CROMERR Application Cover Sheet

Non-Federal: ☒ State Environmental Agency ☐ Tribe ☐ Local Government Agency

Federal: ☐ EPA Program Proposal ☐ EPA Program Conformance Plan

Please do not use acronyms when completing this form

Primary Contact Information			
First Name: Leslie	Last Name: Goldsmith	Position: Data Analysis Operations Division	Agency: Minnesota Pollution Control Agency
Mailing Address (Street Address, Mail Code/Suite, City, State, Zip Code): 520 Lafayette Road North St. Paul, MN 55155-4194		E-mail: leslie.goldsmith@state.mn.us Fax: 651-296-7782	Primary Phone: 651-757-2393 Secondary Phone:

Secondary Contact Information			
First Name: Randy	Last Name: Hedegaard	Position: Manager, Operations Division	Agency: Minnesota Pollution Control Agency
Mailing Address (Street Address, Mail Code/Suite, City, State, Zip Code): 520 Lafayette Road North St. Paul, MN 55155-4194		E-mail: randy.hedegaard@state.mn.us Fax: 651-297-2343	Primary Phone: 651-757-2781 Secondary Phone: 651-261-6950

This application addresses/includes *(check or complete all that apply)*:

☒ Priority Reports ☒ Non-Priority Reports ☒ New Systems ☐ Existing Systems

☒ The OEI CROMERR application checklist is used for this application

1 Number of systems addressed in this application

Certifying Official			
☒ Certification of sufficient legal authority to implement electronic reporting by: Michelle Beeman			
First Name: Michelle	Last Name: Beeman	Title: Deputy Commissioner	Certification Date: 6/9/14
☒ Copies of relevant laws and regulations establishing legal authority are included			

CROMERR System Checklist	
Item	
Registration (e-signature cases only)	
1. Identity-proofing of registrant	
	Business Practices: Minnesota Pollution Control Agency (MPCA) utilizes a Subscriber Agreement (SA) process to satisfy identity proofing requirements, as follows: -Potential submitters create user accounts in the MPCA e-Services system, including a User ID, Password, and Challenge Questions. Users create a certification Personal Identification Number (PIN). -The authority to submit and/or sign priority reports electronically via MPCA e-Services must be approved by the MPCA. Approval is requested and granted by: • The Responsible Official (RO) obtains an e-Services account with the MPCA. • The RO selects the names(s) and facility ID numbers for which signature authority is being requested. • Create a formal SA containing the facility information. • Include the name(s) of any person(s) who will be designated as "duly authorized representatives (DAR)" for signature purposes. • Obtain the hand written signature(s) of any DAR listed. • Submit via mail or hand delivery the original form with original wet ink handwritten signatures. -The SA is received in hard copy form, by mail or other traditional means of hard copy submittal. The MPCA e-Services staff reviews signed SAs for completeness and correctness. -If the SA is complete and correct, then the MPCA e-Services Administrator establishes the RO's authority to sign submittals by verifying that the RO meets the criteria documented in the associated regulation for each facility for which security to electronically sign/submit data is requested. This process may include reviewing MPCA's electronic records and/or paper files for each facility, which may include information from prior permit applications and permits to determine whether the requestor's relationship to the facility as the RO is documented. This process may also include direct contact with the facility when necessary to determine the appropriate signatory. If the MPCA determines the requester does not meet the criteria as the RO, then the SA is rejected and security access to electronically sign/submit data is not granted to the requester or any delegated representatives named in the document. -The requester is granted the role of RO, which includes security access to electronically sign/submit data, the authority to delegate a DAR, and the ability to authorize individuals access to prepare documents only for the facilities for which the requester meets the criteria. -If MPCA is able to verify the requestor's relationship as the RO and authority to sign, then the MPCA e-Services Administrator establishes each named delegated representative authority to sign reports or documents by verifying that they meet the criteria documented in the associated regulation (following the same business process as for the RO) for each facility for which security to electronically sign/submit data is requested. If MPCA determines the delegated representative should not be granted, then (assuming the RO met the criteria) the SA is accepted but security access to electronically sign/submit data is not granted to that delegated representative. -If MPCA determines the delegated representative meets the criteria for some facilities but not others, then the delegated representative is granted security access to electronically sign/submit data for the facilities for which the delegated representative meets the criteria and not for the others.

CROMERR System Checklist	
	Business Practices: (cont.) -Each SA is scanned and archived in the MPCA's Electronic Document Management System (EDMS). MPCA's records in the EDMS are the Official File of Public Record and the SA in the EDMS is protected under the same security of all of MPCA's Official Files of public record. The SA is never purged or removed from this system. These hard copy files are maintained and stored in an off-site MPCA archival room. Access is monitored and access is limited to MPCA staff only. As part of the Official File of Public Record, these documents are available for public viewing under the same security measures of all Official Files of Public Record. Any viewing of the public record is submitted by a Freedom of Information Act (FOIA) request. The public does not have access to the MPCA documents. Files are viewed by MPCA authorized staff and the public may view the documents when they are retrieved by MPCA staff. A copy of MPCA's Electronic Signature User Agreement has been provided as Attachment 1. This allows MPCA to restrict such security to only those ROs and delegated representatives for whom it has verified identity and authority to sign reports and documents. For the services which are not listed In the CROMERR rule as priority reports, identity proofing is accomplished using the information provided in the registration process. For these "non-priority" services the system assigns authority to the registered user to enter the information for the report for which they registered.
	System Functions: MPCAs e-Services system allows potential submitters to establish user accounts and create certification PINs; however, system security prevents such users from electronically signing/submitting data until the MPCA Data Administrator grants RO or delegated representative security to the user's account. Users registering for an MPCA e-Services account must enter personal information that identifies who they are and how they can be contacted. Users will be required to enter their Name, E-Mail, Phone Number, and Mailing Address. A user may change their personal information at any time; however, to protect the integrity of a previously granted user's identity the MPCA e-Services will allow users to modify their First or Last Name after account creation. User generated PIN's are stored in the MPCA e-Services database after being obfuscated by hashing it using the SHA message digest algorithm and then converting the digest to hexadecimal format. While users with lesser security credentials can enter data for priority reports, only Responsible Officials or DAR can electronically sign reports. As described in Business Practices, an MPCA e-Services Administrator will grant RO access after reviewing the SA for accurateness. The MPCA e-Services will provide an online screen for MPCA e-Services Administrators to review and grant pending access requests. In addition to all functions above, the MPCA e-Services will incorporate a second-factor approach (e.g., 20-5-1 question/answer validation) to the e-signature captured during certification. More information on this approach can be found under requirement 13.
	Supporting Documentation (list attachments): The following document provides additional detail about MPCA's approach to meeting identity proofing requirements: Attachment 1 - Signature Agreement (SA). The MPCA requires submitters to provide a signed SA prior to receiving security access to submit electronically signed data via the MPCA e-Services system. This document establishes the identity of potential submitters.

CROMERR System Checklist	
1a. (priority reports only) Identity-proofing *before* accepting e-signatures	
	Business Practices: As described in response to requirement #1, MPCA does not grant a potential submitter security access to electronically sign/submit data using the MPCA e-Services system until the SA is complete, correct, and MPCA has verified the individual's authority to sign/submit data for the requested facility. In conjunction with system security features that prevent users without appropriate access from signing/submitting, this meets the requirement that identity-proofing occur before accepting e-signatures.
	System Functions: As described in response to requirement #1, MPCA e-Services system prevent users from electronically signing/submitting data unless they have been granted security access to do so for the specific facility for which the report or document is being submitted. If the MPCA or the RO has granted the user access to the facility, then the user will be unable to proceed with viewing, entering, or certifying data with the facility. If MPCA has configured the facility within the MPCA e-Services system and MPCA or the RO has granted the user access to the facility, but MPCA has not granted the user security to electronically sign/submit data, then the system will prevent the user from certifying the submittal. In the MPCA e-Services, the user, because of their security settings, will not have the option to certify the data and must notify the appropriate party at that point to perform the certification. In conjunction with MPCA's business process to not grant such security until identity and authority have been verified, this meets the requirement that identity-proofing occur before accepting e-signatures. Users are able to view the status of their access when they are logged into their MPCA e-Services account. Their workspace will display the facilities they have access to, the highest level of access they have to the facility and the status of whether that access is granted or pending.
	Supporting Documentation (list attachments): See requirement #1.
1b. (priority reports only) Identity-proofing method (See 1bi, 1bii, and 1b-alt)	
1bi. (priority reports only) Verification by attestation of disinterested individuals	
1bii. (priority reports only) Information or objects of independent origin	
	Business Practices: An individual accessing the MPCA e-Services can download and print the SA form and will take the downloaded form to a public notary. Once the notary has verified the information and determined the person completing the request is the person presenting it to the notary, the user should sign the SA in the presence of the notary and the notary should sign and attach their seal to the document. The user then mails or hand delivers the SA to the MPCA for manual review and processing.
	System Functions: The individual must first establish an account at the MPCA e-Services. At this point the user has access to several services including account management and PIN acquisition. The PIN acquisition service includes prompting the user for the information that is part of the SA and asking the user to create five security challenge questions and provide answers for each. The security challenge questions and answers are encrypted and stored in the internal, physically secure database. This information is not associated with an account at this point. The user prints the downloaded SA, without the security questions, and takes the agreement to a public notary.

CROMERR System Checklist	
	Supporting Documentation (list attachments):
1b-alt. (priority reports only) Subscriber agreement alternative	
	Business Practices: As described in response to requirement #1, MPCA pursues a SA approach to identify-proofing. The SA described previously functions as the MPCA's SA. See Attachment 1 for a copy of MPCA's SA. An electronic image of the paper copy of each accepted SA is stored in MPCA's EDMS. MPCA's document retention policy does not allow disposal of such documents, which meets the requirement that the SA be retained at least 5 years after the deactivation of the electronic signature device. MPCA does not authorize or allow Local Registration Authorities. All SAs are processed by MPCA.
	System Functions: See the response to requirement #1.
	Supporting Documentation (list attachments): See requirement #1.
2. Determination of registrant's signing authority	
	Business Practices: As described in response to requirement #1, potential submitters complete a SA requesting access to electronically sign/submit data for specified facilities. Completion of the SA requires each potential signatory to review the definition of the requested role (i.e., RO, DAR) and attest with a handwritten signature to the fact that they meet the criteria for the requested role. Additionally, MPCA e-Services Administrator collaborates with MPCA's program staff to confirm the authority of each potential submitter (RO or delegated representative) by verifying that the potential submitter meets the criteria documented in 40 CFR § 122.22. This process may include reviewing MPCA's records for each facility, which may include information from prior permit applications and permits to determine whether the RO or delegated representative's relationship to the facility has previously been established. If MPCA cannot verify the potential submitter's authority to sign/submit data for a facility, then MPCA does not grant that potential submitter's user account security access to do so. Refer to 1 for MPCA's business processes for verifying the potential submitters' signing authority. Refer to 14 for process for revoking signing authority. Each MPCA e-Services RO is responsible for management of their facility's users and security rights including revoking signing authority.
	System Functions: As described in response to requirement #1, security access controls are used to prevent individuals from electronically signing/submitting data unless their user accounts have been granted appropriate security access. By Standard Operating Procedures (SOP), the MPCA does not grant such access until it has verified the individual's authority to sign the submittal.
	Supporting Documentation (list attachments): See Attachment 1 - Signature Agreement (SA)

CROMERR System Checklist	
3. Issuance (or registration) of a signing credential in a way that protects it from compromise	
	Business Practices: In order to obtain security access to electronically sign/submit data, potential submitters must submit a SA that has been signed with a handwritten signature (as described in response to requirement #1). Each individual with signing authority must sign a SA and create their own individual account with their unique combination of User ID, Password, Challenge Questions, and will create their own unique PIN from the system. By signing this document, each potential submitter agrees to not share his/her User ID, Password, Challenge Questions and Answers, and PIN with any other person, to protect these signing credentials at all times, to change their password and request a new PIN immediately upon becoming aware of its compromise, and to report any evidence of compromise to MPCA. A copy of MPCA's SA that shows the conditions to which a potential submitter must agree prior to obtaining security access to electronically sign/submit data has been provided as Attachment 1. In combination with the system security measures described in the following section, this business process protects the PIN from compromise.
	System Functions: In MPCA e-Services system, a User ID, password, certification PIN, and a second-factor validation (e.g., 20-5-1 question/answer validation) comprises the signing credential. The following bullets describe the initial issuance process: • Potential submitters create user accounts in MPCA e-Services system by following the "Create a new account" prompt on the User Login page, entering required information on the User Profile page, and clicking the "Submit Request" button. This process includes choosing a User ID and password and creating a certification PIN. In addition, this process will incorporate a second-factor security approach for the signing ceremony. See requirement #13 for more information. • The User ID must be unique within the MPCA e-Services system. The MPCA e-Services system will give the system an error message if the selected User ID already exists. The User ID must be between 6 and 40 characters. The User ID is displayed on the screen as it is entered by the potential submitter, is displayed in the page header while the user is logged onto the system, and may be known by MPCA employees or other facility personnel; this User ID comprises the "public" part of the credential. The User ID is permanent to an account and cannot be changed by the user. • The Password does not need to be unique within the system. The Password must be a minimum of 6 characters in length and contain at least 1 letter and 1 number. The Password is hidden from view as it is entered by the potential submitter, and is never displayed in the system. Users have the ability to change their Password from within MPCA e-Services. In order to change a Password, the user must enter their old and new Passwords. The same restrictions also apply during change Password as they do during create account in terms of length and containing a letter and number. Password is used for login credentials, while it is the combination of the unique User ID, PIN, and a second-factor approach that comprise the signing credential. If the password is changed by the system (an "I lost my password" scenario) an e-mail is sent to the user notifying them of the new password.

CROMERR System Checklist

System Functions: (cont.)

• The user will be required to select 5 out of 20 Challenge Questions when creating their account. The Challenge Questions and Answers do not need to be unique within the system. Once established during account creation, the questions and answers are never displayed by the system. It is the combination of the unique User ID, the (potentially non-unique) PIN, and a Challenge Question and Answer that comprise the signing credential. The PIN and the Challenge Question and Answer comprise the "private" component of this credential. Users will be unable to change their Challenge Question and Answers online. If a user forgets the answers, they must contact MPCA. MPCA staff does not have access to view a user's PIN or Security Answers since these values are encrypted. MPCA will send an e-mail to the user via the e-mail address on record for that user stating the date on which the request to reset challenge questions was made, that the challenge questions were reset, and that the user should immediately contact the MPCA if they did not make the request. Once MPCA deletes the security answers from their profile, upon logging into the MPCA e-Services system the user will be prompted to set up their Challenge/Response Questions again.

• The PIN does not need to be unique within the system. It is the combination of the unique User ID, the (potentially non-unique) PIN, and a second-factor approach that comprise the signing credential. The user generated PIN and the second factor comprise the "private" component of this credential. This PIN is not known by or shared with MPCA employees or other parties. The PIN is a 6 character alphanumeric string. It is hidden from view as it is entered by the potential submitter, and is never displayed within the system.

In addition to such system features, business processes are also employed to keep the PIN secret (as described in the Business Practices section for this requirement).

