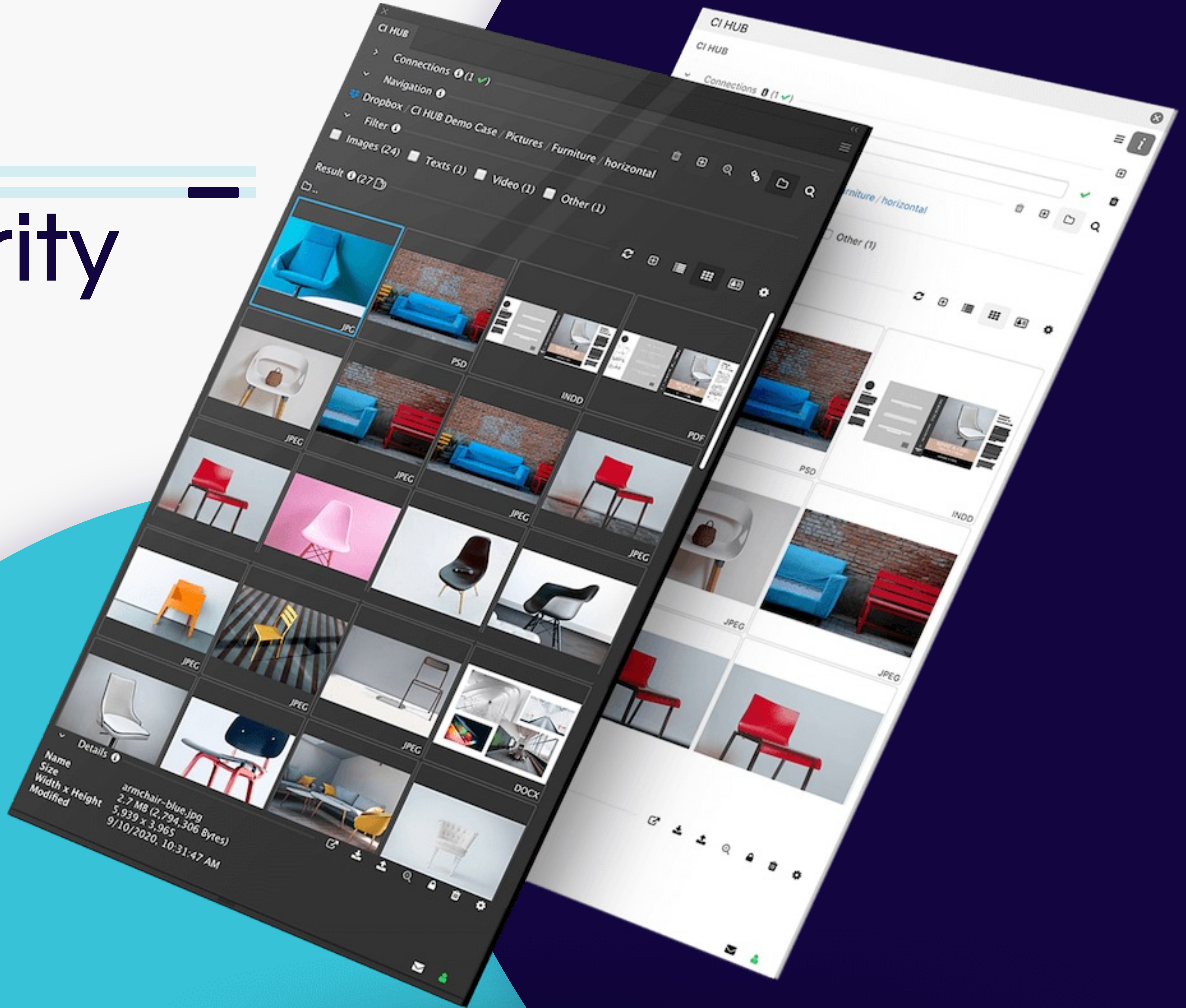
# Advanced Setup & Security Information's (General Technical Information)

Creativity | Teamwork | Standardization



Name armchair-blue.jpg
Size 2.7 MB (2,794,306 Bytes)
Width x Height 5,939 x 3,965
Modified 9/10/2020, 10:31:47 AM

www.ci-hub.com

## Document Version and History

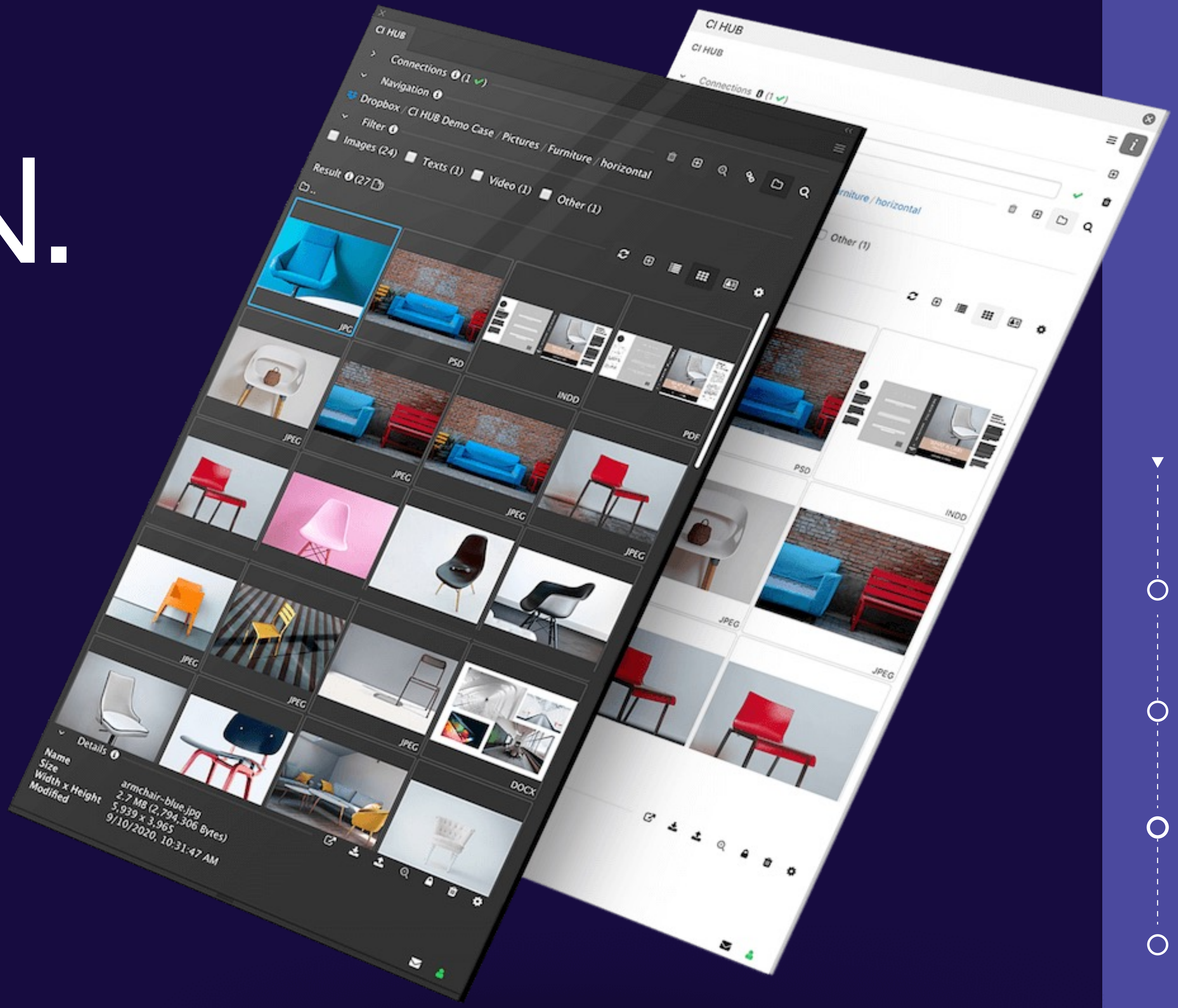
| Change/Info | Editor | Date | Version | info |
|---|---|---|---|---|
| Updated the info for OnPremise and Multi-SaaS Setups | Andreas Michalski | 20. Sep. 2023 | 1.2 | |
| Updated the server URLs and IP addresses on the Firewall page & formatting | Salim Melliti | 21. Sep. 2023 | 1.3 | |
| Updated the Hubspot Server Location to GERMANY<br>Added the new domains, subdomains, the new server IP addresses, and the Transactional E-Mails server to the Firewall page<br>Updated the OAuth Redirect URLs<br>Updated data stored by Keylight | Salim Melliti | 03. Mai 2024 | 1.4 | |

