CROMERR Successful Approaches: Challenge-Question "Second Factor" Approach

CROMERR Authentication Standards

Under CROMERR, systems that accept electronic signatures (e-signatures) must be able to provide proof that the e-signatures they accept are valid and were created with an e-signature device that was not compromised at the time of signature (see rule's pertinent language in 3.2000(b)(5)(i), in the context of 3.2000(b) and 3.2000(b)(5), together with definitions of "valid electronic signature" and "electronic signature device"). This requirement poses a special challenge where the e-signature device is a PIN/password because PIN/passwords are easy to compromise since they are easy to share – either intentionally or by accident – and a PIN/password, once shared, is forever compromised. Specifically, CROMERR requires that a system receiving electronically-signed documents "submitted in lieu of paper documents to satisfy requirements under an authorized program…must be able…to generate data…as needed, and in a timely manner…sufficient to prove…" that the e-signature was valid at the time of signing, that is that the PIN/password was not compromised. Due to the inherent vulnerability to compromise, a PIN/password on its own used to create an e-signature does not provide the receiving system with "…data…sufficient to prove…" that the PIN/password was not compromised at the time of signing. Therefore, EPA has determined that to meet the CROMERR requirement, a system using PIN/password must be accompanied by some other identifier that together with the PIN/password will be sufficient to prove that the e-signature has not been compromised.

One approach is to use the PIN/password in conjunction with a 'second factor' to create an e-signature, so that the PIN/password + second factor combination can be shown to be uncompromised even if there are questions about whether the PIN/password itself has been shared. Under this approach, the second factor must be an item, other than the PIN/password, or some event whose demonstrated presence or occurrence at the time of signature provides independent evidence of the signer's identity. The CROMERR preamble provided examples of second factors in the form of items that would be within the exclusive control of the signer – such as a smart card or other

For More Information:
cromerr@epa.gov

http://www.epa.gov/cromerr/

physical token, or a piece of private information – and would remain within the signer's exclusive control even if the PIN/password in itself were compromised (see page 59870, October 13, 2005, *Federal Register* notice).

Challenge-Question Approach

One successful technology-based approach is having the system present the user with a challenge -question each time a user enters their PIN/password to execute a signature. The system randomly selects the challenge-question from a set of questions for which the user has provided pre-arranged answers. Where an e-signature is executed with a PIN/ password, a challenge-question approach provides a "second factor" to strengthen the PIN/password-based e-signature, helping to ensure that the PIN/password has not been compromised. Systems with PIN/password-based e-signatures that use the challenge-question approach as a "second factor" provide significant added protection against signature repudiation and help meet the CROMERR performance standard that systems use an approach that demonstrates that e-signatures are valid as defined by the rule. States are welcome to propose other options that demonstrate that the PIN/password has not been compromised.

CROMERR-Compliant Solution

EPA has approved several systems that implement the use of challenge questions as a second factor for PIN/passwords. The minimum number of candidate questions, pre-arranged question-answer pairs, and questions asked used in those systems was:

10-5-1 – that is, at the time a user registers to use an electronic reporting system, the user selects from 10 challenge questions 5 that they will answer as part of registration. At the time of signature 1 of these five challenge questions is then chosen at random and posed to the signatory. Only a correct answer to this challenge question will allow the user's PIN and password to be applied to the electronic document. *

*While the list of question choices can be as small as 10, a longer list of at least 20 is recommended to give the registrant a better chance of finding 5 questions s/he can answer from memory.

- Used as an authentication factor, challenge-questions represent a compromise. They are not as strong as solutions based on hardware-tokens or biometrics, but they are much easier and cheaper to implement.
- The number of pre-answered questions should be at least 5, because a lower number would not allow meaningful randomization of questions to be posed at signing. Also, the lower the number of pre-answered questions, the easier it would be for a defendant in a judicial proceeding to make a claim undermining the utility of the challenge-question as evidence of the signer's identity
- No EPA system that receives enforcement-sensitive e-reports implements anything that has fewer questions than 10-5-1. EPA's Central Data Exchange (CDX), which supports most EPA e-reporting, implements 20-5-1.

Other Recommendations

- Careful Selection of Challenge Questions: We recommend that systems carefully select the pool of challenge questions from which users may select at the time of registration.
  - Questions should generally elicit information that cannot be easily researched on the internet and which would not normally be known by anyone other than the registrant.
  - Questions should, whenever possible, elicit a simple, single-word (or numeric) answer.
- Another Important System Feature:
  - The system should check the answers provided at registration for expected variation to ensure that the same answer cannot be provided to all of the challenge questions.
  - The challenge question should generally be posed as part of the signature event, not sign-in. If the challenge question is only posed as part of sign-in, then the system should contain a time-out feature that automatically logs users off after 15 minutes (or sooner).