Keystone Login and Identity Proofing Standard

Effective Date:
January 06, 2025

Category:
Security

Scheduled Review:
June 30, 2025

Supersedes:
ITP-SEC039, OPD-SEC039A, OPD-SEC039B

1. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

2. Purpose

This Standard is to establish and maintain a centralized account management system for online services for the Commonwealth and to establish Standards for online identity proofing of public users accessing Commonwealth IT web services or online applications.

3. Scope

This Standard applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the Standard requirements contained herein.

4. Standard

For definitions found within this document, refer to the *IT Policy Glossary*.

All citizen facing applications are to use Keystone Login for Authentication services. Keystone Login is an account management system for Commonwealth of Pennsylvania online services. The Keystone Login portal provides the following capabilities: account creation and management, Identity Verification, Authentication services and Single Sign-On (SSO) (sign on once to access multiple applications), social media login (e.g., Google), and risk-based multi-factor authentication. The Keystone Login provides citizens with a single credential (username and password) that can be used to access online services from multiple state agencies.

Keystone Login Accounts that have not been accessed in 18 months will be disabled.

4.1 Criminal Justice Information Systems

All CJIS implementations require approval from the Pennsylvania State Police (PSP)

Commonwealth Law Enforcement Assistance Network (CLEAN) Administrative Section at ra-clean@pa.gov. In addition:

- All web facing applications that contain CJIS data or connect to CJIS systems must at a minimum be authenticated at LOA2 (see Section 4.3), leveraging CWOPA user ID, through Keystone Login.
- Systems that connect to the CLEAN network or CJIS data that leverage single sign-on (SSO) capability, must perform a multi-factor authentication (MFA) check before granting access.
- Sessions must lock due to inactivity, in compliance with the *Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication Standard*.
- Application sessions must terminate after inactivity, in compliance with the *Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication Standard*. Network connectivity must terminate in conjunction with session termination.
- The system must enforce a limit of no more than 5 consecutive invalid access attempts in compliance with the *Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication Standard*. The system must automatically lock the account/node for a 10-minute time period unless released by an administrator.
- The information system must display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:
    - The user is accessing a restricted information system.
    - System usage may be monitored, recorded, and subject to audit.
    - Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
    - Use of the system indicates consent to monitoring and recording.
    - Access is restricted to agency owned and managed devices. Device certificate alone, placed on the device, may not be considered valid proof that the device is being operated by an authorized user.
- The information system controls must restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.
- The agency shall validate information system accounts at least annually and shall document the validation process.
- The agency shall immediately notify the PSP CLEAN Administrative Section with all personnel transfers and separation actions that impact access to the CLEAN network and CJIS data.
- The agency shall enforce the most restrictive set of rights or privileges or access needed by users for the performance of specified tasks.
- The agency shall use MFA for all access, including domain administrative access. MFA must use One Time Password (OTP) tokens as an authenticator. The OTP shall meet the requirements described below.

- Be a minimum of six (6) randomly generated characters.
- Be valid for a single session.
- If not used, expire within a maximum of five (5) minutes after issuance.

4.2 Identity Proofing

Identity Proofing is the process of verifying the real-life identity being claimed by a person. For purposes of this Standard, Identity Proofing shall be limited to identity proofing levels and corresponding authentication requirements. Authorization focused on the actions or activities the public user is permitted after authentication has occurred is outside of the scope of this Standard. This Standard DOES NOT seek to establish or to impose business requirements on agency applications or services, particularly with regard to authorization of a public user. Such requirements are left to the agency and/or the appropriate business unit within the agency to determine.

4.3 Levels Of Assurance

The following Levels of Assurance (LOA) are established for the Commonwealth:

LOA1: Self-asserted identity with little or no confidence in who the *person* behind the identity is. This is the lowest level of assurance and should only be used in circumstances where anonymous logons would be allowed and where the true identity of the person is irrelevant.

Examples of use would include:

- Portal logon to greet returning people
- Dissemination of publicly available information
- Preliminary application or registration for a program where the identity is established at a later step.

LOA2: Identity for which there is some level of confidence in who the *person* behind the identity is. The identity may be verified in a number of ways such as presentation of proofing materials (e.g. driver's license) or something that they have knowledge of (e.g. knowledge-based Q&A). A minimum of user ID and password is sufficient for authentication and shall comply with current Commonwealth password standards (*Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication Standard*). This level is generally sufficient

for most online interactions.

The level of assurance needed is determined by the *highest* impact rating. For example, if five of the categories call for a LOA1, but the remaining one calls for a LOA2, the application would require LOA2.

Example 1: If an application is only serving up publicly available information (e.g., State Park schedules), the likely evaluation of the application is as follows since the information is in the public domain. We can conclude that a LOA1 credential (i.e., no identity verification) is adequate.

