Stefan Kania
IT-Consulting durch Training

Einrichtung von TOTP für die Benutzer

Autor:
Stefan Kania

Ort:
St. Michaelisdonn

30. Oktober 2021

Inhalt

1 Einleitung

Nachdem ich in den letzten Artikeln den LDAP-Server für die Verwendung von TOTP eingerichtet habe, soll es jetzt darum gehen, die Benutzerobjekte mit der zwei Faktoren Authentifizierung (2FA) auszustatten. In allen vorherigen Artikeln zum Thema TOPT ging es immer nur um die Konfiguration des Servers.

2 Erstellung der Token über ein Skript

Im ersten Abschnitt erkläre ich Ihnen, wie Sie mithilfe eines Skripts die entsprechenden Attribute in das Benutzerobjekt eintragen können. Dabei schlage ich in dem Skript gleich zwei Fliegen mit einer Klappe, denn im Skript kann zusätzlich das Clientzertifikat für den Benutzer erzeugt werden.

Hier können Sie das Skript zur Tokenerstellung herunter.

Wie schon in den vorherigen Artikeln wird hier ARGON2 als Passworthash genutzt. Der OpenLDAP-Server muss für die Nutzung vorbereitet sein. Wenn sie die Clientzertifikate automatisch erstellen wollen, ist es auch notwendig, dass Sie das entsprechende Modul im OpenLDAP eingebunden haben.

Vor dem ersten Aufruf des Skripts passen Sie das Skript an Ihre Umgebung an. In Listing 2.1 sehen Sie die Parameter die Sie anpassen müssen:

```
USER_DN=$1
USER_MAIL=$2
# Default OU for TOTP parameter
# This is the OU with the ObjectClass oathTOTPParams
USER_OU="ou=users,dc=example,dc=net"
LDAP_SERVER=ldap://ldap25-p01.example.net

# Default Login to the LDAP-Server is via sasl-mech EXTERNAL
# And the socket ldapi:///
USE_LDAPI=1 # set to "0" if userlogin is prefered
USE_TLS=1 # if TLS should not be used set to "0"
#LDAP_ADMIN="uid=ldap-admin,ou=users,dc=example,dc=net"
LDAP_ADMIN="cn=admin,dc=example,dc=net"
LDAP_ADMIN_PW="secret"
TOPT_ISSUER=stka
USER_NAME=""
# You will find all created files in this directory
PATH_FOR_SHARED_KEY="/root/"
USER_SHARED_KEY=""
QR_TEXT=""
USER_PASSWORD=""
# ARGON2_MEM 2^N KiB default is 12 (us as much as possible)
ARGON2_MEMORY=12
# ARGON2_ITERATION default is 3 (choos so that login takes not longer then 1 second)
ARGON2_ITERATION=3
# ARGON2_PARALISSM default is 1 (should be No. of CPU-cores * 2)
ARGON2_PARALISSM=1
# SALT_LENGTH should be at least 20 Bytes long
SALT_LENGTH=20
```

Listing 2.1: Variablen für das Skript

Sie können über die Variable *USE_LDAPI* festlegen, ob die Anmeldung am LDAP für die Änderungen an dem Benutzerobjekt via der LDAPI-Schnittstelle, oder über einen Benutzer, mit den entsprechenden Rechten durchgeführt werden soll. Die Verwendung der LDAP-Schnittstelle ist nur möglich, wenn das Skript direkt auf dem LDAP-Server ausgeführt wird.

Die Standardkonfiguration ist die Anmeldung über die LDAPI-Schnittstelle.

Auch können Sie im Skript auswählen, ob die Verbindung über TLS abgesichert sein soll oder nicht. Wenn Sie das Skript lokal auf dem LDAP-Server einsetzen ist die Verwendung von TLS nicht notwendig. Standard ist die Aktivierung von TLS.

In diesem Teil des Skripts können Sie auch die Parameter für die Generierung des ARGON2-Passworts festlegen. In dem Artikel zur Einrichtung des OpenLDAP wurde die Möglichkeiten für die Konfiguration von ARGON2 bereits besprochen.

Beim Aufrufen des Skripts ist es notwendig, dass Sie den vollständige DN und die Emailadresse des Benutzers, für den der Token erstellt werden soll, als Parameter übergeben.

Haben Sie für mehrere OUs unterschiedliche TOTP-Parameter gesetzt, können Sie währen der Laufzeit des Skripts, noch die OU wechseln aus der die Parameter gelesen werden, es erfolgt immer eine Abfrage.

