Two-Factor Authentication Ahead for Federation Manager

Two-Factor Authentication Ahead for Federation Manager

InCommon is introducing two-factor authentication to protect the Federation Manager, the application site administrators use to update their organization's metadata. This data is critical to establishing the trust backbone of the InCommon Federation. Although the current login system requires the use of strong passwords, adding two-factor authentication will substantially increase account security. This is in response to a risk assessment of the Federation Manager undertaken by the InCommon Technical Advisory Committee.

InCommon chose Duo Security's two-factor authentication technology because it leverages mobile phones, devices almost all users already have. To authenticate, a user first types a password and then confirms the login attempt with the Duo Mobile smartphone app. After confirming the login attempt, the user is authenticated. Duo also supports second-factor delivery via text message, phone call, and one-time password tokens.

InCommon Registration Authority administrators are already using Duo two-factor authentication to log into the Federation Manager. Site administrators will begin logging in with a second factor in June. The transition to Duo two-factor is expected to continue throughout the summer. More information about Duo Security is at www.duosecurity.com.