Privacy IDEA Authenticator Plugin

The Privacy IDEA Authenticator plugin provides an interface for tokens managed by a privacyIDEA authentication server. These tokens can be used to implement Multi-Factor Authentication (though instructions for doing so are beyond the scope of this document). *(experimental)*

⚠️ This plugin is considered Experimental.

Configuration

> ⓘ While this documentation is not intended as a guide towards configuring privacyIDEA, certain hints are provided as they relate to the plugin's expected interaction with the privacyIDEA server.

1. This is a non-core plugin, see Installing and Enabling Registry Plugins for more information.
2. Create a new Server of type HTTP, via *CO* > *Servers* > *Add a new Server*.
    a. Set the **Server URL** to the server name, eg `https://privacyidea.myvo.org`.
    b. Leave **Username** blank.
    c. Create a privacyIDEA admin token and store it in the **Password** field.
        i. ⚠️ privacyIDEA tokens expire after 1 year. There is currently no interface or notification available in Registry to warn of impending token expirations.
3. By default, privacyIDEA does not require special credentials to validate tokens. However, it is possible to define an Authentication Policy that does require a credential. The plugin currently assumes such a policy has been established (although this may change in a future release). As such, a *second* HTTP Server is required to store the validation token.
    a. Set the **Server URL** to the same server name as the first HTTP Server.
    b. Leave **Username** blank.
    c. Store the validation token in the **Password** field, as created using pi-manage.
4. Create a new Authenticator, via *CO* > *Configuration* > *Authenticators* > *Add Authenticator*.
    a. Set the **Plugin Type** to PrivacyIdeaAuthenticator.
    b. On the next page, configure the PrivacyIdeaAuthenticator:
        i. Set the **Server** to the first HTTP Server created above.
        ii. Set the **Validation API Server** to the second HTTP Server created above.
        iii. Set the **PrivacyIDEA Realm** to the appropriate realm. Typically, this realm will be associated with an LDAP Resolver populated using the LDAP Provisioning Plugin.
        iv. Set the **Token Type** to the desired token type. (Each Token Type to be used in the CO requires a separate Authenticator to be instantiated.)
            1. Currently, only TOTP Tokens are supported.
        v. Set the **Identifier Type** to match the *Loginname Attribute* in the LDAP Resolver configuration.
            1. Note the Registry interface will provide the display name for the attribute, but privacyIDEA requires the corresponding LDAP attribute name.

Supported Tokens

The Privacy IDEA Authenticator currently supports TOTP Tokens only. When a new TOTP Token-based Authenticator is added (either directly to the CO Person record, or via the *Establish Authenticators* step of an Enrollment Flow), a QR code will be presented. The CO Person should scan the code with Google Authenticator (or another appropriate app), then enter the next 6 digit code to confirm proper setup of the token. Once this process is complete the token will be flagged as *confirmed*.

Supported Provisioners

The Privacy IDEA Authenticator operates slightly differently from other Authenticator Tokens, in that registration and management of a token via the Registry interface immediately invokes the privacyIDEA REST API. Registry Provisioners are *not* used to directly provision tokens.

Token Management

If the Privacy IDEA Authenticator Token is deleted from the CO Person Authenticator listing, the token will also be deleted from the privacyIDEA server.