• Once the potential submitter has selected a User ID, completes the second-factor security procedures, and creates a PIN, he/she can complete the account creation process. At this time, the User ID, Challenge Questions and Answers, and PIN are transferred from the potential submitter's web browser to the web server and then to the application server and ultimately the database server. MPCA e-Services system utilizes SSL version 3.0 to protect the User ID, Challenge Questions and Answers, and PIN from compromise during transfer from the web browser to the web server. Transfer from the web server to the application server and then to the database server occurs behind a secure firewall, which also protects the User ID, Challenge Questions and Answers, and PIN from compromise during transfer.

• To protect the Challenge Answers and PIN from compromise once it reaches the database, the Challenge Answers and PIN are obfuscated by hashing each using the SHA message digest algorithm and then converting the digest to hexadecimal format. Each byte of the Challenge Answers and PIN is adjusted by its corresponding byte position in the cipher. The Challenge Answers and PIN are ultimately stored in the database in this encrypted format. MPCA's database administrators also employ standard Oracle database security features to restrict read and write access to the table in which the Challenge Answers and PINs are stored in the MPCA e-Services application.

The MPCA e-Services system also supports changing and resetting PINs. The following bullets describe these features:

• If the user forgets his/her PIN, he/she can request a new PIN by clicking the "Forgot Certification PIN?" link on the Certification page and clicking "Request PIN" or by going to their User Profile. The user then answers challenge questions and creates a new PIN.

• If the user suspects compromise, he/she can request a new PIN by navigating to the User Profile page and choosing to 'Request PIN'. Protection of the new PIN during transfer and storage is covered by the same security as is used for initial PIN issuance.

CROMERR System Checklist	
	System Functions: (cont.) • If the user changes the email address registered to their account, then they are forced to create a new PIN. The system maintains a record of the unique user ID, encrypted password, PIN and challenge questions associated with each user. This record is maintained using industry standard encryption techniques and is kept indefinitely.
	Supporting Documentation (list attachments): See Attachment 1 - Signature Agreement (SA).
4. Electronic signature agreement	
	Business Practices: As described in response to requirement #1, MPCA requires submitters to provide a signed SA prior to receiving security access to electronically sign/submit data using the MPCA e-Services system. In order to obtain security access to electronically sign/submit data, potential submitters must submit a SA that has been signed with a handwritten signature. Each individual with signing authority must sign a SA and create their own individual account within their unique combination of User ID, Password, Challenge Questions, and will create their PIN in the system. By signing this document, each potential submitter agrees to not share his/her User ID, Password, Challenge Questions and Answers, and PIN with any other person, to protect these signing credentials all times, to change their password and request a new PIN immediately upon becoming aware of its compromise, and to report any evidence of compromise to MPCA. MPCA provides a phone number and email address to report a compromise of their signature. A copy of MPCA's SA that shows the conditions to which a potential submitter must agree prior to obtaining security access to electronically sign/submit data has been provided as Attachment 1.
	System Functions: N/A. Submittal of SA is handled as a manual process.
	Supporting Documentation (list attachments): See Attachment 1 - Signature Agreement (SA).
Signature Process (e-signature cases only)	
5. Binding of signatures to document content	
	Business Practices: N/A. Binding of the signature to the document content is accomplished via system functions.
	System Functions: The submitter electronically signs each submittal by entering the User ID and password, completing the second-factor authorization (e.g., 20-5-1 question/answer validation) and clicking "Submit," and then entering the certification PIN and clicking "Certify" on the Certification page for the given submittal. These actions initiates the following processing below. Note that after 30 minutes of inactivity at any point during a user's session, they will be timed out and logged off the system. The length of time before timeout is also configurable by MPCA. -A Challenge Question will be presented to the user when they are directed to the Certification page; Java's Random class will be used to generate the Challenge Question at random. On submitting the Answer to the Challenge Question, the User ID and Challenge Question and Answer are transferred from the web browser to the web server and then to the application server, where the Challenge Answer is encrypted as described in response to requirement #3.

CROMERR System Checklist	
	System Functions: (cont.) The encrypted Challenge Answer is then compared to the encrypted Challenge Answer in the database for the specified User ID and Challenge Question. If the encrypted Challenge Answers do not match, then the system gives an error message and prevents certification from continuing. If the encrypted Challenge Answers match, the system proceeds with the certification processing described in the next step. The User ID, Challenge Question and Answer are protected during transfer from web browser to web server by SSL version 3.0. Subsequent processing is performed behind a secure firewall. See requirement #13 for more information on the second-factor authorization. -If the encrypted Challenge Answers match, then the user enters their Certification PIN and the system performs validation, The User ID and PIN are transferred from the web browser to the web server and then to the application server, where the PIN is encrypted as described in response to requirement #3. The encrypted PIN is then compared to the encrypted PIN stored in the database for the specified User ID. If the encrypted PINs do not match, then the system gives an error message and prevents certification from continuing. If the encrypted PINs match, the system proceeds with the certification processing described in the following steps. The User ID and PIN are protected during transfer from web browser to web server by SSL version 3.0. Subsequent processing is performed behind a secure firewall. -The system then stores a certification history record to the database to cross-reference the electronic signature information to the Copy of Record (COR). This record will capture specific information about the certification such as the certifying User ID, Challenge Question, encrypted Challenge Answer, encrypted Certification PIN, certification date/time, certification statement, certification confirmation number, submittal ID, and the filename of the COR zip file. Note, that the COR will always be stored to the file server in zip file format. If attachments were submitted, these will be included as part of the zip file along with the PDF version of the COR. If attachments were not submitted, then just the PDF version of the COR will be included in the zip file. Information is protected during transfer from web browser to web server using SSL v 3.0. Subsequent transfers occur behind a secure firewall. The database table that stores this information is not updateable via the front-end MPCA e-Services application, and access via the back-end is restricted to system administrators using standard Oracle database security features. The COR table will also include database triggers to provide an audit if any change is made to the table. -The system generates a PDF COR of each certified/submitted report or document using PD4ML version 3.51. The PDF COR is in human-readable format and includes the unique User ID, encrypted password, and encrypted challenge questions /answers, certification statement, and certification date/time. The PDF and any attachments uploaded to the submission are zipped to a Zip File, hashed using a SHA-256 algorithm, and are saved to the MPCA EDMS. - In the case of a submittal requiring multiple signatures, multiple records will exist in the database, bound to the same COR. The PDF COR will contain all signatures made for the submittal. -The MPCA EDMS in which the COR is stored is designed in such a way that any changes to a document would create a new document with new metadata associated with it. This metadata includes a time stamp which would enable MPCA to detect when and who attempted to change the document. In fact no one is able to change a document within the system. There are 2 to 3 database Administrators which have the ability to remove a document from the system but even then the fact the document was removed would be recorded in the system. The directory is backed up 5 nights a week. There are database measures of comparing hash values to determine if alterations occurred to a COR. COR and Data are stored per the State of Minnesota approved retention schedule which, for this type of data, is permanently.
	Supporting Documentation (list attachments):

CROMERR System Checklist	
6. Opportunity to review document content	
	Business Practices: N/A. Electronic signing/submittal must occur during an on-line session so information related to this requirement is provided in the System Functions section.
	System Functions: Electronic signature/submittal is performed during an on-line session within MPCA's e-Services system. The following bullets describe applicable system functions: • When an authorized user is ready to electronically sign/submit a report or document, he/she navigates to the Certification page for the particular submittal. This page displays the certification statement and a view of the data to be signed/submitted as part of the transaction. On this page, the user may be required to enter his/her User ID and Password, the second-factor authorization requirement (e.g., an answer to a randomly generated Challenge Question), certification PIN, and click "Certify" to electronically sign and submit the report or document information displayed. In addition to the data entered as part of the submittal, the certification statement, the name of the certifying party as stored in the MPCA e-Services user's profile, and the date of the certification are also displayed. • When an authorized user has electronically signed/submitted the report or document, he/she will be emailed a PDF of the COR. This COR will be sent to each certifier as part of their signing procedure. The COR will be a view of the data displayed on the Certification page and will also contain the certification statement, the name of the certifying party as stored in the MPCA e-Services users' profile, and the date of the certification.
	Supporting Documentation (list attachments): See Attachment 2 - Display Prior to Certification - this attachment provides an example of the submittal data that is displayed prior to certification.
7. Opportunity to review certification statements and warnings	
	Business Practices: N/A. Electronic certification/submittal must occur during an on-line session so information related to this requirement is provided in the System Functions section.
	System Functions: Electronic signature/submittal is performed during an on-line session within MPCA e-Services system. The following bullets describe applicable system functions: • When an authorized user is ready to sign/submit a report or document, he/she navigates to the Certification page for the particular submittal. This page displays the certification statement, which includes language warning that there are significant penalties for submitting false information, including the possibility of fine or imprisonment. • Clicking "Certify" on this page indicates agreement with the certification statement. • Alternately, the user can click the "Cancel" button or close the browser to cancel the certification process. Users can navigate back to the in-progress submittal to make any desired edits. Note that the Certification statement text is stored as data in the MPCA e-Services database, allowing it to be modified by authorized MPCA staff. By SOP, MPCA does not modify the Certification statement unless the change has been approved by its legal counsel. The certification text displayed on the Certification page at the time of electronic signature/submittal is stored in the COR and the certification history database table to maintain a fixed record of the text to which the submitter agreed.

CROMERR System Checklist	
	Supporting Documentation (list attachments): See Attachment 2 – Display Prior to Certification.
Submission Process	
8. Transmission error checking and documentation	
	Business Practices: N/A. Transmission is handled via System Functions.
	System Functions: Submittal content data is saved to the MPCA e-Services database when the user clicks the "Save" or "Continue" button on the various windows used to collect data for a submittal. If an error is encountered, users will see the error online at the top of their screen and are able to resolve it at that time in order to continue to the next screen. The system logs would track any transmission errors. Logs are generated using log4j and are stored on secure servers where access is limited. As described in response to requirement #5, signature data is saved at the time of electronic signature/submittal, provided the PIN and second-factor authorization information provided by the user matches that associated with the User ID. SSL version 3.0 is used to provide protection during transmission from the user's web browser to the web server. Subsequent transfers (i.e., web server to application server, application server to database) occur behind a secure firewall, which protects the data during transmission. Upon certification, the MPCA e-Services system uses PD4ML version 3.51 to create a PDF COR from the submittal content and certification data. The PDF COR is zipped along with any attachments and stored to an MPCA file server. A copy of the zipped PDF COR is also imported and indexed in the MPCA EDMS. This importation to the MPCA EDMS is done automatically by the system and extensive testing has validated that no changes are made in this document during the importation of the document. The PDF file format protects the COR from alteration, as do the file server access restrictions described in response to requirement #5. If attachments were included in the submission, the Zip File version of the COR (which contains the PDF and attachments) will be attached to the email to the certifier. If attachments were not included, then only the PDF version of the COR will be attached to the email to the certifier. Once a user completes a submission, it is migrated to the back office system. If a submission fails to migrate, the MPCA staff has existing procedures in place to address such failures and resolve. A Migration Admin screen is also available to MPCA staff to proactively view any submissions that have failed. For users, all their submissions are listed on their MPCA e-Services workspace, where they can view the status of each submission. In the unlikely event a submission fails migration, users will see the submission failed status; text is available on the page with instructions to contact the MPCA.
	Supporting Documentation (list attachments): N/A.

CROMERR System Checklist

9. Opportunity to review copy of record (See 9a through 9c)

9a. Notification that copy of record is available

Business Practices:
Notification that the COR is available for review is emailed to the user using an automated process. Information about this notification is provided in the System Functions section for this requirement.

System Functions:
Upon certification/submittal, the system generates and sends an automated email message to the email address associated with the certifier's user account. The email message notifies the recipient that the email contains an attachment of the COR for the submittal just processed.

In the future, the MPCA e-Services can be enhanced to maintain a log file and database record containing a record of all emails generated by the system, including the email address to which each email was sent.

If the notification email is not successfully delivered, then the system logs the error to a log file. By SOP, the MPCA regularly reviews the logs and database records and schedules any failed emails for redelivery. If the email again cannot be successfully delivered, then MPCA will contact the submitter to follow up.

At any time email address is changed, including during a session, an email is sent to the previous email as well as the new email address as a validation that the email change was not spurious. This provides an alert to the user in the event that someone who has stolen a password has made a spurious submittal and then changed the notification email address.

In addition to email, the COR will be available from the user's main workspace upon logging into the MPCA e-Services. Users have the opportunity to open and view their COR as well as view the statuses of their submissions.

Supporting Documentation (list attachments):

9b. Creation of copy of record in a human-readable format

Business Practices:
N/A. Creation of the COR is handled as an automated process. Information about COR creation is provided in the System Functions section for this requirement.

System Functions:
Upon certification/submittal of each report or document, the system automatically generates a PDF COR using PD4ML version 3.51 for each submittal that was electronically signed/submitted. The PDF COR displays the submittal content, certification statement, certifier name, and certification date in human-readable format. As described in response to requirement #5, the COR is generated and is saved to an MPCA file server for storage. This COR is also emailed as an attachment to the certifier.

Supporting Documentation (list attachments):
See Attachment 3 – COR. This attachment provides an example of the PDF COR for the existing systems. Any future submittals developed under the MPCA e-Services will be CROMERR compliant.

CROMERR System Checklist

9c. Providing the copy of record

Business Practices:
N/A. Providing the COR is handled as an automated process. Information about providing the COR is included in the System Functions section of this requirement.

System Functions:
Authorized users can view the COR in several ways:

-The COR can be viewed using a PDF reader at any time after the submittal is successfully received. A PDF COR is emailed to the certifying party at the time of certification for viewing. Additionally, the COR will be available within the user's main workspace upon logging into the MPCA e-Services.

-The COR can also be viewed, if necessary, by accessing MPCA's file server via the appropriate channels. As mentioned above in requirement #5, only a small subset of authorized MPCA staff has access to the file server. Individuals needing access to the COR, after the fact, may need to contact an MPCA staff member to retrieve the previously submitted COR.

Supporting Documentation (list attachments):

10. Procedures to address submitter/signatory repudiation of a copy of record

Business Practices:
The anticipated reasons a user would want to repudiate a COR is that the data submitted was incorrect, and a correction needs to be provided; or the user did not submit the COR.

In the case of incorrect data, the MPCA e-Services allow corrections or modification of submittals. Modifications or correction submittals are new CORs. This works just like a paper submittal that is a correction or a modification to original hard copy submission. The receiving system, TEMPO is updated with the corrected data, but a COR of the modification or correction is maintained, as well as the original COR. The original COR is not changed. Users may flag the original COR as accidental. All submissions through the MPCA e-Services are retained. CORs are never altered or destroyed, even in the case of a repudiated or corrected submission.

Corrections or modifications can also be made outside of the MPCA e-Services via hard copy. In this case, the correction or modification is entered by MPCA staff into TEMPO as with any paper submittal, and the hard copy submittal is the COR.

MPCA provides a phone number and email address for a user to report that a submittal was not made by them. User should notify MPCA of the Facility (AI) Number, Submittal ID, and the Facility Name. Upon notification, MPCA instructs the user to immediately change their password. This is consistent with Checklist Requirement #4. The user flags the original COR in the MPCA e-Services with a status indicating it is repudiated. The user will submit a "corrected" document. Procedures for corrections are outlined above. In the event there should not have been a submittal at all, MPCA will remove the spurious data that was updated in its receiving system, TEMPO.

