Delaware Criminal Justice Information System

Standards & Policies

SERVICE INTERFACE STANDARD

1. POLICY IDENTIFICATION

Document ID	STD-SVC-INTERFACE
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 (DELJIS).

4. DEFINITIONS

The following definitions serve to aid readers in understanding the material presented in this publication.

- **TLS** – Transport Layer Security, as defined by the various Internet Engineering Task Force RFC publications.
- **Mutual TLS** (or **mTLS**) – Mutual TLS is a normal TLS connection in which both parties provide an X.509v3 certificate and digital signature to prove their identity to the opposite party.
- **X.509v3** – An ITU standard for the storage of public key certificates. Certificates are signed by special certificate holders, known as authorities, to establish a degree of trust in the holder signed certificate.

5. DECLARATIONS

Services interfacing with the Delaware Criminal Justice Information System repository (CJIS) or other DELJIS systems must be implemented in a manner that protects both parties from outside threats. This standard outlines the approved mechanisms for communicating.

5.1 CONNECTION SECURITY

All connections to DELJIS service interfaces must use one of the following connection modalities. All TLS connections must use at least TLS version 1.2. DELJIS reserves the right to prohibit connections using insecure cipher suites.

5.1.1 MUTUAL TLS CONNECTION

In this modality, one party, the initiator, establishes a TLS connection with the service provider, and both parties are expected to present a signed X.509v3 certificate that identifies them to other party. For services interfacing with DELJIS, the client certificate must be signed by DELJIS.

All new machine-to-machine interfaces must leverage mutual TLS authentication. For the purposes of this document, a machine-to-machine interface is one where the initiator is an automated service and not the end user.

5.1.2 TLS CONNECTION

In this modality, one party, the initiator, establishes a TLS connection with the server. The server presents an X.509v3 certificate that the initiator is required to validate – bypassing certificate validation is strictly prohibited and represents an information security threat.

This modality must be leveraged when the direct initiator is an end user, and a client certificate is unavailable for mutual TLS.

5.1.3 EARLY TERMINATION

All TLS connections to DELJIS service interfaces must be made directly between the authorized initiator and the service interface. This precludes the use of reverse proxies, API gateways or enterprise service buses that terminate the TLS connection.

However, connections may be proxied by products that do not terminate the TLS connection and instead inspect the SNI header to route traffic appropriately – in this circumstance it is vital that network telemetry be maintained (e.g., by using proxy protocol).

5.2 END-USER AUTHENTICATION

The end user must be authenticated using a mechanism approved in the **Authentication Standard** published at https://deljis.delaware.gov/policies. The credentials must be provided to the service interface in accordance with the approved mechanism.