

TA/UTAX Cloud Information Manager:

Security White Paper

Version 2.11

Document Version: 09/2026

September 03, 2026

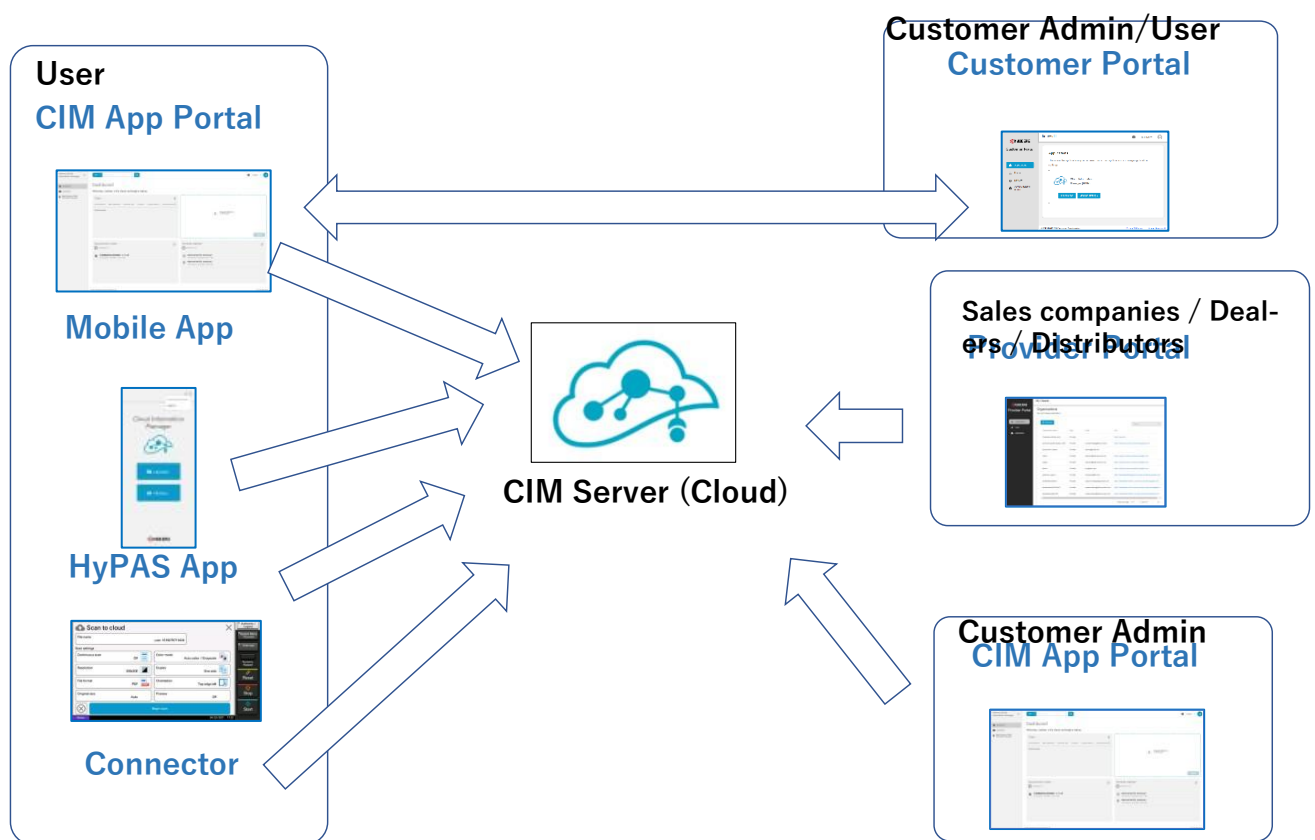
1.	OVERVIEW	2
2.	MULTITENANCY	4
3.	COMMUNICATION SECURITY BETWEEN MODULES	7
3.1.	Security Between HyPAS Applications and CIM Server.....	7
4.	USER IDENTIFICATION AND AUTHENTICATION.....	9
4.1.	Account Lockout Policy	9
4.2.	Password Policy	9
4.3.	Username Policy	9
4.4.	First name/Last name policy	10
4.5.	PIN Authentication policy	10
4.5.1.	PIN Auto-generation	10
4.6.	IC Card Authentication policy	10
4.7.	Multi Factor Authentication policy.....	10
4.8.	Microsoft Entra ID	11
5.	FIREWALL CONFIGURATION	12
6.	KEYCLOAK SECURITY FEATURES	13
6.1.	Threat model Mitigation	13
7.	DATA PROTECTION	14
7.1.	Protection of Stored Data	14
7.1.1.	Access Control.....	14
7.1.2.	Authentication	14
7.1.3.	Encryption	14
7.1.4.	Data Backup	14
7.2.	Protection of Communication Data.....	14
7.2.1.	User Access.....	14
7.2.2.	Access token and refresh token	15
7.2.3.	HTTPS protocol	15
7.3.	Secure communication between the CIM server and databases.....	15
7.4.	Security vulnerability testing.....	15
8.	DEVICE (MFP/MOBILE) AUTHENTICATION.....	16
9.	GOOGLE CLOUD PLATFORM SECURITY TECHNICAL DETAILS	17

