

HLD – KVB   
Kandidaten Verkenner Banenafspraak

Version: 1.1

Date: 18 August 2022

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 For the same reason some references in this document might be ‘outdated’ (i.e. not in this document anymore nor in other related documents).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](#_Toc100591136)

[1.1 Introduction 4](#_Toc100591137)

[1.2 Application use cases 4](#_Toc100591138)

[1.3 Out of Scope 4](#_Toc100591139)

[2 Architecture 5](#_Toc100591140)

[2.1 Conceptual 5](#_Toc100591141)

[2.2 Context diagram 6](#_Toc100591142)

[3 Functional Requirements 11](#_Toc100591143)

[4 Non-Functional Requirements 12](#_Toc100591144)

[4.1 Security & Compliance classifications 12](#_Toc100591145)

[4.2 Capacity and performance (volumetrics) 12](#_Toc100591146)

[4.3 Availability 12](#_Toc100591147)

[4.4 Security requirements 13](#_Toc100591148)

[4.5 System management 13](#_Toc100591149)

[4.6 Backup and Recovery 13](#_Toc100591150)

[4.7 Storage replication 13](#_Toc100591151)

[4.8 Scalability 13](#_Toc100591152)

[4.9 Disaster Recovery 13](#_Toc100591153)

[4.10 Infrastructure Technical Constraints 13](#_Toc100591154)

[4.11 DXC TAB requirements 14](#_Toc100591155)

[5 Solution 15](#_Toc100591156)

[5.1 Architectural Decisions 15](#_Toc100591157)

[5.2 Node descriptions and zone-projections 16](#_Toc100591158)

[5.3 System diagram - Production 17](#_Toc100591159)

[5.4 System diagram Non-Production 17](#_Toc100591160)

[5.5 SBB’s 18](#_Toc100591161)

[5.6 Load balancers 18](#_Toc100591162)

[5.7 Deviations from standards (RAL / EtP) 18](#_Toc100591163)

[5.8 Licenses 18](#_Toc100591164)

[5.9 Service Management 18](#_Toc100591165)

[5.10 Security 19](#_Toc100591166)

[6 Potential future improvements 21](#_Toc100591167)

[Appendix A: Technology and Sizing (at design verification) 22](#_Toc100591168)

[Node details 22](#_Toc100591169)

[Storage 23](#_Toc100591170)

[Software 24](#_Toc100591171)

[Load Balancers 24](#_Toc100591172)

[Appendix B: Network Protocol Matrix 25](#_Toc100591173)

[Appendix C: Users and Groups 26](#_Toc100591174)

[Appendix D: Security 27](#_Toc100591175)

[Appendix E: Glossary 29](#_Toc100591176)

[Appendix F: Legenda 30](#_Toc100591177)

[Legenda Context Diagram 30](#_Toc100591178)

[Legenda System Diagram 30](#_Toc100591179)

[Appendix G: Control 31](#_Toc100591180)

# Application Overview

## Introduction

KVB (Kandidaten Verkenner Banenafspraak - Candidates Explorer for Job Appointment) is an application that is exposed on the Internet and is accessible for registered Employers, UWV Workcoaches (UWV users) and UWV Functional Administrators (UWV FB).

The application provides employers with functions to match jobseekers having a Wajong qualification to vacancies. The application does not contain and/or provide any personal sensitive data. Instead, the application uses reference-IDs.

An employer can contact a workcoach of a WerkgeversServicePunt (WSP) to facilitate contact with the real candidate. There are multiple WerkgeversServicePunt locations. Each location contains several UWV Workcoaches. There is one National WSP and around 30 regional WSPs.

Workcoaches access their SONAR application and can retrieve candidate details via the reference-ID that is exposed in KVB. The Workcoach accesses KVB from the UWV WAN.

KVB uses an interface with Werk.nl OAM to authenticate employers, and a separate interface with Generic OAM/Sonar OID to authenticate Workcoaches and Functional Administrators, and an interface with Sonar to obtain authorization information (what role has the user in the application). The authorization information is only obtained for Workcoaches. Employers have no authorizations apart from access to the application which is arranged via authentication.

The KVB end-user application and KVB Beheerschermen application are hosted in the Acceptance and Production environment.

## Application use cases

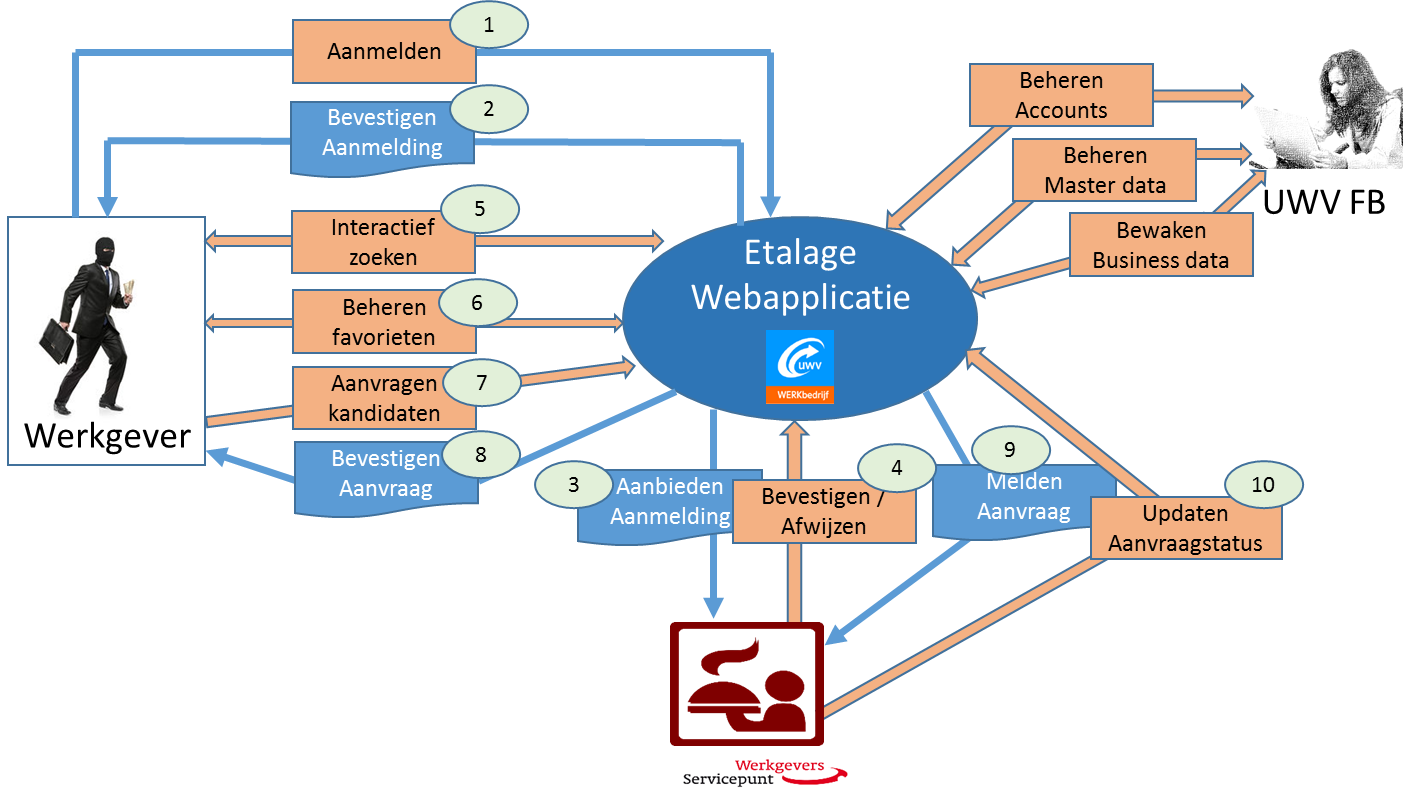
Application use cases are not defined, not applicable, or unknown to DXC.

