**Low Level Design Document**

## ****Upgrade Axway API Management****

**Versi 1.0**

**Copyright ã (2025) by Bank Danamon**

All rights reserved. This material is confidential and proprietary to BANK DANAMON and no part of this material should be reproduced, published in any form by any means, electronic or mechanical including photocopy or any information storage or retrieval system nor should the material be disclosed to third parties without the express written authorization of BANK DANAMON.

**Lembar Tanda Tangan**

Approval Page

|  |  |  |
| --- | --- | --- |
| Prepared by | Angga Tirtakusumah  IT Application Support / Technical Project Manager / Vendor | Date: |
| Reviewed by | Fulsi Wiyata  IT Application Support Manager (System Owner) | Date: |
| IT Support Function\* | Yok Christiyono  IT Security Governance & Engineering Head | Date: |
| Aghiel Prayogo  IT Service Design Head | Date: |
| Hassan Ridwan  IT Database Infrastructure Head | Date: |
| Approved by | Grahita Djati Nugraha  IT Unit Head (System Owner) | Date: |
| Wawan Irawan Wan  IT Infrastructure Management Head | Date: |

\*Mandatory related to respective areas

Please insert additional approval coloumn as needed equal to total of impacted systems/apps.

**Document Template History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Sections changed** | **Version** | **Author** | **Description** |
| 08/03/2025 | Initial Document | 1.0 | Muhamad Fazry Fedro Simangunsong  Andika Dwi H |  |
|  |  |  |  |  |

**Low Level Design Template Instructions**

Sections of the template should NOT be removed. If a section is deemed not applicable for a project, a note is to be inserted at that section, which includes the reason the section is not applicable. For assistance in completing the technical specification document, contact the respective team representative.

NOTE:  When using this document, the portions in ***blue*** are instructional or variable, and should be removed or modified as appropriate.  The examples should also be replaced.  Make sure to remove the Instructions page and reformat the table of contents, update the headers and footers.

**TABLE OF CONTENTS**

# [Federated API Management](#LLDCRF4752FederatedAPIManagementExterna)

# [1.Pendahuluan](#LLDCRF4752FederatedAPIManagementExterna)

# [1.1 Deskripsi](#LLDCRF4752FederatedAPIManagementExterna)

# [2.System Architecture](#LLDCRF4752FederatedAPIManagementExterna)

# [2.1 Spesifikasi Hardware dan Kebutuhan Software](#LLDCRF4752FederatedAPIManagementExterna)

# [2.2 Topologi Database](#LLDCRF4752FederatedAPIManagementExterna)

# [2.3 Topology File System](#LLDCRF4752FederatedAPIManagementExterna)

# [2.4 Rack Layout](#LLDCRF4752FederatedAPIManagementExterna)

# [2.5 Power and Rack Space](#LLDCRF4752FederatedAPIManagementExterna)

# [2.6 Physical Network Connection](#LLDCRF4752FederatedAPIManagementExterna)

# [2.7 Host Logical Network](#LLDCRF4752FederatedAPIManagementExterna)

# [2.8 IP Address](#LLDCRF4752FederatedAPIManagementExterna)

# [2.9 Network Switches](#LLDCRF4752FederatedAPIManagementExterna)

# [2.9.1 Cabling Connection Diagram](#LLDCRF4752FederatedAPIManagementExterna)

# [3.Ketergantungan Dengan Sistem Lain](#LLDCRF4752FederatedAPIManagementExterna)

# [3.1 Detail Perubahan Sistem Yang Terimbas](#LLDCRF4752FederatedAPIManagementExterna)

# [4.Persyaratan Standard Keamanan Infrastruktur](#LLDCRF4752FederatedAPIManagementExterna)

# [5. Availability Requirement](#LLDCRF4752FederatedAPIManagementExterna)

|  |
| --- |
| ****1. Pendahuluan**** |

## ****2.1 Kebutuhan**** Software

* API Gateway and Manager V.7.7.20250530.
* API Gateway and Manager V.7.7.20250530.
* Apache Cassandra 4.1.8.
* API Portal 7.7.20250530.