# INTRODUCTION.

All data transfer takes place via HTTPS with TLS 1.2. There are two variants how data is transferred between CI HUB Client and Integration API:

1. Directly from CI HUB Client to Partner API. This is the case when large amounts of data need to be transferred, for example when an asset is downloaded or uploaded.

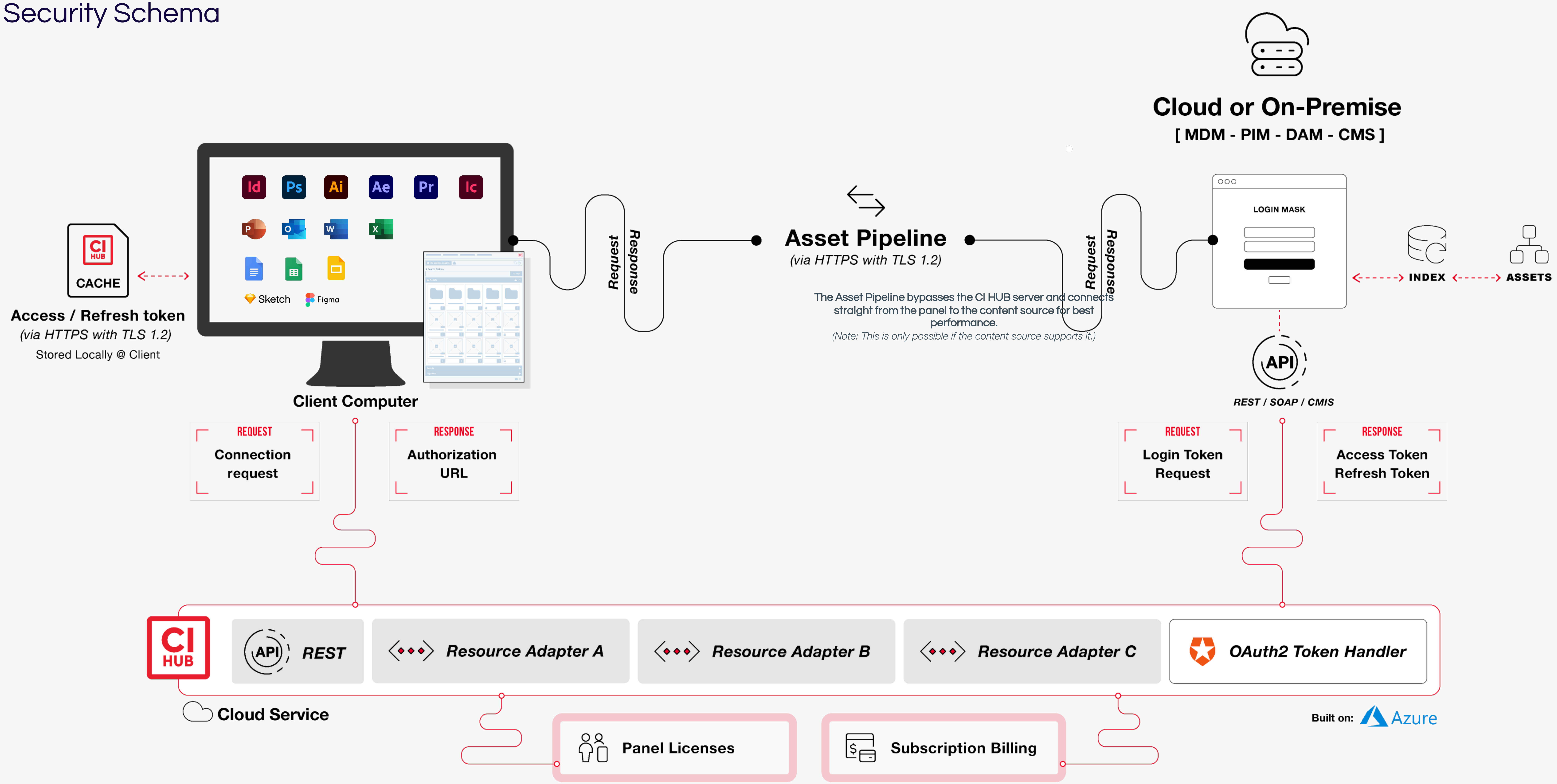
2. From the CI HUB Client via the CI HUB Server to the Partner API. This path is used to perform certain environment-dependent actions or to access secret keys stored in the server. To ensure that these keys & secrets are stored securely, they are stored in an area of our Azure server where no one except CI HUB admins have access. There is no route or similar access mechanism to get this information.



Name armchair-blue.jpg
Size 2.7 MB (2,794,306 Bytes)
Width x Height 5,939 x 3,965
Modified 9/10/2020, 10:31:47 AM

# DATA POINTER

## Security Schema



The Asset Pipeline bypasses the CI HUB server and connects straight from the panel to the content source for best performance.

*(Note: This is only possible if the content source supports it.)*

# DATA POINTER

## Security Schema

**An example of this is our generic login mechanism: As soon as a user wants to login to an integrated system via CI HUB to create a connection in the CI HUB Connector, the following steps are performed:**

1. The CI HUB client requests a connection for a third-party system from the CI HUB server.
2. The server creates an authorization URL for the Integration system.
3. This authorization URL is passed on to the client so that it can log in to the Integration system within a browser window.
4. Upon successful login in the integration login mask, the Integration system sends a code to the CI HUB server, which exchanges the code for an Access Token and a Refresh Token.

CACHE

FOR ADOBE PRODUCTS, WE STORE THE ACCESS / REFRESH TOKEN IN A SETTINGS FILE IN A LOCAL USER DIRECTORY, ONLY THE USER HAS ACCESS TO THIS.

**Windows:** C:\Users\<User>\AppData\Roaming\CI-Hub
**Mac:** Mac HD/User/<username>/Library/ApplicationSupport/CI-Hub/

# DATA POINTER

Security Schema

## In all other products:

Here we store access/refresh token in the **“localStorage”** of the browser in which CI HUB is running. This storage is linked to the origin of the azure system of CI HUB. Other web applications have no access to this information because it can only be used by the CI HUB application via the current user. Since no information is stored on our server that can be queried, we consider both options to be secure.

