Delaware Criminal Justice Information System

Standards & Policies

AUTHENTICATION STANDARD

1. POLICY IDENTIFICATION

Document ID	STD-AUTHENTICATION
Revision	1
Effective Date	2022-11-01

2. AUTHORITY

The State of Delaware grants the Delaware Criminal Justice Information System (DELJIS) Board of Managers the authority to draft and promulgate rules and regulations under Del. Code 11 Ch. 86 § 8605. Sections 6.14 and 7.4 of the rules and regulations published on November 1st, 2022 by the Delaware Register of Regulations grants DELJIS the authority to publish standards and policies at https://deljis.delaware.gov/policies.

3. APPLICABILITY

Per sections 6 and 7 of the rules and regulations, the standards and policies may apply to authorized agencies, contractors and all parties interfacing with the Delaware Criminal Justice Information System.

4. DECLARATIONS

Access to DELJIS must be restricted using the authentication methods outlined in this standard.

4.1 END USER ACCESS

Authorized end users must use their CJIS username and password directly with one of the following approved products, indirectly proxying credentials is strictly prohibited.

Name	**Credential**	**Details**
Direct TN3270 Emulator	CJIS username and password	The end user connects directly to the CJIS mainframe environment using a TN3270 terminal emulator with TLS enabled and certificate validation enforced.
Direct application access	CJIS username and password	The end user authenticates directly with a DELJIS desktop or web application on a trusted computer.
CJIS Identity	OAuth Access Token	The end user establishes a session with a DELJIS protected product by authenticating with CJIS Identity using their CJIS credentials.
Software AG EntireX ACI	CJIS Username and Password	Restricted to services operating on the State of Delaware network. This method is prohibited for use with new products and is deprecated for existing applications – a DELJIS granted waiver is required for continued use.
Legacy Authentication Web Service	CJIS Username and Password	Restricted to services operating on the State of Delaware network. This method is prohibited for use with new products and is deprecated for existing applications – a DELJIS granted waiver is required for continued use.

4.2 SERVICE INTERFACE ACCESS

Systems interfacing with CJIS must authenticate themselves, as well as their end users. End users must be authenticated using one of the approved methods provided outlined under Individual Access. Systems must authenticate themselves in accordance with the section 5.1 of the **Service Interface Standard**.

Additionally, services must authenticate the end users interacting with their services either directly or indirectly. The following list enumerates approved authentication mechanisms (unless otherwise noted).

Name	**Credential**	**Details**
CJIS Identity	OAuth Access Token	
Software AG EntireX ACI	CJIS Username and Password	Restricted to services operating on the State of Delaware network. This method is prohibited for use with new applications and is deprecated for existing applications – a waiver is required for continued use.
Legacy Authentication Web Service	CJIS Username and Password	Restricted to services operating on the State of Delaware network. This method is prohibited for use with new applications and is deprecated for existing applications – a waiver is required for continued use.