Category	**Evaluation**
Inconvenience, distress, or damage to standing or reputation	Low
Financial loss or agency liability	Low
Harm to agency programs or public interests	N/A
Unauthorized release of sensitive or private information	N/A
Personal safety	N/A
Civil or criminal violations	N/A

Example 2: If an application contains background check information, a user wants to know who is trying to access the application and that they are authorized to do so. Financial information, criminal violations, etc. are potentially available in such an application and the user might evaluate it as follows. This would require a LOA3 as determined by the "Unauthorized release…" and "Civil or criminal violations" categories.

Category	**Evaluation**
Inconvenience, distress, or damage to standing or reputation	Mod
Financial loss or agency liability	Mod
Harm to agency programs or public interests	Low
Unauthorized release of sensitive or private information	Mod
Personal safety	N/A
Civil or criminal violations	Mod

The identity verification process and the derived outcome for LOA2 shall be valid for a period of three (3) years from the date of the verification action (effective date). Current LOA and effective date will be stored in the user account record in the Directory.

In determining the appropriate level of assurance to engage for an application or system, the agency must perform a risk assessment and evaluate **the**

potential harm or impact resulting from access by an unverified or erroneous identity as well as **the likelihood** of such harm or impact actually occurring.

Categories of harm and impact include[1]:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive or private information
- Personal safety
- Civil or criminal violations

By assigning potential impact values to these categories – Low, Moderate ("Mod"), High or N/A (if there is no potential impact), the following table can provide guidance as to the necessary level of assurance needed:

Potential Impact Categories for Authentication Errors	**LOA1**	**LOA2**
Inconvenience, distress, or damage to standing or reputation	Low	Mod
Financial loss or agency liability	Low	Mod
Harm to agency programs or public interests	N/A	Low
Unauthorized release of sensitive or private information	N/A	Low
Personal safety	N/A	N/A
Civil or criminal violations	N/A	Low

[1] For an example see, Federal Office of Management and Budget (OMB) M-04-04: *E-Authentication Guidance for Federal Agencies* and Federal Information Processing Standard (FIPS) 199: *Standards for Security Categorization of Federal Information and Information Systems* for detailed discussion.

4.4 Service Description

There are two options to interface agency applications with Keystone Login: Keystone Login Portal and a suite of Keystone Login APIs (Public and Private). The Public APIs are available for integration efforts with SaaS/COTs systems. Keystone Login also offers the ability to login using an existing social media account, such as Google. This is available only by using the Keystone Login Portal, as it cannot be extended through an API.

The following list of functionalities are supported by either option:

Account Creation and Management – Keystone Login allows citizens to create an account in the SRPROD domain and maintain that account by changing account information such as email, mobile phone number, and the Security Questions and Answers used to help recover the account should the citizen forget their username or password. Once their account is created, the citizen can also perform other account management activities such as upgrading their account to a LOA2 verified account (Identity Verification), attach or detach Google social media account (Authentication Services) to their Keystone Login account, and sign-up for Multi-factor authentication (Authentication Services). Keystone Login also allows Commonwealth employees and business partners to authenticate. However, those groups cannot create accounts using Keystone Login, they can only log in.

Authentication – Keystone Login provides this functionality by interacting with the citizen-facing user account domain, and the Commonwealth employee account domain.

Identity Verification – Keystone Login allows SRPROD account owner to verify themselves as LOA2 authenticated accounts. The Commonwealth partners with Experian and the PA Department of Transportation to verify user identities. The account owner can choose either of those options when they decide to elevate their account to LOA2. Agencies can choose, on an application-by-application basis, which of their applications require LOA2 verified accounts.

Keystone Login Authentication Services – Keystone Login allows account owners who have chosen to elevate their accounts to LOA2, to also enable MFA on those accounts. The Keystone Login MFA uses 2 of the 3 Security Questions and Answers, chosen at random, that were created when the account was created. The MFA check is performed at every login.

Single Sign On (SSO) – Keystone Login promotes a Single Sign-On experience by placing a cookie on the user machine. That cookie has a 1-hour lifetime and will allow the user to log into any application that interfaces with Keystone Login and then navigate to other Commonwealth applications without being challenged for credentials again. The user can navigate to non-Commonwealth applications and return to a Commonwealth application and will not be challenged to log in. The user will only be challenged when that 1-hour time has elapsed, if they close their web browsers and then open another instance of the browser, or if they chose to Log Out of Keystone Login

5. Contact

Questions or comments may be directed via email to OA, IT Policy.

6. Exception from Policy

In the event an agency chooses to seek an exception from this policy, a request for a policy exception shall be submitted via the IT policy exception process. Refer to *IT Policy Governance Policy* for guidance.

7. Revision History

This chart contains a history of this publication's revisions. Redline documents outline the revisions and are available to Commonwealth users only during the drafting process.

Version	Date	Purpose of Revision
Original	01/06/2025	Base Document