With both options above there is the possibility to delete a connection. This will delete the local entries again. A security conscious user can delete the connection after use.

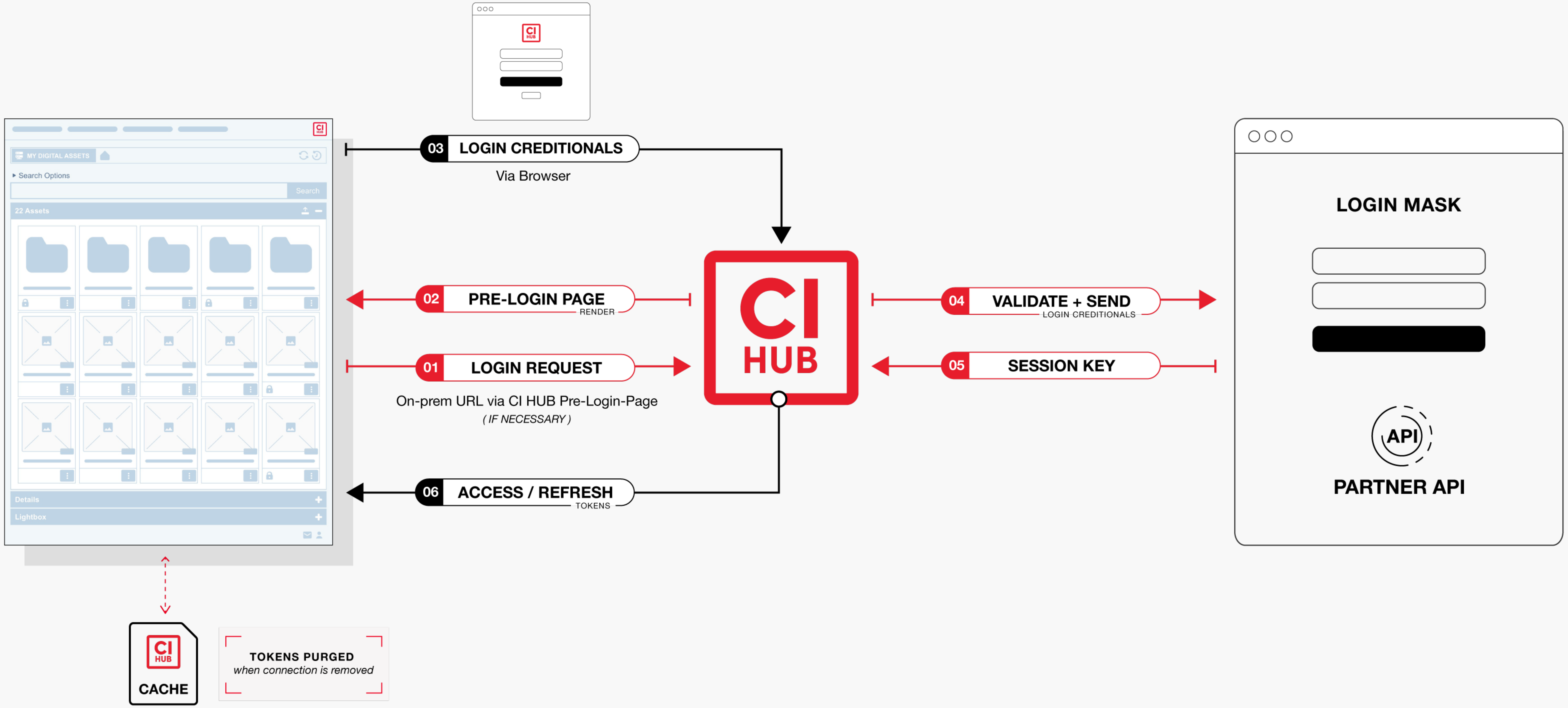
With the Load / Save Connections feature, we store connection data with a password and a symmetric AES-256 crypto algorithm encrypted in Okta. This can be loaded and decrypted with the password. The data leaves the panel only encrypted. There is only one encrypted string in Okta. This mechanism is used only if the user uses the Load / Save Connections feature.