## Out of Scope

* KVB Application development & test is performed by UWV in the OTOD and out of scope for this HLD.
* Eures webtier is hosted on the KVB webtier but is out of scope for this HLD, the Eures webtier is documented in the Eures HLD.
* Spiegel webtier is hosted on the KVB webtier but is out of scope for this HLD, the Spiegel webtier is documented in the Spiegel HLD.
* All components that belong to the UWV Office Infrastructure such as workstations, web browsers are out of scope.

# Architecture

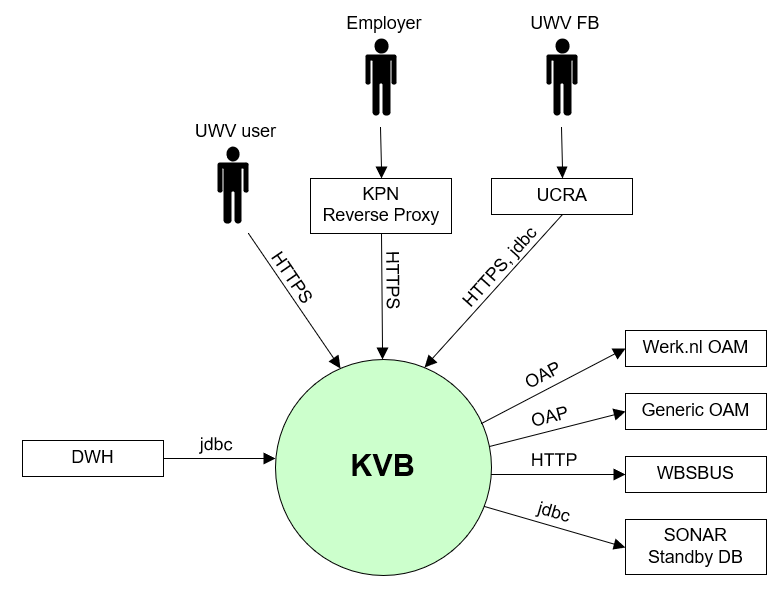
## Conceptual



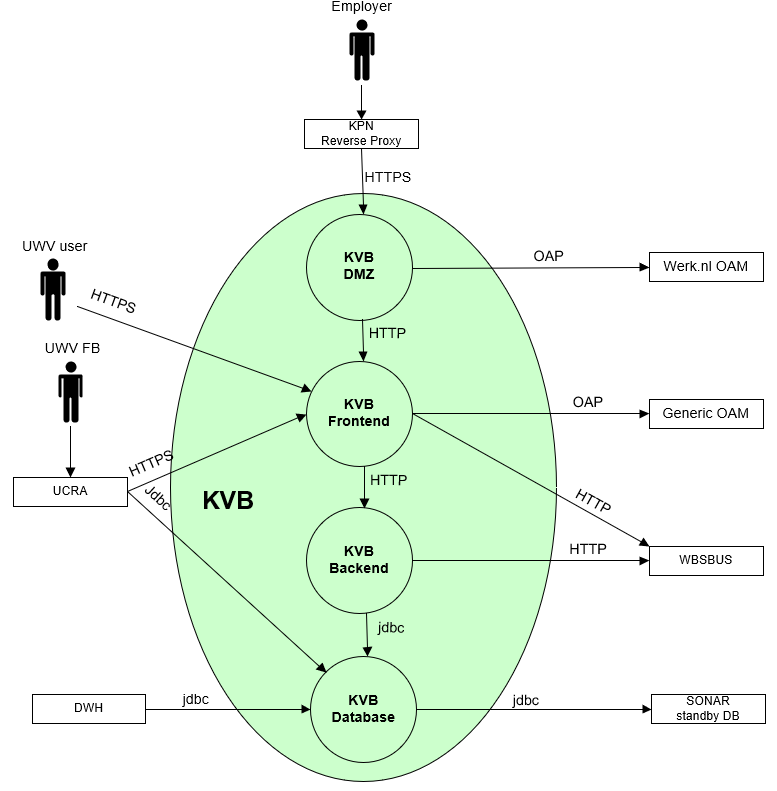
The application provides the following functions:

1. Login and registration screens
2. Confirmation mail for the employer
3. Signin mail to UWV approver
4. Approve or reject by UWV
5. Select: persons
6. Select: characteristics
7. Select: statistics
8. Submit information request
9. Request email to WSP (Werkgevers servicepunt – Employer service point)
10. WSP status management

## Context diagram



Below the same context diagram with some more detail to have a good understanding of the DMZ connections



### External entities

The characteristics of each external entity to the system are specified in the following paragraphs.