Should a written response be requested or needed after the receipt of a dispute, the response would be sent to the user whose signature was compromised. It would contain a summary of the dispute and actions taken to resolve the dispute as well as any follow up instructions required by the user. See revised checklist.

Timeframes or deadlines for repudiation, if they exist, are established by the regulations under which the submittal falls or internal programmatic business processes and are consistent with deadlines for repudiation of paper submittals.

CROMERR System Checklist	
	System Functions: MPCA handles repudiation of the COR via a manual business process. Details of this process are provided in the Business Practices response to this requirement. For users to identify submissions which they have repudiated, a new status to indicate "Repudiated" will appear on the "My Services – Submitted" section of the user's main workspace. Note that if corrections are submitted for a previous submission, the back-office is updated with the corrected data, but the original COR is not changed. A COR of the modification or correction is maintained, as well as the original COR.
	Supporting Documentation (list attachments): N/A
11. Procedures to flag accidental submissions	
	Business Practices: N/A. The MPCA e-Services system includes features to prevent accidental submittals. These features are described in the System Functions section for this requirement.
	System Functions: The system performs validations throughout the submission process for required or invalid fields. If an error is encountered, the user can view them at the top of the screen and must correct any errors prior to continuing and submitting the report. The MPCA e-Services system requires the signatory complete the second-factor authorization procedure, enter his/her PIN, and click a "Certify" button on the certification page in order to sign/submit a report or document. Taking these proactive steps in order to submit suggest intentional and not accidental submittal. Additionally, the MPCA e-Services system displays a submission confirmation message and also sends an automatic email confirmation to the email address associated with the submitter's user account. The confirmation message and/or email would alert the submitter to any accidental submittal, at which time the submitter could notify MPCA (if the submittal was sent prematurely) or could submit a corrected report or document using the MPCA e-Services system. If a corrected report or document is submitted, the system will maintain CORs and signature information for both the original submittal and the correction, but only the corrected version is used by MPCA. Lastly, a new status will be available from the "My Services – Submitted" section of the user's main workspace to indicate if an incomplete or accidental submission was identified – such submissions will be displayed as "Incomplete". Attachment 2, section 8.2.2 provides information about the Certification confirmation page and the email notification process.
	Supporting Documentation (list attachments):

CROMERR System Checklist

12. (e-signature cases only) Automatic acknowledgment of submission

Business Practices:
N/A. Automated acknowledgement of submission is described under the System Functions section for this requirement. See 9a.

System Functions:
Upon electronic signature/submittal, the system generates and sends an automated email message including a PDF COR and an indication that the submittal has been certified. More information about this email is provided in response to requirement #9a.

The email is sent to an out-of-band email address associated with the user's account.

The email will be sent to both the user that submitted the service as well as any additional certifiers of the service. The COR includes all electronic signatures contained in or associated with that document including the date and time of receipt.

Supporting Documentation (list attachments):.

Signature Validation (e-signature cases only)

13. Credential validation (See 13a through 13c)

13a. Determination that credential is authentic

Business Practices:
N/A. Determination of credential ownership is described under the System Functions section for this requirement.

System Functions:
The system supports the second-factor authorization using a 20-5-1 question and answer validation. As part of the account setup, users are required to choose a minimum of five challenge questions and supply answers to those questions. At the time of certification, users will be presented with one of those questions and must supply an answer to it. This will be combined with the PIN to complete the signing ceremony. Upon certifying, the system will validate that each the answer to the challenge question and the PIN match the corresponding user's profile.

As described previously, the submitter electronically signs/submits each report or document submittal by entering his/her User ID and password, a certification PIN, and completing the second-factor authorization procedure (e.g., 20-5-1 question/answer validation) and clicking "Certify" on the Certification page for the given submittal. This action initiates the following processing:

-The User ID, Challenge Question, and Answer are transferred from the web browser to the web server and then to the application server, where the Challenge Answer is encrypted as described in response to requirement #3.

-The encrypted Challenge Answer is compared to the corresponding encrypted Challenge Answer stored in the database for the specified User ID and Challenge Question.

CROMERR System Checklist

System Functions: (cont.)

-If the encrypted Challenge Answers do not match, then the system gives an error message and prevents electronic signature/submittal from continuing. A new Challenge Question is drawn at random for the user to retry.

-If the encrypted Challenge Answers match, the system proceeds with prompting the user to enter Certification PIN.

-The User ID and PIN are transferred from the web browser to the web server and then to the application server, where the PIN is encrypted as described in response to requirement #3.

-The encrypted PIN is then compared to the encrypted PIN stored in the database for the specified User ID.

-If the encrypted PINs do not match, then the system gives an error message and prevents electronic signature/submittal from continuing.

-If the encrypted PINs match, the system proceeds with the electronic signature/submittal process. The User ID, Challenge Answer, and PIN are protected during transfer from web browser to web server by SSL version 3.0. Subsequent processing is performed behind a secure firewall.

If at any time the encrypted Challenge Answers or encrypted PINs do not match, the system throws an error as stated in the above process. After three failed attempts at the Challenge Question & Answer or three failed attempts at entering PIN, the system will log the user out and provide information for them to contact the MPCA for assistance.

The user may close the browser or login again and retry their service.

If a user forgets their Challenge/Response Questions and Answers, they will not be allowed to reset them online. Once the user contacts the MPCA, the MPCA staff must verify the user's identity and then can delete the answers from the user's profile. The next time the user logs into RSP, he/she will again be prompted to set up their Challenge Questions and Answers.

Any failed attempts will also be logged in a database table and the MPCA will have procedures for monitoring that table.

Supporting Documentation (list attachments):

See Attachment 1 - Signature Agreement (SA).

13b. Determination of credential ownership

Business Practices:

In order to obtain security access to electronically sign/submit reports or documents, potential submitters must sign a SA with a handwritten signature. By signing this document, a potential submitter agrees to not share the PIN with any other person, to protect the PIN at all times, to change the PIN immediately upon becoming aware of its compromise, and to report any evidence of compromise to MPCA. This business process is used to protect PINs from compromise. A copy of MPCA's SA that shows the conditions to which a potential submitter must agree prior to obtaining security access to electronically sign/submit report or document submittals has been provided as Attachment 1.

Additionally, if an MPCA e-Services user detects compromise by receiving a confirmation email for a submittal he/she did not submit, then the MPCA e-Services user may follow the business process described in response to requirement #10 to repudiate the submittal.

CROMERR System Checklist	
	System Functions: Upon electronic signature/submittal, the MPCA e-Services system generates and sends an automated email message to the email address associated with the submitter's user account. The email message notifies the recipient of the submittal and indicates that the email contains the PDF COR for the submittal just processed. If an MPCA e-Services user detects compromise by receiving a confirmation email for a submittal he/she did not submit, or for any other reason comes to suspect that his/her PIN or additional security information has been compromised, then the SA that the user signed with a handwritten signature in order to obtain the PIN requires that the user log into the MPCA e-Services system and change his/her MPCA e-Services PIN immediately. Additionally, the terms of the SA require the user to alert MPCA to the possible compromise. Also, the user will have the option to change their additional security information within the system if necessary (i.e., a location to change challenge questions and answers exists in the User Workspace and users can change this information at will). As described in response to requirement #13a, the MPCA e-Services system compares an encrypted version of the Challenge Answer and PIN provided at the time of certification to the encrypted version that corresponds to the User ID used for certification. If the Challenge Answers or PINs differ, then the MPCA e-Services system issues an error message and stops the electronic signature/submittal process.
	Supporting Documentation (list attachments): See Attachment 1 - Signature Agreement (SA).
13c. Determination that credential is not compromised	
	Business Practices: Administrators will periodically review the results of the fraud analysis challenge question failures and the login logs to determine if an account has been compromised. If it is determined that a compromise has occurred, the affected account will be locked, preventing the user from signing, and the user will be contacted to address the situation.
	System Functions: MPCA e-Services includes functions that allow MPCA Administrators and users to detect credential compromises. See Item 15 for a description of these functions. MPCA e-Services allows a user to lock his/her account if he/she suspects the account has been compromised. Administrators also have the ability to lock any user's account. The fact that the account was not locked at the time the submittal was signed provides evidence that neither the user nor administrators believed the credential was compromised at that time.
	Supporting Documentation (list attachments):
14. Signatory authorization	
	Business Practices: If a facility that previously submitted an SA for MPCA e-Services access has a change in their RO/delegated representative official, then the facility must submit a new SA in order to change the status of the RO/delegated representative. When a new SA is submitted by a facility, the MPCA e-Services Administrator will review the existing RO/delegated representative and if there is a change, revoke the security access of the "old" RO/delegated representative as described in the System Functions section for this requirement. The MPCA e-Services Administrator will then process the access request for the "new" RO/delegated representative according to the procedures described in response to requirement #1.

CROMERR System Checklist	
	Business Practices: (cont.) As an additional precaution, when an existing MPCA e-Services facility's permit has been modified or reissued, the MPCA e-Services Administrator will review the RO/delegated representative listed for the facility. If there is a change in the RO/delegated representative and the facility has not submitted a new SA, then the MPCA e-Services Administrator will revoke the security access of the "old" RO/delegated representative as described in the System Functions section for this requirement. The MPCA e-Services Administrator will then contact the facility to request a new SA. Once a new SA has been received, the MPCA e-Services Administrator will follow the procedures described in response to requirement #1 to grant security access to certify/submit data to the new RO/delegated representative.
	System Functions: As described in response to requirement #1, an MPCA e-Services user is only granted security to electronically sign/submit reports or documents for a facility using the MPCA e-Services system once MPCA has verified the user's authority to sign/submit data on behalf of the facility. Additionally, MPCA e-Services system security allows MPCA to revoke security to electronically sign/submit data for a facility from any MPCA e-Services user if the user is no longer authorized to sign/submit data on behalf of the facility (as described in the Business Practices response to this requirement). The MPCA Data Administrator grants or revokes security to sign/submit data for a facility by changing access on a new Manage Users administrative page in the MPCA e-Services system. Note this data can always be changed in the backend e-Services database, if necessary. If an MPCA e-Services user no longer has security access to certify/submit data for a facility, then upon the user attempting to navigate to the Certification page, the system will not offer the user the ability to certify data. In the MPCA e-Services, the user is provided with a link to click for the various certification types required for the submittal. If the user does not have the appropriate security access the MPCA e-Services will not provide this option; users will have the ability to notify other appropriate users who may have access to perform the certification. These security controls prevent the user from signing/submitting the report or document. The RO can also revoke the rights of a delegated representative to view, enter, and sign/submit data for one or more facilities using the "Facility Security Administration" page. The RO must submit a new SA in order to grant a new delegated representative security access to sign/submit data (as although the Facility Security Administration page allows ROs and delegated representatives to grant other MPCA e-Services users access to view or enter data, only the MPCA Data Administrator can grant security access to sign/submit data). Therefore, system security in conjunction with MPCA business processes is used to prevent users without authority to sign/submit data from doing so.
	Supporting Documentation (list attachments):.
15. Procedures to flag spurious credential use	
	Business Practices: If an MPCA e-Services user detects spurious credential use by receiving confirmation emails for submittals he/she did not submit, then the MPCA e-Services user may follow the business processes described in response to requirement #10 to repudiate the submittals. Additionally, in accordance with the terms of the SA the user was required to sign with a handwritten signature in order to obtain security access to sign/submit report or document submittals, the user must notify MPCA of the potential PIN compromise and immediately log onto the MPCA e-Services system to change his/her PIN.

CROMERR System Checklist	
	System Functions: As described in response to requirement #13b, upon signature/submittal the MPCA e-Services system generates and sends an automated email message to the email address associated with the certifier's user account. The email message notifies the recipient of the submittal and indicates that the email contains an attachment of the COR for the submittal just processed. If an MPCA e-Services user detects spurious credential use by receiving confirmation emails for submittals he/she did not submit, then the MPCA e-Services user may follow the business process described in response to requirement #10 to repudiate the submittal. In addition if spurious activity is detected by either fraud analysis or other business criteria the device owner is contacted via telephone or US mail to do further investigation into the activity. Circumstances surrounding this investigation will dictate what actions if any will be taken.
	Supporting Documentation (list attachments): N/A
16. Procedures to revoke/reject compromised credentials	
	Business Practices: As described in response to previous requirements, an MPCA e-Services user must sign a SA with a handwritten signature in order to obtain security access to sign/submit report or documents submittals using the MPCA e-Services system. By signing this agreement, the user agrees to notify MPCA and immediately log onto the MPCA e-Services system and change his/her PIN if he/she suspects it has been compromised. The System Functions section for this requirement describes the system features for changing PINs. Additionally, if necessary, MPCA can revoke an MPCA e-Services user's security access to sign/submit reports or documents by following the procedures described in response to requirement #14.
	System Functions: If a MPCA e-Services user suspects compromise, the user can change his/her PIN by navigating to the User Profile page and choosing to regenerate a new certification PIN. Protection of the new PIN during transfer and storage is covered by the same security as is used for initial PIN issuance, which is described in response to requirement #3. Additionally, if necessary, MPCA can revoke an MPCA e-Services user's security access to sign/submit reports or documents by following the procedures described in response to requirement #14. If MPCA revokes an MPCA e-Services user's security access to sign/submit data, then upon the user navigating to the Certification page for the submittal, the system will not present the user with the option to certify and proceed with the submission. At that point, the user has the ability to return to the main MPCA e-Services page (the User Workspace) or to notify the appropriate party that the submittal is ready for certification. In this way, the MPCA e-Services system prevents unauthorized users from signing/submitting reports or documents. The suspension of a user's authority is controlled by MPCA staff with rights to make that suspension. This suspension will last as long as the MPCA staff determines is needed. MPCA staff has the ability to examine system logs to determine how long and to what extent a compromised credential has been used. Staff at that point will determine the veracity of any documents submitted during this period.

CROMERR System Checklist
Supporting Documentation (list attachments): See Attachment 1 - Signature Agreement (SA).
17. Confirmation of signature binding to document content
Business Practices: N/A. This requirement is addressed via system functions. More information is provided under the System Functions response to this requirement.
System Functions: As described in response to requirement #5, the MPCA e-Services system cross-references the validated electronic signature to the COR document by storing certain signature information, such as the certifying User ID, Challenge Question, encrypted Challenge Answer, encrypted Certification PIN, certification date/time, and certification statement to a history table. The MPCA e-Services will be enhanced to also store the file name of the COR PDF in this database table. The system generates a PDF COR of each certified/submitted report or document using PD4ML version 3.51. The PDF COR is in human-readable format and includes the certifier's name, certification statement, and certification date, as well as the encrypted Challenge Answer and encrypted Certification PIN. The PDF is zipped with any attachments uploaded to the submission and the Zip File is saved to a system-specified directory on an MPCA file server. Direct access to the file server directory in which the COR is stored is limited to a small subset of authorized MPCA staff (approximately 5-6 individuals). Any changes to a COR file would update the timestamp on the file, which would enable MPCA to detect the change. External users do not have access to this file server.
Supporting Documentation (list attachments):
Copy of Record
18. Creation of copy of record (See 18a through 18e)
18a. True and correct copy of document received
Business Practices: N/A. Creation of a true and correct COR is handled via a System Function.
System Functions: As described in response to requirement #9b, the MPCA e-Services system handles creation of a COR by automatically generating a PDF COR using PD4ML version 3.51. Although extensive system testing has shown that the COR generated using this process contains the exact set of data elements as was certified by the user, the system also provides opportunity for the submitter to review and, if necessary, repudiate the COR by generating a confirmation email indicating that the email contains an attachment of the COR for the submittal just processed. Further information about these functions and related business processes are provided in response to requirements #9 and #10.