**For more Information about oAuth2,** see https://datatracker.ietf.org/doc/html/rfc6749.

**For more information about AES256 encryption,** see https://www.atpinc.com/blog/what-is-aes-256-encryption

# DATA POINTER

## Security Schema | **Basic**



**03** LOGIN CREDITIONALS
Via Browser

**02** PRE-LOGIN PAGE RENDER

**01** LOGIN REQUEST
On-prem URL via CI HUB Pre-Login-Page
*( IF NECESSARY )*

**06** ACCESS / REFRESH TOKENS

**04** VALIDATE + SEND LOGIN CREDITIONALS

**05** SESSION KEY

LOGIN MASK

PARTNER API

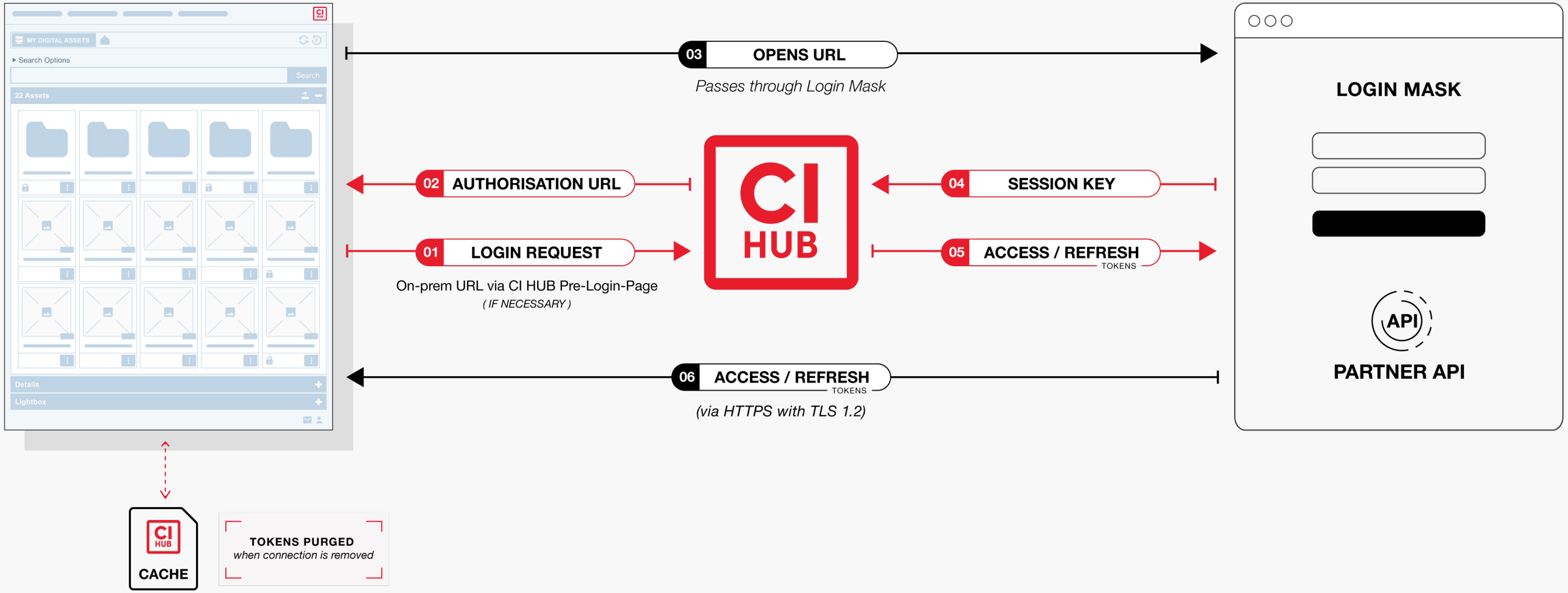
CACHE

TOKENS PURGED
*when connection is removed*

**Access / Refresh Tokens**
Stored Locally @ Client

# DATA POINTER

## Security Schema | **0Auth2**

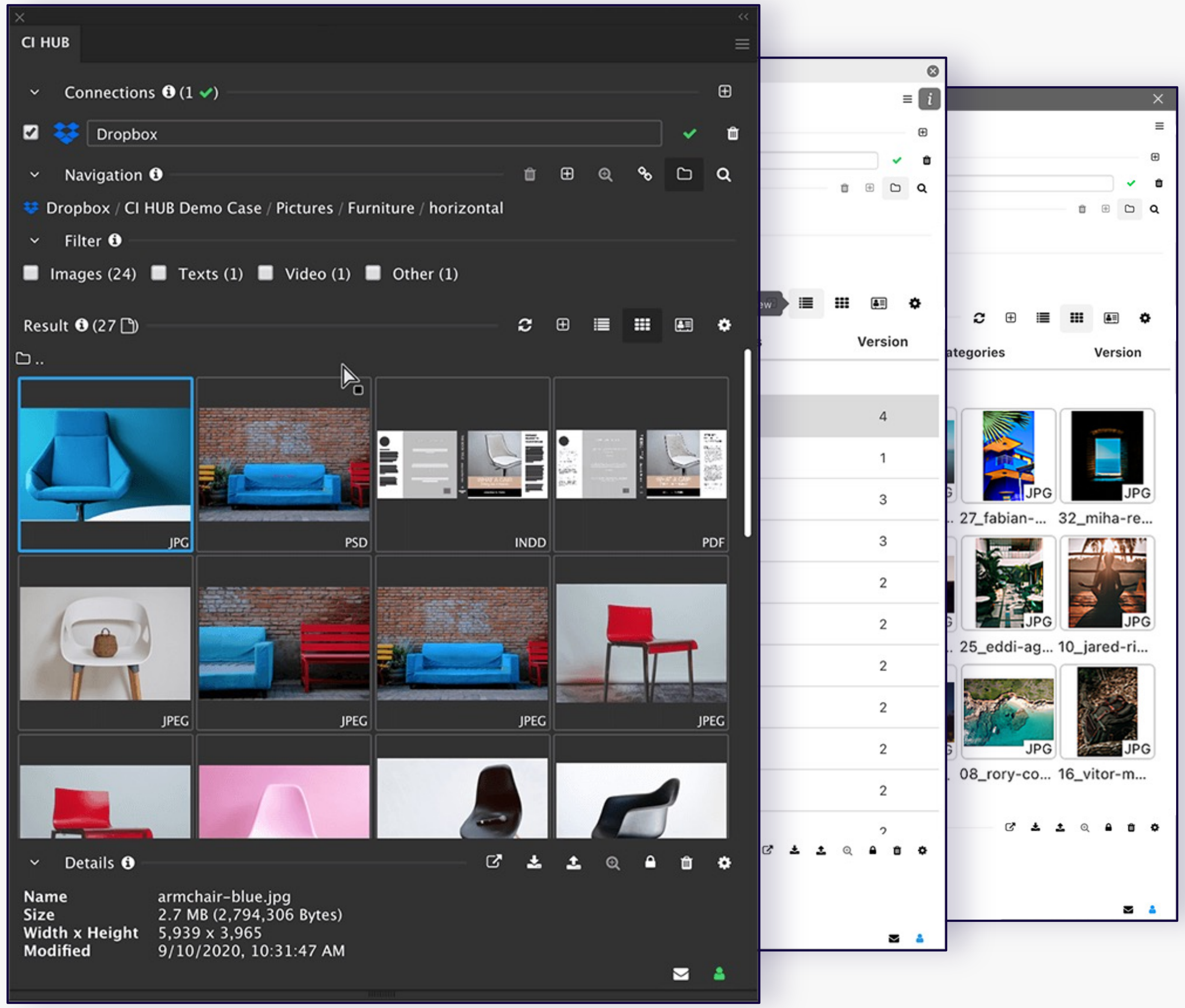


**Access / Refresh Tokens**
Stored Locally @ Client

# DATA POINTER

## Security Schema

1. Neither CI HUB panel nor CI HUB server save any assets at any given time
2. Data access happens purely via content source API
3. Data access permissions apply for connected users as configured in content source system and made available via the API
4. Data transfer (uploads and downloads) takes place between client computer and content source data repository*
5. CI HUB server provides a stateless service to the CI HUB panel and acts only on requests triggered by a user on the client side
6. CI HUB server only maps client requests, as submitted from the CI HUB panel to the content source's specific API resources and vice versa
7. Any communication between CI HUB panel and CI HUB server as well as between CI HUB server and content source takes place on secured network connections (https)*



Dropbox / CI HUB Demo Case / Pictures / Furniture / horizontal

Name armchair-blue.jpg
Size 2.7 MB (2,794,306 Bytes)
Width x Height 5,939 x 3,965
Modified 9/10/2020, 10:31:47 AM

# FIREWALL

Requirements for Firewalls and Ports

COMMUNICATION: HTTP and HTTPS “standard” Ports

DOMAIN & SUBDOMAINS TO INCLUDE:

ci-hub.com
ci-hub.net
ci-hub.io
ci-hub.azurewebsites.net
ci-hub-test.azurewebsites.net
ci-hub-beta.azurewebsites.net
live.ci-hub.com
stage.ci-hub.com
dev.ci-hub.com
api.ci-hub.com
app.ci-hub.com
admin.ci-hub.com

**If wildcard whitelisting is possible, add:**

*.ci-hub.com

*.ci-hub.net

CI HUB SERVER USES FOLLOWING OUTBOUND IP ADDRESSES: (Your Inbound)

104.40.158.55
104.46.42.104
23.101.67.154
23.97.174.44
23.97.177.139
104.40.213.244
104.40.211.253
137.117.175.38
20.73.114.74
20.101.152.141
20.76.7.76
20.109.202.102
20.212.132.38

TRANSACTIONAL E-MAIL SERVER IP:

**Please whitelist this IP on your E-Mail Server to ensure the delivery of critical E-Mails (Invoices & Account Management)**

143.244.87.193

# GENERAL OnPremise

Information

For Systems that are not supporting a „true“ SaaS Solution or that are run in an OnPremise Environment there are some configurations needed.

## HERE WE PROVIDE THE GENERAL OVERVIEW:

To setup these Systems you need to talk to your System Vendor or your System Partner. They can Provide all necessary information.

To setup these Systems you need to order the CI HUB OnPrem/MultiSaas Installation.

**Please email:** sales@ci-hub.com.

## PLEASE PROVIDE US WITH:

The URL to the System: in the form „subdomain.domain.tld“ (e.g. https://fotoweb.company.com or https://myCompany.com)

**Your Client Key:** „string“

**You client Secret:** „string“

**Note:** *Please send these details to support@ci-hub.com and include the Order + Payment information that you have received from our CI HUB Sales Team.*

# GENERAL OnPremise & OAuth

Information

In addition, we will provide a set of redirect URLs that need to be configured in your oAuth settings.

These are maybe System specific.