1. Overview

TA/UTAX Cloud Information manager (CIM) is a cloud-based document management system that allows users easy to manage documents, scan, upload, index and store the documents.

This white paper informs dealers about security measures in CIM. The priority is to provide secure protection of information assets that are handled by CIM. These information assets are rigorously protected by the secure configuration and security features of CIM. Access to the production environment is restricted to authorized operational personnel only and is strictly monitored.

CIM system components are shown in the following architectural diagram:



(Fig. 1-1) CIM system overview

The key components of the CIM system is described below:

- **CIM Server (Cloud):** CIM Server is a cloud document management system that provides document management and user management features to customers.
- **Customer Portal:** The customer portal is a one-stop portal where customer can manage common settings for CIM and other available solutions, as a common platform for supporting multiple applications. The customer admin or customer user can access this portal using a web browser. They can launch a landing page or application settings page within each application portal as well.
- **Provider portal:** The provider portal is an application that supports CIM organization management, user management and document class management. The provider (RHQ, SCs, Dealers, Distributors) can

access the provider portal using a web browser. They can add, edit, or delete organizations for child providers or for their direct customers.

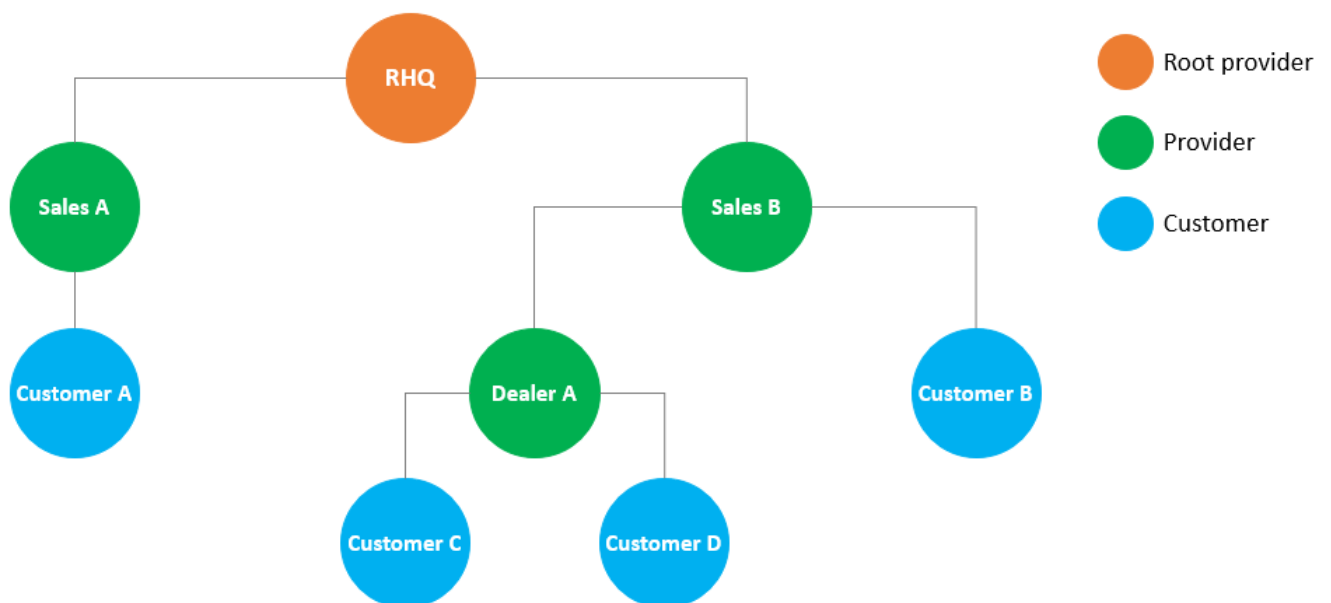
- **CIM App portal:** The customer admin or customer user can access the CIM App portal using a web browser. The customer admin can add user accounts for their own organization and configure access control of document classes. The customer user can upload, edit, delete and search documents.
- **HyPAS App (MFP client):** The HyPAS application must be installed for Multi-Function Printer (MFP) to be able to use the CIM system. The HyPAS application connects to the CIM server. Customers can scan their documents in MFP and upload to CIM server.
- **Mobile App (iOS/Android):** Mobile application connects to the CIM server. Customers can take a photo of their documents and upload them to CIM server.
- **Connector:** By developing a connector, CIM can integrate with other solutions, such as Scanner Vision.

