



Minnesota Judicial Branch Request for Information on eSignature Services

Introduction

The Minnesota Judicial Branch (MJB) is interested in electronic signature (eSignature) services. As a first step in identifying an eSignature tool, along with an integrated service for eSignature, the MJB is issuing this Request for Information (RFI) on available commercial software, dynamic hosting service, licensing, authentication and support for such a tool. This RFI will not result in a contract but the information obtained from responders may provide a basis for further contractual considerations and/or procurement. All interested parties must provide information and a demonstration to the RFI as a qualification to make a bid on a future Request for Proposal (RFP) concerning an eSignature tool. There is no guarantee that any such further contract or procurement process will be issued.

The MJB is not obligated to respond to any submission, nor is it legally bound in any manner whatsoever by the submission of a response. The MJB shall not have any liability to any responder for any costs or expenses incurred in connections with this RFI or otherwise. Any amendments to this RFI will be posted on the MJB website (www.mncourts.gov).

Purpose

The MJB is in the process of implementing an electronic information environment in which active and new cases will be eFiled, and judges and court staff will primarily utilize electronic records for court services. The MJB currently uses Tyler Technology's Odyssey Case Management (Odyssey) system in all trial courts throughout the state. The MJB seeks to augment its statewide electronic business processes with an eSignature solution that will utilize the active directory for internal Single Factor or Two-Factor authentication. Future plans may also require external partner Multi-Factor Authentication. (Please see Appendix A – MJB Policy 702(a), Standard for Electronic Signatures in Court Proceedings.)

This RFI asks vendors to describe their eSignature product, and demonstrate their ability to meet the MJB eSignature needs.

Background

Odyssey has been in place in all trial court locations throughout Minnesota since early 2008. At this time the MJB is focusing on process improvement and efficiency strategies that will enable the MJB to conduct its business through electronic rather than paper based processes.

The MJB is looking for an economical eSignature solution that will initially enable users; judicial officers and court administration, to electronically sign all types of documents in various locations, including on-site and on-the-go. The signing process should be simple and require no, or very few additional steps compared to the process for signing paper documents. The preferred eSignature solution should also provide the ability to pass documents between users to accommodate multiple signatures on single documents, allow for multiple user personas, and utilize on premises storage.

The MJB has approximately 3,000 users, who will need the ability to access and use the eSignature capabilities. Once successfully implemented, the product will be tested in a small number of court locations, with eventual deployment statewide.

Goal

It is the goal of this RFI to identify vendors capable of providing the required eSignature services using the required approach, and to understand the licensing options and costs associated with acquiring the services.

Scope of Information Requested

Vendors are asked to provide the following:

1. A demonstration of their eSignature product and all available add-ons.
2. Product specifications Alternatives for technical environments that will be available to the state, including options for hosting the application at either a court site or a vendor site.
3. Information concerning the available licensing options, and related costs.
4. Information concerning how the product is supported:
 - a. Does the vendor staff a Help Desk?
 - b. What is the ratio of Help Desk staff to customers?
 - c. Are requests for assistance generally cleared by one interaction with the Help Desk?
 - d. Do you offer implementation assistance and/or training assistance?
5. Information documenting whether the vendor has the resources and capacity to implement the project under potentially short deadlines.
6. References from customers who have had the required solution in place in Production for at least 90 days.

Vendors may be invited to provide a product overview and demonstration based upon the information provided in the response to the RFI. A representative of the State Court Administrator's Office (SCAO) will contact vendors to schedule demonstrations. The MJB reserves the right to cancel appointments if the vendor's product is deemed to be unacceptable, or if conflicts in scheduling occur.

Disposition of Responses

All vendor submissions are due by the close of business on Wednesday, October 10, 2012. Materials submitted in response to this RFI become the property of the MJB. Costs associated with preparation of material for the response are the responsibility of the submitter.

The [Rules of Public Access to Records of the Judicial Branch](#) protect vendor submissions that include trade secret information as follows:

- (b) *Submission of Trade Secret.* Except as provided in subparagraph (c) of this subdivision, a common law trade secret or a trade secret as defined in MINN. STAT. § 325C.01 that is required to be submitted in accordance with a judicial branch bid or procurement request provided that:
 - (1) the submitting party marks the document(s) containing the trade secret “CONFIDENTIAL;”
 - (2) the submitting party submits as part of the bid or response a written request to maintain confidentiality; and
 - (3) the trade secret information is not publicly available, already in the possession of the judicial branch, or known to or ascertainable by the judicial branch from third parties.

Except for information submitted in accordance with this section on Trade Secrets, do not include any information in your response that you do not want revealed to the public. Please also note that if a responder at any time eventually ends up with a contract with the judicial branch, the following information will also be accessible to the public: the existence of any resulting contract, the parties to the contract, and the material terms of the contract, including price, projected term, and scope of work.

Questions

Responders may submit questions to Kim Larson at kimberly.larson@courts.state.mn.us. Responses will be posted in the Public Notices section of the Minnesota State Court web site (<http://www.mncourts.gov>) as soon as possible after the question is received.

Minnesota Judicial Branch Policies and Procedures

Policy Source:	State Court Administrator
Policy Number:	702(a)
Category:	Technology
Title:	Standard for Electronic Signatures in Court Proceedings
Origination Date:	12/12/2008
Revision Date:	5/20/2011
Effective Date:	7/1/2011
Contact:	Director of Information Technology

Standard for Electronic Signatures in Court Proceedings

I. PURPOSE

The purpose of this Standard is to ensure the integrity of electronic instruments in connection with court proceedings. This Standard sets forth the current minimum standard for applying electronic signatures by Minnesota Judicial Branch judges and court personnel to electronic instruments used in connection with court proceedings, when electronic signatures are authorized by supreme court rules or orders. The Standard also establishes reporting requirements for Judicial Districts with regard to proposing products for use under this Standard. This Standard is not a source of authority to use electronic signatures; it merely sets a minimum standard for electronic signatures when they are otherwise authorized by supreme court rule or order.

