Commonwealth of Kentucky

KYID Integration

(replaces the current Kentucky Online Gateway (KOG))

KYID Integration

KYID is the Cabinet for Health and Family Services' (CHFS) enterprise identity and access management system and web Single Sign-On (SSO) platform. KYID is to be leveraged for SSO for all new business applications including both authentication and authorization for users based on claims. Currently KYID primarily uses Active Directory and ForgeRock as IDaaS platform (Identity as a Service Provider).

A. Integration Requirements and Supported Authentication Protocols

Integration with KYID is mandatory for all applications. To ensure seamless integration with KYID and adherence to authentication and authorization standards, business applications must be claims-aware. A claim is a declaration made by an entity (e.g., name, identity, group, privilege, attribute, etc.). Applications integrating with KYID must be able to integrate with ForgeRock's Security Token Service using one of the following protocols:

1. SAML 2.0; or
2. OIDC / OAuth 2.0; or
3. WS-Fed (least preferred)

KYID team constantly reviews current security trends, features / functionalities it supports and may update the platform in future. KYID will try to make sure to have minimal impact on client applications and users but as a part of platform update, client applications may have to make changes on their side to point / integrate with new platform.

The below section will discuss the fundamental architecture, technology standards, and implementation options for applications integrating with KYID.

A.1 SSO / SLO, Authentication, Authorization and User Provisioning

1. Applications will interface with KYID through ForgeRock for SSO / SLO. All applications **MUST** support / participate in single sign-on (**SSO**) and single logout (**SLO**) processes using respective protocol.
2. New applications integrating with KYID must be compliant with either SAML 2.0 or OIDC / OAuth 2.0 or WS-Fed; and use Claims for user authentication and authorization.
3. Application access will be handled through the integration with KYID.
4. Authorized users will have access to all of their applications from the KYID dashboard via either static or dynamic widgets / tiles.

A.2 Security Roles

1. User roles will be defined by the consuming application. The application will determine which functions and data elements are available for each user role and is responsible for

implementing / enforcing the functions and permissions of each user role within the application.

2. Users will be assigned user roles in KYID using the KYID interfaces for requesting and assigning user roles. A user's assigned user role(s) will be communicated to the consuming application using Claims.

A.3 User Store

1. KYID will retain ownership of all user accounts and user profile data including entitlements for registered users.
2. Applications will need to read user profile information and authorizations / roles from SAML (in case of SAML or WS-Fed) or JWT (in case of OIDC / OAuth 2.0) claims.
3. KYID also supports secure (HTTPS) JSON based web APIs that client applications can call (out of band) to retrieve user profile information and authorizations.
4. Applications must consume and store the user KYID Unique ID to uniquely identify each user coming from KYID. User's KYID Unique ID is a static GUID used to identify a unique user in KYID.

B. Deployments and Environment Mappings

New applications will be responsible for all aspects of solution environment integration with KYID including:

1. Detailed design documentation;
2. Mapping and integration of application environments to KYID environments (Integrated Dev, Test, UAT, Training, Production);
3. Integration testing;
4. End-to-end testing of all API(s); and
5. Performance testing.

As part of the integration efforts, new applications will also be responsible for providing configuration items including:

1. Integration documentation;
2. Federation metadata;
3. Requirements for any claims that will be passed in the SAML / JWT token;
4. List of application roles;
5. Workflow for each role, if required (i.e., approvers); and
6. Information needed via API must be prescribed.

C. Vendor Responsibilities for Providing Technical Resources

The application owner or application vendor shall be responsible for performing all necessary JAD sessions to complete the design of all security requirements, requirements for integrating the solution into the respective KYID environments, and any development/customizations required by the solutions outside of in-built KYID functionality. The vendor shall be responsible for providing adequate technical resources that have working knowledge in implementing the respective SSO protocol (whichever is applicable) on the client application side. For example, if

the application is going to use the SAML 2.0 protocol, then the technical resources working on the KYID integration from the client application perspective should have working knowledge of how the SAML protocol works in a SSO and SLO scenarios and should be able to sign and send SAML authentication requests, logout response and should be able to validate and consume SAML assertions, logout requests being sent from ForgeRock.

D. Core KYID Functionality for Internal Users

Below is an overview of the core KYID features and functionality that are available to internal users of integrated business applications:

1. **Application Management** – Application-specific configuration in KYID and ForgeRock.
2. **Account Management** – All internal users must have an account on the existing COT-managed Active Directory and defined in KYID.
3. **Role Management** – Each solution shall be defined as an application in KYID and ForgeRock, and any necessary security role types shall be configured and managed in KYID.
4. **Internal User Account Management** – KYID will handle all user account management. This functionality includes assigning, modifying and revocation of user access to each application within KYID. All internal users shall be managed via KYID in order to have access to a specific role for each solution.
5. **Single Sign-On and Single Logout** – All on-boarding applications must participate in the KYID Single Sign-on solution, which will provide access to all solutions via KYID / ForgeRock without requiring the user to sign on to individual applications explicitly. All on-boarding applications must also participate in standard protocol based single logout (SAML 2.0 or OIDC (back-channel) etc.) to make sure that users will be able to logout not only from KYID but also from all signed in applications within SSO session.
6. **Multi-Factor Authentication** – KYID utilizes different authentication frameworks to implement enhanced security, for applications that require multi-factor, KYID offers ForgeRock, Microsoft, Google Authenticator, Symantec VIP, SMS/text, voice calls and email based codes for users.

D.1 Additional KYID Functionality for External Users

1. **Self-Service Account Creation** – Citizen user registration shall occur via KYID. The process shall require the requesting user to provide their First Name, Last Name, (alternate email address or mobile phone number for easy account / password recovery), and an active e-mail address in order to submit and complete e-mail verification process.
2. **Self-Service Access Request** – Following user registration, KYID provides the user with the ability to request access to an application through an app store-styled dashboard.
3. **Remote Identity Proofing –** Depending upon requirements user may be asked to go through remote identity proofing as a part of access request process.
4. **Password Management** – During user registration the user shall be required to provide a password. KYID password management includes current industry security standards.

E. Vendor Responsibilities for KYID Security

1. Work with the CHFS security team and KYID team to facilitate JAD sessions necessary to identify and design all aspects of the solutions necessary to assure a seamless integration with KYID.
2. Coordinate, communicate, and facilitate business and technical JAD sessions in order for the vendor to design and develop all security roles and validation requirements and any required additional components to assure robust security for all solutions.
3. Applications integrating with KYID shall be designed as ForgeRock/OIDC/OAuth2.0/SAML 2.0 compliant. In case of SAML integration, KYID needs client applications to use public CA-issued certificates to use for SAML signing and encryption purposes in all environments (non-production and production). The Vendor shall work with the CHFS security and KYID team to define custom claim data necessary for secure access to the solutions.
4. Design, develop, test, and implement all solutions functionality required to assure access to information is restricted by security role and custom claim data, and any required additional security components necessary for successful implementation of the solutions.
5. Design and develop all solutions to be claims aware and participate in single sign-on and single logout.
6. Design and develop all solutions to utilize role-based security
7. Provide necessary information for the initial onboarding of users to new solutions, which shall include, but not be limited to, working with the CHFS Security team and KYID team to compile, provide data mapping including initial user provisioning for all existing / new users.
8. Design, integrate, test, and map solution environments with the KYID environments including performance testing.
9. Vendor’s business applications must adhere to current KYID functionality whenever possible.