Für jeden Benutzer wird ein eigener Sharedkey generiert, der in dem vorher festgelegten Verzeichnis abgelegt wird. Den QR-Code geben Sie anschließend an den Benutzer.

Für den Benutzer wird dann ein neues, mit den im Skript definierten Parametern, ARGON2-Passwort vergeben.

Anschließend werden die Änderungen am Benutzerobjekt durchgeführt und der QR-Code erzeugt und genau wie der Sharedkey im angegebenen Verzeichnis abgelegt.

Ganz am Ende des Skripts habe Sie die Möglichkeit gleich eine Clientzertifikate für den Benutzer zu erzeugen und in seinem Objekt zu speichern. Denken Sie daran, dafür muss der entsprechende Modul im OpenLDAP konfiguriert sein.

So können Sie über die Kommandozeile die TOTP-Einstellungen für Ihre Benutzer realisieren.

3 Erstellung des Tokens über den LAM

Der LAM in der Pro-Version kann ebenfalls den Token und den QR-Code für die Benutzer erzeugen.

Der Vorteil bei der Verwendung des LAMs ist der, dass Sie dem Benutzer beim Anlegen nur ein Passwort geben und der Benutzer anschließend über das SelfService-Modul des LAM seinen Token und den QR-Code selbst erzeugen kann.

4 Konfiguration des LAM

Bevor ich mit der Konfiguration beginne, hier noch einmal der Hinweis, für die Nutzung des *SelfService*-Moduls verwende ich den LAM in der Pro Version, die freie Variante unterstützt das nicht.

Ich gehe davon aus, dass der LAM bereits für die Verwaltung der Benutzer und Gruppe eingerichtet ist. Hier wird nur die Konfiguration des *SelfService* beschrieben.

Auf der Startseite des LAMs klicken Sie auf den Link oben rechts LAM-Einstellungen, Sie gelangen dann in das Auswahlfenster für die verschiedenen Konfigurationen, so wie in Abbildung 4.1.

Abbildung 4.1: Auswahl der Einstellung

Klicken Sie dort auf SelfService bearbeiten. Da im Moment noch kein Profil für das Modul vorhanden ist, klicken Sie, im folgenden Fenster, auf SelfService-Profile verwalten.

Im nächsten Schritt erstellen Sie ein neues Profil, in dem Sie dem Profil einen Namen geben und auf Hinzufügen klicken. Bestätigen Sie die Aktion mit dem Masterpasswort des LAM.

Sie landen anschließend in dem Abschnitt Allgemeine Einstellungen des Profils. Dort tragen Sie die entsprechenden Daten Ihrer Umgebung ein. Ich habe hier die Serverdaten und Namen aus dem vorherigen Artikel zum Einrichten des OpenLDAP-Servers genutzt. In Abbildung 4.2 sehen Sie die von mir eingetragenen Werte.

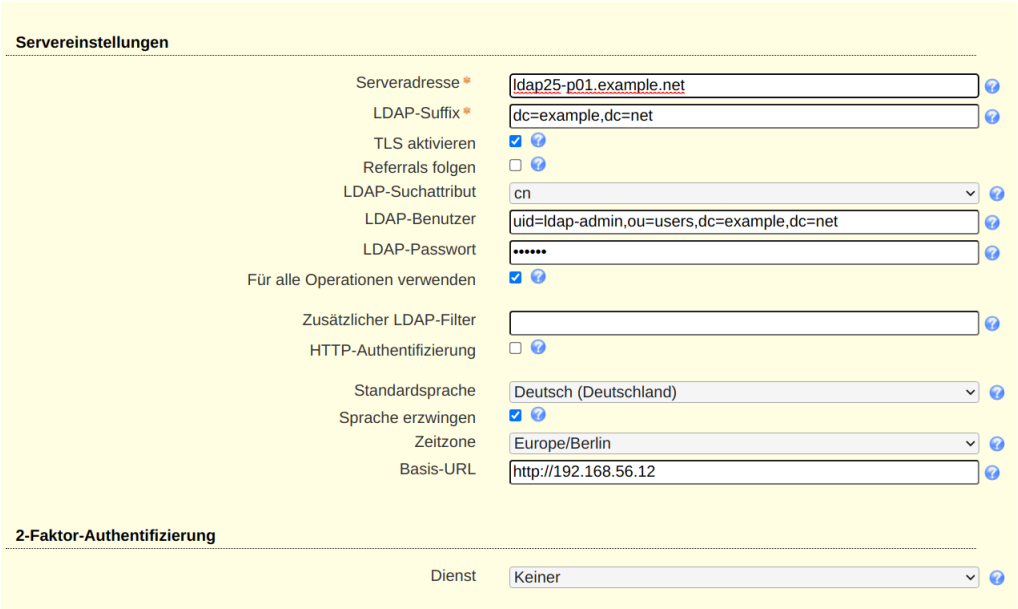

Abbildung 4.2: Allgemeine Einstellungen des Profils

Wichtig ist an der Stelle, dass Sie als *LDAP-Benutzer* einen Benutzer angeben, der das Schreibrecht an allen Benutzern hat und das Sie den Haken bei *Für alle Operationen verwenden* setzen.

