axians

Multi Factor Authentification (MFA) on IBM i

2026

VINCI ENERGIES

Overview

- About me and the CEAC
- Password security
- New OS USRPRF with R760
- MFA as an integrated part of the OS R760
- Prerequisites
- Implementation native OS or via IBM Navigator for I
- SST/DST
- Standards and Links

axians

About the speaker

Katharina Karner

- Started 2000 at IBM AS400 Hotline
- Specialization in software HA solutions (MIMIX, iTERA, Quick-EDD, iCluster, Maxava HA etc.)
- Member of the CEAC since 2024

CEAC (Common Europe Advisory Council) Member

IBM

IBM i

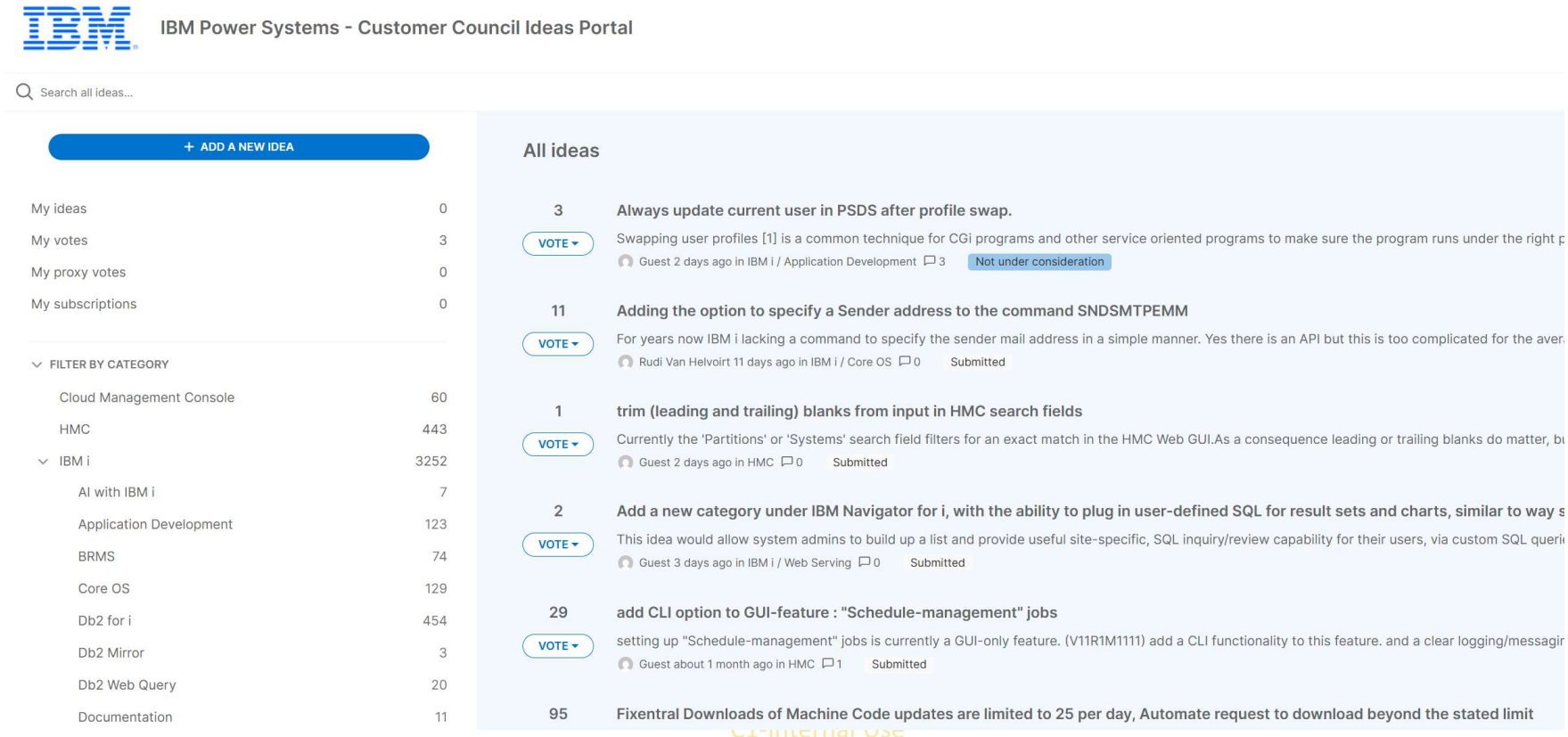
CEAC (Common Europe Advisory Council)