A. How and where to setup these, please refer to your System Provider or Partner.

B. The URLs will be as follows. The URLs are System Specific.

## GENERAL SCHEME:

https://ci-hub.azurewebsites.net/api/v1/auth/login/"SYSTEM"

https://ci-hub-beta.azurewebsites.net/api/v1/auth/login/"SYSTEM"

https://ci-hub-test.azurewebsites.net/api/v1/auth/login/"SYSTEM"

http://localhost:8080/api/v1/auth/login/"SYSTEM"

https://live.ci-hub.com/api/v1/auth/login/"SYSTEM"

https://stage.ci-hub.com/api/v1/auth/login/"SYSTEM"

https://dev.ci-hub.com/api/v1/auth/login/"SYSTEM"

https://ci-hub.net/api/v1/auth/login/"SYSTEM"

https://api.ci-hub.com/auth/login/"SYSTEM"

# SPECIFIC OnPremise & OAuth

Information for FOTOWARE

## Example OAuth Redirect Settings for Fotoware:

https://ci-hub.azurewebsites.net/api/v1/auth/login/fotoware

https://ci-hub-beta.azurewebsites.net/api/v1/auth/login/fotoware

https://ci-hub-test.azurewebsites.net/api/v1/auth/login/fotoware

**http://**localhost:8080/api/v1/auth/login/fotoware

https://live.ci-hub.com/api/v1/auth/login/fotoware

https://stage.ci-hub.com/api/v1/auth/login/fotoware

https://dev.ci-hub.com/api/v1/auth/login/fotoware

https://ci-hub.net/api/v1/auth/login/fotoware

https://api.ci-hub.com/auth/login/fotoware

# FAQ

Frequently Asked Questions

Q: Which cloud platform or hosting provider is the application operated?

A: Currently we use Microsoft Azure Services. CI HUB is built in a way to support multiple Providers. User can choose between Azure, Amazon AWS or Custom Providers.

Q: Which certificates does the SaaS provider or platform providers have? For example: ISO Certificate 27001

A: Information about the Compliance provided by Microsoft can be found at: [https://learn.microsoft.com/en-us/compliance/regulatory/offering-home](https://learn.microsoft.com/en-us/compliance/regulatory/offering-home)

Q: Are all data transmitted between end users and providers encrypted?

A: CI HUB uses an HTTPS protocol for transferring data. If the Integration used by the User is supporting these options depends on the possibilities offered by the Integration. *Please contact the respective integration software provider.*

# FAQ

Frequently Asked Questions

Q: In which countries / regions are data held?
A: No data is kept

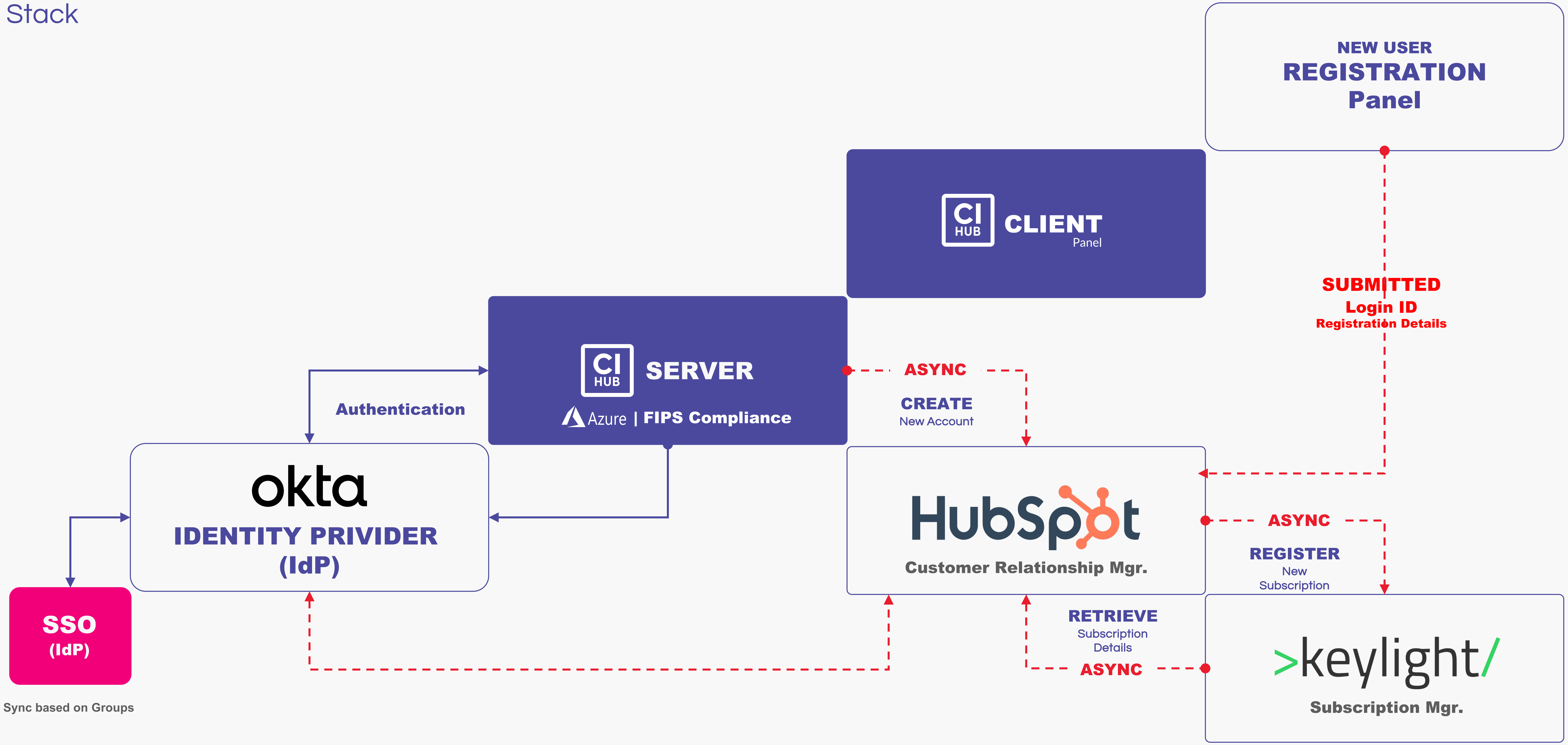
Q: Which authentication options does the provider support? Which of the following possibilities for data interfaces to other systems are offered if needed?
Basic, Client Certificate, MFA, SAML 2.0, OAuth, None

A: We use a full OKTA system for all AIM tasks. All available options of the OKTA offering can be found on the integration software provider website. www.okta.com

Some of the additional options come with additional cost and services. Please refer to our Sales Department.

# REGISTRATION

Stack



NEW USER
REGISTRATION
Panel

CI HUB CLIENT
Panel

SUBMITTED
Login ID
Registration Details

CI HUB SERVER
Azure | FIPS Compliance

Authentication

ASYNC
CREATE
New Account

okta
IDENTITY PRIVIDER
(IdP)

SSO
(IdP)

Sync based on Groups

HubSpot
Customer Relationship Mgr.

