Multi-Factor Authentication

NEBRASKA
Good Life. Great Vision.
OFFICE OF THE CIO

April 2018

1. Rate: Per user, per month $4.00

2. General Overview:

Multi-factor authentication (MFA) is a method of computer and network access control that involves at least two of three categories:

- Knowledge factors ("things only the user knows"), such as passwords;
- Possession factors ("things only the user has"), such as tokens or fobs;
- Inherence factors ("things only the user is"), such as biometrics.

Requiring a second factor from a different category greatly strengthens computer and network security. For this reason, MFA is becoming widely adopted for protecting sensitive data, and some federal agencies already mandate MFA whenever accessing their information.

The MFA Service allows a choice of either a hardware token, software token, text message, or phone call. The hardware token is a separate device that the user keeps in possession. It generates a random number that is synchronized with the central MFA manager. The cost of the hardware token is a separate charge.

3. Service Description:

How Multi-Factor Authentication (MFA) Works

When receiving a request to access a protected resource, the system prompts the user for another factor. The factor could be responding to a phone call or a text message, entering a passcode displayed on the mobile app or hard token, or responding to a simple Approve/Deny prompt on the mobile app.

On a system protected by the MFA Service, the login request is coordinated with the Multi-Factor Authentication service for validation from the user's additional factor.

The MFA Service includes:

- Unlimited use of the service for each user
  - Up to three devices at a time for the mobile app
- MFA server management
- MFA software maintenance
- Help Desk Support for users
- Security setup/deletion of users
- Normal trouble-shooting (to the point of determining whether a problem is with the MFA system or with the user's PC and local infrastructure

The service does NOT include:

- DeepNet SafeID Mini hardware token (available as a separate cost)
- On-site support (which is available as a separate service and billed as time and materials)

Benefits include:

- MFA provides a much higher level of security
- Compliance with security standards for systems that require greater security than simple passwords.

4. Roles and Responsibilities:

Responsibilities of the Office of the CIO:

- Management of the Multi-Factor Authentication (MFA) Service
- Assistance to agencies in determining whether MFA is justified
- Documentation and initial train-the-trainer methods for implementation and use of the service in an agency

Responsibilities of the Customer:

- Classification of applications and data to determine whether MFA is justified
- Compliance with NITC Security Standards (http://www.nitc.nebraska.gov/standards/), including those pertaining to data, passwords, and authentication and authorization in general
- On-site support (which is available as a separate service and billed as time and materials)

5. Requesting Service

Contact the Office of the CIO Service Desk (402-471-4636) or cio.help@nebraska.gov) with any questions or to request service.

6. Billing Information:

The Office of the CIO uses a system of billing accounts, job codes and work orders for authorizing work and tracking costs for specific projects. The customer may designate which job code and work order to use or request a new jobs code and work order. Contact the Office of the CIO for assistance with developing an accounting structure that meets the needs of your organization.

7. Service Hours, Response Times and Escalation:

The Multi-Factor Authentication (MFA) Service is available 24 x 7. Report problems to the Office of the CIO Service Desk (402-471-4636) or cio.help@nebraska.gov).

For further information, please contact:

Office of the CIO Service Desk
cio.help@nebraska.gov
402-471-4636 or 800-982-2468