https://comeur.org/what-is-ceac/

- Mission: dialogue with IBM on strategic and long-term issues
- Organisation: part of Common Europe, members are IT professionals with extensive IBM I experience
- Our work:
  - Monthly online meetings to discuss IBM ideas with IBM liaison, give updates about enhancements and roadmap presentations
  - Face to face meetings twice a year, usually follow on from the Common conferences. Key members from IBM also attend this event.
- Our motivation: dedication to IBM i as the membership is on a voluntary basis only.

CEAC / IBM i Customer Council Ideas Portal

https://ibm-power-systems-cc.ideas.ibm.com/ideas/



Password security

2023 Password Cracking Times with Brute Force Program

Number of characters	Just numbers	Lowercase letters	Uppercase and lowercase letters	Numbers, uppercase and lowercase letters	Numbers, Letters & Symbols
6	Right away	Right away	Right away	Right away	Right away
7	Right away	Right away	1 second	2 seconds	4 seconds
8	Right away	Right away	28 seconds	2 minutes	5 minutes
11	Right away	32 minutes	1 month	10 months	3 years
12	1 second	14 hours	6 years	53 years	226 years
14	52 seconds	1 year	17,000 years	202,000 years	1 million years
18	6 days	481,000 years	126 billion years	2 trillion years	26 trillion years

Source: https://www.oberlin.edu/cit/bulletins/passwords-matter

New user profiles on OS R760

Non-changeable users for OS functions

```
                        Mit Benutzerprofilen arbeiten

Auswahl eingeben und Eingabetaste drücken.
  1=Erstellen   2=Ändern   3=Kopieren   4=Löschen   5=Anzeigen
  12=Mit Objekten eines Eigners arbeiten

Ausw  Benutzerprofil  Text

 _      QPGMR_NC       Nicht änderbares QPGMR-Profil
 _      QSECOFR_NC     Nicht änderbares QSECOFR-Profil
 _      QSYSOPR_NC     Nicht änderbares QSYSOPR-Profil
 _      QUSER_NC       Nicht änderbares QUSER-Profil
```

