

Law Enforcement Electronic Signature Procedures and Technical Standards

- A. A law enforcement officer who wants to file a document in paper format that has been prepared and signed electronically may do so if his or her law enforcement agency has entered into a memorandum of agreement with the State of Connecticut Judicial Branch permitting such filings.

- B. A document that is prepared and signed electronically by a law enforcement officer and that is to be filed with the Superior Court in paper format must be prepared and signed electronically using a system under the control of the officer's agency that uses the following safeguards and procedures:
 - 1. Each officer must be assigned a unique, unshared set of credentials consisting of a username/ID and password;
 - 2. The log-in process must use active directory authentication;
 - 3. Complex passwords (a minimum of 15 characters is recommended) must be used and expire every year;
 - 4. Network traffic must be encrypted using a minimum of Advanced Encryption Standard (AES) 128 bit encryption;
 - 5. All signature information must be stored on the server, not on the laptop or desktop used by the officer;
 - 6. A PDF copy of the document must be stored in the agency's database once the document is signed; and
 - 7. When signing a document, the officer must:
 - a. Log in using active directory authentication,
 - b. Authenticate each time the officer applies a signature to a document.