2. Multitenancy

CIM and DCP uses multi-tenancy to accommodate multiple sales companies, dealers, and customer organizations. Each sales company, dealer, and customer are treated as one organization. Access control is enforced through a hierarchical tree structure. (Fig. 2-1)

Organizations are classified into two types: a provider organization and a customer organization. A provider organization is focused on managing one or more customer organizations. Provider organizations have managing child organizations, users, and applications features while customer organizations would provide the document management feature.

The hierarchical structure is patterned after the common sales hierarchical structure used in TA/UTAX. An RHQ (regional headquarters) is the parent organization (root provider organization) with sales companies under the RHQ as children provider organizations. Customers of sales companies would be the customer organizations and leaf nodes in the hierarchical tree structure.



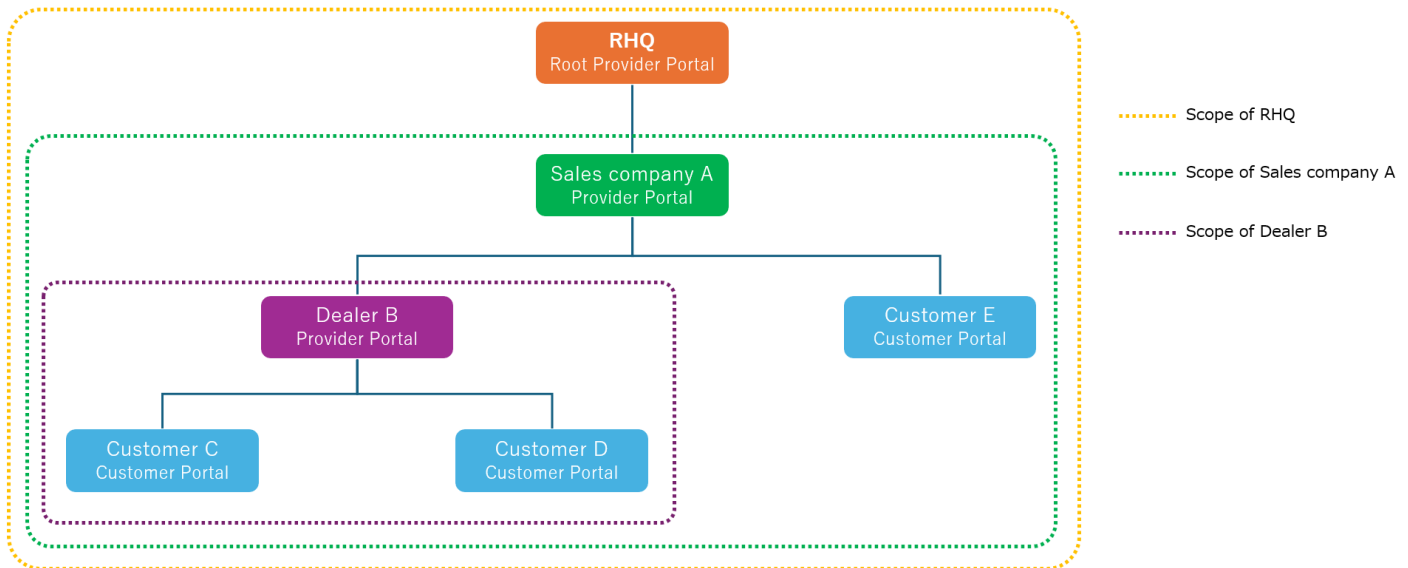
(Fig. 2-1) Hierarchical structure of DCP Organizations