CROMERR System Checklist	
	System Functions: (cont.) Following certification/submittal, the COR is stored on a secure file server. As described for requirement #5, access to the file storage location is limited to a small number of authorized MPCA staff. The MPCA e-Services system allows users to submit corrections to previously submitted priority reports and documents; however, the system treats such revisions as new submittals with respect to generating the COR and cross-referencing the signature to the submittal (i.e., a separate COR and history record is created for the revision). The COR and certification history information for previously submitted reports or documents is not modified as part of this process.
	Supporting Documentation (list attachments):
18b. Inclusion of electronic signatures	
	Business Practices: N/A. Inclusion of electronic signatures is handled via a System Function.
	System Functions: As described in response to requirement #5, upon successful certification the system stores a history record to the database. This record captures information such as the certifying User ID, certification date/time, certification statement and the Challenge Question, encrypted Challenge Answer, and encrypted Certification PIN used to certify the submittal. This table cross-references detailed certification information to the COR. For informational purposes, the PDF COR displays the certifier name, certification statement, and certification date. However, the certification history information and not the information displayed on the PDF COR links the signature to the COR document. The signature device information is stored in a separate file within the COR.
	Supporting Documentation (list attachments):
18c. Inclusion of date and time of receipt	
	Business Practices: N/A. Inclusion of certification date and time is handled via a System Function.
	System Functions: As described in response to requirement #5, upon successful certification the system stores a history record to the database. This record captures information such as the certifying User ID, certification date/time, certification statement and the Challenge Question, encrypted Challenge Answer, and encrypted Certification PIN used to certify the submittal. This record is then cross-referenced with the detailed certification information to the COR. For informational purposes, the PDF COR displays the certifier name, certification statement, and certification date, however, the certification history information and not the information displayed on the PDF COR links the signature to the COR document.
	Supporting Documentation (list attachments):

CROMERR System Checklist	
18d. Inclusion of other information necessary to record meaning of document	
	Business Practices: This requirement is addressed via system functions. More information is provided under the System Functions response to this requirement.
	System Functions: The PDF COR generated by the system includes submission information as entered by the MPCA e-Services user. Additional elements displayed in the COR (i.e., Certification Statement, Certifier Name, Certification Date) are labeled with intuitive field labels. An example of the PDF COR is provided as Attachment 3.
	Supporting Documentation (list attachments): See Attachment 3 – Copy of Record.
18e. Ability to be viewed in human-readable format	
	Business Practices: N/A. This requirement is addressed via system functions. More information is provided under the System Functions response to this requirement.
	System Functions: As described in response to requirement #9b, the PDF COR uses a human-readable format containing all information captured as part of the submittal. Attachment 3 provides an example of the MPCA e-Services COR.
	Supporting Documentation (list attachments): See Attachment 3 – Copy of Record
19. Timely availability of copy of record as needed	
	Business Practices: Access to the CORs is available through the MPCA e-Services, MPCA's receiving system TEMPO, MPCA's EDMS and may be made available through other query tools. MPCA does not archive its CORs, nor are CORs destroyed. Should MPCA determine the need for CORs to be archived or destroyed in the future, they will be retained minimally according to their retention period identified in associated regulations or law. Also see System Functions below.
	System Functions: As described in response to requirement #9c, authorized users can view the PDF COR from the MPCA e-Services system in several ways: -After displaying the Certification confirmation page, the MPCA e-Services system will return the user to the User Workspace. From this page, the user can navigate to the "My Services – Submitted" section of the User Workspace page to view a list of submittals and a link to view the submittal. For any submittal, regardless of the current status, the user can view the entered data by clicking the "View" link. The submittal is displayed in html format and can be printed if necessary. For those submittals that have not yet been certified, there is no certification signature or certification date displayed. For completed submissions, the COR will be made available in a new column being added to the "My Services – Submitted" section. If the COR included attachments, a Zip File will be displayed containing the PDF COR and attachments. If no attachments were included, only the PDF version of the COR will be displayed.

CROMERR System Checklist	
	System Functions: (cont.) -Immediately after the submission is certified, an email is sent to the certifier with a COR attachment. The COR can be viewed at that time. -Users with security access to the facility for which a Priority report or document was submitted can return to the system at any time and view the COR by navigating to the User Workspace page. If the user was the individual certifying the submittal, the PDF COR can be viewed by opening the Zip or PDF file as described above. -If for any reason a COR failed to generate, MPCA will have instructions in place to regenerate it. Once a COR is regenerated, MPCA will save it to the appropriate location and email it to the user.
	Supporting Documentation (list attachments):
20. Maintenance of copy of record	
	Business Practices: N/A. This requirement is addressed via system functions.
	System Functions: As described in response to requirement #5, the COR is imported to the MPCA's EDMS for storage while the certification electronic signature information is saved to a history table in the MPCA e-Services system database. Direct access to the file server for the EDMS in which the COR is stored is limited to a small subset of authorized MPCA staff (approximately 2 individuals). Any changes to a COR file would update the timestamp on the file, which would enable MPCA to detect the change. The directory is backed up in an offsite secured location in the following schedule: • 5 nights a week • weekly, • monthly, and • annually. All file back-ups are stored off site in a secured location. The MPCA services are located in a server room to which only a select few authorized staff are given access using a key card. The system tracks which of the staff's key cards was used to gain access to the room including the date and time of that access. The system includes an extensive suite of tools used for intrusion protection, virus detection, and firewall among other security measures which meet or exceed the State of Minnesota's Department of Administration standards. These standards include protections against deleting or modifying system log entries. These entries are maintained per the State of Minnesota retention schedule which is three years after all necessary follow-up actions have been completed. When a COR is retrieved, it will be re-hashed and the value will be compared against the hash value stored in the database. If these two values do not match, a message will be displayed to the user explaining there is an issue with the COR and they should contact the MPCA for further information. The MPCA e-Services database, which stores the history record that cross-references the certification/signature information to the PDF COR, is backed up to disk and then to tape on a nightly basis, using Oracle's Recovery Manager. Access to the history table is limited to the MPCA e-Services application and a small set of authorized MPCA users.

CROMERR System Checklist	
	System Functions: (cont.) The MPCA EDMS provides on-line and off-line access to store, index, search, and retrieve documents. It also supports a public portal for search and retrieval of appropriately flagged documents. Documents are stored in a secured file system with metadata and pointers from an Oracle database. The Oracle database includes a variety of indices (metadata) including company, document type, etc. The State of Minnesota retention schedule requires that these types of records are kept permanently.
	Supporting Documentation (list attachments): See Attachment 3 – Copy of Record.

CROMERR Application Cover Sheet

Complete for each system addressed by the application.
For additional systems, please make copies of this page.

System 1 of 1						
System Name:	MPCA e-Services					
Please complete the information below for each report received by this system. For additional reports, please make copies of this page.						
Report Name	**40 CFR Citation**	**Associated EPA Office**	**Applicable EPA Region**	**Requires Signature**	**Electronic Signature**	**Priority Report**
Air Quality Permit Applications	52, 70, 71, 82, 89, 90, 91, 92, 94	Office of Air and Radiation	5	Yes	Yes	Yes
Air Quality Permit Applications	52, 70, 71, 82, 89, 90, 91, 92, 94	Office of Air and Radiation	5	Yes	Yes	No
Air Quality Reports	51, 60, 61, 63, 65, 68, 70, 71, 72, 74, 75, 79, 80, 82, 86, 90, 91, 92	Office of Air and Radiation	5	Yes	Yes	Yes
Air Quality Reports	51, 60, 61, 63, 65, 68, 70, 71, 72, 74, 75, 79, 80, 82, 86, 90, 91, 92	Office of Air and Radiation	5	Yes	Yes	No
Water Quality National Pollutant Discharge Elimination System (NPDES) Permit Applications	122	Office of Water	5	Yes	Yes	Yes
Water Quality NPDES Permit Applications	122	Office of Water	5	Yes	Yes	No
Discharge Monitoring Reports	122, 403	Office of Water	5	Yes	Yes	Yes
RCRA – Hazardous Waste Permit Applications	270	Office of Solid Waste and Emergency Response	5	Yes	Yes	Yes

Report Name	40 CFR Citation	Associated EPA Office	Applicable EPA Region	Requires Signature	Electronic Signature	Priority Report
Hazardous Waste Reports	262, 264, 265, 266, 268, 270, 720, 721	Office of Solid Waste and Emergency Response	5	Yes	Yes	Yes
Hazardous Waste Reports	262, 264, 265, 266, 268, 270, 720, 721	Office of Solid Waste and Emergency Response	5	Yes	Yes	No
Underground Storage Tank Notifications	280	Office of Solid Waste and Emergency Response	5	Yes	Yes	Yes

Brief Overview of System:

The Minnesota Pollution Control Agency (MPCA) plans the implementation of a consolidated web-based system, referred to as MPCA e-Services, as the single point of access for control/mediation of a set of web-based functionalities:

- application access
- application security
- user authentication
- user authorization
- electronic signatures
- Cross-Media Electronic Reporting Requirements (CROMERR)-related requirements

These functionalities are responsible for achieving CROMERR compliancy for applications utilizing MPCA e-Services capabilities.

The MPCA e-Services are being designed to give our user stakeholders a more efficient method for submitting environmental reports to the MPCA.

The MPCA e-Services system consists of a robust, modular framework of sub-systems which isolate various aspects of application access, registration, authentication, authorization, document submission, electronic signatures and in-band and out-of-band email notifications.

Attachments included in this application for this system:

☒ Description of how this system complies with CROMERR requirements under 40 CFR 3.2000

☐ Schedule of planned upgrades or changes to this system

☒ Other Attachments (Please list):

Attachment 1: MPCA e-Services Signature Agreement
Attachment 2: Submittal Data Displayed Prior to Certification
Attachment 3: Copy of Record
Attachment 4: Attorney General's Statement of Legal Authority for Electronic Reporting

Minnesota Pollution Control Agency
e-Services Authorization Agreement

User information
(preprinted by system)

User Name

User ID

Phone number

Email address

Terms and conditions

By signature on this agreement, the user named above requests the Minnesota Pollution Control Agency (MPCA) to allow electronic submittal and/or certification of the documents for the facilities indicated below. The submittals will be considered authentic only if certified by the Responsible Official (RO) or the Duly Authorized Representative (DAR) with legal authority and authorization to do so.

By signature on this agreement, the named User(s) agrees to:

1. Protect the account password, PIN, and answers to challenge questions from compromise.
2. Not allow anyone else access to the account.
3. Not share the account password, PIN, or answers to challenge questions.
4. Promptly report to the MPCA any evidence of loss, theft, or other compromise of the account password, PIN, or answers to challenge questions.
5. Change the account password, PIN, or answers to challenge questions if there is reason to believe any have been become known to another person.
6. Notify the MPCA if any authorized individuals named in this document are no longer representing the named facilities in the capacity indicated by the authorization requested here as soon as the change in relationship becomes known.
7. Review in a timely manner the email onscreen acknowledgements and copies of record submitted and certified through my account to MPCA e-Services.
8. To report any evidence of discrepancy between the document submitted and what the MPCA e-Services received.

By signature below, I understand I will be held as legally bound, obligated, and responsible by the electronic signature created as by a handwritten signature.

Part A. Facility Information (preprinted by system) (standard for all authorizations)

Facility ID	Permit No.	Facility Name(s)	Submittal type

Part B. Responsible Official Authorization Request

By submitting this authorization request to the MPCA, I certify that:

1. I have read, understand and accept the terms and conditions of this e-Services authorization agreement.
2. Under penalty of law, I understand and will comply with the certification requirements of Minn. R. (citation here), including the penalties for submitting false information.
3. I have a current user account in place with MPCA e-Services.
4. I am the responsible official.

Please authorize as the Responsible Official: (filled in by facility)

First Name:	Last Name:
Title:	
Signature:	
Telephone (with area code):	User ID:
Email address:	

Part C. Request for Duly Authorized Representative authorization

This section is used to request Duly Authorized Representative (DAR) authorization for the above named facilities. Users with DAR authorization have authorization to submit and certify all documents for the facilities named above.

Both the Duly Authorized Representative and the Responsible Official must sign below.

By submitting this authorization request to the MPCA, I certify that:

1. I have read, understand and accept the terms and conditions of this e-Services authorization agreement.
2. Under penalty of law, I understand and will comply with the certification requirements of Minn. R. (citation here), including the penalties for submitting false information.
3. I have a current user account in place with MPCA e-Services.
4. I am the responsible official.

Please authorize as the Duly Authorized Representative: (filled in by facility)

First Name:	Last Name:
Title:	
Signature:	
Telephone (with area code):	User ID:
Email address:	

As responsible official, I approve this authorization: (filled in by facility)

First Name:	Last Name:
Title:	
Signature:	
Telephone (with area code):	User ID:
Email address:	

Submittal Data Displayed Prior to Certification

Please review the following information for accuracy, then press **Next**. Press the **Back** button to edit data.

Narrative Activities and SIC Codes
4011: Railroads, Line-Haul Operating – **Primary**

Facility Information

Name:	BNSF Northtown Yard - ISW
Facility Owner:	BNSF Railway Co
Address:	80 44th Ave NE
City:	Blaine
State:	MN
Zip Code:	55421
Facility Size in Acres:	46

Facility Activities Description: Railroad yard

Facility Location

Latitude:	45.04777527
Longitude:	-93.2687149
Location Determination Date:	06/30/1999
Collection Method:	Bing Maps

Owner Permittee

Business Name:	BNSF Railway Co
First Name:	Robert
Last Name:	Kale
Title:	Environmental Operations Mgr
Email:	robert.kale@bnsf.com
Business Phone:	701.667.2201
Mailing Address:	PO Box 1205
City:	Mandan
State:	MN
Zip Code:	585541205

Operator Contact

Company Name:	BNSF Railway Co
First Name:	Robert
Last Name:	Kale
Title:	Environmental Operations Mgr
Email:	robert.kale@bnsf.com
Business Phone:	701.667.2201
Address:	PO Box 1205
City:	Mandan
State:	MN
Zip Code:	585541205

Facility Contact

Company Name:	BNSF Railway Co
First Name:	Robert
Last Name:	Kale
Title:	Environmental Operations Mgr
Email:	robert.kale@bnsf.com
Business Phone:	701.667.2201
Address:	PO Box 1205
City:	Mandan
State:	MN
Zip Code:	585541205

Municipal Storm Sewer System Receiving Industrial Stormwater
Anoka County

Waterbodies
Name: Mississippi
Waterbody Type: River
Within one mile of facility: Y
Impaired Water: N
Outstanding Resource Value
Water: N

Monitoring Locations
Monitor Name: South East corner of yard
Subsector Code: P1
Latitude: 45.08826
Longitude: -93.27009
Location Determination Date: 6/4/2014 12:00:00 AM
Collection Method: Bing Maps

Does this facility have a monitoring location from which a discharge flows to and is within one mile of an Outstanding Resource Value Water, 303d listed Impaired Water, Trout Stream, Trout Lake, or Wetland? (No)

Please review the following information for accuracy, then press **Next**. Click on the **Back** button to edit data.