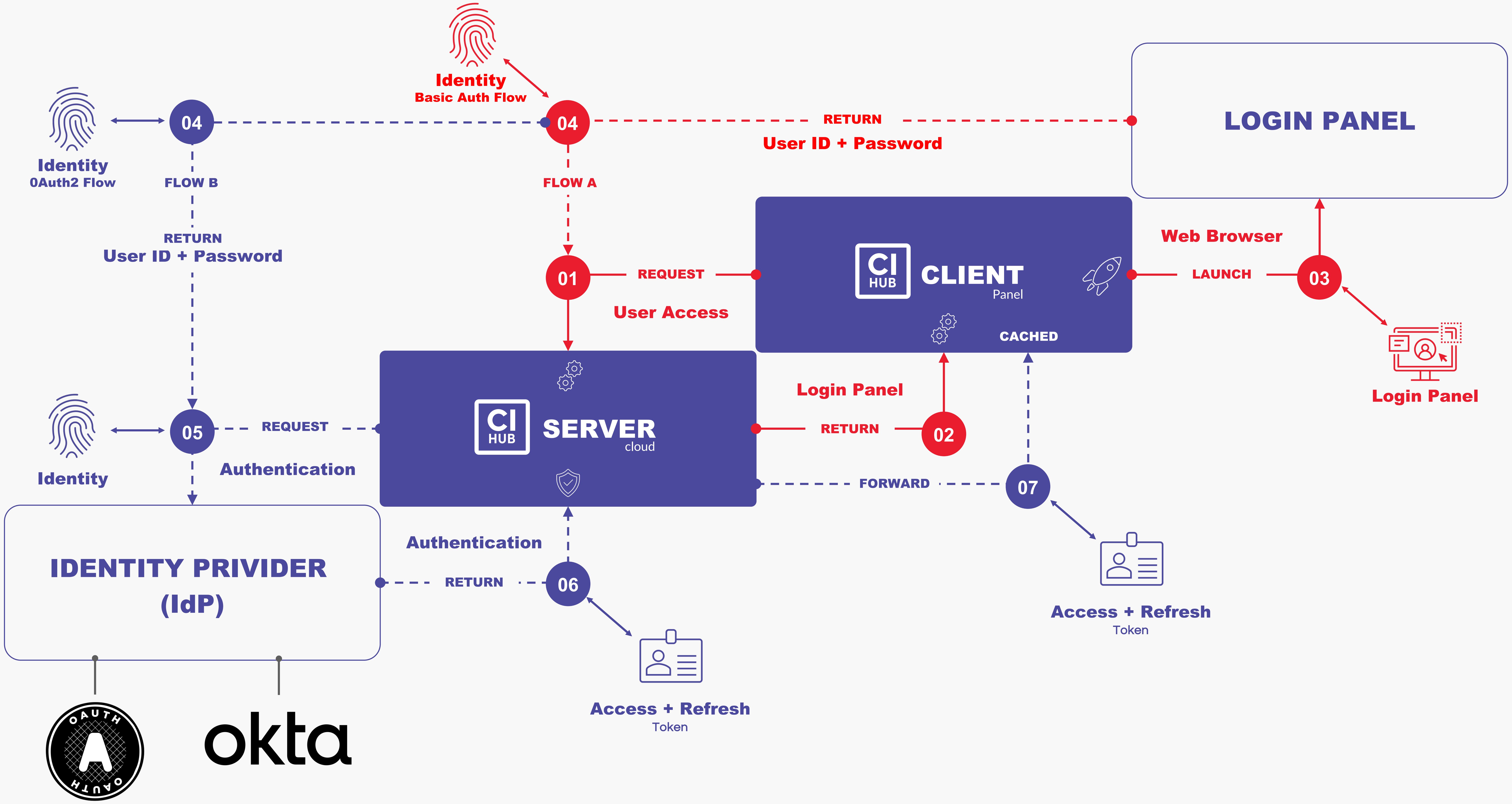
ASYNC
REGISTER
New
Subscription

RETRIEVE
Subscription
Details
ASYNC

>keylight/
Subscription Mgr.

# LOGIN

Flows



Identity
Basic Auth Flow

04
RETURN
User ID + Password

LOGIN PANEL

FLOW A

01
REQUEST
User Access

CI HUB CLIENT Panel
CACHED

Web Browser
LAUNCH
03

Login Panel

Identity
0Auth2 Flow

04
FLOW B
RETURN
User ID + Password

Identity
05
REQUEST
Authentication

CI HUB SERVER cloud

Login Panel
RETURN
02

FORWARD
07

Access + Refresh
Token

IDENTITY PRIVIDER
(IdP)

