Fornetix VaultCore

Multi-Factor Authentication (MFA) Solution

» OVERVIEW

The purpose of Multi-Factor Authentication (MFA) is to provide the user with additional authentication for logging into the VaultCore appliance beyond the current username and password. The current design for MFA is to add certificate-based authentication to the appliance.

» METHODS

There are two ways in which the customer can utilize this implementation to access the appliance to the perform their administrative functions:

1. A user can insert an identification card into a card reader prior to logging into the appliance with a username and password.
2. A .pem file can be provided by System/Server admin to each User which can be loaded into the Users browser to access the system.

» ADVANTAGES

There are several benefits of this method versus some other options that are available:

1. The VaultCore System Admin has access to the certificates for a given user and can manage user credentials the same way the VaultCore appliance manages device credentials today.
2. It is a feasible option in a secure environment versus relying on other technologies that would require other 3rd party devices.
3. The system does not require access to internet.

Additionally, VaultCore supports authentication to an external system via LDAP. External authentication systems have their own configurations and can make use of additional mechanisms such as RSA tokens and CAC cards (For Example: Microsoft Active Directory, NIS+, and OpenLDAP).