QSTRUP continues to run under QPGMR

axians

Benefits of Integrated MFA Implementation on IBM I

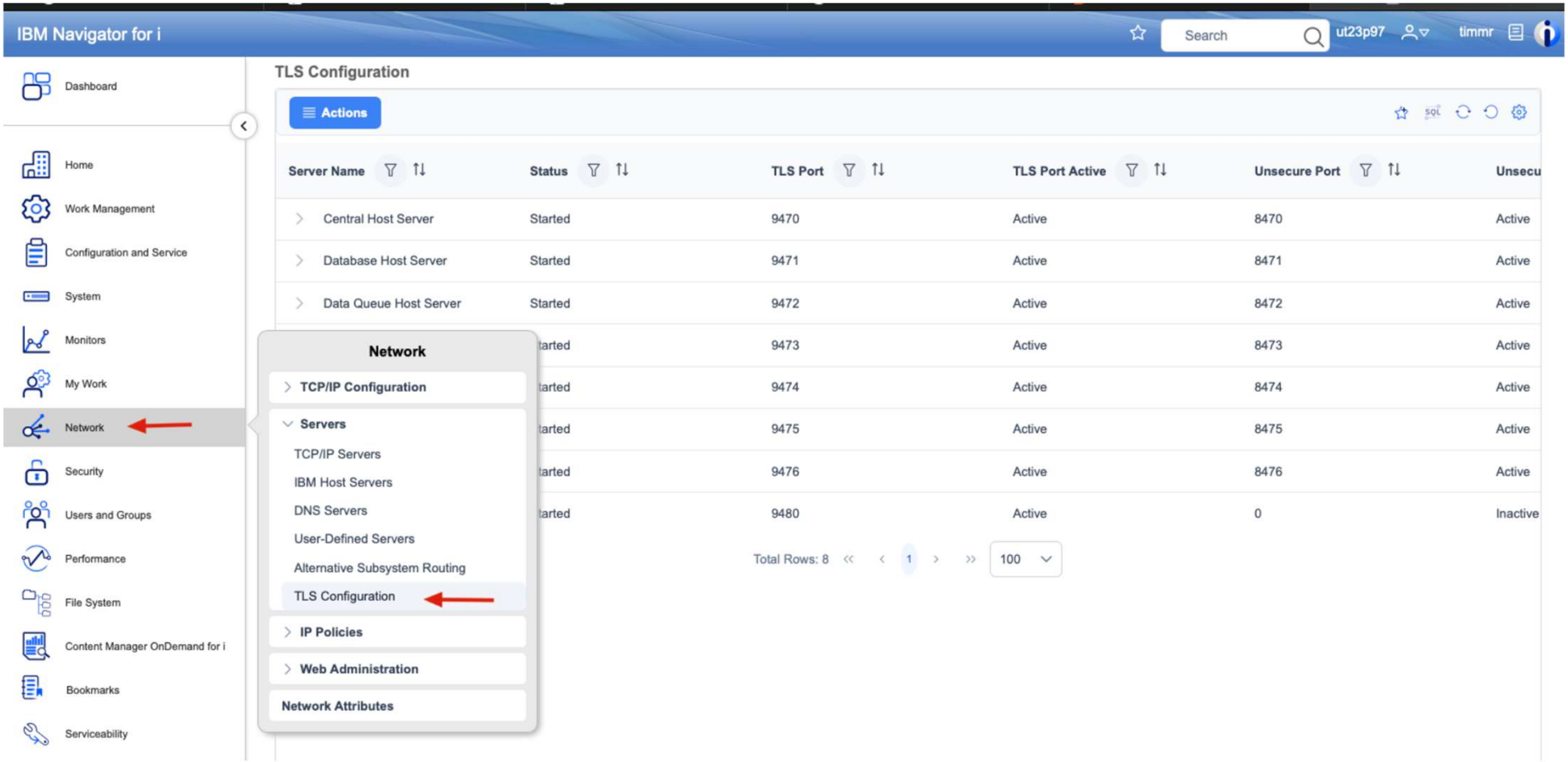
- Multi-factor authentication (MFA) adds an additional authentication factor to password authentication to verify your identity.
- The IBM i integrated MFA solution includes a time-based one-time password key (TOTP).
- Integrated with IBM i 7.6 operating system, no additional software required
- Compatible with many TOTP client authenticators
- The Service Tools User Profiles for SST and DST are also supported.
- Universal Authentication Exit Point: (QIBM_QSY_AUTH)
- Third-party MFA solutions can be used to integrate into heterogeneous landscapes

axians

Prerequisites

- POWER 10 Hardware and IBM i Release 7.6
- TLS Transport Layer Security must be configured and enabled
- Security Level 40 oder 50 - SYSVAL(QSECURITY)
- The password level must be set to 4 - SYSVAL(QPWDLVL)
  - Do a SAVSECCDTA before changing the values, no undo button.
- MFA Function Activation - CHGSECA ADLSGNFAC(*ENABLED)
- An IPL is required to enable the MFA feature.
- Since the system requires an accurate time for TOTP, NTP (Network Time Protocol) should be used as the client. CFGTCPAPP (*NTP)