Authentication
RETURN
06

Access + Refresh
Token

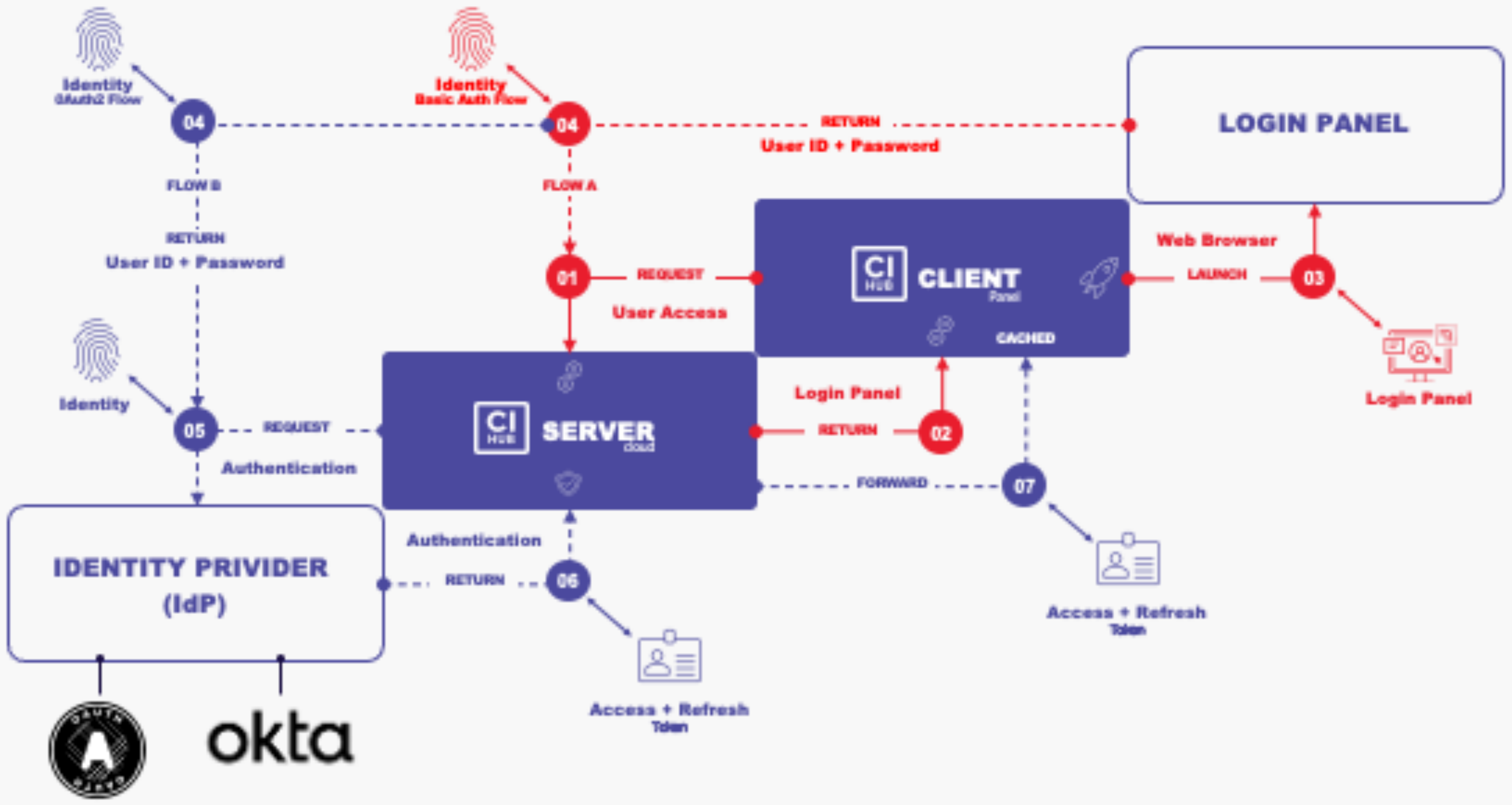
OAUTH
okta

# LOGIN

## Flows

1. The client requests either login to the CI HUB Panel or integration to the CI HUB Server.
2. The server responds by providing the correct login panel information, including the authentication URL.
3. The user opens the login panel, which can be either the CI HUB Okta Login Panel or the Integration Login Panel.
4. FLOW A: In the case of basic authentication integrations, after the user enters their credentials in the panel, the username and password are passed to the CI HUB Server.

   FLOW B: Alternatively, if the integration supports OAuth2, the user enter their credentials in the OAuth2 login page provided by the partner, customer IDP, or integration partner OAuth2. Our Okta then validates the request.
5. Security information is exchanged between our server and the IDP/partner using the OAuth2 protocol.
6. Upon successful security check, the partner IDP/OAuth2/Okta login returns the access and refresh tokens to our server.
7. The access and refresh tokens are then forwarded directly to the client, where they are cached for future use.



CI HUB

| Auth Flow<br>Availability | IdP<br>Identity Provider | Credentials<br>Source | Login Panel<br>Provider | SSO<br>Support |
|---|---|---|---|---|
| 01 | okta | CI HUB | okta | - |
| 02 | okta | PARTNER<br>Platform | okta | ✓ |
| 03 | OAUTH | PARTNER<br>Platform | OAUTH | ✓ |
| 04* | **Basic Auth**<br>**Legacy** | CI HUB | CI HUB | - |

DSP DATA SUB-PROCESSOR

# Azure

**Type:** Hosting & Infrastructure | **LOCATION:** ECC Netherlands

| DATA TYPE | PROFILE: | USAGE | CLIENT CONFIGURATION | LICENSE INFORMATION: |
|---|---|---|---|---|
| Stored Operational | none | none | none | none |
| Passed-through Operational | • User Identifier for the Integration (e.g., e-mail)<br>• CI HUB ID | All data is secured by TLS 2.x | none | none |
| Bypassed Operational (Client/Integration) | none | Based on Integration capabilities. Min. Standard Requirement is TLS 2.x | none | none |

DSP DATA SUB-PROCESSOR

# HubSpot

**Type:** CRM | **LOCATION:** Germany

| DATA TYPE | PROFILE: | USAGE | CLIENT CONFIGURATION | LICENSE INFORMATION: |
|---|---|---|---|---|
| Stored Operational | • Names (SSO: Provided by IDP)<br>• E-Mail Addresses (SSO: Provided by IDP)<br>• Company Names<br>• SSO only: Group Name | • Used Host Systems,<br>• Used Content Integrations | • STAGE System assignment (Demo Server)<br>• Connector Black / Whitelist | • Expiry dates<br>• Product EAN |
| Passed-through Operational | none | none | none | none |
| Bypassed Operational (Client/Integration) | none | none | none | none |

DSP DATA SUB-PROCESSOR

# >keylight/

**Type:** Provisioning System | **LOCATION:** AWS Frankfurt

| DATA TYPE | PROFILE: | USAGE | CLIENT CONFIGURATION | LICENSE INFORMATION: |
|---|---|---|---|---|
| Stored Operational | • Names of License (only Admin and Customer Rep).<br>• CI HUB ID (e.g., e-mail Addresses)<br>• First name last name, and e-mail of invited license user<br>• Company Names<br>• Company Domain<br>• Company address (opt) | none | none | Not assigned to a CI HUB ID (user)<br>• Expiry dates<br>• Product EAN |
| Passed-through Operational | none | none | none | none |
| Bypassed Operational (Client/Integration) | none | none | none | none |

DSP DATA SUB-PROCESSOR

# okta

**Type:** IAM | **LOCATION:** AWS Frankfurt

| DATA TYPE | PROFILE: | USAGE | CLIENT CONFIGURATION | LICENSE INFORMATION: |
|---|---|---|---|---|
| Stored Operational | • Names (if SSO: filled by IDP, based on Customer decision )<br>• CI HUB ID (if SSO: filled by IDP, based on Customer decision )<br>• If SSO: filled by IDP, based on Customer decision with Group assignment required by CI HUB | • Authentication Timestamps | • OPT. IF USER OPTS FOR THE CLIENT CONFIGURATION. TO BE INTERCHANGEBEL BETWEEN HOSTSYSTEMS.<br>• Connector Black / Whitelist | • Expiry dates<br>• Product EAN |
| Passed-through Operational | none | none | none | none |
| Bypassed Operational (Client/Integration) | none | none | none | none |

# SSO - General

PLEASE REFERRE TO THE SPECIFIC SSO INFO DOCUMENT

## PROCESS:

1: Check if your SSO setup is supported by CI HUB

2. Order Setup and Required Users.

3. The CI HUB Team will setup a Preparing Call as soon as the Order is Recived and we have reived all ness Informations from the Customer.

4. CI HUB will involve our Implementation Partner “xxxxxx” to lead the implementation.

5. Signoff

## COST:

**There is a Setup Fee of 6.500 € that needs to b the Process. This fee also applies to change**

In addition there is a Yearly SA User and Month, based on a yearly prepay

Both SSO Prod ed via the License Admin System or via emai om.

Saas Fee for the users we need a fixed abount f are based on the required ‘UserLicences not on the actual

## SI D IDP’S

## You hav ?

(ex. AWS D, Google cloud identity management…)

Send a email to sales@ci-hub.com

# SSO - IdP Requirements

PLEASE REFERRE TO THE SPECIFIC SSO INFO DOCUMENT

## GROUPS

To effectively manage licenses, the Identity Provider (IdP) needs to provide the Service Provider (SP) with the required groups. These groups are specifically named as follows:

[COMPANY_NAME]-SSO-[HOST APPLICATION]

Examples.
MY-CORPORATION-AG-SSO-ADOBE

MY-CORPORATION-AG-SSO-MICROSOFT

SG-MY-CORPORATION-AG-DEPARTMENT-1-SSO-SKETCH

## SUPPORTED HOST APPLICATIONS:

ADOBE
Any of the following Adobe products
(Photoshop, InDesign, Illustrator, After Effe InCopy)

MICROSOFT
Any MS Office Applicatio , excel, outlook...)

GOOGLE-WO
the goog sheets, docs, slides...)

CH

WORDPRESS

SHAREPOINT:
Microsoft SharePoint

ADOBEEXPRESS
The Adobe Express Web App.

## SAML 2.0 RE NTS

(ex. AWS IAM gle cloud identity management...)

It is imp e that the SAML 2.0 protocol includes the user's email address, first name, last name, and relevant CI HUB groups in the SAML response. To guarantee a flawless setup, kindly furnish us with your Metadata XML file as soon as you receive ours. Furthermore, it is crucial that the **relayState** is transmitted as a **POST** parameter when sending the SAML response.

