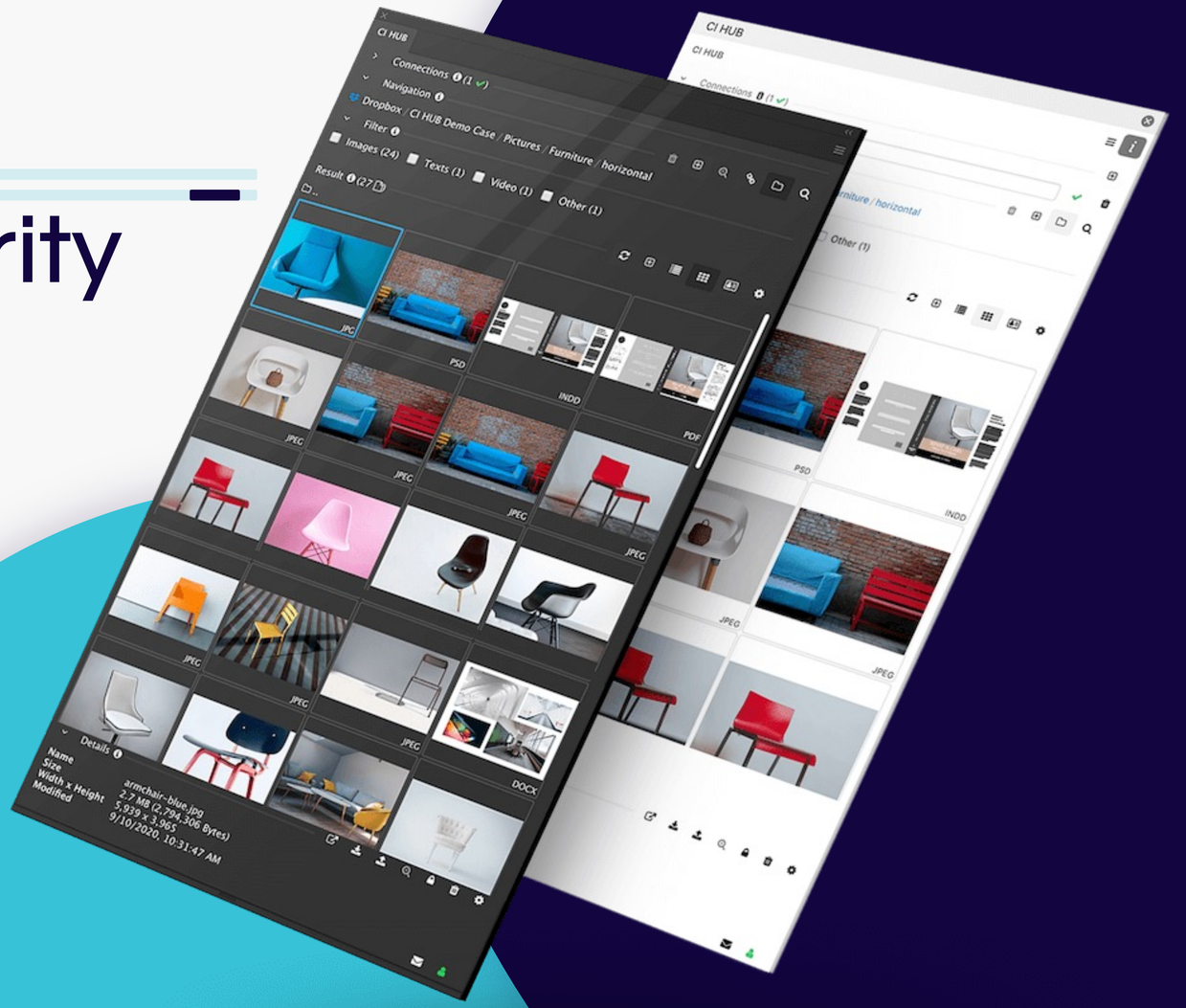
Advanced Setup & Security Information's (General Technical Information)

Creativity | Teamwork | Standardization



www.ci-hub.com

Copyright © 2025 CI HUB GmbH. All rights reserved.

Document Version and History

Change/Info	Editor	Date	Version	info
Updated the info for On-Premise 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 Added the new domains, subdomains, the new server IP addresses, and the Transactional E-Mails server to the Firewall page Updated the OAuth Redirect URLs Updated data stored by Keylight	Salim Melliti/Michalski	07. Mai 2024	1.4	
Added the end of support date for the old Infrastructure URIs and domains Added a warning Notice	Salim Melliti	16. Sep. 2024	1.5	
Updated the IPs in the firewall Section	Salim Melliti	25. Sep. 2024	1.7	
Adding the Open Source Information	Andreas Michalski	17.Okt. 2024	1.8	
Updateing OnPrem infos incl. Systemvendor info	Andreas Michalski	10. Feb. 2025	1.9	
Updated: Only HTTPS communication.	Robin Honsowitz	06. März 2025	2.0	

Copyright © 2025 CI HUB GmbH. All rights reserved.