Service Information

Service ID:	1254
Service Name:	Lee Peterson
Service Type:	New Permit
Created On:	06/19/2013

Contacts

Name: Lee Peterson
Title:
Contact Type: Application Contact
Organization Name:
Organization Type: RSP
E-Mail: lee.peterson@cgi.com
Phone: (276) 889-7590 (Work Phone Number)
Contact Address: 1234567890 rt
, Mississippi 12345

Name: Lee Peterson
Title:
Contact Type: Applicant
Organization Name:
Organization Type: RSP
E-Mail: lee.peterson@cgi.com
Phone: (276) 889-7590 (Work Phone Number)
Contact Address: 1234567890 rt
, Mississippi 12345

Name: Lee Peterson
Title:
Contact Type: Landowner
Organization Name:
Organization Type: RSP
E-Mail: lee.peterson@cgi.com
Phone: (276) 889-7590 (Work Phone Number)
Contact Address: 1234567890 rt
, Mississippi 12345

SUBMITTAL DISPLAY

KNOWN IDENTIFIERS

Number: 2299
Type: OLWR Groundwater Withdrawal Permit Number

BENEFICIAL USE

Primary Beneficial Use: Livestock
Secondary Beneficial Use: Flood Protection
Additional Beneficial Use(s): Fire Protection

Any Additional Remarks:

LOCATION

County: Noxubee

Legal Location: NW Quarter of the SE Quarter of Section 30, Township 25N, Range 17E

GROUNDWATER SOURCE

Completion Date (Proposed or Actual): 06/01/2013
Do you have a meter installed on your well?:
Depth of Well: 23 feet
Surface Casing Diameter: 18 inches
Casing Type: Black Iron
Screen Type: Open Hole

Attachment 4

STATE OF MINNESOTA

OFFICE OF THE ATTORNEY GENERAL

LORI SWANSON
ATTORNEY GENERAL

SUITE 900
445 MINNESOTA STREET
ST. PAUL, MN 55101-2127
TELEPHONE: (651) 297-1075

November 3, 2008

Mr. Mark Luttner, Director
U.S. Environmental Protection Agency
Office of Environmental Information
Office of Information Collection
1200 Pennsylvania Avenue, N.W.
Washington, D.C. 20460

RE: Certification of Legal Authority for Electronic Reporting as Required by Cross-Media Electronic Reporting Regulation (CROMERR), 40C.F.R. Part 3

Dear Mr. Luttner

Pursuant to the authority delegated to me by the Minnesota Attorney General, and in accordance with the Cross Media Electronic Reporting Regulation (CROMERR), 40 CFR §§ 3.1000(b)(1)(i) and 3.2000(c), it is my opinion that the laws of the State of Minnesota provide adequate authority to carry out all aspects of the program submitted by the Minnesota Pollution Control Agency (MPCA) to the United States Environmental Protection Agency (EPA) to administer and enforce electronic reporting under CROMERR. My opinion is based on the statutes and rules identified below, all of which are lawfully adopted and fully effective.

I hereby certify:

(1) that the State of Minnesota has sufficient legal authority provided by Minnesota's lawfully enacted or promulgated statutes or regulations to implement the electronic reporting component of its authorized programs consistent with 40 Code of Federal Regulations § 3.2000 and with this application;

(2) that such statutes or regulations are in full force and effect on the date of this certification; and

(3) that the State of Minnesota has authority to enforce the affected programs using electronic documents collected under these programs.

I have included with this certification all Minnesota statutes and regulations relevant to this application. To assist EPA's review of this application, I also have included a description specifically linking the provisions of 40 C.F.R. § 3.2000(c) with relevant portions of Minnesota's statutes.

I. LEGAL AUTHORITY TO IMPLEMENT ELECTRONIC REPORTING.

CROMERR requires that a state must have "sufficient legal authority provided by lawfully enacted or promulgated statutes or regulations that are in full force and effect on the date of the certification to implement the electronic reporting component of its authorized programs consistent" with 40 CFR § 3.2000. 40 CFR § 3.1000(b)(1).

Minnesota has general statutory and regulatory authority to implement electronic reporting under the Minnesota Electronic Authentication Act (UEAA), Minn. Stat. ch. 325K (2008); the Uniform Electronic Transactions Act (UETA), Minn. Stat. ch. 325L (2008); and under administrative rules for electronic authentication promulgated by the Minnesota Secretary of State, Minn. R. ch. 8275 (2008).

The specific source of the Minnesota Pollution Control's authority to implement electronic reporting is the following statutory provision:

> (a) Except as otherwise provided in section 325L.12, paragraphs (f) and (g), each governmental agency of this state shall determine whether, and the extent to which, it will send and accept electronic records and electronic signatures to and from other persons and otherwise create, generate, communicate, store, process, use, and rely upon electronic records and electronic signatures.
>
> (b) To the extent that a governmental agency uses electronic records and electronic signatures under paragraph (a), the governmental agency giving due consideration to security, may specify:
>
> (1) the manner and format in which the electronic records must be created, generated, sent, communicated, received, and stored and the systems established for those purposes;
>
> (2) if electronic records must be signed by electronic means, the type of electronic signature required, the manner and format in which the electronic signature must be affixed to the electronic record, and the identity of, or criteria that must be met by, any third party used by a person filing a document to facilitate the process;
>
> (3) control processes and procedures as appropriate to ensure adequate preservation, disposition, integrity, security, confidentiality, and auditability of electronic records; and

> (4) any other required attributes for electronic records which are specified for corresponding nonelectronic records or reasonably necessary under the circumstances.
>
> (c) Except as otherwise provided in section 325L.12, paragraph (f), this chapter does not require a governmental agency of this state to use or permit the use of electronic records or electronic signatures.

Minn. Stat. § 325L.18 (2008). Definitions of the terms in § 325L.18 are located at Minn. Stat. § 325L.02 (2008). This statute must be construed and applied to "facilitate electronic transactions consistent with other applicable law." Minn. Stat. § 325L.06 (2008). The UETA "applies to any electronic record or electronic signature created, generated, sent, communicated, received, or stored on or after August 1, 2000." Minn. Stat. § 325L.04 (2008).

II. APPROPRIATE CIVIL AND CRIMINAL PENALTIES FOR FAILURE TO COMPLY WITH REPORTING REQUIREMENTS.

CROMERR requires that an authorized program must ensure that "[a] person is subject to any appropriate civil, criminal penalties or other remedies under state, tribe, or local law for failure to comply with a reporting requirement if the person fails to comply with the applicable provisions for electronic reporting." 40 CFR § 3.2000(c)(1).

Under Minnesota law, any person who fails to comply with any requirement, including reporting requirements, is subject to enforcement.

> Any person who violates any provision of this chapter or chapter 114C or 116, except any provisions of chapter 116 relating to air and land pollution caused by agricultural operations which do not involve national pollutant discharge elimination system permits, or of (1) any effluent standards and limitations or water quality standards, (2) any permit or term or condition thereof, (3) any national pollutant discharge elimination system filing requirements, (4) any duty to permit or carry out inspection, entry or monitoring activities, or (5) any rules, stipulation agreements, variances, schedules of compliance, or orders issued by the agency, shall forfeit and pay to the state a penalty, in an amount to be determined by the court, of not more than $10,000 per day of violation except that if the violation relates to hazardous waste the person shall forfeit and pay to the state a penalty, in an amount to be determined by the court, of not more than $25,000 per day of violation.

Minn. Stat. § 115.071, subd. 3 (2008). *See also* Minn. Stat. § 116.072, subd. 1 ("The commissioner may issue an order requiring violations to be corrected and administratively assessing monetary penalties for violations of this chapter and chapters 114C, 115, 115A, 115D, and 115E, any rules adopted under those chapters, and any standards, limitations, or conditions

established in an agency permit; and for failure to respond to a request for information under section 115B.17, subdivision 3.")

The UETA contains several provisions that ensure that a person who fails to comply with the applicable provisions for electronic reporting is subject to appropriate enforcement. The UETA provides, "A transaction subject to this chapter is also subject to other applicable substantive law." Minn. Stat. § 325L.03(e) (2008). Similarly, "Whether an electronic record or electronic signature has legal consequences is determined by this chapter and other applicable law." Minn. Stat. § 325L.05(e) (2008). These provisions ensure that the underlying reporting requirements, and the sanctions prescribed by Minnesota law for noncompliance with those reporting requirements, are not affected by whether the person uses electronic reporting.

In addition, the UETA states:

(a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

(b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

(c) If a law requires a record to be in writing, an electronic record satisfies the law.

(d) If a law requires a signature, an electronic signature satisfies the law.

Minn. Stat. § 325L.07 (2008). These provisions also ensure that an electronic signature must be given the same legal effect as a handwritten signature.

The UETA also provides

(a) If parties have agreed to conduct transactions by electronic means and a law requires a person to provide, send, or deliver information in writing to another person, the requirement is satisfied if the information is provided, sent, or delivered, as the case may be, in an electronic record capable of retention by the recipient at the time of receipt. An electronic record is not capable of retention by the recipient if the sender or its information processing system inhibits the ability of the recipient to print or store the electronic record.

(b) If a law other than this chapter requires a record (i) to be posted or displayed in a certain manner, (ii) to be sent, communicated, or transmitted by a specified method, or (iii) to contain information that is formatted in a certain manner, the following rules apply:

(1) the record must be posted or displayed in the manner specified in the other law;

(2) except as otherwise provided in paragraph (d), clause (2),[1] the record must be sent, communicated, or transmitted by the method specified in the other law;

(3) the record must contain the information formatted in the manner specified in the other law.

Minn. Stat. § 325L.08(a) and (b) (2008). This provision ensures that if a person has agreed to conduct transactions electronically and is required to send written information to the MPCA, the person is not in compliance with the electronic reporting requirement unless the person sends the information in an electronic record that can be stored or printed or otherwise retained by the MPCA, or in the specific form required by the MPCA.

The UETA also states:

An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.

Minn. Stat. § 325L.09(a) (2008). This provision ensures that the specific individual who submits an electronic record that does not comply with the applicable provisions for electronic reporting can be identified and held accountable for failure to comply with reporting requirements.

Finally, the UETA provides:

In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.

Minn. Stat. § 325L.13 (2008). This section of the UETA ensures that Minnesota's ability to take enforcement action against an individual for failure to comply with a reporting requirement will not be impaired or otherwise affected by the fact that the record or signature in issue is in electronic form.

---

[1] Paragraph (d)(2) states:

The requirements of this section may not be varied by agreement, but . . . (2) a requirement under a law other than this chapter to send, communicate, or transmit a record by first-class mail, postage prepaid or regular United States mail may be varied by agreement to the extent permitted by the other law." Minn, Stat. § 325L.08(d)(2) (2008).

III. AN ELECTRONIC SIGNATURE LEGALLY BINDS OR OBLIGATES THE SIGNATORY.

CROMERR requires that an authorized program must ensure that:

> Where an electronic document submitted to satisfy a state, tribe, or local reporting requirement bears an electronic signature, the electronic signature legally binds or obligates the signatory or makes the signatory responsible, to the same extent as the signatory's handwritten signature on a paper document would, if the paper document were submitted to satisfy the same reporting requirement.

40 CFR § 3.2000(c)(2).

Minnesota law provides that electronic signatures are accorded the same status under law as a traditional handwritten signature. The UETA states:

> (a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
>
> (b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.
>
> (c) If a law requires a record to be in writing, an electronic record satisfies the law.
>
> (d) If a law requires a signature, an electronic signature satisfies the law.

Minn. Stat. § 325L.07 (2008).

In addition, Minnesota law provides for notarizing or otherwise verifying an electronic signature or electronic record. The UETA states:

> If a law requires a signature or record to be notarized, acknowledged, verified, or made under oath, the requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the signature or record.

Minn. Stat. § 325L.11 (2008). This provision ensures that if a reporting requirement includes a requirement that a signature must be notarized, verified, or made under oath, an electronic signature that accompanies an electronic record can fulfill this requirement.

IV. AN ELECTRONIC SIGNATURE CAN BE ATTRIBUTED TO A SPECIFIC INDIVIDUAL.

CROMERR requires that an authorized program must establish the following with respect to its electronic reporting program:

> Proof that a particular electronic signature device was used to create an electronic signature that is included in or logically associated with an electronic document submitted to satisfy a state, tribe, or local reporting requirement will suffice to establish that the individual uniquely entitled to use the device at the time of signature did so with the intent to sign the electronic document and give it effect.

40 CR § 3.2000(c)(3).

The UETA states:

> (a) An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.
>
> (b) The effect of an electronic record or electronic signature attributed to a person under paragraph (a) is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement, if any, and as otherwise provided by law.

Minn. Stat. § 325L.09 (2008). This provision ensures that the use of a particular electronic device to create an electronic signature can be attributed to the individual who was uniquely entitled to use that device at the time. This provision also ensures that where an electronic signature is attributable to a specific individual, the individual's intent to sign the document and give it intent can be determined in the same manner as with a handwritten signature.

V. ELECTRONIC DOCUMENTS ARE FULLY ADMISSIBLE IN EVIDENCE IN ENFORCEMENT PROCEEDINGS.

CROMERR requires that an authorized program must show that "[n]othing in the authorized program limits the use of electronic documents or information derived from electronic documents as evidence in enforcement proceedings." 40 CFR § 3.2000(c)(4).

As indicated above, Minnesota law accords the same status to electronic signatures and records as it does to more conventional formats. The UETA states:

(b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

(c) If a law requires a record to be in writing, an electronic record satisfies the law.

(d) If a law requires a signature, an electronic signature satisfies the law.

Minn. Stat. § 325L.07 (2008). The UETA also provides:

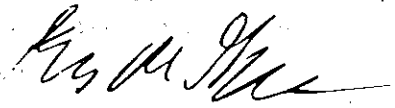
> In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.

Minn. Stat. § 325L.13 (2008). Together, these two provisions ensure that nothing in the authorized program or in Minnesota law limits the use of electronic documents or electronic signatures as evidence in enforcement proceedings.

VI. CONCLUSION.

If you have further questions regarding the MPCA's legal authority to implement and enforce electronic reporting under CROMERR, please feel free to contact Assistant Attorney General Lawrence W. Pry at (651) 215-1535.

Very truly yours,



STEVEN M. GUNN
Deputy Attorney General

(651) 296-8954 (Voice)
(651) 297-4139 (Fax)

Enclosures

AG: #2328702-v1

2008 Minnesota Statutes

Chapter 325L, Uniform Electronic Transactions Act

325L.01 SHORT TITLE.

This chapter may be cited as the "Uniform Electronic Transactions Act."

History: 2000 c 371 s 1

325L.02 DEFINITIONS.

In this chapter:

(a) "Agreement" means the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations, and procedures given the effect of agreements under laws otherwise applicable to a particular transaction.

(b) "Automated transaction" means a transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or

both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction.

(c) "Computer program" means a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result.

(d) "Contract" means the total legal obligation resulting from the parties' agreement as affected by this chapter and other applicable law.