## SUPP DP'S

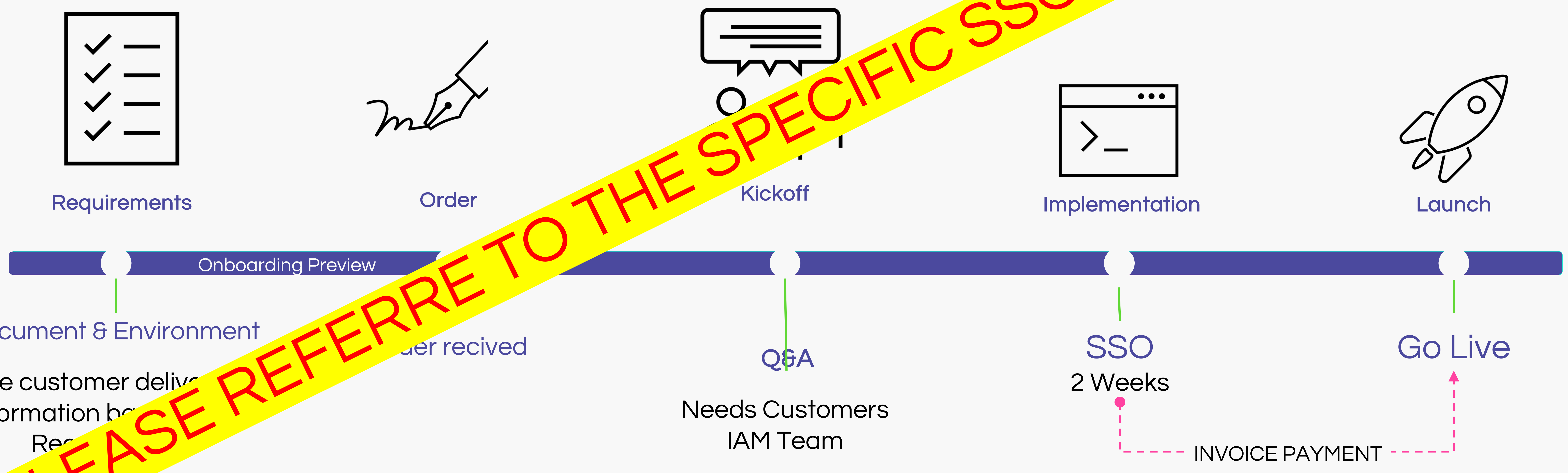
- 2.0
- Any OpenID Connect (OIDC)
- ✓ Amazon
- ✓ Apple
- ✓ Discord
- ✓ Facebook
- ✓ GitHub
- ✓ GitLab
- ✓ Google
- ✓ LinkedIn
- ✓ Login.gov
- ✓ Microsoft
- ✓ PayPal
- ✓ Salesforce
- ✓ Xero
- ✓ Yahoo
- ✓ Yahoo Japan

If your Identity Provider (IdP) is not included in the list, it is not possible to implement the Single Sign-On (SSO) Integration.

# SSO Implementation flow

Using CI HUB made easy

PLEASE REFERRE TO THE SPECIFIC SSO INFO DOCUMENT



The customer deliv
information b
Re

by Customer
& CI HUB

Needs Customers
IAM Team

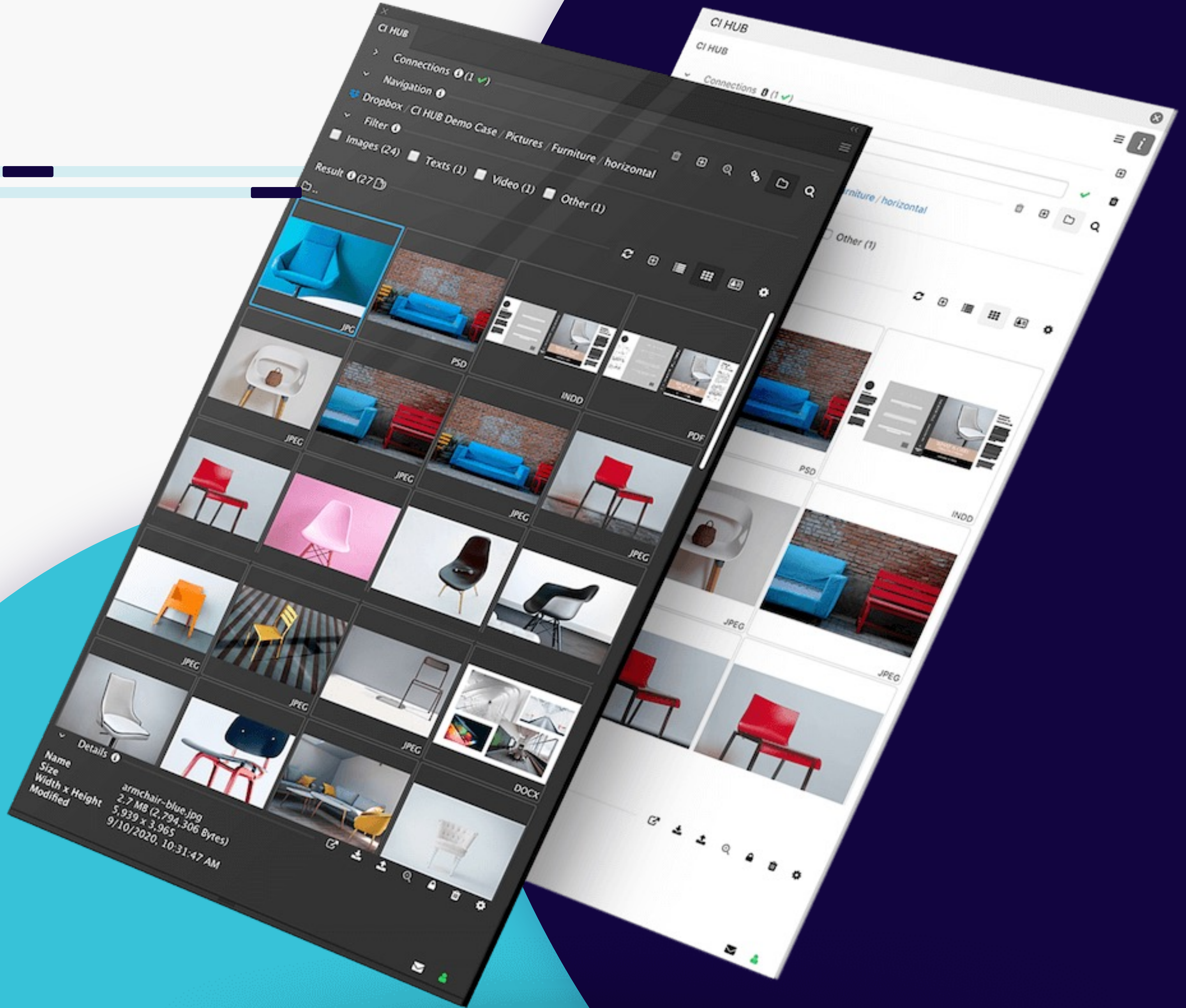
Coordination with:
sso@ci-hub.com

CI HUB tells if there are
chages to the standard offer

# Focus on your creativity.

Creativity | Teamwork | Standardization

www.ci-hub.com



Name armchair-blue.jpg
Size 2.7 MB (2,794,306 Bytes)
Width x Height 5,939 x 3,965
Modified 9/10/2020, 10:31:47 AM