II. DEFINITIONS

- a. "Audit Data" means data that is required to be collected as part of the Current Minimum Standard set forth herein. The purpose for including Audit Data in the Current Minimum Standard is to provide a meaningful audit trail of Electronic Signatures applied by Minnesota Judicial Branch judges and court personnel.
- b. "Authentication" means to systematically verify a person's identity as authentic or valid.
- c. "Biometrics" means the discipline of computer science that involves uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.
- d. "Digital Signature" means an Electronic Signature that uses asymmetric cryptography and a third party for validation.
- e. "Electronic signature" means an electronic or digital method of signing an electronic instrument and identifying a particular individual as the source of the signature. This includes a broad range of methods, from a mere typed signature to an attached signature image to a user ID/password as a signature to a Digital Signature. This term is defined broadly so that it may be used now and in the future as technologies change for applying signatures to electronic instruments.¹

¹ This definition is from the Minnesota Judicial Branch Enterprise Technology Architecture Governance.

- f. “Single-Factor Authentication” means Authentication using a single factor, such as a password, together with a user ID that identifies the person being authenticated. For example, if a password is used as the single factor, it must be used with a user ID to identify the person providing the password. It should be noted that the user ID referenced in this definition is a required component but is not considered a “factor.”²
- g. “Two-Factor Authentication” means Authentication using two independent factors, such as a password and a biometric identifier, together with a user ID that identifies the person being authenticated. The second factor does not have to be biometric data; it can be a smart card, RSA token, or other industry-recognized type of factor. For example, if a password is used as the first factor together with a network ID to identify the person being authenticated, a fingerprint may be used as a second factor (together with a network ID), to accomplish Two-Factor Authentication. It should be noted that the user ID referenced in this definition is a required component of Authentication but is not considered a “factor.”³
- h. “Multi-Factor Authentication” means Authentication using three or more factors. See definitions of Single-Factor Authentication and Two-Factor Authentication, above.

III. APPLICABILITY

This Standard is applicable to Electronic Signatures applied by Minnesota Judicial Branch judges and court personnel in connection with court proceedings. It does not apply to Electronic Signatures used in any other context, such as administrative or personnel matters. This Standard may also apply to other Electronic Signatures as authorized by Supreme Court Rule or order.

IV. AUTHORITY

Under the implementation authority of Judicial Council Policy 7.00, *Technology Use & Strategy*, the State Court Administrator hereby sets forth its Standard for Electronic Signatures in Court Proceedings. This Standard is hereby made part of the Security Domain of the Enterprise Information and Technology Architecture, as described by Judicial Council Policy 7.00.

This policy may be waived as provided herein (see section VI, below).

² Ibid.

³ Ibid.

V. CURRENT MINIMUM STANDARD

The following minimum Standard must be met for all electronic signatures governed by this policy:

This Standard includes all three parts listed below:

Authentication: *An Electronic Signature of a particular individual may be applied by that individual to an electronic instrument using various methods but Single-Factor Authentication is the minimum form of Authentication at the time an Electronic Signature is applied. Two-Factor Authentication or Multi-Factor Authentication may also be used and is encouraged.*

Audit Data: *The following Audit Data must be captured at the point in time when an Electronic Signature is applied to an electronic instrument: date, time, and the user ID that was used for Authentication. This set of Audit Data is required for each Electronic Signature applied to an electronic instrument and must be retained for the life of the signed instrument. Additional Audit Data may also be captured and is encouraged.*

Preservation and Retention of Content of Signed Instrument: *When an Electronic Signature is applied to an electronic instrument, the original content of such instrument at the time of Electronic Signature must be preserved and retained for the life of the signed instrument.*

VI. WAIVER

This Standard may be waived by written directive of the State Court Administrator or by Supreme Court rule or order.

VII. REPORTING REQUIREMENTS FOR JUDICIAL DISTRICTS

Judicial Districts are required to report to the Director of the Information Technology Division any product proposed for use under this Standard, accompanied by a detailed technical explanation as to why such product meets this Standard. Within 30 days of receiving a district report, the Director of the Information Technology Division will either affirm compliance with the Standard or challenge the use of the product and request collaboration with the Judicial District to perform additional testing and provide appropriate documentation. This paragraph has no effect on the Minnesota Judicial Branch procurement process.


VIII. RELATED DOCUMENTS

- Judicial Council Policy 7.00, *Technology Use & Strategy*
- Judicial Branch Enterprise Information & Technology Architecture, including the Security Domain
- Rule 1.06 of the Rules of Criminal Procedure
- Report and Proposed Amendments to the Minnesota Rules of Criminal Procedure (Aug. 29, 2008).
- Order Amending E-Filing Pilot Project, ADM10-8011 (Minn. S. Ct. filed March 10, 2011)

IX. REVISION HISTORY

Date	Description
12/12/2008	Original Standard issued.
5/20/2011	Revised definitions in Section II; revised Section III to clarify that this Standard applies to the application of Electronic Signatures by Minnesota Judicial Branch Personnel; modified the Current Minimum Standard in Section V; added a new Section VI; and renumbered the remaining Sections to accommodate the insertion of the new Section VI.

Approval:



State Court Administrator Signature

May 20, 2011
Date