## ****1.1 Deskripsi****

Bank Danamon memiliki lebih dari 5 juta transaksi API dalam sehari yang diatur dan dilayani oleh API Management External dan Internal. Kebutuhan API yang semakin meningkat dan beragam harus diikuti oleh kinerja aplikasi API Management baik dari sisi fitur, keamanan, pengembangan, dan dukungan Principal aplikasi.

Saat ini versi API Management yang diimiliki Bank Danamon adalah versi 7.7.20230830, di mana versi tersebut telah memasuki masa End of Support. Jika aplikasi telah memasuki masa End of Support, terdapat limitasi layanan dari Principal. Untuk tetap memiliki kinerja API Management yang handal, stabil dan aman maka dibutuhkan upgrade versi aplikasi API Management ke versi terakhir yakni versi 7.7.20250530.

Aplikasi Axway versi 7.7.20250530 memerlukan database cassandra dengan versi 4.1.8 yang sebelumnya menggunakan versi 4.0.10, pada versi cassandra versi 4.1.8 terdapat peningkatan performance dan stability improvements.

API Portal digunakan untuk calon partner agar dapat mencoba memanggil API tanpa mengakses sistem backend yang sebenarnya (production).

**1.2 Tujuan**

* Pemeliharaan system aplikasi API Management External dan Internal sebagai upaya mencegah kerusakan, mengurangi downtime dan menjaga performa.
* Mendapatkan dukungan Principal jika terdapat masalah pada aplikasi API Management External dan Internal.
* Patch pada versi aplikasi jika terdapat bug.

**1.3 Ruang Lingkup Proyek**

**Objective:**

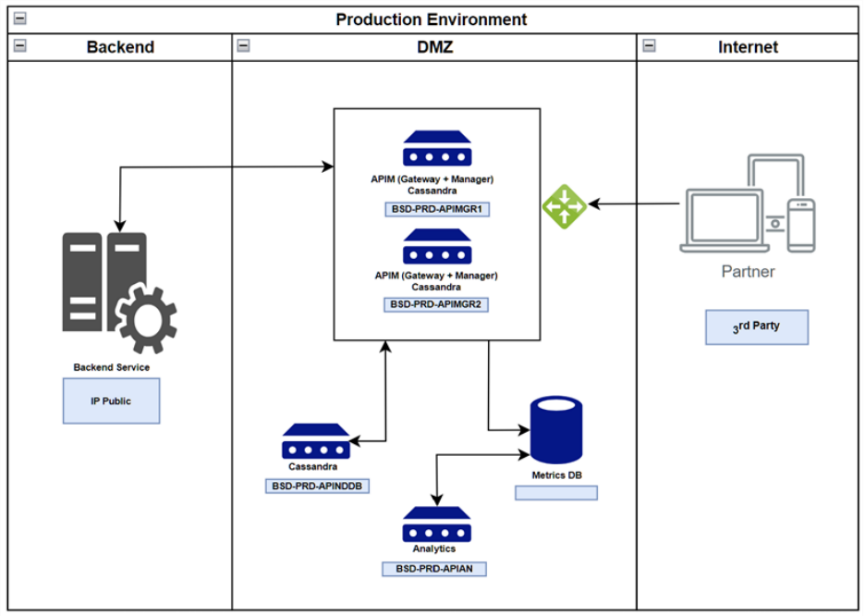
* System application API Management has been upgraded to the latest version that supported by Axway; version 7.7.20250530.
* System application API Portal has been upgraded to the latest version that supported by Axway; version 7.7.20250530.
* Database Cassandra has been upgraded to the latest version that supported by Axway; version 4.1.8.

