

STATE OF MAINE
SUPREME JUDICIAL COURT
AMENDMENT TO
MAINE RULES OF EVIDENCE

2026 Me. Rules 04

Effective: November 1, 2026

All of the Justices concurring therein, the following amendment to the Maine Rules of Evidence is adopted to be effective on the date indicated above. The specific amendment is stated below. To aid in the understanding of the amendment, an Advisory Note appears after the text of the amendment. The Advisory Note states the reason for recommending the amendment, but the Advisory Note is not part of the amendment adopted by the Court.

1. Rule 902 of the Maine Rules of Evidence is amended to read as follows:

RULE 902. EVIDENCE THAT IS SELF-AUTHENTICATING

The following items of evidence are self-authenticating; they require no extrinsic evidence of authenticity in order to be admitted:

....

(13) Certified Records Generated by an Electronic Process or System. A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).

(14) Certified Data Copied from an Electronic Device, Storage Medium, or File. Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).

Advisory Note – November 2026

Subdivision (13) has been added to provide a procedure by which parties can authenticate certain electronic evidence other than through the testimony of a foundation witness. The language of the Rule tracks that of Federal Rule 902(13), which was adopted in 2017. The policy considerations supporting the Federal Rule apply with equal force to Maine. The Advisory Committee Notes to the Federal Rule are thus instructive.

The time, expense and inconvenience of producing a witness to authenticate an item of electronic evidence is often unnecessary. It is often the case that a party goes to the expense of producing an authentication witness, and then the adversary either stipulates to authenticity before the witness is called or fails to challenge the authentication testimony once it is presented. By cross-referencing Rules 902(11) and (12), the amendment provides a procedure under which the parties can determine in advance of trial whether a real challenge to authenticity will be made and can then plan accordingly. The reference to the “certification requirements of Rule 902(11) or (12)” is only to the procedural requirements for a valid certification. There is no intent to require, or permit, a certification under this Rule to prove the requirements of Rule 803(6). Rule 902(13) is solely limited to authentication, and any attempt to satisfy a hearsay exception must be made independently.

A proponent establishing authenticity under Rule 902(13) must present a certification containing information that would be sufficient to establish authenticity were that information provided by a witness at trial. If the certification provides information that would be insufficient to authenticate the record if the certifying person testified, then authenticity is not established under this Rule.

A certification under Rule 902(13) can establish only that the proffered item has satisfied the admissibility requirements for authenticity. The opponent remains free to object to admissibility of the proffered item on other grounds—including hearsay, relevance, or in criminal cases the right to confrontation. A challenge to the authenticity of electronic evidence may require technical information about the system or process at issue, including possibly retaining a forensic technical expert; such factors will affect whether the opponent has a fair opportunity to challenge the evidence given the notice provided.

Subdivision (14) has been added to provide a procedure by which parties can authenticate data copied from an electronic device, storage medium, or an electronic file, other than through the testimony of a foundation witness. The language of the Rule tracks that of Federal Rule 902(14), which was adopted in 2017. The policy considerations supporting the Federal Rule apply with equal force to Maine. The Advisory Committee Notes to the Federal Rule are thus instructive.

The time, expense and inconvenience of producing a witness to authenticate an item of electronic evidence is often unnecessary. It is often the case that a party goes to the expense of producing an authentication witness, and then the adversary either stipulates to authenticity before the witness is called or fails to challenge the authentication testimony once it is presented. By cross-referencing Rules 902(11) and (12), the amendment provides a procedure under which the parties can determine in advance of trial whether a real challenge to authenticity will be made and can then plan accordingly. The reference to the “certification requirements of Rule 902(11) or (12)” is only to the procedural requirements for a valid certification. There is no intent to require, or permit, a certification under this Rule to prove the requirements of Rule 803(6). Rule 902(14) is solely limited to authentication, and any attempt to satisfy a hearsay exception must be made independently.

Data copied from electronic devices, storage media, and electronic files are ordinarily authenticated by “hash value.” A hash value is a number that is often represented as a sequence of characters and is produced by an algorithm based upon the digital contents of a drive, medium, or file. If the hash values for the original and copy are different, then the copy is not identical to the original. If the hash values for the original and copy are the same, it is highly improbable that the original and copy are not identical. Thus, identical hash values for the original and copy reliably attest to the fact that they are exact duplicates.

This amendment allows self-authentication by a certification of a qualified person that they checked the hash value of the proffered item and that it was identical to the original. The Rule is flexible enough to allow certifications through processes other than comparison of hash value, including by other reliable means of identification provided by future technology. A proponent seeking to establish authenticity under this Rule must present a

certification containing information that would be sufficient to establish authenticity were that information provided by a witness at trial. If the certification provides information that would be insufficient to authenticate the record if the certifying person testified, then authenticity is not established under this Rule.

A certification under this Rule can establish only that the proffered item has satisfied the admissibility requirements for authenticity. The opponent remains free to object to admissibility of the proffered item on other grounds—including hearsay, relevance, or in criminal cases the right to confrontation. A challenge to the authenticity of electronic evidence may require technical information about the system or process at issue, including possibly retaining a forensic technical expert; such factors will affect whether the opponent has a fair opportunity to challenge the evidence given the notice provided.

Dated: October 8, 2026

FOR THE COURT,*

_____/s/_____
VALERIE STANFILL
Chief Justice

ANDREW M. MEAD
CATHERINE R. CONNORS
RICK E. LAWRENCE
WAYNE R. DOUGLAS
JULIA M. LIPEZ
CHRISTOPHER C. TAUB
Associate Justices

* This Rule Amendment Order was approved after conference of the Court, all Justices concurring therein.