#### UWV user (Workcoach)

|  |  |
| --- | --- |
| **Description** | The Workcoach (adviseurs) are UWV employees that use various applications (e.g., WBS, SONAR) to support employers and facilitate jobseekers in finding a suitable job.  The Workcoaches are grouped in “WerkGeversServicepunt”, which is organised in several regions and one central location (the National WerkgeversServicePunt). |
| **Protocol and Port** | HTTPS (443) |
| **DC (Datacenter) connection** | External |
| **Direction** | Inbound |
| **Direct connection** | yes |
| **Security Controls** | Yes, Workcoach must logon to their applications (e.g., SONAR).  (Sonar OID user authentication) |
| **Number of users** | There are 300 workcoaches that will access the application in a month during working days/hours.  From this number and by doubling it, it can be derived that 0,3 Workcoaches will access the system concurrently in a 5-minute period during working days (Mon-Fri) and working hours (07.00-19.00h). |
| **Number of transactions** | not specified |
| **Frequency of transactions** | not specified |
| **Volume of data** | not specified |

#### Employer

|  |  |
| --- | --- |
| **Description** | Employer represents HR personnel and intermediaries (like Randstad). |
| **Protocol and Port** | HTTPS (443) |
| **DC (Datacenter) connection** | External |
| **Direction** | Inbound |
| **Direct connection** | No, via KPN Reverse Proxy |
| **Security Controls** | Yes, Employers must successfully identify & authenticate before they are allowed access to the application.  (Werk.nl OID user authentication) |
| **Number of users** | There will be 4000 Employers that access the application in a month during working days/hours.  From this number and by doubling it, it can be derived that 3 Employers will access the system concurrently in a 5-minute period during working days (Mon-Fri) and working hours (07.00-19.00h).  However, from usage statistics it has been determined that there are less than 5 Employer sessions per day. |
| **Number of transactions** | not specified |
| **Frequency of transactions** | not specified |
| **Volume of data** | not specified |

#### UWV FB

|  |  |
| --- | --- |
| **Description** | Functional Support can manage access of Employers and settings in the application. |
| **Protocol and Port** | HTTPS (443), jdbc (1526) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Inbound |
| **Direct connection** | No, via UCRA |
| **Security Controls** | Yes, Role Based Access (Generieke OAM / Sonar OID) |
| **Number of users** | Less than 5 totals assumed |
| **Number of transactions** | not specified |
| **Frequency of transactions** | not specified |
| **Volume of data** | Low |

#### Werk.nl OAM

|  |  |
| --- | --- |
| **Description** | Identification and Access control using Werk.nl/OAM solution. OAM user store (Werk.nl OID (Oracle Internet Directory)) contains account information of Employers |
| **Protocol and Port** | OAP (5575) |
| **DC (Datacenter) connection** | internal |
| **Direction** | outbound |
| **Direct connection** | yes |
| **Security Controls** | Yes, therefore https is used by the UWV user to prevent exchange of clear text passwords over the network. |
| **Number of users** | 4300 in a month (for P environment), (<250/day for A environment) |
| **Number of transactions** | 3,3 logons/5 minutes |
| **Frequency of transactions** | During working days/hours |
| **Volume of data** | Small |

#### Generic OAM

|  |  |
| --- | --- |
| **Description** | Identification and Access control for Workcoaches and Functional Support using Generic OAM solution. |
| **Protocol and Port** | OAP (5575) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | Yes |
| **Security Controls** | Yes, therefore https is used by the UWV user to prevent exchange of clear text passwords over the network. |
| **Number of users** | 4300 in a month (for P environment), (<250/day for A environment) |
| **Number of transactions** | 3,3 logons/5 minutes |
| **Frequency of transactions** | During working days/hours |
| **Volume of data** | Small |

#### WBSBUS

|  |  |
| --- | --- |
| **Description** | Werk.nl Middleware Services, Werk.nl has reference data that KVB needs. Reference data is obtained from BO&C (Beroepen, Opleidingen en Competencies) services, Postcode services and WSP-services through the WBSBUS. |
| **Protocol and Port** | HTTP (80) |
| **DC (Datacenter) connection** | Internal |
| **Direction** | Outbound |
| **Direct connection** | yes |
| **Security Controls** | Not specified |
| **Number of users** | Not specified |
| **Number of transactions** | Low |
| **Frequency of transactions** | Not specified |
| **Volume of data** | 250MB |

#### DWH

|  |  |
| --- | --- |
| **Description** | DataWareHouse gathers data from a materialized view in the KVB database. DWH provides this data to the MIP application. |
| **Protocol and Port** | jdbc (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | inbound |
| **Direct connection** | yes |
| **Security Controls** | No, the data does not contain sensitive personal data. |
| **Number of users** | 1 database user for P (also 1 user for A). |
| **Number of transactions** | <10 queries per environment for the data export and extract |
| **Frequency of transactions** | Weekly refresh |
| **Volume of data** | 45MB (30,000 records of 1,5kB each) |

#### Sonar Standby database

|  |  |
| --- | --- |
| **Description** | The Sonar standby database is queried using a dblink over SQLNet to get candidates that apply for KVB. The Sonar standby database is kept up to date with the primary Sonar database. The Sonar standby database also contains authorization information for the workcoaches that can access the KVB application. The authorization information is obtained using jdbc over SQLNet from the standby database. |
| **Protocol and Port** | Jdbc (1521) |
| **DC (Datacenter) connection** | internal |
| **Direction** | outbound |
| **Direct connection** | yes |
| **Security Controls** | No, the data does not contain sensitive personal data. |
| **Number of users** | * Candidate’s query: 1 database user for P (also 1 user for A). * Security controls: 300 for P environment, <30 for A environment. |
| **Number of transactions** | <10 queries per environment for data extract |
| **Frequency of transactions** | The security control queries are performed every time a user starts a session in the KVB application to obtain user roles.  Daily sync (in the evening) |
| **Volume of data** | 45MB (30,000 records of 1,5kB each) |

# Functional Requirements

* Access to the application is only allowed with the https protocol.
* Eures Webtier also needs to be hosted on the KVB DMZ system (Eures Webtier connections are documented in the Eures HLD)

# Non-Functional Requirements

## Security & Compliance classifications

For the BIV Rating the following repository is used: “2020 UWV-brede Risico Applicatie Lijst v1.0”

|  |  |
| --- | --- |
| **Application** | KVB |
| **Owner** | WB |
| **Availability (Beschikbaarheid)** | 3 |
| **Integrity (Integriteit)** | 2 |
| **Confidentiality (Vertrouwelijkheid)** | 1 |
| **Type of information /Data Classification** | Persoonsgegevens klanten of derden |
| **Direct or Indirect part of the primary information chain** | Indirect |

### Risk analysis UWV

No risk analysis provided by UWV

### Applicable security and compliance frameworks

|  |  |
| --- | --- |
| Security & Compliance Framework | Applicable |
| BIR 2017 | Yes |
| AVG / GDPR | No |
| DIGID | No |
| SUWI | No |
| Additional frameworks | Not Available |

## Capacity and performance (volumetrics)

* Regular data update: new data is uploaded at regular intervals (i.e. every week). The solution must support a minimum of 10 years of weekly increments of data to the database.
* Maximum size of data updates: One Sonar data update (obtained from Sonar standby database) has a maximum size of 500 kB.