(e) "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(f) "Electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances, in whole or in part, without review or action by an individual.

(g) "Electronic record" means a record created, generated, sent, communicated, received, or stored by electronic means.

(h) "Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

(i) "Governmental agency" means an executive, legislative, or judicial agency, department, board, commission, authority, institution, or instrumentality of the federal government or of a state or of a county, municipality, or other political subdivision of a state.

(j) "Information" means data, text, images, sounds, codes, computer programs, software, databases, or the like.

(k) "Information processing system" means an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information.

(l) "Person" means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or any other legal or commercial entity.

(m) "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

(n) "Security procedure" means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.

(o) "State" means a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any territory or insular possession subject to the jurisdiction of the United States. The term includes an Indian tribe or band, or Alaskan

to conduct transactions by electronic means. Whether the parties agree to conduct transactions by electronic means is determined from the context and surrounding circumstances, including the parties' conduct.

(c) If a party agrees to conduct a transaction by electronic means, this chapter does not prohibit the party from refusing to conduct other transactions by electronic means. This paragraph may not be varied by agreement.

(d) Except as otherwise provided in this chapter, the effect of any of its provisions may be varied by agreement. The presence in certain provisions of this chapter of the words "unless otherwise agreed," or words of similar import, does not imply that the effect of other provisions may not be varied by agreement.

(e) Whether an electronic record or electronic signature has legal consequences is determined by this chapter and other applicable law.

History: 2000 c 371 s 5

325L.06 CONSTRUCTION AND APPLICATION.

This chapter must be construed and applied to:

(1) facilitate electronic transactions consistent with other applicable law;

(2) be consistent with reasonable practices concerning electronic transactions and with the continued expansion of those practices; and

(3) effectuate its general purpose to make uniform the law with respect to the subject of this chapter among states enacting it.

History: 2000 c 371 s 6

325L.07 LEGAL RECOGNITION OF ELECTRONIC RECORDS, ELECTRONIC SIGNATURES, AND ELECTRONIC CONTRACTS.

(a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

(b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

(c) If a law requires a record to be in writing, an electronic record satisfies the law.

(d) If a law requires a signature, an electronic signature satisfies the law.

History: 2000 c 371 s 7

325L.08 PROVISION OF INFORMATION IN WRITING; PRESENTATION OF RECORDS.

(a) If parties have agreed to conduct transactions by electronic means and a law requires a person to provide, send, or deliver information in writing to another person, the requirement is satisfied if the information is provided, sent, or delivered, as the case may be, in an electronic record capable of retention by the recipient at the time of receipt. An

electronic record is not capable of retention by the recipient if the sender or its information processing system inhibits the ability of the recipient to print or store the electronic record.

(b) If a law other than this chapter requires a record (i) to be posted or displayed in a certain manner, (ii) to be sent, communicated, or transmitted by a specified method, or (iii) to contain information that is formatted in a certain manner, the following rules apply:

(1) the record must be posted or displayed in the manner specified in the other law;

(2) except as otherwise provided in paragraph (d), clause (2), the record must be sent, communicated, or transmitted by the method specified in the other law;

(3) the record must contain the information formatted in the manner specified in the other law.

(c) If a sender inhibits the ability of a recipient to store or print an electronic record, the electronic record is not enforceable against the recipient.

(d) The requirements of this section may not be varied by agreement, but:

(1) to the extent a law other than this chapter requires information to be provided, sent, or delivered in writing but permits that requirement to be varied by agreement, the requirement under paragraph (a) that the information be in the form of an electronic record capable of retention may also be varied by agreement; and

(2) a requirement under a law other than this chapter to send, communicate, or transmit a record by first-class mail, postage prepaid or regular United States mail may be varied by agreement to the extent permitted by the other law.

History: 2000 c 371 s 8

325L.09 ATTRIBUTION AND EFFECT OF ELECTRONIC RECORD AND ELECTRONIC SIGNATURE.

(a) An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.

(b) The effect of an electronic record or electronic signature attributed to a person under paragraph (a) is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement, if any, and as otherwise provided by law.

History: 2000 c 371 s 9

325L.10 EFFECT OF CHANGE OR ERROR.

If a change or error in an electronic record occurs in a transmission between parties to a transaction, the following rules apply:

(1) if the parties have agreed to use a security procedure to detect changes or errors

and one party has conformed to the procedure, but the other party has not, and the nonconforming party would have detected the change or error had that party also conformed, the conforming party may avoid the effect of the changed or erroneous electronic record;

(2) in an automated transaction involving an individual, the individual may avoid the effect of an electronic record that resulted from an error made by the individual in dealing with the electronic agent of another person if the electronic agent did not provide an opportunity for the prevention or correction of the error and, at the time the individual learns of the error, the individual:

(i) promptly notifies the other person of the error and that the individual did not intend to be bound by the electronic record received by the other person;

(ii) takes reasonable steps, including steps that conform to the other person's reasonable instructions, to return to the other person or, if instructed by the other person, to destroy the consideration received, if any, as a result of the erroneous electronic record; and

(iii) has not used or received any benefit or value from the consideration, if any, received from the other person;

(3) if neither clause (1) nor clause (2) applies, the change or error has the effect provided by other law, including the law of mistake, and the parties' contract, if any;

(4) clauses (2) and (3) may not be varied by agreement.

History: 2000 c 371 s 10

325L.11 NOTARIZATION AND ACKNOWLEDGMENT.

If a law requires a signature or record to be notarized, acknowledged, verified, or made under oath, the requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the signature or record.

History: 2000 c 371 s 11

325L.12 RETENTION OF ELECTRONIC RECORDS; ORIGINALS.

(a) If a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record which:

(1) accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise; and

(2) remains accessible for later reference.

(b) A requirement to retain a record in accordance with paragraph (a) does not apply to any information whose sole purpose is to enable the record to be sent, communicated, or received.

system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record;

(2) is in a form capable of being processed by that system; and

(3) enters an information processing system outside the control of the sender or of a person that sent the electronic record on behalf of the sender or enters a region of the information processing system designated or used by the recipient which is under the control of the recipient.

(b) Unless otherwise agreed between a sender and the recipient, an electronic record is received when:

(1) it enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record; and

(2) it is in a form capable of being processed by that system.

(c) Paragraph (b) applies even if the place the information processing system is located is different from the place the electronic record is deemed to be received under paragraph (d).

(d) Unless otherwise expressly provided in the electronic record or agreed between the sender and the recipient, an electronic record is deemed to be sent from the sender's place of business and to be received at the recipient's place of business. For purposes of this paragraph, the following rules apply:

(1) if the sender or recipient has more than one place of business, the place of business of that person is the place having the closest relationship to the underlying transaction;

(2) if the sender or the recipient does not have a place of business, the place of business is the sender's or recipient's residence, as the case may be.

(e) An electronic record is received under paragraph (b) even if no individual is aware of its receipt.

(f) Receipt of an electronic acknowledgment from an information processing system described in paragraph (b) establishes that a record was received but, by itself, does not establish that the content sent corresponds to the content received.

(g) If a person is aware that an electronic record purportedly sent under paragraph (a), or purportedly received under paragraph (b), was not actually sent or received, the legal effect of the sending or receipt is determined by other applicable law. Except to the extent permitted by the other law, this paragraph may not be varied by agreement.

History: 2000 c 371 s 15

325L.16 TRANSFERABLE RECORD.

(a) In this section, "transferable record" means an electronic record that:

to enforce the transferable record shall provide reasonable proof that the person is in control of the transferable record. Proof may include access to the authoritative copy of the transferable record and related business records sufficient to review the terms of the transferable record and to establish the identity of the person having control of the transferable record.

History: 2000 c 371 s 16; 2001 c 195 art 2 s 20; 2004 c 162 art 3 s 9

325L.17 CREATION AND RETENTION OF ELECTRONIC RECORDS AND CONVERSION OF WRITTEN RECORDS BY GOVERNMENTAL AGENCIES.

Each governmental agency of this state shall determine whether, and the extent to which, it will create and retain electronic records and convert written records to electronic records. Records of a government agency are subject to sections 15.17 and 138.17.

History: 2000 c 371 s 17

325L.18 ACCEPTANCE AND DISTRIBUTION OF ELECTRONIC RECORDS BY GOVERNMENTAL AGENCIES.

(a) Except as otherwise provided in section 325L.12, paragraphs (f) and (g), each governmental agency of this state shall determine whether, and the extent to which, it will send and accept electronic records and electronic signatures to and from other persons and otherwise create, generate, communicate, store, process, use, and rely upon electronic records and electronic signatures.

(b) To the extent that a governmental agency uses electronic records and electronic signatures under paragraph (a), the governmental agency giving due consideration to security, may specify:

(1) the manner and format in which the electronic records must be created, generated, sent, communicated, received, and stored and the systems established for those purposes;

(2) if electronic records must be signed by electronic means, the type of electronic signature required, the manner and format in which the electronic signature must be affixed to the electronic record, and the identity of, or criteria that must be met by, any third party used by a person filing a document to facilitate the process;

(3) control processes and procedures as appropriate to ensure adequate preservation, disposition, integrity, security, confidentiality, and auditability of electronic records; and

(4) any other required attributes for electronic records which are specified for corresponding nonelectronic records or reasonably necessary under the circumstances.

(c) Except as otherwise provided in section 325L.12, paragraph (f), this chapter does not require a governmental agency of this state to use or permit the use of electronic records or electronic signatures.

History: 2000 c 371 s 18

325L.19 INTEROPERABILITY.

The governmental agency of this state which adopts standards pursuant to section 325L.18 may encourage and promote consistency and interoperability with similar requirements adopted by other governmental agencies of this and other states and the federal government and nongovernmental persons interacting with governmental agencies of this state. If appropriate, those standards may specify differing levels of standards from which governmental agencies of this state may choose in implementing the most appropriate standard for a particular application.

History: 2000 c 371 s 19

Electronic Signature

Signator:	Lee Peterson
Signator ID:	LPETERSON
Challenge/Response Question:	What is the first name of your first boyfriend or girlfriend?
Challenge/Response Answer:	******
eSignature PIN:	******
Date/Time of eSignature:	02/05/2014 12:02

"I certify under penalty of law that I believe the information provided in this document is true, accurate, and complete. I am aware that there are significant civil and criminal penalties, including the possibility of fine or imprisonment or both, for submitting false, inaccurate or incomplete information."

Lee Peterson	02/05/2014
Signatory	**Date**

Submission

Date/Time of Submission:	02/05/2014 12:02

2008 Minnesota Statutes

Chapter 325K. Electronic Authentication

325K.001 SHORT TITLE.

This chapter may be cited as the Minnesota Electronic Authentication Act.

History: 1997 c 178 s 1

325K.01 DEFINITIONS.

digital signature.

Subd. 24. **Public key.** "Public key" means the key of a key pair used to verify a digital signature.

Subd. 25. **Publish.** "Publish" means to record or file in a repository.

Subd. 26. **Qualified right to payment.** "Qualified right to payment" means an award of damages against a licensed certification authority by a court having jurisdiction over the certification authority in a civil action for violation of this chapter.

Subd. 27. **Recipient.** "Recipient" means a person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate and is in a position to rely on it.

Subd. 28. **Recognized repository.** "Recognized repository" means a repository recognized by the secretary under section 325K.25.

Subd. 29. **Recommended reliance limit.** "Recommended reliance limit" means the monetary amount recommended for reliance on a certificate under section 325K.17.

Subd. 30. **Repository.** "Repository" means a system for storing and retrieving certificates and other information relevant to digital signatures.

Subd. 31. **Revoke a certificate.** "Revoke a certificate" means to make a certificate ineffective permanently from a specified time forward. Revocation is effected by notation or inclusion in a set of revoked certificates, and does not imply that a revoked certificate is destroyed or made illegible.

Subd. 32. **Rightfully hold a private key.** "Rightfully hold a private key" means the authority to utilize a private key:

(1) that the holder or the holder's agents have not disclosed to a person in violation of section 325K.13, subdivision 1; and

(2) that the holder has not obtained through theft, deceit, eavesdropping, or other unlawful means.

Subd. 33. **Secretary.** "Secretary" means the Minnesota secretary of state.

Subd. 34. **Subscriber.** "Subscriber" means a person who:

(1) is the subject listed in a certificate;

(2) accepts the certificate; and

(3) holds a private key that corresponds to a public key listed in that certificate.

Subd. 35. **Suitable guaranty.** (a) "Suitable guaranty" means:

(1) a surety bond or an irrevocable letter of credit issued for the benefit of persons holding qualified rights of payment against the licensed certification authority named as the principal of the bond or the customer of the letter of credit; or

(2) a policy of insurance that provides that claims may be made and resolved without obtaining a qualified right to payment.

(b) The suitable guaranty must:

of quality and financial responsibility it provides to persons who rely on certificates issued by licensed certification authorities;

(3) specify reasonable requirements for the form of certificates issued by licensed certification authorities, in accordance with generally accepted standards for digital signature certificates;

(4) specify reasonable requirements for record keeping by licensed certification authorities;

(5) specify reasonable requirements for the content, form, and sources of information in certification authority disclosure records, the updating and timeliness of the information, and other practices and policies relating to certification authority disclosure records;

(6) specify the form of the certification practice statements; and

(7) specify the procedure and manner in which a certificate may be suspended or revoked.

Subd. 4. **Certification practice statement.** The secretary in the role of licensed certification authority may adopt and amend a certification practice statement without using the provisions of chapter 14.

History: 1997 c 178 s 4; 1998 c 321 s 9; 1999 c 250 art 1 s 94

325K.04 FEES.

(a) The secretary shall set reasonable fees for all services rendered under this chapter, in amounts sufficient to compensate for the costs of all services provided by the secretary under this chapter. Until July 1, 2001, the fees need not be set by rule.

(b) The digital signature account is created in the special revenue fund. All fees recovered by the secretary must be deposited in the digital signature account. Money in the digital signature account is appropriated to the secretary to pay the costs of all services provided by the secretary.

History: 1997 c 178 s 5; 1999 c 250 art 1 s 95

325K.05 LICENSURE AND QUALIFICATIONS OF CERTIFICATION AUTHORITIES.

Subdivision 1. **License conditions.** To obtain or retain a license, a certification authority must:

(1) be the subscriber of a certificate issued by the secretary and published in a recognized repository;

(2) employ as operative personnel only persons who have not been convicted within the past 15 years of a felony or a crime involving fraud, false statement, or deception;

(3) employ as operative personnel only persons who have demonstrated knowledge and proficiency in following the requirements of this chapter;

(4) file with the secretary a suitable guaranty, unless the certification authority is a department, office, or official of a federal, state, city, or county governmental entity that is self-insured;

(5) use a trustworthy system, including a secure means for limiting access to its private key;

(6) present proof to the secretary of having working capital reasonably sufficient, according to rules adopted by the secretary, to enable the applicant to conduct business as a certification authority;

(7) register its business organization with the secretary, unless the applicant is a governmental entity or is otherwise prohibited from registering;

(8) require a potential subscriber to appear in person before the certification authority, or an agent of the certification authority, to prove the subscriber's identity before a certificate is issued to the subscriber; and

(9) comply with all further licensing requirements established by rule by the secretary.

The secretary may, by rule, establish standards by which the in-person registration required in clause (8) may be waived.