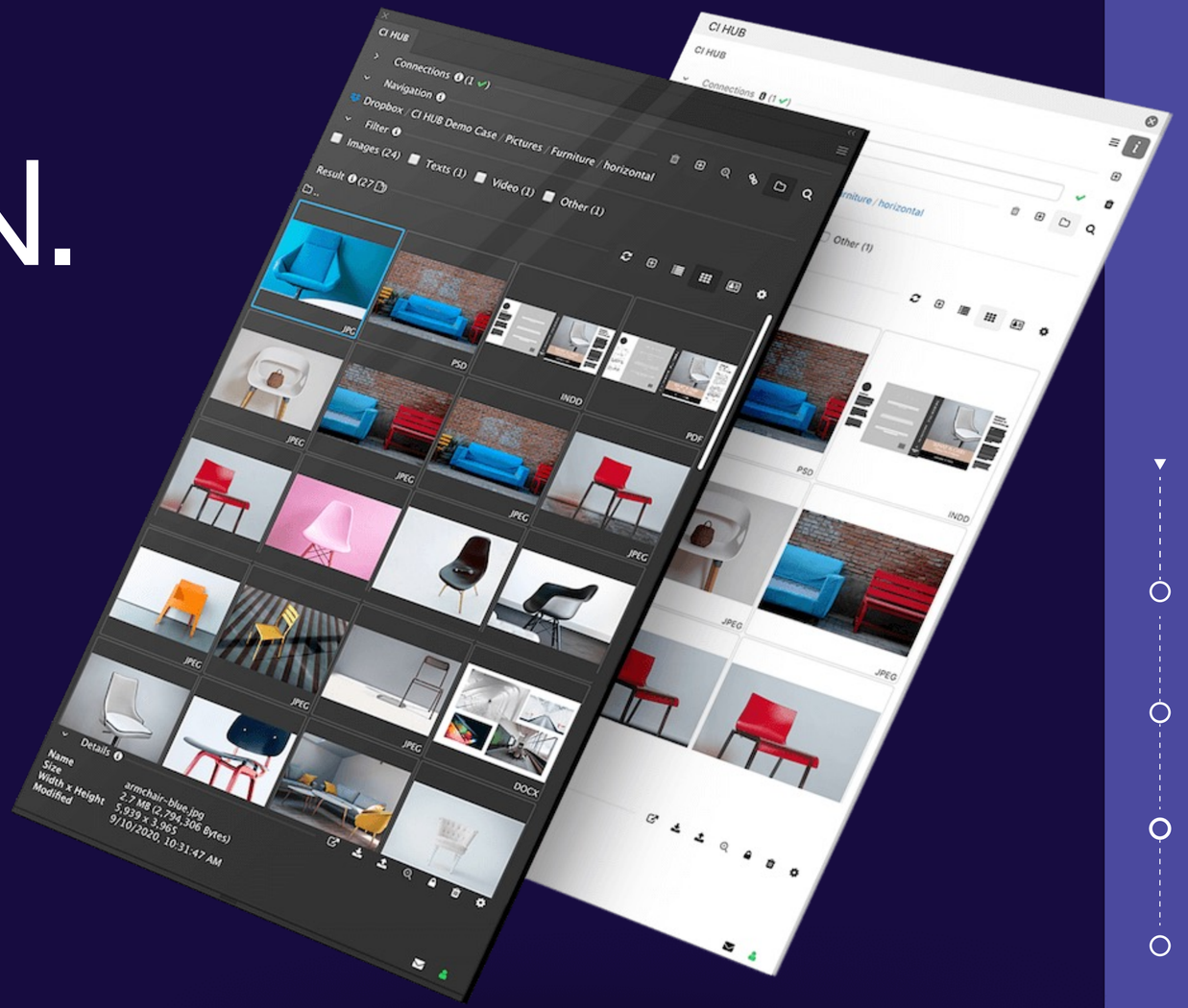
©2025

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.

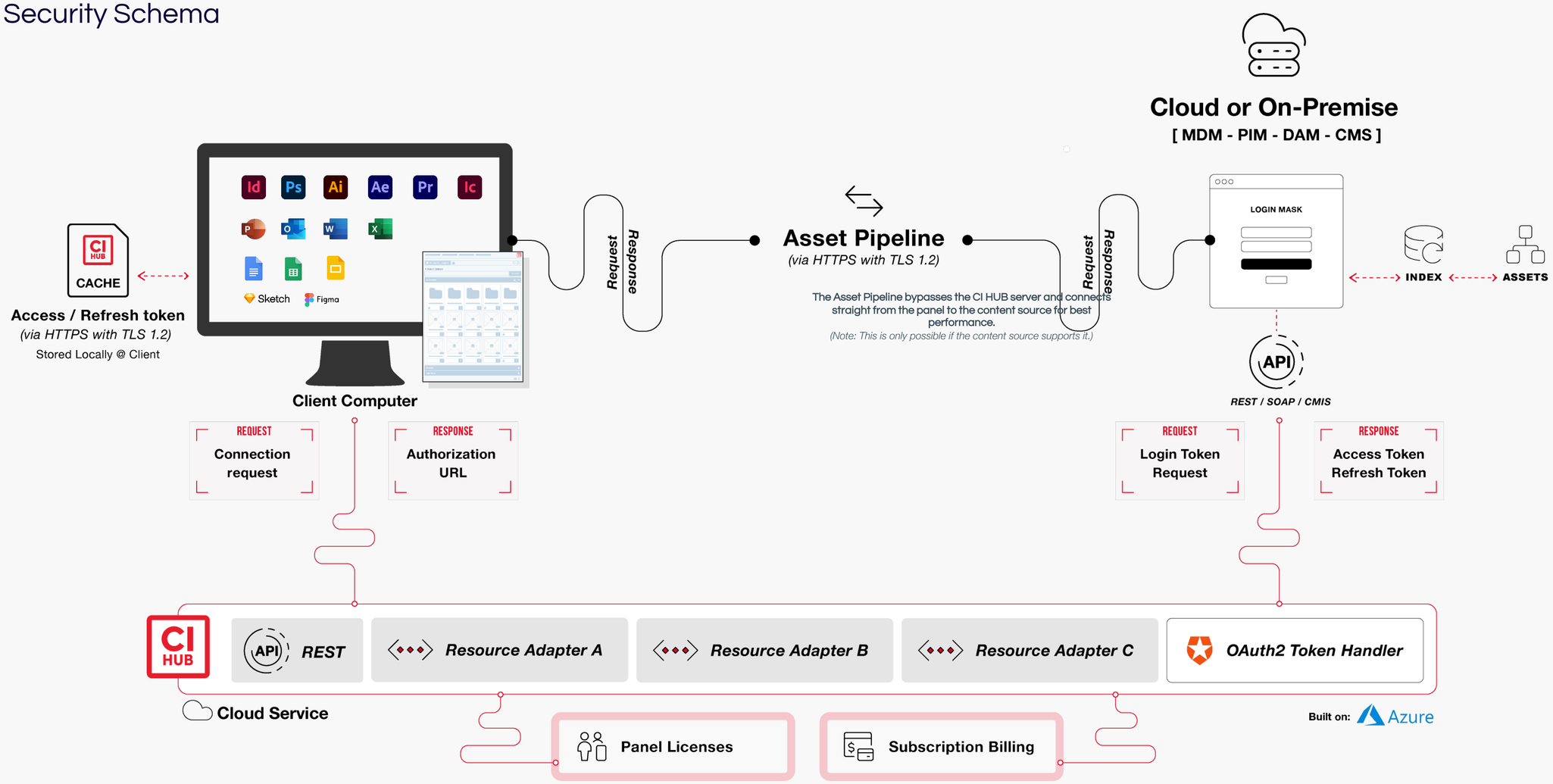
2. From the CI HUB Client via the CI HUB Server to the Partner API. This path is used to perform certain environment-dependent actions or to access secret keys stored in the server. To ensure that these keys & secrets are stored securely, they are stored in an area of our Azure server where no one except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