## Availability

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Environment** | **Application Target** | **Application Service Hours** | **Infra Target** | **Infra Service Hours** |
| Production | 98% | 5 x 12 (Mo-Fr, 7 - 19h) | 98% | 5 x 12 (Mo-Fr, 7 - 19h) |
| Acceptance | 98% | 5 x 12 (Mo-Fr, 7 - 19h) | 98% | 5 x 12 (Mo-Fr, 7 - 19h) |
| Acceptance (KATO) | 98% | 5 x 12 (Mo-Fr, 7 - 19h) | 98% | 5 x 12 (Mo-Fr, 7 - 19h) |

## Security requirements

### Application Access Controls

Access to the application must be secured. Only registered Employers and registered Workcoaches are allowed to access the application. A valid User-ID and password are required to access the application. Authorization information must be retrieved from Sonar standby database

### Identity and Access Management

* Employers that access the application must be registered in the Werk.nl OID (Oracle Internet Directory). Access to resources must be managed and controlled with Werk.nl OAM (Oracle Access Manager).
* UWV users (WSP / work coaches) or UWV FB that access the application must be registered in the Sonar OID (Oracle Internet Directory). Access to resources must be managed and controlled with the Generic OAM (Oracle Access Manager).

### System logging

No specific system logging requirements are applicable

Detailed Standard Security requirements are documented in Appendix D

## System management

UWV standard system management is applicable.

## Backup and Recovery

No specific Backup and Recovery requirements are applicable.

## Storage replication

|  |  |
| --- | --- |
| **Environment** | **Storage Replication** |
| Production | Replicated storage |
| Acceptance | Non-replicated storage |

## Scalability

The KVB solution must be scalable (both horizontally and vertically) to support increased numbers of users and requests.

## Disaster Recovery

No specific disaster recovery requirements applicable.

## Infrastructure Technical Constraints

No infrastructure technical constraints.

## DXC TAB requirements

|  |  |
| --- | --- |
| **Category** | **Description** |
| Deployment (existingTAB Deployment server) | TAB Deployment server is used, exact ports will be determined during implementation (see Appendic B - connectivity sheet v1.1) |
| Deployment (XLdeploy) | XLdeploy is used |
| Shared Storage (existing TAB NFS server) | Shared storage is not used |
| Application monitoring (Sitescope) | No specific requirements |

# Solution

## Architectural Decisions

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Decision** | **Comments** | **Status** |
| 1 | KVB will have its own separate DMZ system which is also used by Eures and Spiegel. | Werk.nl External Access servers will not be used by KVB, Eures and Spiegel | approved |
| 2 | Each KVB Backend server (PROD, WATO and KATO) will be hosted on a dedicated Virtual Machine | DXC does not have an application hotel (where KVB Backend is currently hosted), instead dedicated VM’s are deployed | approved |
| 3 | Each KVB Database server (PROD, WATO and KATO) will be hosted on a dedicated Virtual Machine | DXC does not have a database hotel (where KVB database is currently hosted), instead dedicated VM’s are deployed | approved |
| 4 | The KVB DMZ system in acceptance is shared for WATO and KATO | KATO and WATO share the same webtier | approved |
| 5 | The KVB DMZ systems are placed in security zone External DMZ | According to the Security zone guidelines (System is accessed by internet users) | approved |
| 6 | The KVB Frontend systems are placed in security zone FrontOffice | According to the Security zone guidelines (System is accessed by UWV users) | approved |
| 7 | The KVB Backend systems are placed in security zone BackOffice | According to the Security zone guidelines | approved |
| 8 | The KVB Database systems are placed in security zone BackOffice | According to the Security zone guidelines (database does not contain data with confidentiality rating 2+ or higher) | approved |
| 9 | KVB databases will be hosted on Linux | Linux is the standard for Oracle Databases in the Private Cloud | approved |
| 10 | KVB DMZ systems will be hosted on Linux | If possible, Linux (Private Cloud) is preferred. In this case this can be changed from AIX to Linux without risks, similar situation as for the EDVLP External Access servers | approved |
| 10 | KVB DMZ systems will use Apache HTTP server | Similar config as for the EDVLP external access servers is preferred | approved |
| 11 | KVB DMZ and Frontend systems will use Oracle webgate version 12.2.1.4.0 | Werk.nl OAM and Generic OAM are on version 12.2.1.4.0 | approved |
| 12 | KVB DMZ will use Oracle webgate for the connection to Werk.nl OAM | Similar setup is used as for EDVLP, OAM configuration for Internet users | approved |
| 13 | KVB Frontend will use Oracle webgate for the connection to Generic OAM | OAM configuration for Internal UWV users | approved |