Subd. 2. **License procedures.** The secretary must issue a license to a certification authority that:

(1) is qualified under subdivision 1;

(2) applies in writing to the secretary for a license; and

(3) pays a filing fee adopted by rule by the secretary.

Subd. 3.[Repealed, 1998 c 321 s 31]

Subd. 4. **Revocation or suspension.** (a) The secretary may revoke or suspend a certification authority's license, in accordance with the Administrative Procedure Act, chapter 14, for failure to comply with this chapter or for failure to remain qualified under subdivision 1.

(b) The secretary may order a summary suspension of a license. The written order for summary suspension may include a finding that the certification authority has:

(1) used its license in the commission of a state or federal crime or of a violation of sections 325F.68 to 325F.70; or

(2) engaged in conduct giving rise to serious risk of loss to public or private parties if the license is not immediately suspended.

Subd. 5. **Other authorities.** The secretary may recognize by rule the licensing or authorization of certification authorities by non-Minnesota governmental entities, provided that those licensing or authorization requirements are substantially similar to those of this state. If licensing by another governmental entity is so recognized:

(1) sections 325K.19 to 325K.24 apply to certificates issued by the certification

subscriber may use only a trustworthy system:

(1) to issue, suspend, or revoke a certificate;

(2) to publish or give notice of the issuance, suspension, or revocation of a certificate; or

(3) to create a private key.

Subd. 2. **Disclosure required.** A licensed certification authority shall disclose any material certification practice statement and disclose any fact material to either the reliability of a certificate that it has issued or its ability to perform its services. A certification authority may require a signed, written, and reasonably specific inquiry from an identified person and payment of reasonable compensation as conditions precedent to effecting a disclosure required in this subdivision.

Subd. 3. **Acceptance.** A recipient who accepts a digital signature when the certificate was issued by a licensed certification authority becomes a party to and accepts all of the terms and conditions of the licensed certification authority's certification practice statement.

History: 1997 c 178 s 10; 1999 c 250 art 1 s 97

325K.10 ISSUANCE OF CERTIFICATE.

Subdivision 1. **Conditions.** A licensed certification authority may issue a certificate to a subscriber only after all of the following conditions are satisfied:

(1) the certification authority has received a request for issuance signed by the prospective subscriber;

(2) the prospective subscriber or the prospective subscriber's duly authorized agent must appear before the licensed certification authority to present the request; and

(3) the certification authority has confirmed that:

(i) the prospective subscriber is the person to be listed in the certificate to be issued;

(ii) if the prospective subscriber is acting through one or more agents, the subscriber duly authorized each agent to have custody of the subscriber's private key and to request issuance of a certificate listing the corresponding public key;

(iii) the information in the certificate to be issued is accurate;

(iv) the prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate;

(v) the prospective subscriber holds a private key capable of creating a digital signature;

(vi) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber; and

(vii) the certificate provides information sufficient to locate or identify one or more

authorities licensed or authorized by that governmental entity in the same manner as it applies to licensed certification authorities of this state; and

(2) the liability limits of section 325K.17 apply to the certification authorities licensed or authorized by that governmental entity in the same manner as they apply to licensed certification authorities of this state.

Subd. 6. **Applicability to digital signatures.** Parties may provide by contract for the effectiveness, enforceability, or validity of any digital signature as between those parties. Sections 325K.19 to 325K.24 do not apply to a certificate and associated digital signature issued by an unlicensed certification authority.

Subd. 7. **Nonapplicability.** A certification authority that has not obtained a license is not subject to the provisions of this chapter, except as specifically provided.

History: 1997 c 178 s 6; 1998 c 321 s 10-*14*; 1999 c 250 art 1 s 96; 2000 c 395 s 15

325K.06 PERFORMANCE AUDITS.

Subdivision 1. **Annual audit; auditor qualifications; rules.** A certified public accountant having expertise in computer security must audit the operations of each licensed certification authority at least once each year to evaluate compliance with this chapter. The secretary may by rule specify the qualifications of auditors.

Subd. 2. **Compliance categories.** Based on information gathered in the audit, the auditor must categorize the licensed certification authority's compliance as one of the following:

(a) **Full compliance.** The certification authority appears to conform to all applicable statutory and regulatory requirements.

(b) **Substantial compliance.** The certification authority appears generally to conform to applicable statutory and regulatory requirements. However, one or more instances of noncompliance or of inability to demonstrate compliance were found in an audited sample, but were likely to be inconsequential.

(c) **Partial compliance.** The certification authority appears to comply with some statutory and regulatory requirements, but was found not to have complied or not be able to demonstrate compliance with one or more important safeguards.

(d) **Noncompliance.** The certification authority complies with few or none of the statutory and regulatory requirements, fails to keep adequate records to demonstrate compliance with more than a few requirements, or refused to submit to an audit.

The secretary shall publish in the certification authority disclosure record it maintains for the certification authority the date of the audit and the resulting categorization of the certification authority.

Subd. 3.[Repealed, 1998 c 321 s 31]

Subd. 4.[Repealed, 1998 c 321 s 31]

Subd. 5.[Repealed, 1998 c 321 s 31]

false;

(2) the certificate satisfies all material requirements of this chapter; and

(3) the certification authority has not exceeded any limits of its license in issuing the certificate.

The certification authority may not disclaim or limit the warranties of this subdivision.

Subd. 2. **Negotiable warranties to subscribers.** Unless the subscriber and certification authority otherwise agree, a certification authority, by issuing a certificate, promises to the subscriber:

(1) to act promptly to suspend or revoke a certificate in accordance with section 325K.14 or 325K.15; and

(2) to notify the subscriber within a reasonable time of any facts known to the certification authority that significantly affect the validity or reliability of the certificate once it is issued.

Subd. 3. **Warranties to those who reasonably rely.** By issuing a certificate, a licensed certification authority certifies to all who reasonably rely on the information contained in the certificate that:

(1) the information in the certificate and listed as confirmed by the certification authority is accurate;

(2) all information foreseeably material to the reliability of the certificate is stated or incorporated by reference within the certificate;

(3) the subscriber has accepted the certificate; and

(4) the licensed certification authority has complied with all applicable laws of this state governing issuance of the certificate.

Subd. 4. **Warranties following publication.** By publishing a certificate, a licensed certification authority certifies to the repository in which the certificate is published and to all who reasonably rely on the information contained in the certificate that the certification authority has issued the certificate to the subscriber.

History: 1997 c 178 s 12

325K.12 REPRESENTATIONS AND DUTIES UPON ACCEPTING CERTIFICATE.

Subdivision 1. **Subscriber warranties.** By accepting a certificate issued by a licensed certification authority, the subscriber listed in the certificate certifies to all who reasonably rely on the information contained in the certificate that:

(1) the subscriber rightfully holds the private key corresponding to the public key listed in the certificate;

(2) all representations made by the subscriber to the certification authority and material to the information listed in the certificate are true; and

Subd. 4. **Terminating suspension.** A certification authority must terminate a suspension initiated by request only:

(1) if the subscriber named in the suspended certificate requests termination of the suspension and the certification authority has confirmed that the person requesting suspension is the subscriber or an agent of the subscriber authorized to terminate the suspension; or

(2) when the certification authority discovers and confirms that the request for the suspension was made without authorization by the subscriber. However, this clause does not require the certification authority to confirm a request for suspension.

Subd. 5. **Contract limitation or preclusion.** The contract between a subscriber and a licensed certification authority may limit or preclude requested suspension by the certification authority, or may provide otherwise for termination of a requested suspension. However, if the contract limits or precludes suspension by the secretary when the issuing certification authority is unavailable, the limitation or preclusion is effective only if notice of it is published in the certificate.

Subd. 6. **Misrepresentation.** No person may knowingly or intentionally misrepresent to a certification authority the person's identity or authorization in requesting suspension of a certificate. Violation of this subdivision is a misdemeanor.

Subd. 7.[Repealed, 1998 c 321 s 31]

Subd. 8. **Completion of suspension.** A suspension under this section must be completed within 24 hours of receipt of all of the information required in this section.

Subd. 9. **Administrative procedures.** For purposes of this section, the provisions of chapter 14 do not apply when the secretary acts as a licensed certification authority for governmental entities.

History: 1997 c 178 s 15; 1998 c 321 s 20-*24*; 1999 c 250 art 1 s 99

325K.15 CERTIFICATE REVOCATION.

Subdivision 1. **After request.** A licensed certification authority must revoke a certificate that it issued but which is not a transactional certificate, after:

(1) receiving a request for revocation by the subscriber named in the certificate; and

(2) confirming that the person requesting revocation is the subscriber, or is an agent of the subscriber with authority to request the revocation.

Subd. 2. **After identity confirmed.** A licensed certification authority must confirm a request for revocation and revoke a certificate within one business day after receiving both a subscriber's written request and evidence reasonably sufficient to confirm the identity and any agency of the person requesting the suspension.

Subd. 3. **After death or dissolution.** A licensed certification authority must revoke a certificate that it issued:

(1) upon receiving a certified copy of the subscriber's death record, or upon

of the violation of this chapter that is the basis for the claim. Notice under this subdivision need not include the requirement imposed by subdivision 3, paragraph (a), clause (2).

History: 1997 c 178 s 19; 1998 c 321 s 27,28; 2000 c 395 s 19

325K.19 SATISFACTION OF SIGNATURE REQUIREMENTS.

(a) Where a rule of law requires a signature, or provides for certain consequences in the absence of a signature, that rule is satisfied by a digital signature, if:

(1)(i) the digital signature is that of a public or local official as defined in section 10A.01, subdivisions 22 and 35, on government records described in section 15.17; or

(ii) no party affected by a digital signature objects to the use of digital signatures in lieu of a signature, and the objection may be evidenced by refusal to provide or accept a digital signature;

(2) that digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority;

(3) that digital signature was affixed by the signer with the intention of signing the message and after the signer has had an opportunity to review items being signed; and

(4) the recipient has no knowledge or notice that the signer either:

(i) breached a duty as a subscriber; or

(ii) does not rightfully hold the private key used to affix the digital signature.

(b) However, nothing in this chapter precludes a mark from being valid as a signature under other applicable law.

History: 1997 c 178 s 20; 2000 c 395 s 20

325K.20 UNRELIABLE DIGITAL SIGNATURES.

Unless otherwise provided by law or contract, the recipient of a digital signature assumes the risk that a digital signature is forged, if reliance on the digital signature is not reasonable under the circumstances. If the recipient determines not to rely on a digital signature under this section, the recipient must promptly notify the signer of any determination not to rely on a digital signature and the grounds for that determination. Nothing in this chapter shall be construed to obligate a person to accept a digital signature or to respond to an electronic message containing a digital signature.

History: 1997 c 178 s 21

325K.21 DIGITALLY SIGNED DOCUMENT IS WRITTEN.

(a) A message is as valid, enforceable, and effective as if it had been written on paper, if it:

(1) bears in its entirety a digital signature; and

I

CHAPTER 8275

SECRETARY OF STATE

ELECTRONIC AUTHENTICATION

8275.0005 SCOPE AND PURPOSE OF CHAPTER.

This chapter implements the Minnesota Electronic Authentication Act, codified as Minnesota Statutes, chapter 325K.

Statutory Authority: *MS s 325K.01; 325K.03; 325K.04; 325K.05; 325K.06; 325K.07*

History: *23 SR 1352*

Posted: *October 27, 2003*

8275.0010 DEFINITIONS.

Subpart 1. **Scope.** For purposes of this chapter, the terms in Minnesota Statutes, chapter 325K, have the meanings given them in that chapter, and the terms in subparts 2 to 5 have the meanings given them in this part.

Subp. 2. **Business organization.** "Business organization" means any type of business association recognized under Minnesota law.

Subp. 3. **Interested party.** "Interested party" means a jurisdiction, certification authority, subscriber, relying party, or potential subscriber or relying party.

Subp. 4. **Operative personnel.** "Operative personnel" means one or more individuals acting as a certification authority or its agent, or in the employment of, or under contract with, a certification authority, and who have duties directly involving the issuance of certificates including the identification of persons requesting a certificate from a certification authority, creation of private keys, or administration of a licensed certification authority's computing facilities.

Subp. 5. **X.509.** "X.509" means the Information Technology - Open Systems Interconnection - The directory authentication framework authored and published by the International Telecommunication Union which is incorporated by reference in part 8275.0060.

Statutory Authority: *MS s 325K.01; 325K.03; 325K.04; 325K.05; 325K.06; 325K.07*

History: *23 SR 1352*

Posted: *October 27, 2003*

8275.0015 APPLICATION FOR LICENSE AS CERTIFICATION AUTHORITY.

To be licensed, a certification authority shall demonstrate compliance with the requirements of Minnesota Statutes, section 325K.05, by submitting the following:

A. a completed application containing:

(1) the applicant's name as registered with the secretary;

(2) the registration number assigned by the secretary to the business registration;

(3) the applicant's mailing address, including the country, if appropriate, and the zip or other postal code;

(4) the applicant's electronic mailing address, which the applicant will monitor regularly for incoming mail to facilitate communication under this chapter;

(5) a Uniform Resource Locator (URL) for the applicant's presence on the Internet; and

(6) the applicant's telephone and facsimile numbers including area code and country code, if applicable.

B. the fee or fees provided by part 8275.0050;

C. a certificate issued by the secretary that shows the applicant as the subscriber and is published in a recognized repository;

D. a suitable guaranty, described by part 8275.0025, unless the applicant is the secretary, or a federal, state, or city governmental entity that is self-insured;

E. demonstration of sufficient working capital as required by part 8275.0030;

F. documentation, in the form of an information systems audit, establishing that the applicant has the use of a trustworthy system as defined by part 8275.0040. The audit required by this item must be performed according to part 8275.0070, except that it is not required to establish anything more than that the applicant has the use of a trustworthy system;

G. a statement that each person employed as operative personnel has qualified to act as operative personnel and that a criminal background check has been conducted;

H. registration of the underlying business organization with the secretary, unless the registration is prohibited by law, and in the event the registration is prohibited, the applicant shall provide to the secretary the name and address in Minnesota of an agent for the service of process; and

I. a written certification practice statement as described in part 8275.0045.

Statutory Authority: *MS s 325K.01; 325K.03; 325K.04; 325K.05; 325K.06; 325K.07*

History: *23 SR 1352*

Posted: *October 27, 2003*

8275.0020 ISSUANCE OF LICENSE OR RENEWAL.

Subpart 1. **Requirements.** The secretary shall issue a license as a certification authority if the applicant has submitted all of the documentation required by part 8275.0015.

Subp. 2. **Term.** A license is valid for one year. To renew a license, the applicant must submit all of the documentation required by part 8275.0015. The license may be renewed for successive one-year periods. If information contained in the application changes, the certification authority has ten days to submit information to the secretary to update its record.