©2025

DATA POINTER

Security Schema



Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

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.

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/

Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

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.

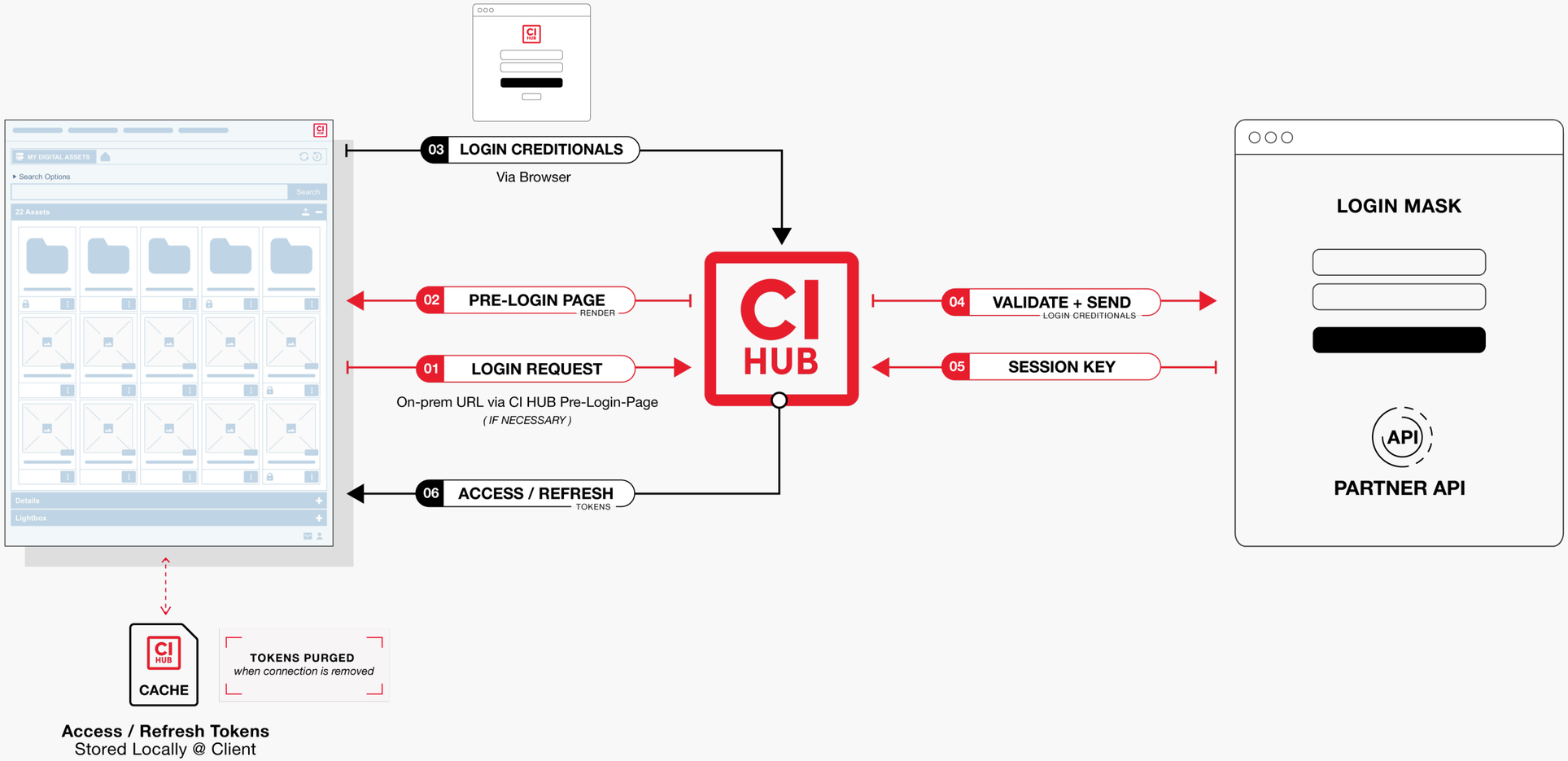
For more information about AES256 encryption, see https://www.atpinc.com/blog/what-is-aes-256-encryption

Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

DATA POINTER

Security Schema | Basic

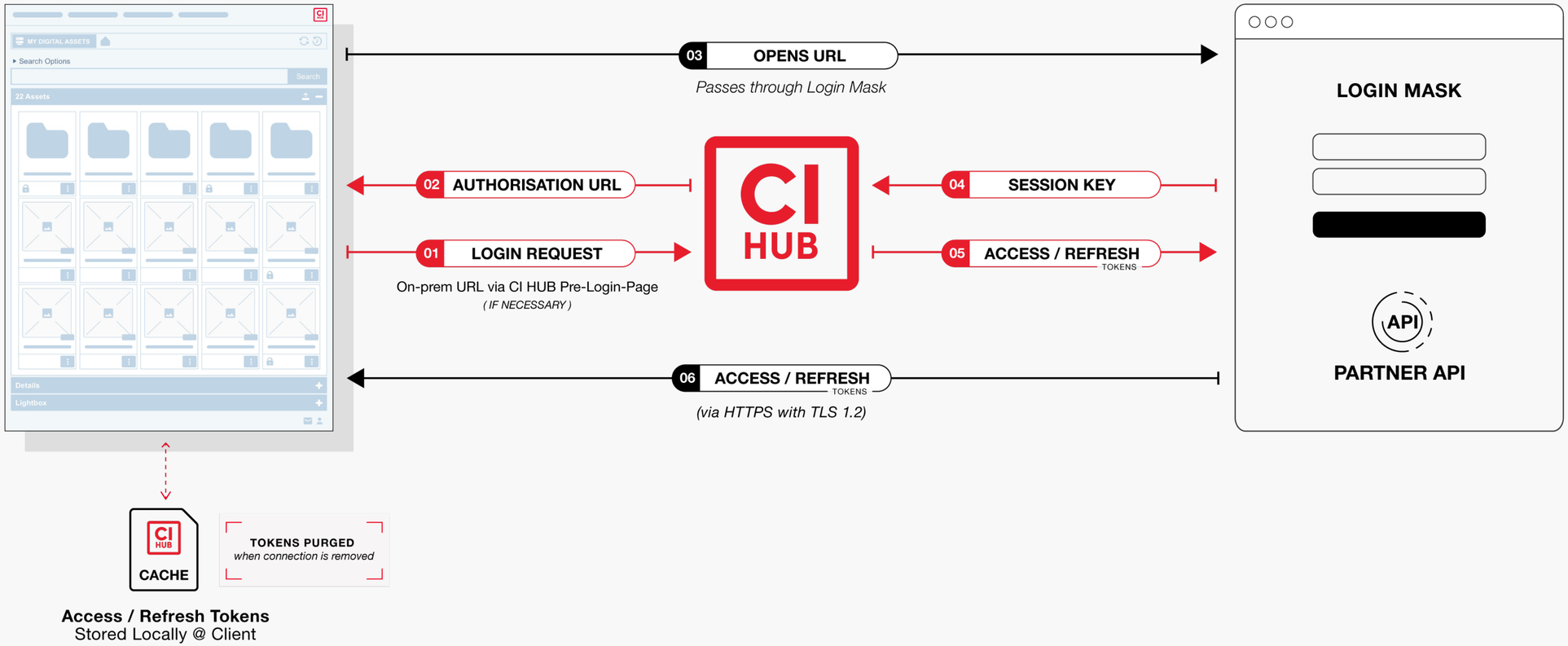


Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

DATA POINTER

Security Schema | 0Auth2



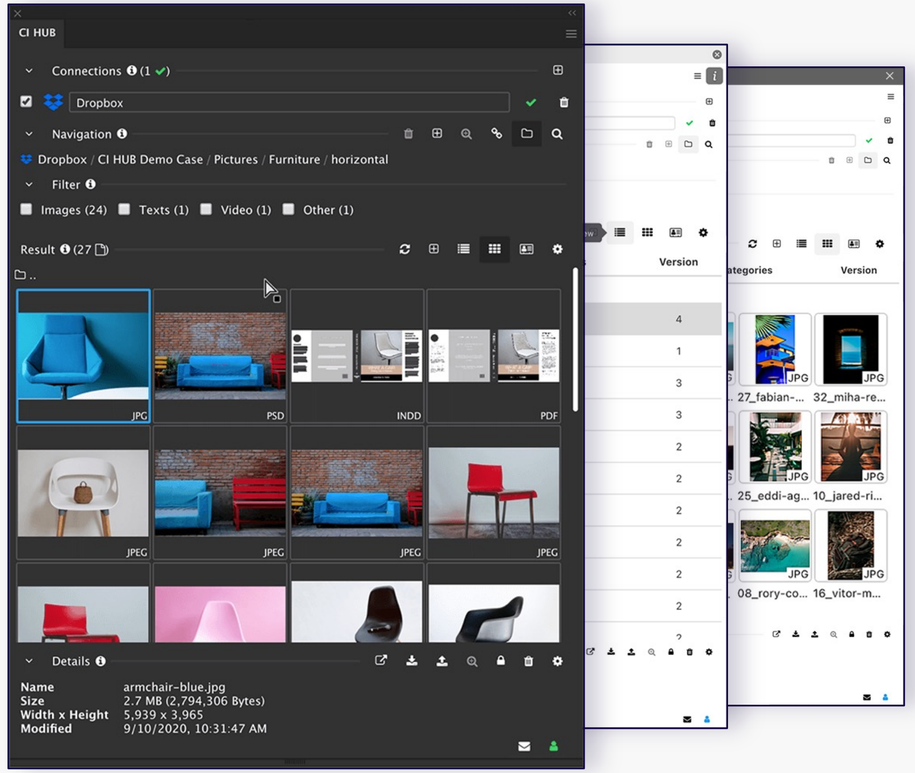
Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

