBS and OBS and moved database in KLUIS.  Chapter 5.4.3 Introduced servers for SBS and OBS and moved database in KLUIS.  Chapter 5.9.2 Added internal connections to database as they are now in KLUIS, also added connections between SBS and OBS to database.  Chapter 6. added 2 new Potential Future Improvements; Migration of complex started some time ago we already need to think about GOH to the next versions of Windows and RHEL. Also it might be prudent to have one centralised UWV TWS Generic server being used for all applications, investigate possibilities.  Appendix A: Changed node details of database to Kluis, also added the OBS and SBS servers. Also mentioned the 2 nodes for GOLD AIX in the PowerHA, it used to be assumed, now it is made visible. Same for storage ofc.  Appendix D: Added 3 new service accounts needed during implementation. |
| Version 1.1.1 | 07-11-2022 | DXC architecture team | Post implementation HLD  Changes based on removal of ADLAS connections to the Excasso Application.  Replaced Context Diagram in 2.2  Removed reference to ADLAS in 2.2.1 and Appendix B.  Replaced System Diagram Production in 5.3  Replaced System Diagram Acceptance in 5.4  Adjustments on Appendix A. sizing database servers and Cobol servers |
| Version 1.2 | 1-05-2023 | DXC architecture team | Post Aftercare HLD  Added Sjaak and TWDA in 2.2 context diagram as external entities. Also in Production Design 5.3.  Added 2 more ETP’s in 5.7 regarding RTPA.  Appendix A   1. adjusted Query database to 8 vCPU and 128 GB Mem (due to lack of indexing there needs to be more processing power and internal memory to keep up with changes in the primary database) 2. Adjusted storage for AIX servers. During the project a lot of changes needed to be made on the Cobol servers including Storage. Excasso is very batch dependend. Actual numbers of legacy dc storage where delivered by operation as these figures are not in SSP or CMDB.   Appendix B. Included Sjaak en TWDA in matrix |
| Version 1.3 | 17-11-2023 | DXC architecture team | CHG0137021  TPV is phased out, needs to be removed from HLD.  MAWW new connection external application via SI.  New connection to klantbeeld from GUP server.  AcuCobol version updated to 10.5 from 10.3.1  Adjust Cobol Server memory for education server to 64 GB   * Changes in Chapter 2.2 (diagram) and 2.2.1 * Changes in 4.2.2 * Changes in 5.3 (Diagram), 5.4.1 (Diagram) * Appendix A * Appendix B |