Statutory Authority: *MS s 325K.01; 325K.03; 325K.04; 325K.05; 325K.06; 325K.07*

History: *23 SR 1352*

Posted: *October 27, 2003*

8275.0025 SUITABLE GUARANTY.

The suitable guaranty required for licensure as a certification authority under part 8275.0015, item D, may be in the form of a surety bond executed by an insurer lawfully operating in this state, an irrevocable letter of credit issued by a financial institution authorized to do business in this state, or a policy of insurance issued by an insurance company authorized by the commissioner of commerce to do business in this state. The suitable guaranty must be in an amount of at least $100,000. The suitable guaranty must:

A. identify the insurer or financial institution upon which it is drawn, including the name, mailing address, and physical address, and identify by number or copy its licensure or approval as an insurer or financial institution in this state;

B. identify the certification authority on behalf of which it is issued;

C. be issued payable (1) for the benefit of persons holding qualified rights of payment against the licensed certification authority named as principal of the bond or customer of the letter of credit; or (2) based on claims made against the insured and resolved without first obtaining a qualified right to payment;

D. state that it is issued under the Minnesota Electronic Authentication Act, Minnesota Statutes, chapter 325K; and

E. specify a term of effectiveness of at least five years.

Statutory Authority: *MS s 325K.01; 325K.03; 325K.04; 325K.05; 325K.06; 325K.07*

History: *23 SR 1352*

Posted: *October 27, 2003*

8275.0030 WORKING CAPITAL.

Subpart 1. **Generally.** A certification authority's working capital is sufficient for licensing or renewal purposes if, at the time application for licensure or renewal is made, its current assets minus current liabilities exceeds $50,000.

The existence of working capital must be demonstrated through an audited financial statement authenticated by a licensed certified public accountant and dated no more than 60 days before the date it is received by the secretary.

Subp. 2. **Governmental entities.** A federal, state, or city governmental entity is considered to have sufficient working capital without providing any documentation.

Statutory Authority: *MS s 325K.01; 325K.03; 325K.04; 325K.05; 325K.06; 325K.07*

History: *23 SR 1352*

Posted: *October 27, 2003*

8275.0035 QUALIFICATION OF OPERATIVE PERSONNEL.

The certification authority shall determine whether an individual employed or acting as operative personnel qualifies to act as operative personnel according to Minnesota Statutes, sections 325K.01, subdivision 21, and 325K.05, subdivision 1, clauses (2) and (3). The determination must be made after a criminal background check of the individual and based on the individual's knowledge of this chapter and Minnesota Statutes, chapter 325K. The certification authority shall continue to monitor the qualifications of operative personnel on an ongoing basis. If at any time operative personnel are determined to not be qualified as defined in this part, the individual's employment as operative personnel with the certification authority must be immediately terminated. The steps that a certification authority takes to assess an individual's qualification to be employed as operative personnel must be disclosed in the certification practice statement.

Statutory Authority: *MS s 325K.01; 325K.03; 325K.04; 325K.05; 325K.06; 325K.07*

History: *23 SR 1352*

Posted: *October 27, 2003*

8275.0040 TRUSTWORTHY SYSTEM.

The certification authority or repository must operate a trustworthy system. A system shall be regarded as trustworthy if it satisfies the most current adopted version of Common Criteria (CC) Protection Profile

(PP) for Commercial Security 2 (CS2), (CCPPCS), developed and published by the National Institute of Standards and Technology (NIST). The determination whether a departure from CCPPCS is material is governed by part 8275.0070, subpart 2. For purposes of this chapter, CCPPCS shall be interpreted in a manner that is reasonable in the context in which a system is used and is consistent with other state and federal laws. Until the referenced standard is adopted by NIST, the standard applicable for purposes of this chapter shall be the draft of CCPPCS dated March 1998. The March 1998 draft and all subsequent revisions is incorporated by reference and is not subject to frequent change. The draft is available from the State Law Library and NIST at http://csrc.nist.gov/nistpubs/cc/pp/pplist.htm/#cs2.

Statutory Authority: *MS s 325K.01; 325K.03; 325K.04; 325K.05; 325K.06; 325K.07*

History: *23 SR 1352*

Posted: *October 27, 2003*

8275.0045 CERTIFICATION PRACTICE STATEMENTS.

Subpart 1. **Required contents.** Each licensed certification authority shall file with the secretary a certification practice statement demonstrating compliance with the requirements of Minnesota Statutes, chapter 325K. This statement must disclose:

A. the practices the certification authority uses in issuing, suspending, and revoking certificates. If certificates are issued by class or level of service, the necessary criteria for each class or level of service must also be disclosed;

B. any warnings, liability limitations, warranty disclaimers, and indemnity and hold harmless provisions on which the certification authority intends to rely;

C. any disclaimers and limitations on obligations, losses, or damages to be asserted by the certification authority;

D. a written description of all representations by the subscriber to the certification authority about the subscriber's responsibility to protect the secrecy of the private key;

E. any mandatory dispute resolution process, including choice of forum and choice of law provisions;

F. where the summary of the most recent report of the auditor may be found which may be in the form of a URL;

G. the method used to determine that operative personnel are qualified to act and have knowledge regarding this chapter and Minnesota Statutes, chapter 325K, both initially and periodically throughout employment; and

H. the method used to initially determine that operative personnel have not been convicted within the past 15 years of a felony or a crime involving fraud, false statement, or deception and the method used to continue to evaluate the status of operative personnel.

Subp. 2. [Repealed, L 1999 c 250 art 1 s 115]

Statutory Authority: *MS s 325K.01; 325K.03; 325K.04; 325K.05; 325K.06; 325K.07*

History: *23 SR 1352; L 1999 c 250 art 1 s 115*

Statutory Authority: *MS s 325K.01; 325K.03; 325K.04; 325K.05; 325K.06; 325K.07*

History: *23 SR 1352*

Posted: *October 27, 2003*

8275.0065 RECORD KEEPING.

Subpart 1. **General requirement.** A licensed certification authority shall make, keep, and preserve records that demonstrate compliance with:

A. Minnesota Statutes, section 325K.05, subdivision 1;

B. Minnesota Statutes, section 325K.10, including all notices of suspension of certificates according to Minnesota Statutes, section 325K.10, subdivision 4;

C. Minnesota Statutes, section 325K.14, subdivision 1;

D. Minnesota Statutes, section 325K.15; and

E. Minnesota Statutes, section 325K.18.

Subp. 2. **Subscriber identity records.** A licensed certification authority shall maintain a database file that contains:

A. records of the identity of the subscriber named in each certificate issued by the certification authority, including all the facts represented in the certificate other than the extension data referenced in X.509;

B. the date of issuance of the certificate; and

C. the certificate serial number as defined in X.509.

Subp. 3. **Time stamp records.** A licensed certification authority shall maintain a database file of certificate-related time-stamps issued by the certification authority, including the name of the subscriber, a reference to the certificate used in the transaction such as a serial number, and a description of the item being time-stamped.

Subp. 4. **Retention period.** All records retained under this part must be kept by the licensed certification authority for at least ten years.

Subp. 5. **Form and accessibility.** Records may be inscribed on any tangible medium or stored in an electronic or other medium so long as they are retrievable, readable, accurate, complete, and accessible. The records must be indexed, stored, preserved, and reproducible so as to be authentic, reliable, complete, and accessible. Certificate extension data, referenced in X.509, is not required to be part of any publicly accessible record.

Statutory Authority: *MS s 325K.01; 325K.03; 325K.04; 325K.05; 325K.06; 325K.07*

History: *23 SR 1352*

Posted: *October 27, 2003*

8275.0070 COMPLIANCE AUDITS.

8275.0090 CIVIL PENALTIES.

The secretary may, by order, impose and collect a civil monetary penalty against a licensed certification authority for a violation of Minnesota Statutes, chapter 325K, as provided by Minnesota Statutes, section 325K.07, subdivision 3.

Statutory Authority: *MS s 325K.01; 325K.03; 325K.04; 325K.05; 325K.06; 325K.07*

History: *23 SR 1352*

Posted: *October 27, 2003*

8275.0095 CRITERIA FOR DETERMINING PENALTY AMOUNTS.

In determining the appropriate penalty amount against a licensed certification authority for violation of this chapter or Minnesota Statutes, chapter 325K, the secretary may consider the nature of the violation and the extent or magnitude of the severity of the violation, including:

A. the damages arising from the violation, including:

(1) the financial impact of the violation to any subscriber, relying party, or other person;

(2) the costs incurred by the state in enforcement, including reasonable investigative costs; or

(3) the nonfinancial consequences of the violation, including harm to any subscriber, relying party, or other person;

B. the nature of the violation, including whether it was continuing in nature, involved criminal conduct, or tended to significantly impair the reliability of any certificate or key pair;

C. the presence of any aggravating circumstances, including whether the violator:

(1) intentionally committed the violation with knowledge that the conduct constituted a violation;

(2) attempted to conceal the violation;

(3) was untruthful or uncooperative in dealing with the secretary or the secretary's staff;

(4) had committed prior violations found by the secretary; or

(5) incurred no other sanction as a result of the violation;

D. the presence of any mitigating circumstances, including whether the violator:

(1) had taken any prior action to correct the violation or mitigate its consequences;

(2) had previously paid damages to a party resulting from the violation;

(3) acted without intention to commit a violation; or

(4) acted reasonably in light of any other mitigating factors considered relevant by the secretary.

Statutory Authority: *MS s 325K.01; 325K.03; 325K.04; 325K.05; 325K.06; 325K.07*

History: *23 SR 1352*

The requirement to update information does not apply to changes in the certification authority's financial condition. Updates of financial information are made only on receipt of audited financial statements.

Subp. 3. **Use of secretary of state's records.** In compiling and maintaining certification authority disclosure records, the secretary shall use the records of the Office of the Secretary of State, and is not obligated to conduct any affirmative investigation or review beyond the face of those records.

Statutory Authority: *MS s 325K.01; 325K.03; 325K.04; 325K.05; 325K.06; 325K.07*

History: *23 SR 1352*

Posted: *October 27, 2003*

8275.0110 RECOGNITION OF REPOSITORIES.

A repository desiring to be recognized shall demonstrate compliance with Minnesota Statutes, section 325K.25, by submitting all of the following:

A. the name of the licensed certification authority, or applicant for licensure as a certification authority, requesting recognition of a repository;

B. the applicant's registration number assigned by the secretary to the business registration of the repository;

C. the applicant's mailing address, including the country, if appropriate, and the zip or other postal code;

D. the applicant's telephone and facsimile numbers, including the area code and country code, if appropriate;

E. the applicant's electronic mail address which the applicant will monitor regularly for incoming mail to facilitate communication under this chapter;

F. a URL for the applicant's presence on the Internet;

G. a description of the database and system architecture demonstrating that it satisfies the requirements of Minnesota Statutes, section 325K.25, subdivision 1, clause (3);

H. registration of the underlying business organization with the secretary unless the registration is prohibited by law, and in the event the registration is prohibited, the applicant shall provide the secretary the name and address of an agent for service of process; and

I. the fee required by part 8275.0050.

Statutory Authority: *MS s 325K.01; 325K.03; 325K.04; 325K.05; 325K.06; 325K.07*

History: *23 SR 1352*

Posted: *October 27, 2003*

8275.0115 REVOCATION OF RECOGNITION OF REPOSITORY.

Subpart 1. **Grounds.** This part describes the secretary's procedure for revoking the recognition of a repository without also revoking the license of the certification authority that operates the repository.

Because a valid license as a certification authority is a statutory requirement for recognition of a repository, the secretary shall automatically revoke the recognition of any repository operated by a certification authority whose license is revoked, expired, or otherwise inoperative.

The secretary may revoke recognition of a repository according to Minnesota Statutes, section 325K.25, subdivision 3, for failure to comply with any requirement of this chapter or Minnesota Statutes, section 325K.25, or for failure to comply with a lawful order of the secretary.

Subp. 2. **Notice.** The secretary shall inform a licensed certification authority that operates a recognized repository by a notice directed to the mailing address and the electronic mail address of a decision to revoke or suspend the license. If an electronic mail message is used, it must be sent as a direct message and not as an attachment to electronic mail. The notice must state when the revocation or suspension will be effective, which cannot be less than 30 days following the issuance of the order except in the case of a summary suspension.

Subp. 3. **Effective date.** If the licensee files an application for a contested case hearing before the effective date of revocation or suspension, the suspension or revocation will not take effect until so ordered by the administrative law judge, except in the case of a summary suspension. The secretary may order the summary suspension of a license pending proceedings for revocation or other action as described in Minnesota Statutes, section 325K.14. A summary suspension of a license is effective from the date of the secretary's order.

Statutory Authority: *MS s 325K.01; 325K.03; 325K.04; 325K.05; 325K.06; 325K.07*

History: *23 SR 1352*

Posted: *October 27, 2003*

8275.0120 CONTRACT FOR SECRETARY OF STATE REPOSITORY PUBLICATION.

The secretary may either directly operate, or contract for the operation of, a repository including an on-line publicly accessible database described in Minnesota Statutes, section 325K.01, subdivision 6. If the secretary contracts for the operation of the repository, the contractor shall be a licensed certification authority and shall agree to operate according to all requirements of Minnesota Statutes, chapter 325K. The contract may be rescinded for any reason that would form a basis for revoking recognition of a repository.

Statutory Authority: *MS s 325K.01; 325K.03; 325K.04; 325K.05; 325K.06; 325K.07*

History: *23 SR 1352*

Posted: *October 27, 2003*

8275.0125 PUBLICATION IN SECRETARY OF STATE REPOSITORY.

The secretary shall maintain, either directly or under contract, a repository for the purpose of publishing information required by statute. Information published in the secretary's repository must include:

A. the certification authority disclosure record for each certification authority licensed or certified in Minnesota;

B. a list of all judgments filed with the secretary within the previous five years pursuant to Minnesota Statutes, section 325K.03, subdivision 2; and

C. any other information necessary or appropriate for publication in the secretary's repository according to this chapter or Minnesota Statutes, chapter 325K.

Statutory Authority: *MS s 325K.01; 325K.03; 325K.04; 325K.05; 325K.06; 325K.07*

History: *23 SR 1352*

Posted: *October 27, 2003*

8275.0130 PROCEDURE UPON DISCONTINUANCE OF BUSINESS AS REPOSITORY.

Each licensed certification authority that discontinues providing services as a recognized repository must deposit the records required by part 8275.0065 in escrow once each calendar year with the organization conducting the audit required by this chapter. The escrowed records must also include a copy of the software needed to read the records or the records must be stored in a retrievable, readable, accurate, complete, and accessible manner. Escrowed records must be kept permanently by the auditor. A licensed certification authority that discontinues providing services as a recognized repository without making other arrangements for preservation of the certification authority's records must submit the escrowed records held by the auditor to another recognized repository or repositories designated by the secretary or to another recognized repository not licensed but recognized in this state, but designated by the secretary.

If the auditor goes out of business, it must transfer all of the escrowed records to another auditing firm designated by the secretary.

Statutory Authority: *MS s 325K.01; 325K.03; 325K.04; 325K.05; 325K.06; 325K.07*

History: *23 SR 1352*

Posted: *October 27, 2003*

8275.0135 USE OF FOREIGN LICENSED CERTIFICATION AUTHORITIES.

Subpart 1. **Presumptions.** Digital signatures made pursuant to a certificate issued by a certification authority are entitled to the presumptions in Minnesota Statutes, sections 325K.19 to 325K.24:

A. if the parties mutually agree to the provisions in a contract;

B. if the certification authority obtains a license as a certification authority from the secretary; or

C. if the certification authority is licensed by a governmental entity other than the state of Minnesota and the secretary determines that the requirements for licensure in that jurisdiction are

Posted: *October 27, 2003*