Transport Layer Security (TLS) Configuration



axians

QPWDLVL 4

Careful examination required

Berechtigte Benutzer anzeigen

Benutzer-profil	Gruppen-profil	Kennwort zuletzt geändert	Kennwort Stufe 0 oder 1	Kennwort Stufe 2 oder 3	Kennwort Stufe 4	Lok. Knwrt verw.
JOGS		23.06.25	*NO	*NO	*YES	*YES
KKARNER		25.06.25	*NO	*NO	*YES	*YES
QANZAGENT		23.06.25	*NO	*NO	*NO	*YES
QAUTPROF		23.06.25	*NO	*NO	*NO	*YES
QBRMS		23.06.25	*NO	*NO	*NO	*YES
QCLUMGT		23.06.25	*NO	*NO	*NO	*YES
QCLUSTER		23.06.25	*NO	*NO	*NO	*YES
QCOLSRV		23.06.25	*NO	*NO	*NO	*YES
QDBSHR		23.06.25	*NO	*NO	*NO	*YES
QDBSHRDO		23.06.25	*NO	*NO	*NO	*YES

- In QPWDLVL 4, all passwords of password level 0-1 are deleted, level 2-3 if no implementation is possible.
- If the user profile does not have a password that can be used at password level 4, the password is *NONE after the QPWDLVL system value is set to 4.
- Password level 4 is a one-way password encryption algorithm.
- Testing with DSPAUTUSR +F11 or PRTUSRPRF TYPE(*PWDLVL).
- Recommendation: run **SAVSECDATA** prior to any conversion.

SIGNON Screen

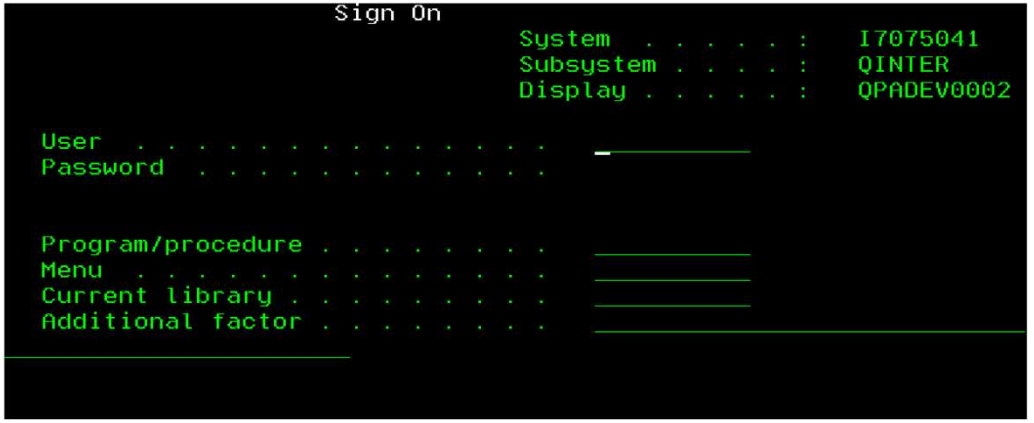
If the Signon screen is adjusted, the program must be updated