Any organization cannot view the data of another organization except for the parent organization. The parent provider only can get usage counter information and the contact information of the organization representative from the customer. For the license model, the usage count is the data related to the license information such as OCR page, document count, document size usage and the contract information. For subscription model, the usage count is the storage size. Data is scoped and access to data is limited. (Table 2-1)

User type	Users of customer organization	Documents of customer organization	Document class information	Subscription information (Storage size)
Provider Admin/Support	Inaccessible	Inaccessible	Accessible	Accessible
Customer Admin	Accessible	Accessible	Accessible Access right management	Accessible
Customer user	Inaccessible	Accessible	Inaccessible	Accessible

(Table 2-2) Access to organization and user data by user type (Subscription model)

Scopes are formed between parent and child organizations, and are used for data inheritance and access management. At the organization level, when a child organization is created, its parent organization's document class definition data (document classes and attributes of the document classes) are inherited. Also, the parent organization can manage the license-related information or the subscription information of the customer child organization (e.g. how many OCR pages, document size allowed) to help with billing. (Fig 2-2)



(Fig. 2-2) Access to license-related information for each organization

3. Communication security between modules

Transport Layer Security (TLS) is a standard security technology for establishing an encrypted link between a server and a client. In CIM, TLS is used to secure and protect sensitive information that is shared between CIM and a browser, device, mobile or database. This information includes:

- CIM user and DCP credentials and passwords
- User data
- Document information (document, OCR data, index data, metadata, comments, etc)
- Document count metrics (OCR page counts, document size, document count, etc.)

This ensures that third parties on the network cannot decrypt or tamper with the payload during transmission.

3.1. Security Between HyPAS Applications and CIM Server

The table below lists the TLS versions available when a HyPAS application is installed on a model supported by CIM. Models that list multiple versions in the Supported TLS Version column use different TLS versions depending on the device's firmware version. When the latest firmware is installed, TLS 1.3 is used.

	Project name	TA/UTAX brand	Support TLS version
A3 MFP	Athena	9515ci 8515ci 7515ci 10565i 9565i 8565i 7565i	1.3
	Matsuri 3	P-3241i MFP	1.3
	Iris 2024	7009ci 6009ci 5009ci 4009ci 3509ci 2509ci	1.3
	Iris 2024 mono	7059i 6059i 5059i	1.3
	Tomcat 4	4063i 3263i	1.3
	Iris 2	6007 ci 5007 ci 4007 ci 3207 ci 2507 ci	1.3/1.2
	Iris 2020	7008 ci 6008 ci 5008 ci 4008 ci 3508 ci 2508 ci	1.3
	Iris 2020 mono	7058 i 6058 i 5058 i	1.3

A4 MFP	Iris 2 mono	6057 i 5057 i	1.3/1.2
	Zeus 4	9057 i 8057 i 7057 i	1.2
	Mercury 4	8307ci 7307ci	1.2
	Polaris E Plus	P-6038if MFP P-6038i MFP	1.2
	Virgo	P-C3563i MFP P-C3567i MFP P-C4063i MFP P-C4067i MFP 358ci 458ci	1.3
	Polaris Next	P-4532i MFP P-6039i MFP P-5539i MFP P-4539i MFP	1.3
	Perseus2 High	352ci 402ci 502ci	1.3/1.2

4. User Identification and Authentication

When accessing CIM, the user must log in with an activated account. An unauthorized user cannot access CIM. The following features are supported as security features for login.