**Deliverables:**

* Upgrade API Management External from version 7.7.20230830 to 7.7.20250530: Production (Cluster), UAT (Single), PT (Cluster) and Sandbox (Single).
* Upgrade API Management Internal from version 7.7.20230830 to 7.7.20250530: Production (Multi DC), UAT (Single) and PT (Cluster).
* Upgrade Database Cassandra External from version 4.0.10 to 4.1.8: Production (Cluster), UAT (Single), PT (Cluster) and Sandbox (Single).
* Upgrade Database Cassandra Internal from version 4.0.10 to 4.1.8: Production (Multi DC), UAT (Single), PT (Cluster).
* Upgrade API Portal External from version 7.7.20230830 to 7.7.20250530: Production (Single), UAT (Single)

|  |
| --- |
| ****2.System Architecture**** |

## ****2.2 Topologi Database****



## ****2.3 Topology File System****

**D1UAPIMAPPLV001**

|  |  |
| --- | --- |
| Nama Server | API Gateway UAT Internal |
| OS | RHEL 8.10 |
| Application | /apps/Axway-7.7.0/apigateway |
| Log Application | /apps/Axway-7.7.0/apigateway/events  /apps/Axway-7.7.0/apigateway/trace |

**D1UCASSDBALV001**

|  |  |
| --- | --- |
| Nama Server | Cassandra node 1 UAT Internal |
| OS | RHEL 8.10 |
| Database | /apps/Axway-7.7.0/cassandra |
| Log Database | /apps/Axway-7.7.0/cassandra/logs |

**D1UCASSDBALV002**

|  |  |
| --- | --- |
| Nama Server | Cassandra node 2 UAT Internal |
| OS | RHEL 8.10 |
| Database | /apps/Axway-7.7.0/cassandra |
| Log Database | /apps/Axway-7.7.0/cassandra/logs |

**D1UCASSDBALV003**

|  |  |
| --- | --- |
| Nama Server | Cassandra node 3 UAT Internal |
| OS | RHEL 8.10 |
| Database | /apps/Axway-7.7.0/cassandra |
| Log Database | /apps/Axway-7.7.0/cassandra/logs |

**D1UAPIAAPPLV001**

|  |  |
| --- | --- |
| Nama Server | API Analytics UAT Internal |
| OS | RHEL 8.10 |
| Application | /apps/Axway-7.7.0/analytics |
| Log Application | /apps/Axway-7.7.0/analytics/trace |
| Database | /apps/mysql |
| Log Database | /apps/mysql |

**KSI-UAT-APIMGR**

|  |  |
| --- | --- |
| Nama Server | API Gateway UAT External |
| OS | RHEL 8.10 |
| Application | /apps/Axway-7.7.0/apigateway |
| Log Application | /apps/Axway-7.7.0/apigateway/events  /apps/Axway-7.7.0/apigateway/trace |

**BSD-PRD-APIAN**

|  |  |
| --- | --- |
| Nama Server | API Analytics |
| OS | RHEL 8.10 |
| Application | /apps/Axway-7.7.0/analytics |
| Log Application | /apps/Axway-7.7.0/analytics/trace |
| Database | /apps/mysql |
| Log Database | /apps/mysql |

**KSI-UAT-APIPRTL**

|  |  |
| --- | --- |
| Nama Server | API PORTAL External |
| OS | RHEL 8.10 |
| Application | /opt/Axway |

**BSD-PRD-APIMGR1**

|  |  |
| --- | --- |
| Nama Server | API Gateway PT External |
| OS | RHEL 8.10 |
| Application | /apps/Axway-7.7.0 |
| Log Application | /apps/Axway-7.7.0/apigateway/events  /apps/Axway-7.7.0/apigateway/trace |

**BSD-PRD-APIMGR2**

|  |  |
| --- | --- |
| Nama Server | API Gateway PT External |
| OS | RHEL 8.10 |
| Application | /apps/Axway-7.7.0 |
| Log Application | /apps/Axway-7.7.0/apigateway/events  /apps/Axway-7.7.0/apigateway/trace |