QSYS/QAWTSSRC

Sources for Signon

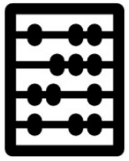
SIGNON SCREEN

Additional Signon Factor *ENABLED



How a TOTP algorithm works

TOTP generates a one-time password that changes regularly



A key is generated at the host

The key is imported into the client

A timestamp gives a time value

HMAC calculation of a digit based on the common key and timestamp

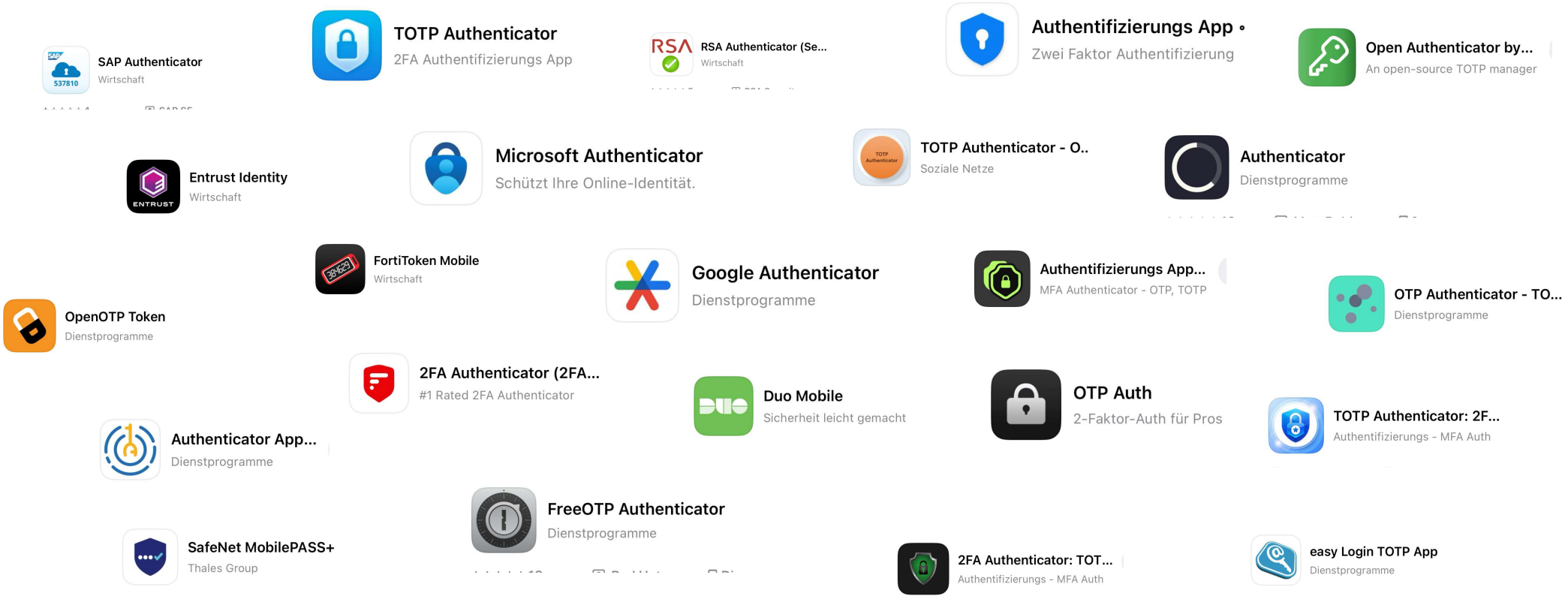
The generated OPT is entered

The algorithm calculates the validity, based on key and timestamp

axians

TOTP Clients

Some examples



Generating the key

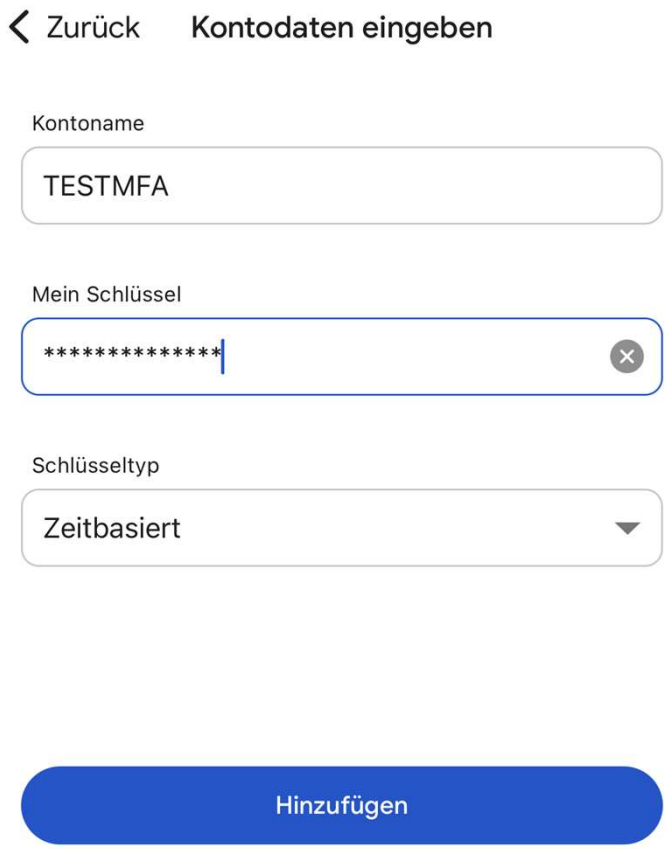
CHGTOTPKEY *GEN is performed by the user