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)*



Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

FIREWALL

Requirements for Firewalls and Ports

COMMUNICATION: HTTPS “standard” Ports

DOMAIN & SUBDOMAINS TO INCLUDE: (The ones marked in **red** will be sunset in June 2025)

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

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	104.40.213.244	20.8.213.62	4.245.29.138	20.73.114.74
104.46.42.104	104.40.211.253	4.245.27.176	4.245.26.15	20.101.152.141
23.101.67.154	137.117.175.38	20.103.242.193	4.245.26.168	20.76.7.76
23.97.174.44	20.31.195.152	20.8.214.71	4.245.27.82	20.109.202.102
23.97.177.139	20.8.212.253	4.245.28.130	20.101.155.169	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

Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

GENERAL On-Premise

Information

Some configurations are needed for systems that do not support a „proper“ SaaS Solution or run in an on-premise Environment. (Not providing a “GlobalKey”)

HERE WE PROVIDE THE GENERAL OVERVIEW:

To set up these Systems, you must talk to your System Vendor or System Partner. They can Provide all the necessary information. To set up these Systems, you need to order the CI HUB OnPrem/Multi-SaaS Installation.

Please email: sales@ci-hub.com.

If you are a Systemvendor, and need to setup this, then Connect with you CI HUB Team via SLACK, and Provide all informations and Order Confirmation.

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“

Your Client Secret: „string“

If your System requires additional infos YOU must provide them. (eg. Rootfolder ID, recource basepath etc.)

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.*

Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

GENERAL OAuth Redirect URIs

Information

In addition, we will provide a set of system-specific redirect URLs that need to be configured in your OAuth settings for the authentication to work.

A. Please refer to your system provider or partner for instructions on how and where to set these up.

B. It's important to remember that these URLs are unique to your system. The URLs will be as follows, and they are system-specific. “SYSTEM” must be replaced with your integration identifier , which you will find in the OBD-C Document

GENERAL SCHEME: (The ones marked in red will be sunset in 28.02.2025)

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"

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

Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

SPECIFIC OAuth Redirect URIs

Example OAuth Redirect URIs for DROPBOX

The system identifier for DROPBOX is dropbox, so the correct Redirect URIs are:

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

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

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

http://localhost:8080/api/v1/auth/login/dropbox

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

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

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

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

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

https://identity.ci-hub.com/auth/login/ dropbox

NOTE: The links marked in red will be sunset on the **28.02.2025**

Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

IMPORTANT NOTICE

To avoid service disruption, ensure you have added all the redirect URI to your OAuth system and whitelisted all the described domains and IPs.

The domains and URIs in the FIREWALL and OAUTH Redirect section, which are marked in red, will be sunset on **28.02.2025**

Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

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

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.*

Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

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.

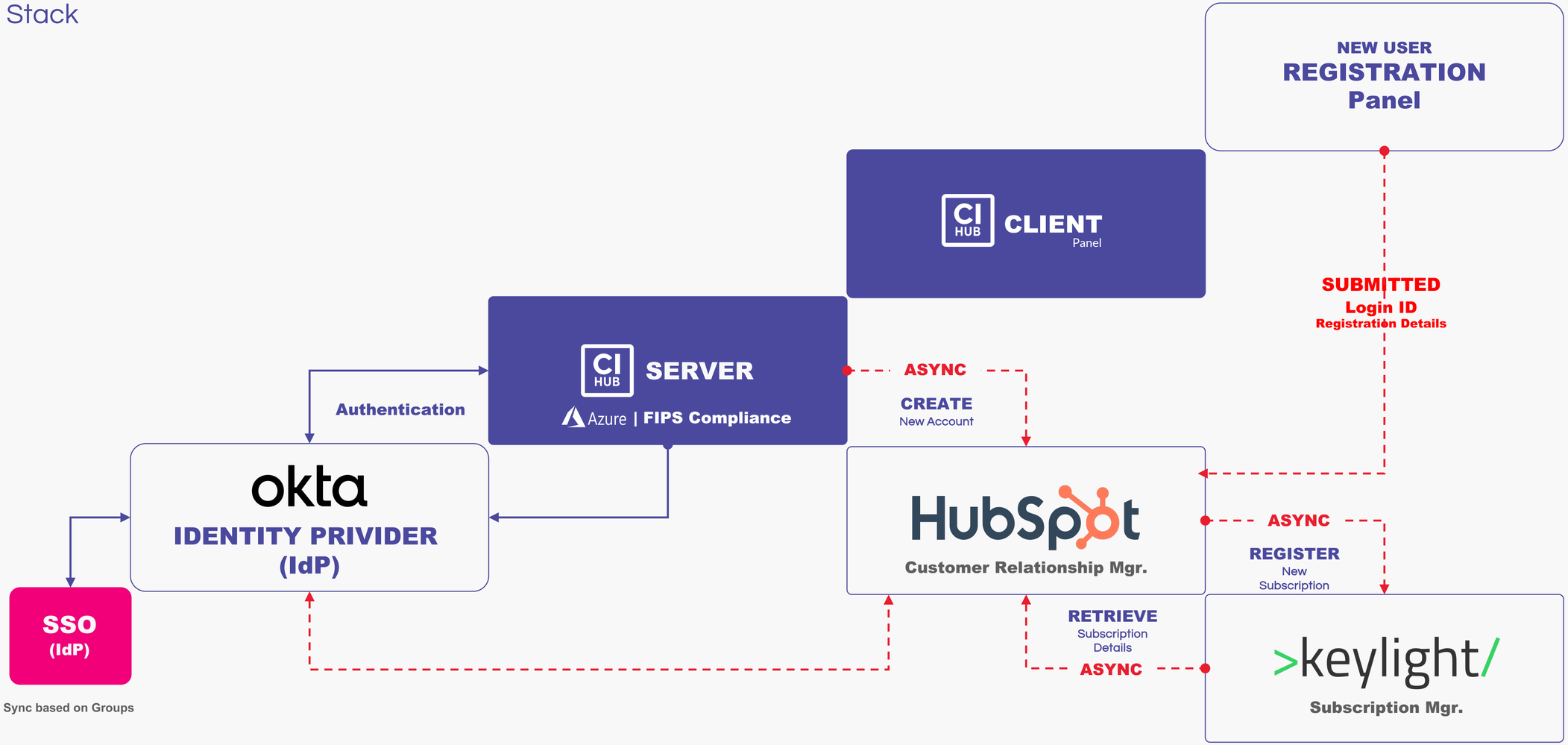
Q: What OpenSource Products are you using?
A: We are using industrie best Praxis for integration OS Software. We are using the following Open Source Projekte: axios, express, node-js & vue-js. We licence them via MIT.

Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

REGISTRATION

Stack

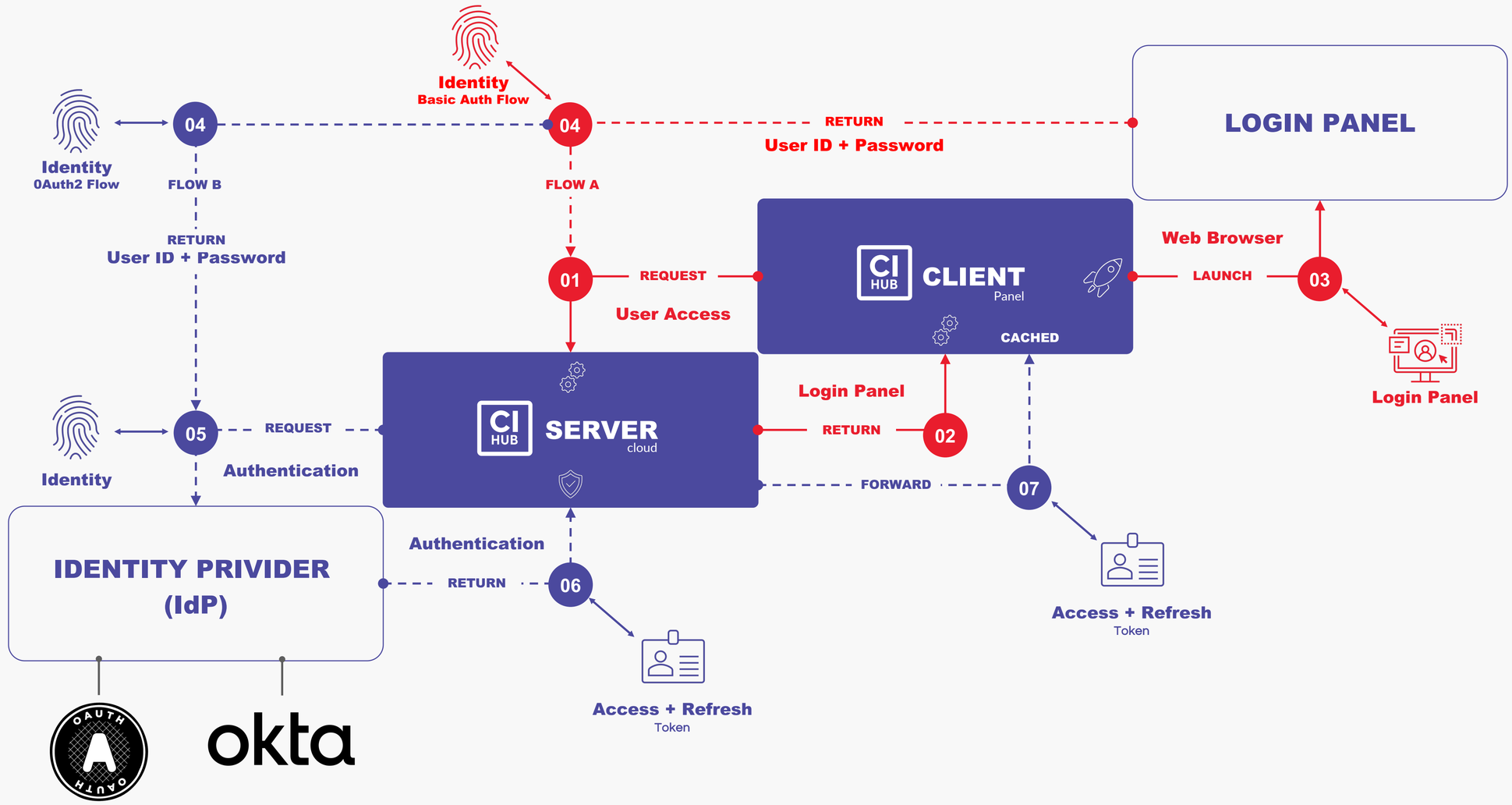


Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

LOGIN

Flows



Copyright © 2025 CI HUB GmbH. All rights reserved.