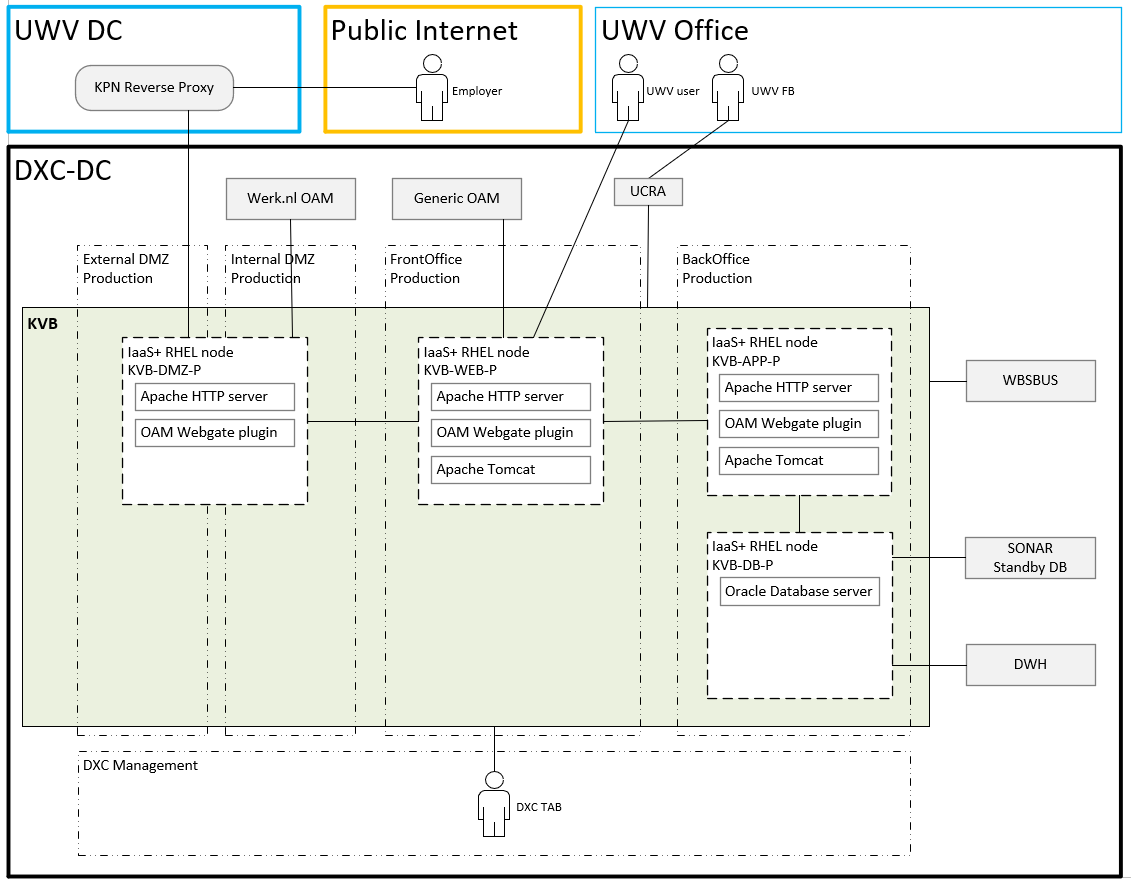
## Node descriptions and zone-projections

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Security Zone** | **Domain** | **Server Type** | **Node ID** | **Infra Service Level** |
| External DMZ | Production | Web server | KVB-DMZ-P | Bronze |
| FrontOffice | Production | Web server | KVB-WEB-P | Bronze |
| BackOffice | Production | Application server | KVB-APP-P | Bronze |
| BackOffice | Production | Database server | KVB-DB-P | Bronze |
| External DMZ | Acceptance | Web server | KVB-DMZ-A | Bronze |
| FrontOffice | Acceptance | Web server | KVB-WEB-A | Bronze |
| BackOffice | Acceptance | Application server | KVB-APP-A | Bronze |
| BackOffice | Acceptance | Database server | KVB-DB-A | Bronze |
| FrontOffice | Acceptance (KATO) | Web server | KVB-WEB-K | Bronze |
| BackOffice | Acceptance (KATO) | Application server | KVB-APP-K | Bronze |
| BackOffice | Acceptance (KATO) | Database server | KVB-DB-K | Bronze |

### DNS (customer facing name)

|  |  |  |
| --- | --- | --- |
| **Domain** | **Customer facing name** | **DNS suffix** |
| Production | KVB | P-dc.ba.uwv.nl |
| Production | KVB | A-dc.ba.uwv.nl |
| Acceptance | KVB-kato | A-dc.ba.uwv.nl |

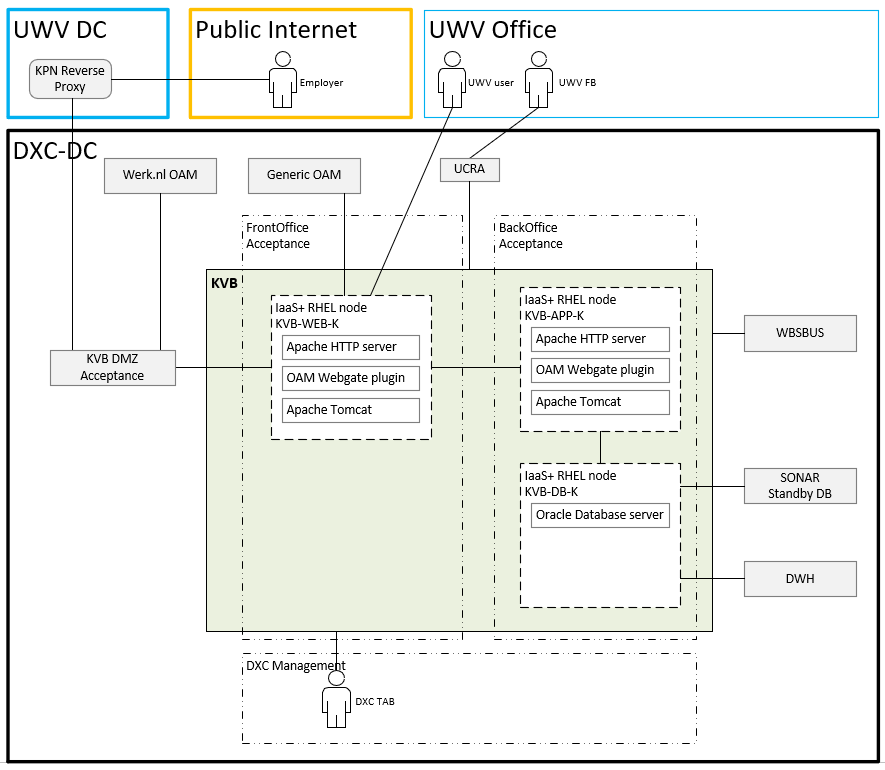
## System diagram - Production



## System diagram Non-Production

No separate diagram for Acceptance because the setup is the same as for Production.

KATO is shown below, setup is a little bit different, it uses the KVB DMZ from Acceptance.