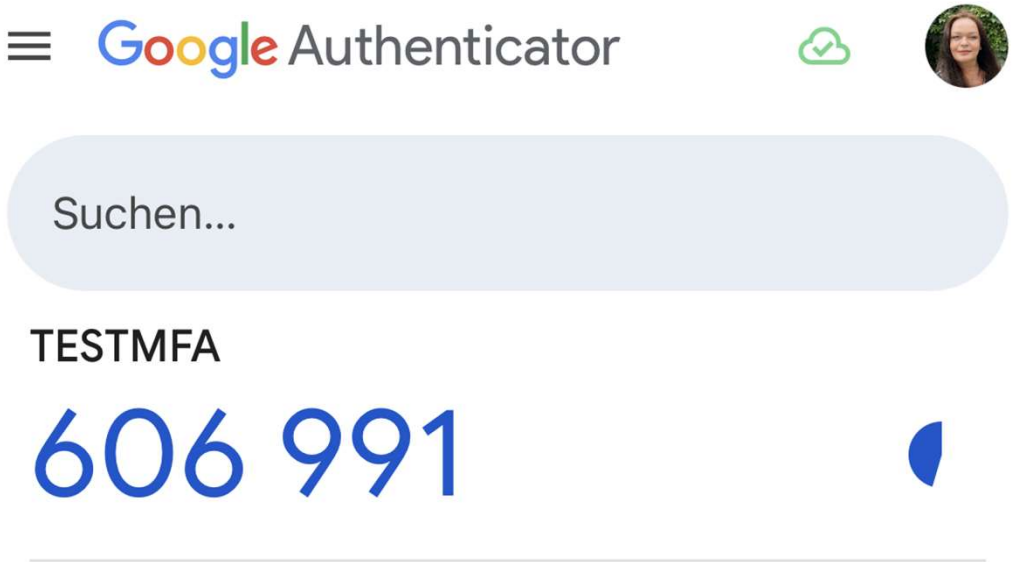
```
TOTP key  . . . . . :   FQT4 JVFV IPSL G5FO 43YP EEEF 7LIQ QD6N
Copy/paste version  . . :   FQT4JVFVIPSLG5FO43YPEEEF7LIQQD6N


Recovery key  . . . . . :   CC92F6DDF43AF5D6B95C817547FF39D3
                            9F269CE7B88ED580CD496220F6225297

The TOTP key has been saved in your profile. It must also be entered
into your TOTP generator client application, without the blanks.

Save the recovery key for this TOTP key in a safe place.
```