CIM uses OAuth 2.0 authentication method by Keycloak. Keycloak is a user authentication management software sponsored by RedHat.

4.1. Account Lockout Policy

The Account Lockout Policy protects CIM from password cracking attacks. When a user fails to login a pre-determined number of times, the user account will be locked for a certain period.

As shown in the table below, when reaching the account lockout threshold for failed login attempts of three times, the account will be locked. The setting will unlock the account after 30 minutes. The locked account also can be unlock by the admin manually. Password reset will unlock the account if the login attempt is coming from same browser(same tab_id) that requested password reset.

Number of continuous failed login attempts	3 attempts in 15 minutes
Auto Unlock Time	30 minutes

4.2. Password Policy

A user needs to employ a strong password that is difficult to be analyzed and must be applicable to the CIM Password Policy.

A password that does not meet the password policy is prohibited. This policy prevents users from setting simple passwords and guards against unauthorized access by a third party.

All authentication is securely processed based on OAuth 2.0 using keycloak.

The password length and complexity of password are defined in the table below.

Password Length	Between 8 to 64 characters
Password Complexity	Include at least one character from each category: Upper case (A ~ Z) Lower case (a ~ z) Numbers (0 ~ 9) Symbols (!"#\$%&'()*+,-./:;<=>?@[^_`{ }~)

4.3. Username Policy

Username policy is put in place to verify if the value is a valid username. This prevents special characters which may be used in SQL injection¹ vulnerabilities.

Username Length	Between 4 to 64 characters
Prohibited characters	Symbols \ / : , ; * ? " < > [] { } \$ % ` & () + = ! # ' ~ ^ spaces

Note: Users who have created a username including spaces or ! # ' ~ ^ prior to v2.5.2 may still login and

¹ Refer to [SQL injection - Glossary | CSRC \(nist.gov\)](#) for more detail information.

continue CIM usage, however, it is recommended to update your login username. When updating your username, the new policy must be followed to save.

4.4. First name/Last name policy

A policy for first name/last name fields is in place to prevent certain special characters which may be used in SQL injection vulnerabilities. The validator checks if the value is a valid person name as an additional barrier for attacks such as script injection.

Allowed symbols	-@.~+;,
-----------------	---------

Note: Users who have created a first name/last name prior to v2.5.2 which included any symbols other than the above mentioned, may continue CIM usage, however, it is recommended to update your first name/last name fields to follow the new policies. When updating your first name/last name fields, the new policy must be followed to save.

4.5. PIN Authentication policy

PIN authentication is an authentication method available only when logging in through the HyPAS application. Users can log in using a 6-digit or 8-digit numeric code that they set themselves. Administrators can configure the code length policy to balance ease of use and security.

Initial setting	Off
PIN code length	6-or 8-digit codes (Initial value:6 digit)

4.5.1. PIN Auto-generation

The Customer Portal supports a PIN auto-generation feature. When this feature is used, the system automatically generates and assigns a random PIN that is not currently in use within the organization. This helps reduce the use of easily guessable PINs and enhances the security of PIN-based authentication. Administrators can configure, through the Customer Portal, whether users are permitted to set their own custom PINs.

When custom PIN is allowed:

- Users may create and use a PIN of their own choosing.
- Alternatively, users may use a randomly generated PIN provided by the system.

When custom PIN is not allowed:

- Users can only use a PIN generated by the system.
- User-defined PIN creation or modification is not permitted.

*To prevent abuse of the PIN generation function and reduce unnecessary system load, a cooldown period is enforced after a PIN is automatically generated. During this period, users cannot request another PIN generation.

4.6. IC Card Authentication policy

IC card authentication is an authentication method available only when logging in through the HyPAS application. It's simple and fast authentication process enhances overall user convenience.

4.7. Multi Factor Authentication policy

Multi-Factor Authentication (MFA) enhances account security by requiring users to enter a one-time access code after providing their username and password. The code can be delivered through a registered email

address or generated by a supported authentication application. This additional verification step helps protect accounts from unauthorized access, even if user credentials are compromised.