Im Abschnitt *2-Faktor-Authentifizierung* wählen Sie als Dienst unbedingt *Keiner* aus, da hier der OpenLDAP eigene TOTP-Dienst genutzt wird.

Klicken Sie jetzt auf den Karteireiter Seitenlayout, denn dort wird die entsprechende Möglichkeit für die Benutzer konfiguriert, sodass später die Benutzer ihren eigenen Token generieren können.

Die wichtigen Änderungen werden in dem Abschnitt *Eingabefelder* vorgenommen. An dieser Stellen konfigurieren Sie jetzt die Erstellung des Tokens. Zu Beginn sieht der Abschnitt so aus wie in Abbildung 4.3.

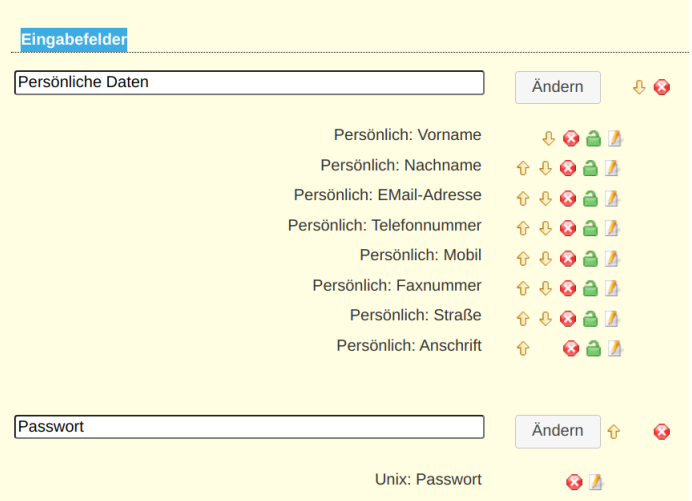

Abbildung 4.3: Grundeinstellung des Layouts

Über den Abschnitt *Feld hinzufügen* fügen Sie jetzt die beiden *OpenLDAP TOTP*-Felder *Neuen Token registrieren* und *Seriennummer* zu den *Persönlichen Daten* hinzu.

Der Abschnitt *Eingabefelder* hat sich jetzt so geändert wie es die Abbildung 4.4 zeigt.

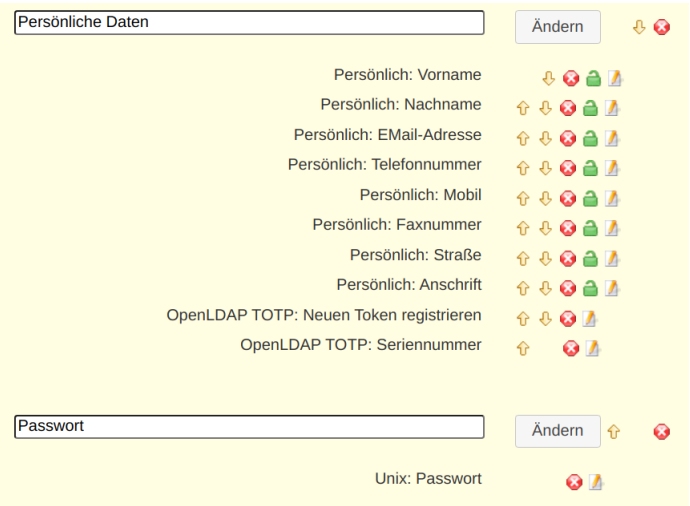

Abbildung 4.4: Um TOTP ergänztes Layout

Klicken Sie jetzt auf den Karteireiter MODULEINSTELLUNGEN um dort die OU anzugeben in der Sie die TOTP-Parameter konfiguriert haben. Beim LAM können Sie nur eine OU angeben, wenn Sie mehrere OUs mit TOTP-Parametern konfiguriert haben, legen Sie zusätzliche Profile im LAM an. Achten Sie dann darauf, dass Sie den entsprechenden Benutzern den passend Link auf die SelfService-URL geben.