axians

Set up TOTP

Example Google Authenticator





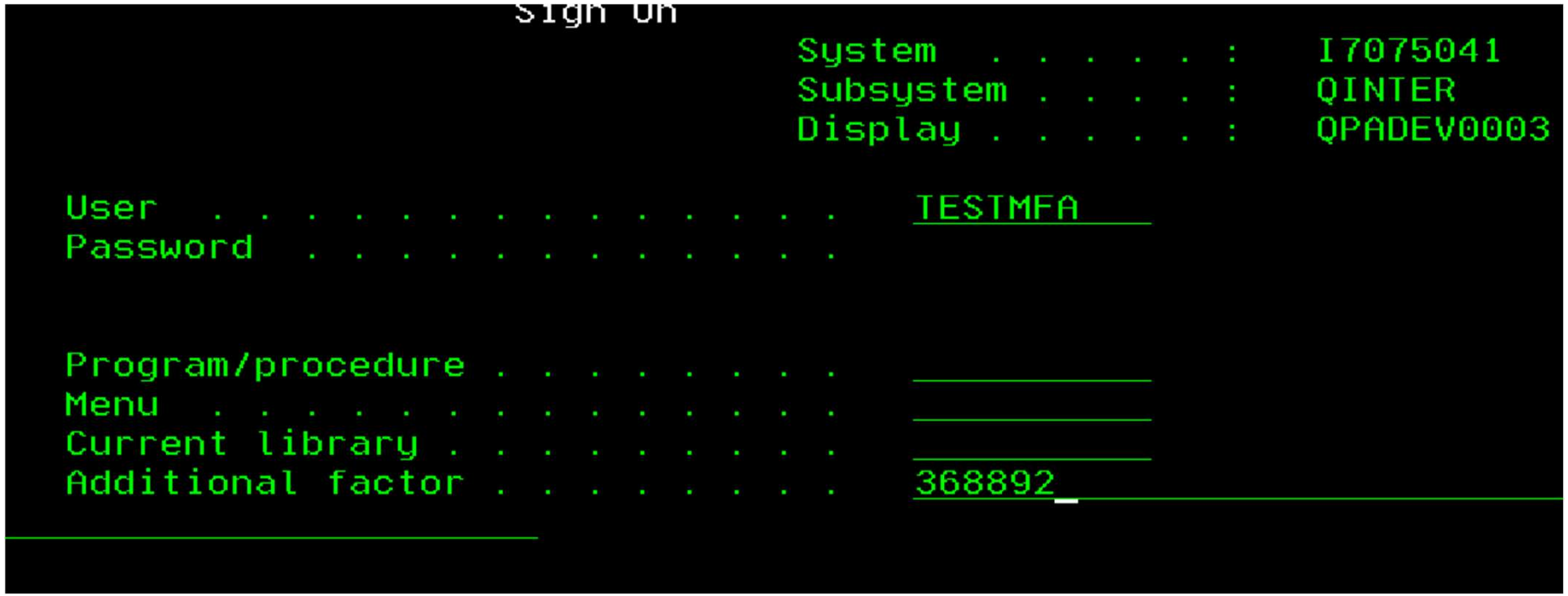
axians

CHGUSRPRF by sysadmin

Activate TOTP, user by user

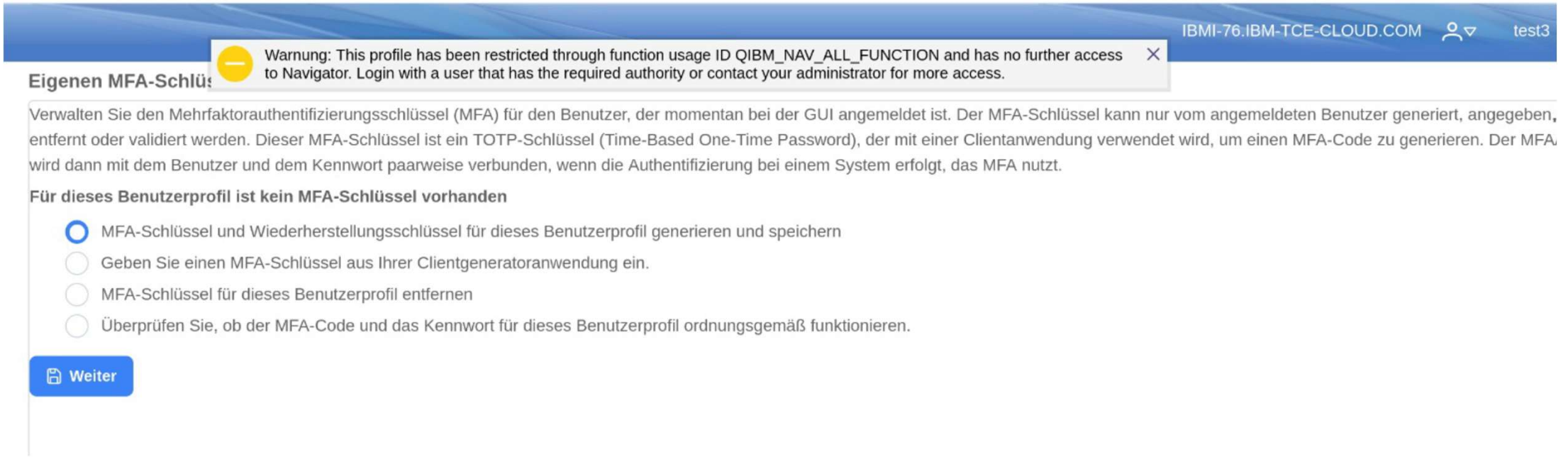
Optional TOTP interval: *NONE = a token is required every time you log in. Number = minutes until a new token is requested.