One-time access code expiration (E-mail)	5 minutes
One-time access code expiration (Authentication application)	*It depends on the authentication application being used by the user.

4.8. Microsoft Entra ID

CIM give administrators to configure their organization to link their Entra ID tenant, sync users from the Entra ID tenant to DCP and give users the option of logging in using their Entra ID credentials.

Following the OAuth 2.0 authentication flow, a pop-up window for entering Entra ID credentials will be managed by Entra ID, including MFA if enabled from the Entra ID-side. Note that the Entra ID MFA is separate from and not managed by the MFA setting on the customer portal.

In v2.11, Microsoft Entra ID authentication is available for the customer portal.

5. Firewall Configuration

To allow applications operated by customer administrators and customer users to access the cloud servers on the Digital Cloud Platform, the firewall settings in the customer environment must be modified to permit communication through specific ports.

The ports that require modification are as follows:

Case	Source	Destination	Protocol	Port	Service
1	HyPAS App (MFP Client)	Cloud Server (CIM)	HTTPS/TCP	443	Scan image upload
2	HyPAS App (MFP Client)	Cloud Server (Customer Portal)	HTTPS/TCP	443	Login, Logout
3	Server App (Web browser)	Cloud Server (CIM)	HTTPS/TCP	443	Document Checking, Indexing, Permission, Task Workflow, etc.
4	Customer Portal (Web browser)	Cloud Server (Customer Portal)	HTTPS/TCP	443	Login, Logout, Manage user/role
5	Mobile App (iOS/Android)	Cloud Server (CIM)	HTTPS/TCP	443	Image upload
6	Mobile App (iOS/Android)	Cloud Server (Customer Portal)	HTTPS/TCP	443	Login, Logout
7	CIM Connector	Cloud Server (CIM)	HTTPS/TCP	443	Document upload
8	CIM Connector	Cloud Server (Customer Portal)	HTTPS/TCP	443	Login, Logout

The cloud servers are published to the Internet through a load balancer, which has a fixed IP address assigned. This configuration ensures that the destination IP address for the service remains constant, enabling stable and secure access control.

Permitted IP Addresses

Register the fixed IP address of the load balancer provided by the service.

Registering by IP address instead of a domain name or URL avoids potential issues caused by DNS resolution or caching.

How to Obtain the IP Address

To identify the IP address from the cloud server's URL, use one of the following methods:

- Using the ping command
Example: Run ping [hostname] in Command Prompt or Terminal. The IP address of the responding host will be displayed.
- Using the nslookup command
Example: Run nslookup [hostname] to obtain the IP address from the DNS forward lookup results.

There are three types of IP addresses depending on the case. Obtain each IP address from the following hostnames:

- Cases 1, 2, 5, 6, 7, 8: Hostname device.dpio.kyocera.biz
- Case 3: Hostname from the URL of screens other than the login screen
- Case 4: Hostname from the URL of the login screen

Register all three IP addresses obtained using these methods in the firewall.

To open these ports for communication, please consult with your IT department.

6. Keycloak security features

CIM/DCP uses Keycloak as its identity and authentication management service that supports OAuth 2.0. Keycloak is an open-source authentication management system that provides a wide range of security features.

6.1. Threat model Mitigation

Keycloak mitigates the below possible security vulnerabilities as an authentication server.

- Password guess: brute force attacks
- Clickjacking
- Cross-site request forgery (CSRF) Attacks
- Unspecific Redirect URIs

7. Data Protection

7.1. Protection of Stored Data

CIM's information assets must be protected and not leaked or lost. TA/UTAX implements security protection measures for stored information assets and a data recovery support through the features described below.

7.1.1. Access Control

CIM allows administrators to configure detailed access permissions for each document class and each root folder on a per-user basis. Users can access CIM's document information (documents and metadata) according to the permissions assigned to them.

Access permissions for documents can be assigned by document class and/or by root folder. With these two types of access control, organizations can restrict access not only by document type but also by storage location, providing greater flexibility and security in managing sensitive information.