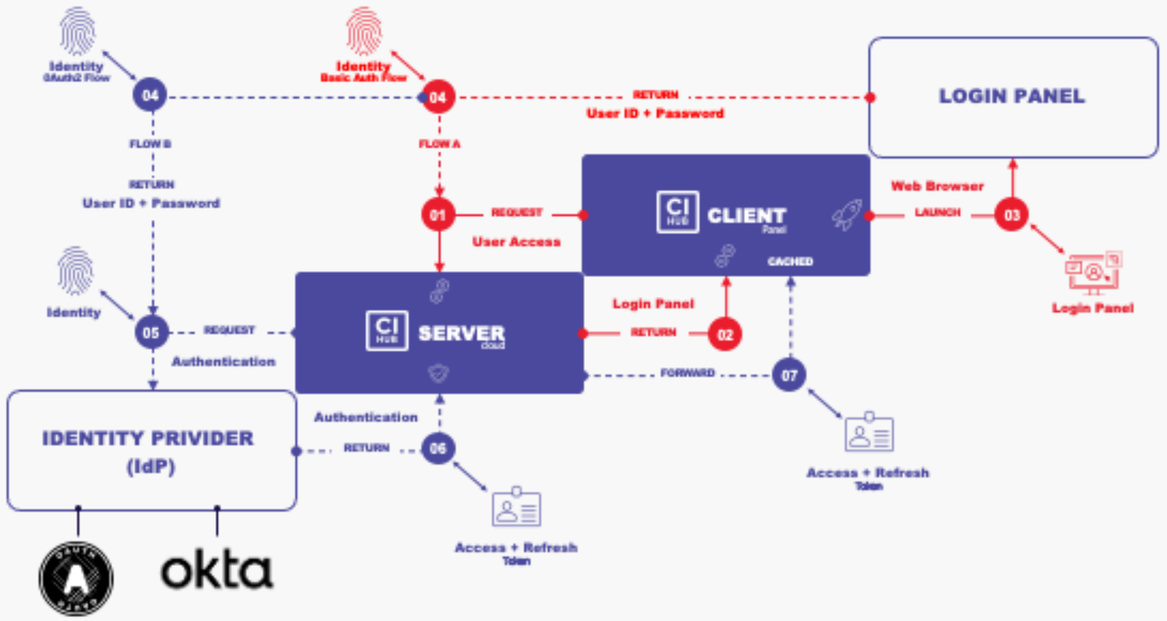
©2025

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.



Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

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

Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

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) • 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

Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

DSP DATA SUB-PROCESSOR

HubSpot

Type: CRM | **LOCATION:** Germany

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

Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

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). • CI HUB ID (e.g., e-mail Addresses) • First name last name, and e-mail of invited license user • Company Names • Company Domain • Company address (opt)	none	none	Not assigned to a CI HUB ID (user) • Expiry dates • Product EAN
Passed-through Operational	none	none	none	none
Bypassed Operational (Client/Integration)	none	none	none	none

Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

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) • CI HUB ID (if SSO: filled by IDP, based on Customer decision) • 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. • Connector Black / Whitelist	• Expiry dates • Product EAN
Passed-through Operational	none	none	none	none
Bypassed Operational (Client/Integration)	none	none	none	none

Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

SSO - General

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 P… xx" to lead the implementation.

5. Signoff

COST:

There is a Setup Fe… …eeds to be ordered to start the Process. This f… …changes after setup.

In a… …early SA… …0,40 € per User and Month, …y prepay…

…SSO Prod… …ed via the License Admin System or via emai… …com.

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

SUPPORTED IDP'S

You hav… …?
(ex. AWS… …B, Google… …gement…)

Send a… …mail t… …ub.com

PLEASE REFERRE TO THE SPECIFIC SSO INFO DOCUMENT found in SalesClub: CIHDOC_TI_002_CI HUB_INFO_SSO_TECH.pdf

Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

SSO - IdP Requirements

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-DEPART… …SKETC…

SUPPORTED HOST A…

ADOBE
Any of the follo… …ers
(Photosh… …ator, Afte… Effects, Premiere Pro, InCopy)

…ce Applic… …, word, excel, outlook…)

GOOGLE …
the … …pps: sheets, docs, slides…)

…KETCH

…ORDPRESS

…EPOINT:
…rosoft SharePoint

ADOBEEXPRESS
The Adobe Express Web App.

SAML 2.0 … …IENTS
(ex. AWS … …D, Google … …gement…)

It is imp…ative th… …L 2.0 protocol includes the user's email address, first name, last name, and relevant CI HUB groups in t… …sponse. To guarantee a flawless setup, kindly furnish us with your Metadata XML file as soon as you recei… …Furthermore, it is crucial that the **relayState** is transmitted as a **POST** parameter when sending the SAML response.

SUPPORTED IDP'S

- ✓ Any SAML 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.