**BSD-PRD-APINDDB**

|  |  |
| --- | --- |
| Nama Server | Cassandra PT External |
| OS | RHEL 8.10 |
| Database | /apps/Axway-7.7.0/cassandra |
| Log Database | /apps/Axway-7.7.0/cassandra/logs |

## ****2.4 Rack Layout****

**N/A**

## ****2.5****Power and Rack Space

**N/A**

## 2.6 Physical Network Connection

**N/A**

## ****2.7 Host Logical Network****

**N/A**

## ****2.8 IP Address****

|  |  |
| --- | --- |
| **SERVER 1** | |
| Hostname | D2PAPIDAPPLV001 |
| IP Address | 10.192.74.201 |
| **SERVER 1** | |
| Hostname | D2PAPIDAPPLV001 |
| IP Address | 10.192.74.201 |
| **SERVER 1** | |
| Hostname | D2PAPIDAPPLV001 |
| IP Address | 10.192.74.201 |
| **SERVER 1** | |
| Hostname | D2PAPIDAPPLV001 |
| IP Address | 10.192.74.201 |
| **SERVER 1** | |
| Hostname | D2PAPIDAPPLV001 |
| IP Address | 10.192.74.201 |
| **SERVER UAT INTERNAL** | |
| Hostname | D1UAPIMAPPLV001 |
| IP Address | 10.197.36.21 |
| **SERVER UAT INTERNAL** | |
| Hostname | D1UCASSDBALV001 |
| IP Address | 10.197.36.23 |
| **SERVER UAT INTERNAL** | |
| Hostname | D1UCASSDBALV002 |
| IP Address | 10.197.36.24 |
| **SERVER UAT INTERNAL** | |
| Hostname | D1UCASSDBALV003 |
| IP Address | 10.197.36.25 |
| **SERVER UAT INTERNAL** | |
| Hostname | D1UAPIAAPPLV001 |
| IP Address | 10.197.36.22 |
| **SERVER UAT EXTERNAL** | |
| Hostname | KSI-UAT-APIMGR |
| IP Address | 10.197.19.105 |
| **SERVER UAT EXTERNAL** | |
| Hostname | BSD-PRD-APIAN |
| IP Address | 10.197.19.106 |
| **SERVER UAT EXTERNAL** | |
| Hostname | KSI-UAT-APIPRTL |
| IP Address | 10.197.19.107 |
| **SERVER PT EXTERNAL** | |
| Hostname | BSD-PRD-APIMGR1 |
| IP Address | 10.197.17.30 |
| **SERVER PT EXTERNAL** | |
| Hostname | BSD-PRD-APIMGR2 |
| IP Address | 10.197.17.31 |
| **SERVER PT EXTERNAL** | |
| Hostname | BSD-PRD-APINDDB |
| IP Address | 10.197.17.36 |

## ****2.9**** Network Switches

### ****2.9.1 Cabling Connection Diagram****

**N/A**

**2.9.2 Layer 1, 2, 3 Network Information**

**N/A**

|  |
| --- |
| ****3.Ketergantungan Dengan Sistem Lain**** |

**N/A**

## ****3.1 Detail Perubahan Sistem Yang Terimbas****

**N/A**

|  |
| --- |
| ****4.****Persyaratan Standard Keamanan Infrastruktur |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No** | **Cyber Security**  **Requirements for LLD** | **Related Units** | **Reff**  **No:** | **FSO**  **(Yes/No)** | **Remarks** |
| 1 | Hardening  1. IT Parameter Hardening (ITPH)  2. Implementator Hardening | 1. IT Security Governance  2. IT Midrange System |  | YES |  |
| 2 | Security Access Matrix (SAM) /Privilege Access Document (PAD). | IT Security Assurance |  | YES |  |
| 3 | Application Request Firewall (ARF) | IT Security Assurance |  | - |  |
| 4 | Vulnerability Assessment (VA) | IT Security Operations |  | YES |  |
| 5 | Server Vulnerability Assessment (SVS) | IT Security Operations |  | YES |  |
| 6 | Penetration Testing (PT) | IT Security Operations |  | - |  |
| 7 | User Access Matrix (UAM) | Internal Control Compliance |  | - |  |