7.1.2. Authentication

CIM database requires user authentication to gain access to database data. Authentication credentials are configured during initial release of the instance.

7.1.3. Encryption

CIM database uses AES256 algorithm for encryption.

7.1.4. Data Backup

CIM database backups are performed automatically every day. The backups are encrypted with AES256 and stored in Google Cloud Storage. The retention period for backup data is seven days.

The backup data is stored in secure locations that are separated from the primary hosting environment and is replicated across multiple locations to meet geographic redundancy and disaster recovery requirements. In addition, the data is distributed and stored redundantly across multiple regions within the applicable area, ensuring that it can be restored even in the event of a hosting environment failure or a regional disaster.

7.2. Protection of Communication Data

CIM protects communication data regarding user access to use CIM, and data communication to transfer data between CIM and devices, respectively.

In order to protect CIM communication data from masquerading, tapping or modifying the data, the communication data is encrypted, and CIM components are mutually authenticated.

7.2.1. User Access

When a user accesses CIM from a web application using a browser, an authenticated communication channel is established. CIM user can access CIM web portal from the Web browser's client UI regardless of the user role. When a user accesses CIM web portal, the user is always identified and authenticated. If this identification and authentication are successful, access token will be issued and the user can access CIM web portal based on user's role. CIM web portal protects the communication data through HTTPS.

7.2.2. Access token and refresh token

Once the authentication is successful, an access token and refresh token will be issued and user session will be maintained. User session will be used to access for all document operations. Access token will be used to access user management and contract management operations. The access token's life span is 15 minutes and can be refreshed using refresh token whenever any access of BE API after access token expired. UI will be logged out in case of 15 minutes inactivity.

7.2.3. HTTPS protocol

HTTPS works over underlying secure protocols (TLS 1.3/1.2) that encrypt all traffic between browsers and servers. TLS require a certificate with a private key, a public key, domain information, and a chain of signatures by certificate authorities.

7.3. Secure communication between the CIM server and databases

CIM will establish network connection to database using TLS and AES 128 encrypted network traffic.

7.4. Security vulnerability testing

In order to keep the CIM application up-to-date with the latest security measures the following schedule will be followed for security vulnerability assessment:

- Perform internal security vulnerability assessment for each software release build release.
- Periodic vulnerability assessment in accordance with server management regulation.
- If the configuration of the public server has changed significantly, such as an upgrade, perform vulnerability assessment as necessary.

8. Device (MFP/Mobile) Authentication

To protect sensitive information transmitted between CIM and devices, security is enforced through HTTP over TLS. The supported TLS versions are 1.3 and 1.2.

User must authenticate through CIM authentication from the device application to establish the network connection between CIM and the device.

The client authentication will be authenticate using user id, password, client-id and client-secret. Mobile and MFP have different client-id and client-secret.

9. Google Cloud Platform Security Technical Details

CIM is hosted on the Google Cloud Platform. GCP meets the broad set of internationally recognized information security controls and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1/2/3, GDPR, CCPA (see the detailed list of compliant standards in GCP Cloud Compliance, <https://cloud.google.com/security/compliance>).

The hosting environment is designed to utilize the GCP provided services and security features to help secure and monitor our application. The various features that are utilized include:

- Various GCP credential for login/access
- Security logs
- Instance isolation
- Firewalls/API access
- Secure HTTPS access points
- Network security (VPC isolation, Network Security groups, Network Access Control List, Internet Gateway, etc.),
- Storage
- Simple Notification Service monitoring CloudWatch application logs

CIM is deployed to the following GCP datacenter:

- Belgium/St.Ghislain (europe-west1)

CIM uses managed storage and PostgreSQL Database hosted on GCP.

Compliance status of the hosting infrastructure is not automatically applied to hosted applications (in this case, the CIM application).

This white paper explicitly states the following facts:

- Regarding the CIM application itself, no independent third-party compliance testing has been conducted separately from GCP's compliance status.
- Technical vulnerability tests, such as vulnerability assessments and security scans, have been performed; however, their purpose and scope differ from third-party evaluations of compliance status.
- Compliance assessment for hosted applications is, at present, based on self-assessment.