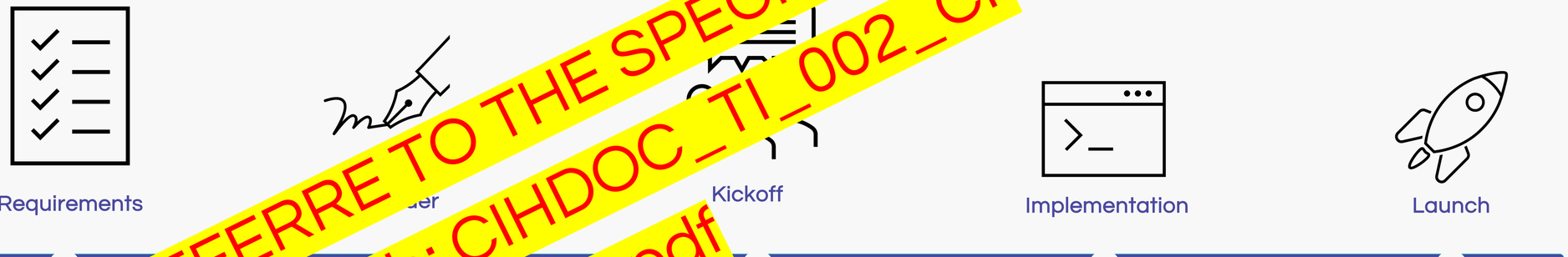
PLEASE REFERRE TO THE SPECIFIC SSO INFO DOCUMENT found in SalesClub: CIHDOC_TI_002_CI HUB_INFO_SSO_TECH.pdf

Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

SSO Implementation fl

Using CI HUB made easy



Needs Customers
IAM Team

Coordination with:
sso@ci-hub.com

CI HUB tells if there are
chages to the standard offer

PLEASE REFERRE TO THE SPECIFIC SSO INFO DOCUMENT found in SalesClub: CIHDOC_TI_002_CI HUB_INFO_SSO_TECH.pdf

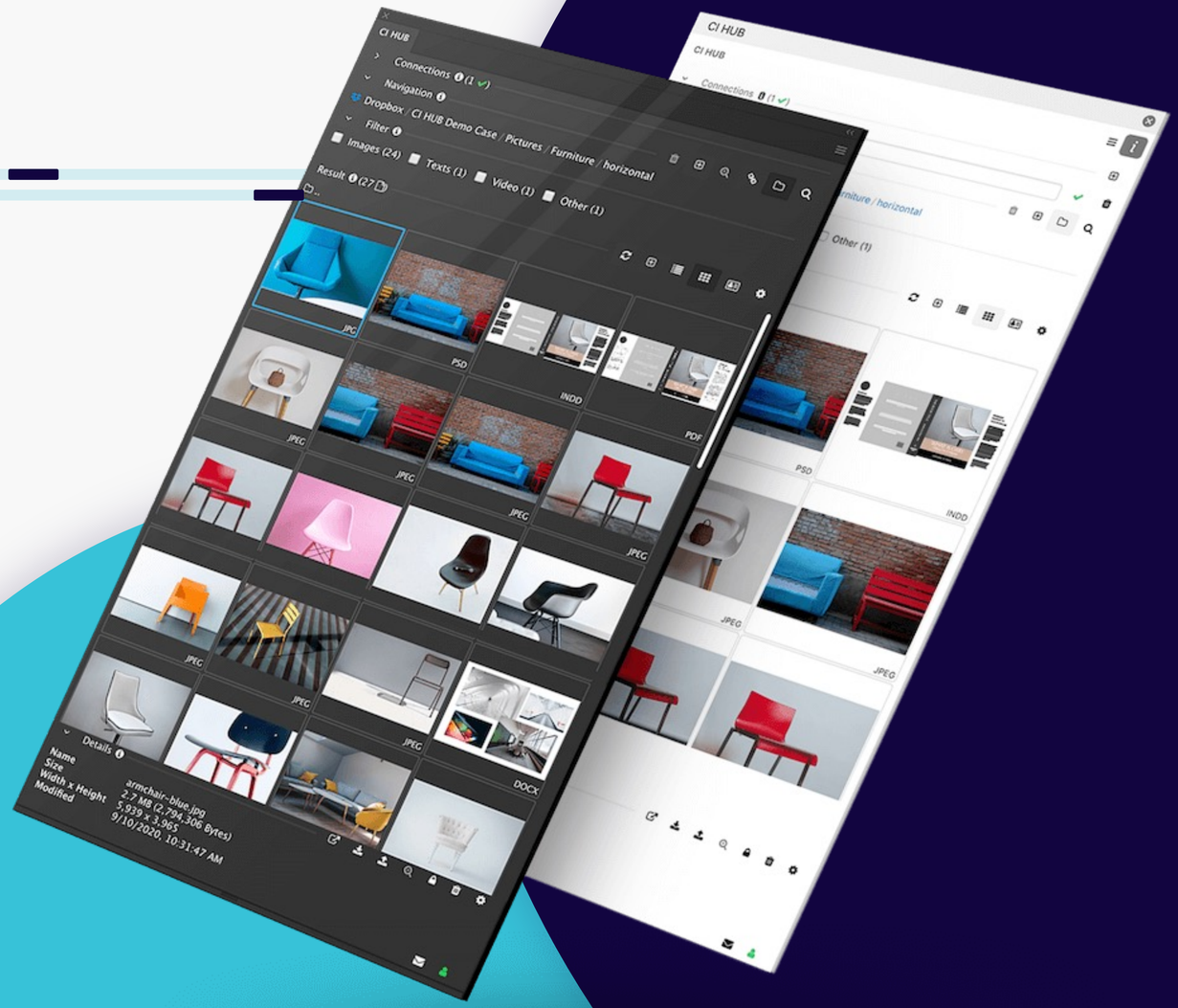
Copyright © 2025 CI HUB GmbH. All rights reserved.

©2025

Focus on your creativity.

Creativity | Teamwork | Standardization

www.ci-hub.com



Copyright © 2025 CI HUB GmbH. All rights reserved.