## SBB’s

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

## Load balancers

|  |  |  |  |
| --- | --- | --- | --- |
| **Domain** | **Load balancer** | **Load balancer type** | **Description** |
| Production | No | Not applicable | Not applicable |
| Acceptance | No | Not applicable | Not applicable |

## 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 | Unsupported opensource (without vendor support): Apache HTTP webserver | Y | 20220316-00 |
| 2 | Connection from KVB DMZ (External DMZ – Internal interface) to Werk.nl OAM (BackOffice) required for authentication of employers accessing KVB | Y | 20220408-001 |

## Licenses

| **License required for** |
| --- |
| Oracle Database server 19.1 |
|  |

## Service Management

|  |  |  |  |
| --- | --- | --- | --- |
| **Environment** | **Infra Hosting** | **Database / Middleware Management** | **Technical Application Management** |
| Production | Bronze | TAB Basis | TAB Basis |
| Acceptance | Bronze | TAB Basis | TAB Basis |
| Acceptance (KATO) | 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

* Internal users: UWV user (WSP / work coaches), UWV FB

Authentication is done through Generic OAM (Sonar OID), authorization information is retrieved from the SONAR Standby database. User / group management is done by UWV.

* External users: Employers

Authentication is done through Werk.nl OAM (Werk.nl OID), authorization information is retrieved from the SONAR Standby database. User / group management is done by UWV

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 KVB the following is applicable:

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Connection Type** | **Between (component 1)** | **And (component 2)** |
| Internal | HTTP | KVB DMZ server | KVB Frontend (Web) server |
| Internal | HTTP | KVB Frontend (Web) server | KVB Backend (App) server |
| Internal | jdbc | KVB Backend (App) server | KVB database (DB) server |
| External (outside DXC) | HTTPS | KPN Reverse Proxy (Employer) | KVB DMZ server |
| External (outside DXC) | HTTPS | UWV Werkplek (UWV user and UWV FB) | KVB Frontend (Web) server |

For details see Appendix B

# Potential future improvements

|  |  |  |
| --- | --- | --- |
| **ID** | **Proposed improvement** | **Reason** |
| 1 | UWV to evaluate the classification vs service level. | BIV rating Availabilty=3 and and SLA= bronze does not seem to be in line with each other |
| 2 | UWV to investigate if vendor support for the Appache HTTP server is required | Apache HTTP Server provides an open-source HTTP server with the current HTTP standards that is supported by RedHat Linux |

# 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 | FrontOffice | AM3 | Acceptance | KVB-WEB-K  UWVA3VLAAPP0082 | 1 | 8 | RHEL 7.9 | IaaS+ | Bronze | no |
| Private Cloud | BackOffice | AM3 | Acceptance | KVB-APP-K  UWVA3VLAAPP0083 | 1 | 4 | RHEL 7.9 | IaaS+ | Bronze | no |
| Private Cloud Oracle DB | BackOffice | AM3 | Acceptance | KVB-DB-K  UWVA3VLAORA0043 | 2 | 8 | RHEL 7.9 | PaaS | Bronze | no |
| Private Cloud | External DMZ | AM2 | Acceptance | KVB-DMZ-A  uwvm2vlaweb0004 | 2 | 8 | RHEL 7.9 | IaaS+ | Bronze | no |
| Private Cloud | FrontOffice | AM2 | Acceptance | KVB-WEB-A  UWVA2VLAAPP0075 | 1 | 8 | RHEL 7.9 | IaaS+ | Bronze | no |
| Private Cloud | BackOffice | AM2 | Acceptance | KVB-APP-A  UWVA2VLAAPP0074 | 1 | 4 | RHEL 7.9 | IaaS+ | Bronze | no |
| Private Cloud Oracle DB | BackOffice | AM2 | Acceptance | KVB-DB-A  UWVA2VLAORA0021 | 2 | 8 | RHEL 7.9 | PaaS | Bronze | no |
| Private Cloud | External DMZ | AM2 | Production | KVB-DMZ-P  uwvm2vlpweb0005 | 2 | 8 | RHEL 7.9 | IaaS+ | Bronze | yes |
| Private Cloud | FrontOffice | AM2 | Production | KVB-WEB-P  UWVA2VLPAPP0074 | 1 | 8 | RHEL 7.9 | IaaS+ | Bronze | yes |
| Private Cloud | BackOffice | AM2 | Production | KVB-APP-P  UWVA2VLPAPP0070 | 1 | 4 | RHEL 7.9 | IaaS+ | Bronze | yes |
| Private Cloud Oracle DB | BackOffice | AM2 | Production | KVB-DB-P  UWVA2VLPORA0040 | 2 | 8 | RHEL 7.9 | PaaS | Bronze | yes |

## Storage

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Node ID** | **Domain** | **Disk 0 – Mountpoint 1 OS (mandatory) GB** | **Disk 1 – Mountpoint 1 App (mandatory) GB** | **Disk 1 – Mountpoint 2 (optional)** | **Disk 1 – Mountpoint 3 (optional)** | **Disk 2 – Mountpoint 1 (optional)** |
| KVB-WEB-K  UWVA3VLAAPP0082 | Acceptance | 100 | 50 | n/a | n/a | n/a |
| KVB-APP-K  UWVA3VLAAPP0083 | Acceptance | 100 | 50 | n/a | n/a | n/a |
| KVB-DMZ-A  uwvm2vlaweb0004 | Acceptance | 100 | 50 | n/a | n/a | n/a |
| KVB-WEB-A  UWVA2VLAAPP0075 | Acceptance | 100 | 50 | n/a | n/a | n/a |
| KVB-APP-A  UWVA2VLAAPP0074 | Acceptance | 100 | 50 | n/a | n/a | n/a |
| KVB-DMZ-P  uwvm2vlpweb0005 | Production | 100 | 50 | n/a | n/a | n/a |
| KVB-WEB-P  UWVA2VLPAPP0074 | Production | 100 | 50 | n/a | n/a | n/a |
| KVB-APP-P  UWVA2VLPAPP0070 | Production | 100 | 50 | n/a | n/a | n/a |

*Linux Application server(s)*

*Oracle Database server(s)*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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** |
| KVB-DB-K  UWVA3VLAORA0043 | Acceptance | 100 | 100 | 100 | 50 | 50 | 50 | 50 |
| KVB-DB-A  UWVA2VLAORA0021 | Acceptance | 100 | 100 | 100 | 100 | 100 | 50 | 50 |
| KVB-DB-P  UWVA2VLPORA0040 | Production | 100 | 100 | 100 | 100 | 100 | 50 | 50 |