**4.1 Authentication**

*<Describe existing authentication technology being leveraged or new technology being used >*

**4.2 Entitlement/Authorization**

**4.3 Input Validation**

*<Describe the process of input validations being used, including those enforced for file uploads/downloads/transfers whenever relevant or used by the application. Input validation controls should at least cover the following:*

1. *Ensuring that the given input is according to the expected data types. For example, a field expected an input data type of integer should only accept integers not floats – the application must be able to ensure this*
2. *Especially for file transfers/uploads/downloads, additional aspects are required: extensions, maximum and minimum file size, headers, footers, embedded contents, checksums, and business logic related contents*
3. *Error handlings and reporting>*

**4.4 Files and Directories**

*<This section is specifically reserved if the communication between interfacing systems involves file transfers or accessing of files or directories. For example, even if it is not an SFTP process, but if a direct file or directory access is involved (for instance, online messages converted into text files), then this section is still applicable>*

**4.5 Messaging or File Transfer Mechanisms**

*<This section details out how messaging and/or file transfers are performed between interfacing systems. For example, if a messaging uses a certain standard format like ISO-8583, it should be briefly mentioned in this section. Also, if an SFTP is actually initiated using a SQL Server xp\_cmdshell it definitely must be mentioned>*

**4.6 Error Handling**

*<This section details out how errors thrown during the communication between interfacing systems are handled so as not to allow end users receiving the full details of error description (for example, the entire Java exception throw details) back in their UI screen>.*

| **#** | **Event** | **Error Code** | **Message Format** | **Error Message** | **Error Handling Logic** |
| --- | --- | --- | --- | --- | --- |
| *<1>* | *<Blank fields in Input file>* | *<R001>* |  | *<Invalid File, blank values cannot be sent for mandatory fields.>* | *<Roll Back update*  *Move the file to Error folder.* |
|  |  |  |  |  |  |

**4.7 Audit Trails**

*<Describe audit trails to detail which duties were performed or skipped, and whether they succeeded or failed. Audit trails should incorporate at least the following aspects: Who; What (Before vs. After); When; and Where>*

**4.8 Session Management**

*<Describe how the application handles or manages sessions accessing it. This section should sufficiently describe how the application recognizes an authenticated session and an authorized one – they are NOT the same. Additionally, this section should also describe how the application enforces session expiry, especially to safeguard against session replay attacks.>*

**4.9 Credential and Sensitive Information Management**

*<Describe the design approach in keeping credentials and sensitive information secure. Credentials include the following: Passwords, Passphrases, Encryption Keys, Salts, Private Keys, Smart Cards, and any other piece of information or object used for authentication purposes.*

*An information will be considered sensitive if it contains any of the following: Privacy, Financial, SFTP-related transferred files, Credentials, and any other business-related information deemed to be sensitive or confidential by the business users.*

*This section should sufficiently detail how all of the above information are guarded whether in the form of being encrypted, hashed, or restricted of their access.*

*Regarding encryption, the following details are expected:*

1. What algorithm is used
2. The length of the encryption key (or keys, if it is a multi-encryption scheme) and its complexity
3. The creation or generation process of the encryption key
4. The storage of the encryption key, including its dual custodianship nature as well as ACL (access control list to provide restricted access to it)
5. The process required to change and reset the encryption key
6. Any other additional information relating to the encryption key; for example, whether IV or padding is used and what kind

As for hashing, the following details are expected:

1. The algorithm used
2. The creation or determination of the salt used, and how it will ultimately be stored
3. How the full string is constructed from the base input before it is hashed
4. The storage of the hash values and its ACL

## ****5.**** Availability Requirement

2.8.1 Service Level Agreements (SLA)

**N/A**