CAIA Onboarding Guide - IGT
(IPAC & G-Invoicing)

Revision Date: 08/11/2023

Introduction

CAIA (**C**ommon **A**pproach to the **I**dentity **A**ssurance) provides a consistent user experience for multifactor authentication to the Fiscal Accounting applications. The CAIA solution is similar to the existing Treasury Single Sign-On system to allow users to authenticate to Treasury applications, however the IBM Security Identity Manager (ISIM) username and password will no longer be utilized. ISIM will be replaced with SailPoint IdentityIQ for application permission management.

The Fiscal Accounting applications listed below will be migrating to **C**ommon **A**pproach to **I**dentity **A**ssurance (CAIA) and a Cloud Infrastructure. Multifactor authentication (MFA) and Cloud technology will enable Fiscal Service applications to provide enhanced security, scalability, and resilience.

The Treasury mandate for CAIA is to be implemented before the end of "**Q3 2023"** (calendar year) for all Fiscal Accounting applications. The Cloud migration dates will be provided by each application in a future communication.

Applications

- Q3 Shared Accounting Module **(SAM)**
- Q3 Central Accounting Reporting System **(CARS)**
- Q3 Intra-Governmental Transactions **(G-Invoicing)**
- Q3 Intra-Governmental Payment and Collection **(IPAC)**
- Q2 Government wide Treasury Account Symbol Adjusted Trial Balance System **(GTAS)**

Why Migrate

Executive Order 14028: Improving the Nation's Cybersecurity & OMB Zero Trust Strategy require Fiscal Service to implement multi-factor authentication (MFA) and Cloud Infrastructure.

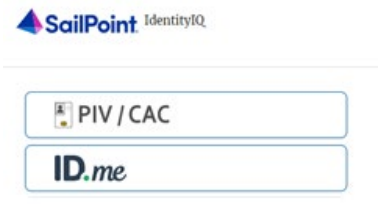
All application users will be required to authenticate with an identity that supports multifactor authentication. Username and password will no longer be accepted. CAIA will support one of the following MFA methods.
1. PIV/PIV-I, CAC **2**. ID.me.

3rd Party Credential Service Provider (CSP)

ID.me
If you have an existing personal account with ID.me, you will need to add your work email address to your existing account. ID.me will require your work email address to be listed as your Primary email address.

If you **do not** have a PIV/PIV-I/CAC card and are not able to obtain a PIV, PIV-I/CAC card, please register with the 3rd Party Credential Service Provider (CSP) via SailPoint IIQ. Additional information about ID.me https://help.id.me/hc/en-us/articles/4416509221271-Treasury-and-ID-me

https://iiq.fiscal.treasury.gov



Login.gov

Login.gov does not have a current IAL2 compliant offering leaving ID.me as the only current CAIA-enabled CSP IAL2 offering. The IAL2 rating is unique to each Treasury application, hence the reason why Login.gov may be available for other applications. The following implementation guidance was provided for systems enabling MFA prior to September 30, 2023.

- For applications with a DIRA requiring IAL1, you may select to enable from:
  - Login.gov
  - ID.me
- For applications with a DIRA requiring IAL2, enable: (**IPAC and GINV are IAL2 rated applications**)
  - ID.me

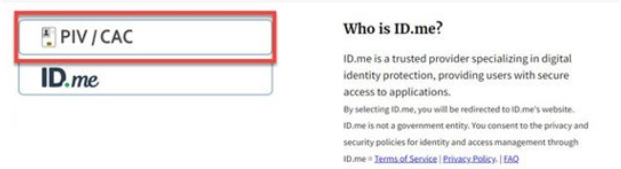
Fiscal Service and Treasury are monitoring Login.gov's plans around IAL2 compliance and an update will be provided if additional options become available.

New Login Screen

Once applications have migrated to CAIA, the new login screen will provide users with the methods to authenticate to access the applications:
1) **PIV Card** 2) **ID.me**

Existing Application Login Experience

New Login Experience



Training

G-Invoicing - G-Invoicing: Training (treasury.gov)

All G-INV Administrators will be notified when training material is published as well as the dates for follow on office hours where the provisioning process will be demoed. During these office hours sessions agency administrators will have the opportunity to ask questions about the new process.

IPAC - Intra-Governmental Payment and Collection: Training (treasury.gov)

Additional information will be provided when IPAC training material is published, and sessions are scheduled.

Frequently Asked Questions (FAQ)

How will I know when an application is cutting over to CAIA?

A: UPDATE: Deployment dates will be posted to the G-Invoicing "News and information" and IPAC "Must See Message"

Will there be any changes required if I have a PIV,PIV-I, CAC card already?

A: UPDATE: If you have linked your existing PIV, PIV-I or CAC there is no further action needed at this time. When logging into CAIA for the first time, users will be prompted to provide their real email address and link their PIV/CAC card using a one-time PIN code sent via email.

Will I be able to use my existing test account in CAIA?

A: Test accounts with fake email addresses will no longer be supported. It is recommended to link your existing card to your account in the pre-prod QA environment if you are using your real email address. The linking process will not work with a fake email. If you do not have a PIV/CAC card to link, more information will be provided regarding test accounts.

Will there be any changes required to access the application when migrating to CAIA?

A: UPDATE: Information is provided in this document to establish a CSP account if you currently do not have a PIV, PIV-I or CAC card. Additional details will be forthcoming to provision access to each Fiscal Accounting application. The Agency Implementation Team (AIT) will be providing additional support documentation and upcoming training to establish access in CAIA.

Will automated "system IDs" used for APIs or automated file transfers be changing for CAIA?

A: No changes are expected; however, application teams will provide more details if necessary or as they become available.

Will my existing BOT account migrate to CAIA?

A: UPDATE: A new "non-human" identity will need to be established and each application team will provide more information.

Robotic Process Automation (RPA/BOTs) Migration

The Treasury "CAIA Federation Service" link provides the details to support multifactor authentication after the CAIA migration. The agency contact that completes the certificate form must digitally sign with a PIV/CAC and is responsible for properly securing the certificate. The certificate is **prohibited** from being transferred to other individuals.

Migrating an existing BOT:

Digital Worker Authentication CAIAFederationService (treasury.gov)

Completing the Certificate Form

- Applicant Phone Number(s)
- Applicant Work Address
- **Common Name**: *existing bot userid*
- **Email Address**: *the same email address associated with the existing bot*
- **Certificate Authority**: TOCA Development (QA preprod bot)
  TOCA Production – (production bot)
- **Certificate Type**: Device or Server
- **Action:** Create New Certificate
- **Special Instructions**: Migrating existing RPA/BOT "userid" to "certificate" authentication for CAIA

Please return the signed certificate form to the appropriate team for processing.
STLS G-Inv CBAF STLS.G-Inv.CBAF@stls.frb.org or STLS IPAC CBAF STLS.IPAC.CBAF@stls.frb.org

Requesting a new BOT:

The certificate form noted above will need to be completed and submitted. However, there will be an additional Security Intake Form and application Enrollment provided when the certificate form is received.

Please return the signed certificate form to the appropriate team for processing.
STLS G-Inv CBAF STLS.G-Inv.CBAF@stls.frb.org or STLS IPAC CBAF STLS.IPAC.CBAF@stls.frb.org

Will there be any changes required to access the application after migrating to the Cloud?

A: The transition to Cloud is expected to have minimal impact to users, however if there are any changes to the "system ID" for API or automated file transfers, more information will be provided.