## Software

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Node Description** | **Suite** | **Software** | **Version** | **Supported by vendor** |
| KVB-DMZ-A, KVB DMZ-P | 1-OS | RHEL | 7.9 | Red Hat |
| KVB-DMZ-A, KVB DMZ-P | 4-Middleware | Apache HTTP server | 2.4 |  |
| KVB-DMZ-A, KVB DMZ-P | 4-Middleware | OAM Webgate plugin | 12.2.1.4.0 | Oracle |
| KVB-DMZ-A, KVB DMZ-P | 5-Application | KVB WG-webtier |  |  |
|  |  |  |  |  |
| KVB-WEB-K, KVB-WEB-A, KVB-WEB-P | 1-OS | RHEL | 7.9 | Red Hat |
| KVB-WEB-K, KVB-WEB-A, KVB-WEB-P | 2-Library | Java JRE | 8 | Oracle |
| KVB-WEB-K, KVB-WEB-A, KVB-WEB-P | 4-Middleware | Apache Tomcat | 9.0.56 |  |
| KVB-WEB-K, KVB-WEB-A, KVB-WEB-P | 4-Middleware | Apache HTTP server | 2.4 | Apache |
| KVB-WEB-K, KVB-WEB-A, KVB-WEB-P | 4-Middleware | OAM Webgate plugin | 12.2.1.4.0 | Oracle |
| KVB-WEB-K, KVB-WEB-A, KVB-WEB-P | 5-Application | KVB WG-fe |  |  |
| KVB-WEB-K, KVB-WEB-A, KVB-WEB-P | 5-Application | KVB WSP-fe |  |  |
| KVB-WEB-K, KVB-WEB-A, KVB-WEB-P | 5-Application | KVB Beheer-fe |  |  |
| KVB-WEB-K, KVB-WEB-A, KVB-WEB-P | 5-Application | KVB WSP/Beheer-webtier |  |  |
|  |  |  |  |  |
| KVB-APP-K, KVB-APP-A, KVB-APP-P | 1-OS | RHEL | 7.9 | Red Hat |
| KVB-APP-K, KVB-APP-A, KVB-APP-P | 2-Library | Java JRE | 8 | Oracle |
| KVB-APP-K, KVB-APP-A, KVB-APP-P | 4-Middleware | Apache Tomcat | 9.0.56 | Apache |
| KVB-APP-K, KVB-APP-A, KVB-APP-P | 5-Application | KVB WG-be |  |  |
| KVB-APP-K, KVB-APP-A, KVB-APP-P | 5-Application | KVB WSP-be |  |  |
| KVB-APP-K, KVB-APP-A, KVB-APP-P | 5-Application | KVB Beheer-be |  |  |
|  |  |  |  |  |
| KVB-DB-K, KVB-DB-A, KVB-DB-P | 1-OS | RHEL | 7.9 | Red Hat |
| KVB-DB-K, KVB-DB-A, KVB-DB-P | 3-Database | Oracle Database Server | 19.1 | Oracle |
|  |  |  |  |  |

## Load Balancers

Not applicable for this application

# 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** |
| KVB-DMZ-P | KVB-WEB-P | HTTP | 80 |  |
| KVB-DMZ-A | KVB-WEB-A, KVB-WEB-K | HTTP | 80 |  |

**KVB DMZ server to KVB Frontend server**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| KVB-WEB-P | KVB-APP-P | HTTP | 8080 |  |
| KVB-WEB-A | KVB-APP-A | HTTP | 8080 |  |
| KVB-WEB-K | KVB-APP-K | HTTP | 8080 |  |

**KVB Frontend server to KVB Backend server**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| KVB-APP-P | KVB-DB-P | jdbc | 1521 |  |
| KVB-APP-A | KVB-DB-A | jdbc | 1521 |  |
| KVB-APP-K | KVB-DB-K | jdbc | 1521 |  |

**KVB Backend server to KVB Database server**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| KPN Reverse Proxy (Employer) | KVB-DMZ-P, KVB-DMZ-A | HTTPS | 443 |  |

**KPN Reverse Proxy to KVB DMZ server**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **ports** | **Comments** |
| UWV Werkplek (UWV user, UWV FB) | KVB-WEB-P, KVB-WEB-A, KVB-WEB-K | HTTPS | 443 |  |

**UWV Werkplek to KVB Frontend server**

**Only for HLD version 1.1:**

****

# Appendix C: Users and Groups

DXC Managed Users and groups are documented by DXC TAB in the TMM (Technical Maintenance Manual) during the realization phase

***Any DXC deviations must be documented in HLD v1.1!***

***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** |
|  |  |  |  |

# Appendix D: Security

| Security & Compliance requirement | Deviations from the standard | Implementation of the requirements |
| --- | --- | --- |
| Authorization | No deviation | See Appendix C |
| OS hardening | No deviation | Standard hardening |
| Additional Middleware / database security configuration settings | No deviation | Standard hardening |
| Firewall ports (GRIP SSD-1) | Applicable | See Appendix B |
| UWV Admin / console interface  (GRIP SSD-17) | Applicable | Admin console available: Yes |
| 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) | Not Applicable | KVB Tomcat instances do not work is this enabled, therefore the configuration deviates from the preferred settings |
| Disable Directory Listing  (GRIP SSD-29) | Not Applicable |  |
| TLS/SSL Certificates | Applicable | New SSL certificates must be created. Specify the details on all SSL certificates necessary for this application. Entrust certificate must be requested |
| Session Encryption - HTTPS  (GRIP SSD-4) | Applicable | If applicable specify: HTTPS |
| Session Encryption – SFTP  (GRIP SSD-4) | Not Applicable | If applicable specify: SFTP (to SI File Transfer) |
| Session Encryption – TLS version (GRIP SSD-4) | Applicable | If applicable specify TLS version (1.2 is required). Minimal TLS 1.2 is used  Only allowed cyphers are implemented. 1) |
| Security of Data in Transit External | No deviation |  |
| Security of Data in Transit Internal | No deviation |  |
| Segregation in security zones for Production | No deviation | See Appendix A |
| Segregation of Development, Test, Acceptance and Production environment | No deviation | See Appendix A |
| All software used must be supported by the vendor | No deviation | See Appendix A |
| Malware protection | No deviation | Standard scanning |
| Security Logging and -Monitoring retention  (default=1 year) | No deviation | 1 year |

