

Law Enforcement Electronic Signature Procedures and Technical Standards
(Revised November 1, 2016)

- A. A law enforcement officer who wants to file a document in paper **or electronic** format that has been prepared and signed electronically may do so if his or her law enforcement agency or the agency that supervises the law enforcement officer 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 **or electronic** format must be prepared and signed electronically using a system under the control of the officer's agency or the agency that supervises the law enforcement officer 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;
 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; **and**
 8. **The signature must be placed on the signature line of any document and must contain the signing officer's name surrounded by forward slashes, e.g., "/Trooper Jones/."**
- C. A document that is prepared electronically by a law enforcement officer and that is signed electronically by a person other than a law enforcement officer and that is to be filed with the Superior Court **in paper or electronic format** must be prepared and signed electronically using a system under the control of the officer's agency or the agency that supervises the officer that uses the following safeguards and procedures:
1. The system must comply with the requirements of paragraphs 1-6 of Section B above;
 2. The officer must log in to the system using active directory authentication;
 3. The officer must verify the identity of each individual who signs the document;
 4. The individual signing the document must sign the document under the supervision of the logged-in officer;
 5. The system must retain a record of the officer who supervised the signature of the individual;
 6. The electronic device used to capture the individual's signature must contain minimum touchpad resolution of 400 dots per inch.
- D. Any document that is signed electronically and that is to be filed with the Superior Court **in paper or electronic format** and that requires the administration of an oath by an officer must be in compliance with sections 1-22 through 1-25 of the Connecticut General Statutes.