Im Abschnitt *OpenLDAP TOTP* tragen Sie Ihre OU ein, so wie Sie es in der Abbildung 4.5 sehen.

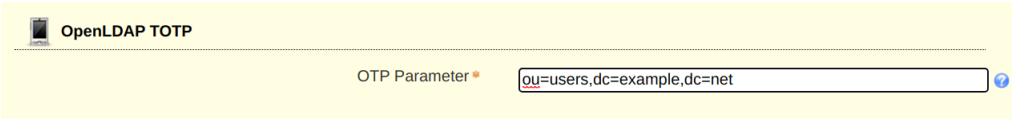

Abbildung 4.5: Eintrag der OU mit den TOTP-Parametern

Hier sind keine weiteren Änderungen notwendig.

Hinweis!

Bevor Sie die Einstellungen speichern klicken Sie oben in dem Fenster auf SelfService-Login Es öffnet sich ein neues Fenster mit dem Anmeldedialog für den SelfService. Speichern Sie die URL. Geben Sie diese URL Ihren Benutzern. Über diese URL können die Benutzer ihren Token und den QR-Code selbst erstellen.

Speichern Sie jetzt die Einstellungen.

Im Anschluss an die Konfiguration, legen Sie, wie gewohnt, einen neuen Benutzer an. Klicken Sie dabei auf den Karteireiter OpenLDAP TOTP kommt die Meldung *Der Token kann im Self Service gesetzt werden*. Den Token kann, mit dem LAM, nur der Benutzer selber erzeugen. Sie vergeben lediglich das Passwort für den Benutzer. Der Benutzer meldet sich mit seinem Passwort am *SelfService* an und generiert dort seinen Token und den QR-Code selbst.

Das Modul *SelfService* des LAMs kann noch erheblich mehr, aber hier ging es nur darum die TOTP-Funktion zu erklären und einzurichten.

Meldet der Benutzer sich jetzt am *SelfService* an, erscheint das Fenster aus Abbildung 4.6.

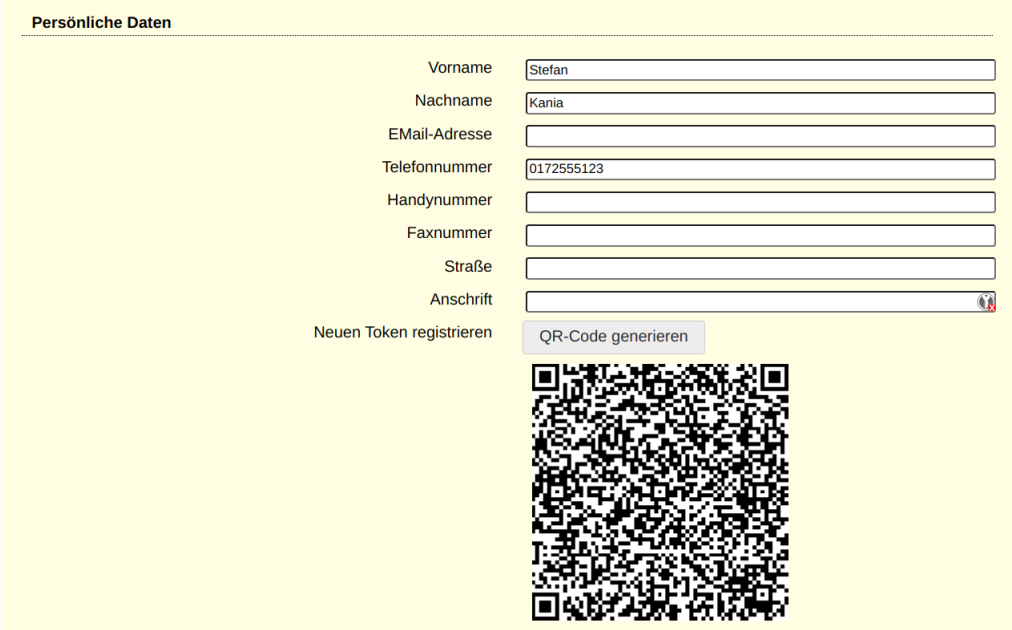

Abbildung 4.6: Verwaltungsseite für den Benutzer

Hier kann der Benutzer jetzt auf QR-Code generieren klicken und es wird er Token und der QR-Code generiert. Alle benötigten Attribute werden dabei in seinem Objekt eingetragen. Die Änderungen an dem Benutzerobjekt werden mit dem Konto aus den Grundeinstellungen des SelfService durchgeführt.

