ICAOS Practice Guide: Electronic Signatures

Electronic signatures have become a convenient and efficient way to sign documents and are legally recognized in every state and US territory. However, the acceptance of an electronic signature may vary depending on the context, the parties involved, and the specific laws of each state. States allow digital signatures and notarization of documents utilizing versions of the Uniform Electronic Transactions Act as well as the Electronic Signatures in Global and National Commerce Act.

The following information is intended to assist Compact offices in navigating the procedures surrounding electronic signatures.

What should a receiving state do when the validity of a signature is questionable, or the electronic signature is unreadable or recognizable?

Present your concerns to the other state prior to rejecting the case. If the other state is unable to validate the signature, try to obtain it through alternate means before rejecting the case.

In general, it is a mark or identifier associated with a document or record and executed by a person with an explicit intent to sign. Legally, this can be as simple as an 'X.'

What best practices can states utilize to prevent confusion on the validity of electronic signatures?

Compact staff should include additional comments in the Transfer Request indicating that the signature is valid and can be referenced by ICOTS users in either the sending or receiving state. Additionally, ICOTS users attest that the form was properly signed and retained when uploading the 'Offender Application for Transfer.'

Have there been any legal challenges to the use of electronic signatures?

With few exceptions, state and federal e-signature rules generally specify that an agreement may not be denied legal effect or enforceability just because it is in electronic form, and that if a signature is required, an electronic signature is sufficient.

Can a receiving state reject a transfer case solely because an electronic signature is obtained remotely?

If the sending state validates the authenticity of the signature, the receiving state should not reject the transfer.

Are there any liability concerns if the receiving state assists in obtaining a signed application?

No, unless there is a specific statutory exception to acceptance and use in the receiving state.

Do you have to be physically present to witness the supervised individual signing the application?

Each state has its own laws that dictate what they are willing to accept in terms of witnessing electronic signatures. Compact offices should refer to the specific requirements outlined in their state's legislation to ensure compliance with state law or consult with their agency's legal counsel.

It is also important to verify the signature's authenticity. This includes implementing measures such as identity verification, ensuring appropriate documentation, and creating a reliable audit trail.

What factors are considered when determining the validity of a witness signature?

It is good practice to confirm with your state's law or legal counsel first. An electronic signature is most likely to be enforceable if it can meet the following requirements:

- The signature can be authenticated and attributed to an individual person.
- The party using the electronic signature "intended" to execute a transaction through that signature on a particular record or document.
- The signature can be associated with a specific record or document.

What if the supervised individual and witness don't sign on the same date?

States may work together to accept it if the states can provide documentation on the circumstances that prevented the witness from signing on the same date and verify that the supervised individual was witnessed when signing. Consult with your state's legal counsel for more guidance when necessary.

Who is responsible for determining the validity of a witness signature?

It is the sending state's responsibility to attest to the validity of documents presented to the receiving state.