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

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

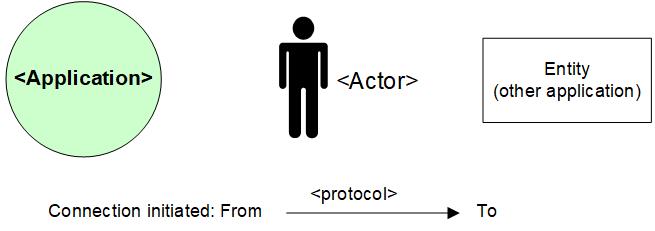
* *TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384*
* *TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256*
* *TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384*
* *TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256*
* *TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384*
* *TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA*
*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

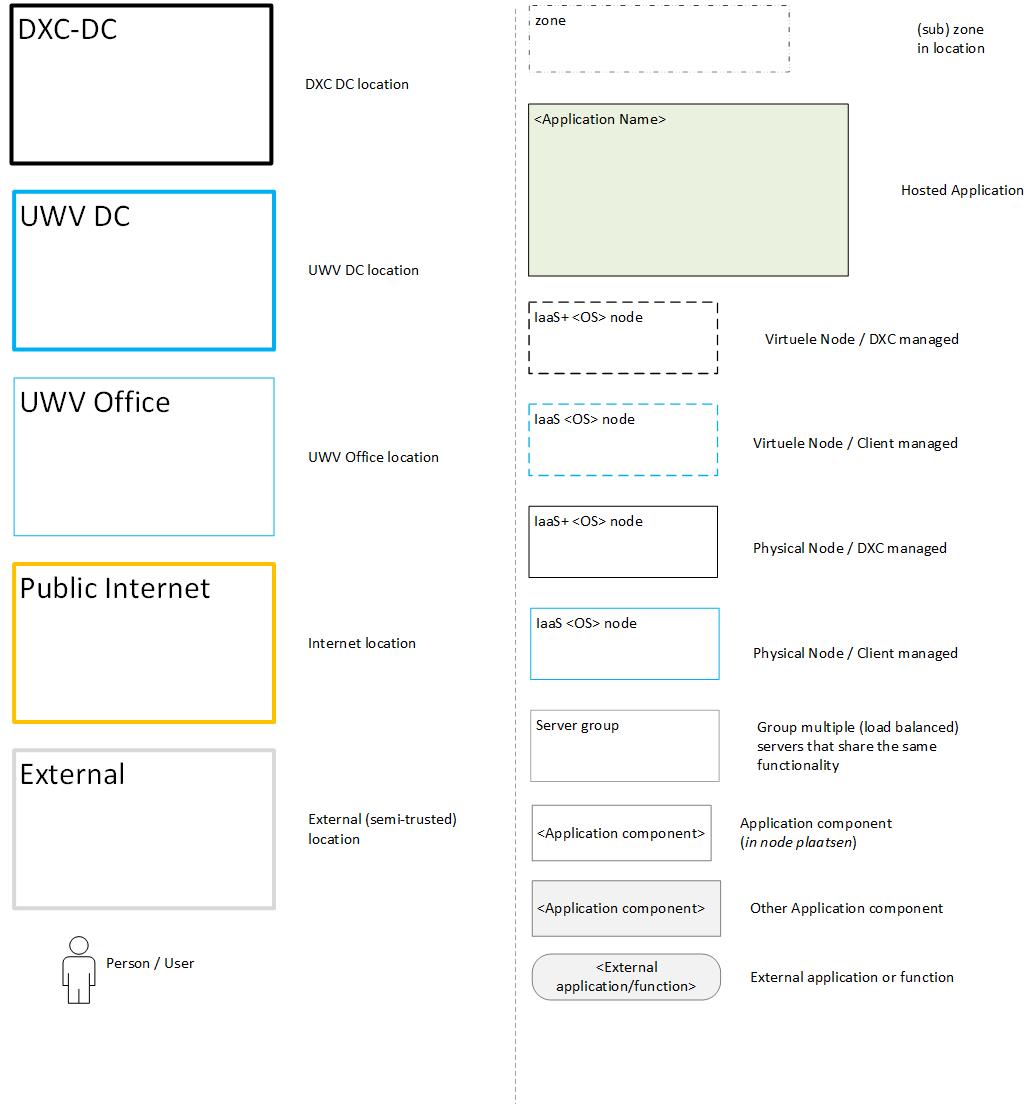
|  |  | **Notes** |
| --- | --- | --- |
| **ASO** | Account Security Officer |  |
| **CMO** | Current Mode of Operation refers to the old situation at IBM |  |
| **DXC managed systems** | All systems in the datacenters where DXC is responsible for |  |
| **EoS** | End of Support |  |
| **MSS** | DXC’s 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 1.81.docx |

**DOCUMENT AUTHORISATION**

| Name | Role | Date |
| --- | --- | --- |
| Cora Kuijper | DXC Technical Transformation Lead (verification) | 31-03-2022 |
| Nic van Spronsen | UWV Lead Architect (verification) | 13-04-2022 |
| Harry Hageman (delegated to Hans Kreisel) | DXC Account Delivery Lead (acceptance) | 11-04-2022 |

**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 | 03-09-2021  06-09-2021  08-09-2021 | DXC architecture team | First iteration of the HLD   * Version 0.1 * Version 0.2 * Version 0.3 |
| SharePoint version | 11-11-2021  11-03-2022  14-03-2022 | DXC architecture team | Second iteration of the HLD   * 0.4 – Initial version fro UWv review * 0.6 – Processed comments from UWV * 0.7 – Final version for UWV review |
| Verification version 0.8 | 07-04-2022 | DXC architecture team | Third iteration of the HLD |
| Verification version 0.9 | 11-04-2022 | DXC architecture team | Design Office verification |
| Version 1.0 | 13-04-2022 | DXC architecture team | Positive verified HLD |
| Version 1.1 | dd-mm-yyyy | DXC architecture team | Post implementation HLD   * Appendix B: Added connectivty sheet v1.1 * Appendix A: Updated location for the acceptance servers from AM3 to AM2 because they where requested in AM2 * Appendix A: added servernames * Updated according to latest connectivity sheet: UWV FB via UCRA, added DB connection and added connection from KVB Web to WBSBSUS |