Nach dem Speichern der Änderungen kann der Benutzer sich jetzt mit dem TOTP-Token anmelden.

Der QR-Code kann mit der *Google authenticator*-App oder einer ähnlichen Anwendung gescanned werden. Der 6-stellige Code, also der 2. Faktor, wird dann direkt an das Passwort bei der Anmeldung angehängt. Hat der Benutzer das Passwort *geheim* und die App zeigt den Token *123456* gibt er bei der Anmeldung *geheim123456* ein, ohne Leerzeichen zwischen Passwort und Token.

5 Der Linux-Client

Bis jetzt habe ich lediglich erklärt, wie Sie den OpenLDAP-Server und die Benutzer für die 2FA konfigurieren. Im letzten Abschnitt folgt jetzt die Einrichtung für einen Linux-Client, denn auch dort sollen sich alle Benutzer in Zukunft mit der 2FA anmelden.

Ich werde an dieser Stelle einen Linux-Client ohne GUI nutzen. Wenn Sie Clients mit GUI mit der 2FA ausstatten wollen ändert sich für die GUI nichts.

Als LDAP-Clientsoftware verwende ich ausschließlich den *sssd* da mit dem sssd die sicherste Methode für die Anbindung eines Linux-Clients an einen LDAP gegeben ist. Im Grunde ändert sich dort nichts gegenüber der Konfiguration ohne TOTP. Sie installieren die das sssd-Paket (unter Debian mit `apt install sssd`) und erstellen die Konfigurationsdatei sssd.conf im Verzeichnis /etc/sssd. Den Inhalt meiner Konfiguration sehen Sie in Listing 5.1:

```
[sssd]
config_file_version = 2
services = nss, pam
domains = LDAP

[nss]
filter_groups = root
filter_users = root
reconnection_retries = 3

[pam]
reconnection_retries = 3
offline_credentials_expiration = 2
offline_failed_login_attempts = 3
offline_failed_login_delay = 5

[domain/LDAP]
ldap_schema=rfc2307
ldap_uri = ldap://ldap25-p01.example.net:389
ldap_search_base=dc=example,dc=net
ldap_default_bind_dn=uid=sssd-user,ou=users,dc=example,dc=net
ldap_default_authtok=geheim
id_provider=ldap
auth_provider=ldap
chpass_provider = ldap
ldap_chpass_uri = ldap://ldap25-p01.example.net:389
cache_credentials = True
enumerate = false
ldap_tls_cacertdir = /etc/ssl/zertifikate/demoCA
ldap_tls_cacert = /etc/ssl/zertifikate/demoCA/cacert.pem
ldap_id_use_start_tls = True
ldap_purge_cache_timeout = 1000000
ldap_enumeration_refresh_timeout = 5000
```

Listing 5.1: Die Datei sssd.conf

Hinweis!

Achten Sie darauf, dass die Datei die Berechtigung auf 600 gesetzt hat und die Datei dem Benutzer *root* gehört. Ohne diese Berechtigungen lässt sich der sssd später nicht starten.

Eine Änderung an der Datei /etc/nsswitch.conf ist bei der Verwendung des sssd nicht notwendig, alle benötigten Änderungen werde bei der Installation der Pakte vorgenommen.

Nach der Erstellung oder der Änderung der sssd.conf starten Sie den sssd neu. Im Anschluss können Sie sich die Benutzer mittels `getent passwd <ein-ldap-benutzer>` auflisten lassen.

Alle Benutzer können sich so am Client authentifizieren, egal ob mit oder ohne 2FA.

Nachdem Sie die Anmeldung erfolgreich eingerichtet haben, können Sie jetzt alle Clients anpassen. Habe Sie die LDAP-Anmeldung bereits über den sssd für alle Clients eingerichtet, dann können die Benutzer die 2FA auch sofort nutzen.

6 Was noch zu tun ist

Wenn Sie die 2FA via TOTP erst später eingerichtet haben, sprich alle Benutzer haben bereits ein Passwort und melden sich am den Clients an, ist es recht einfach die Benutzer auf die 2FA umzustellen. Schicken Sie allen Personen den Link zum SelfService setzen Sie dann das Ablaufdatum aller Passwörter auf ein bestimmtes Datum. Die Benutzer können dann über den Link ihr Passwort ändern und die 2FA aktivieren.

Viele Erfolg bei der Einrichtung und Umstellung.

Index