MFA is active



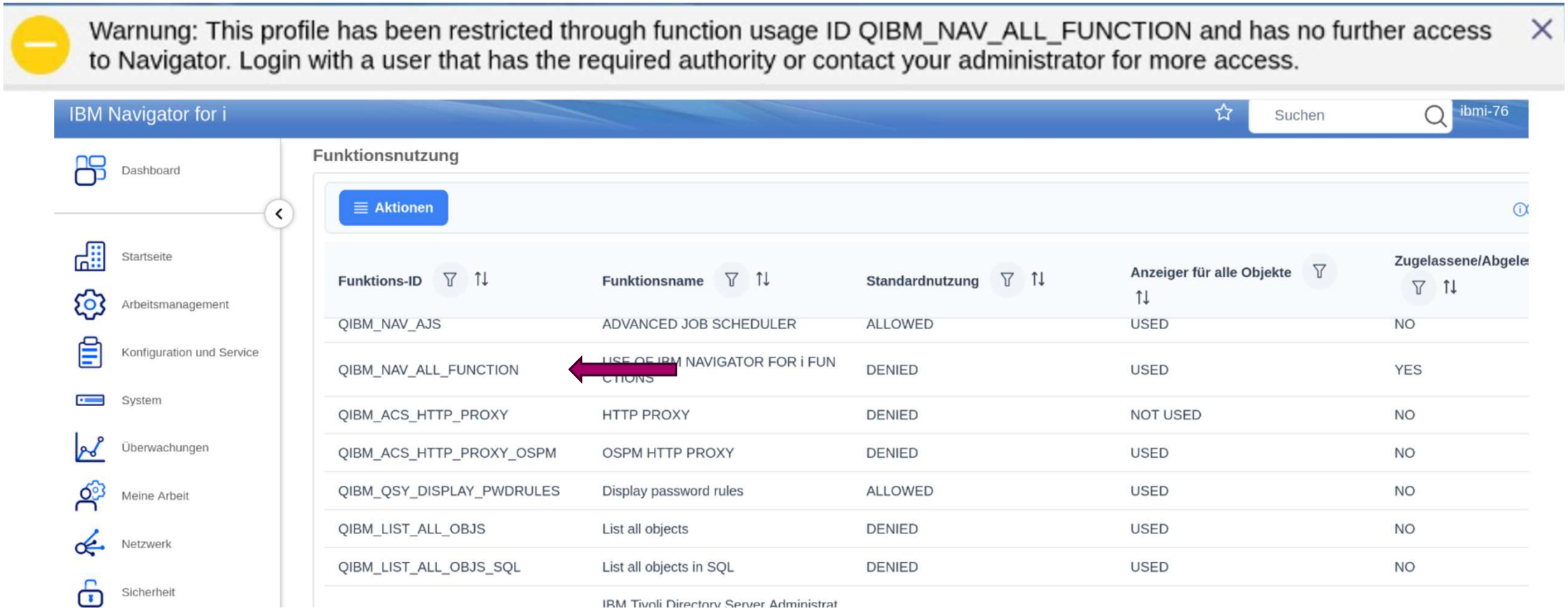
CHGUSRPRF via Navigator for I

MFA Key Setup by User



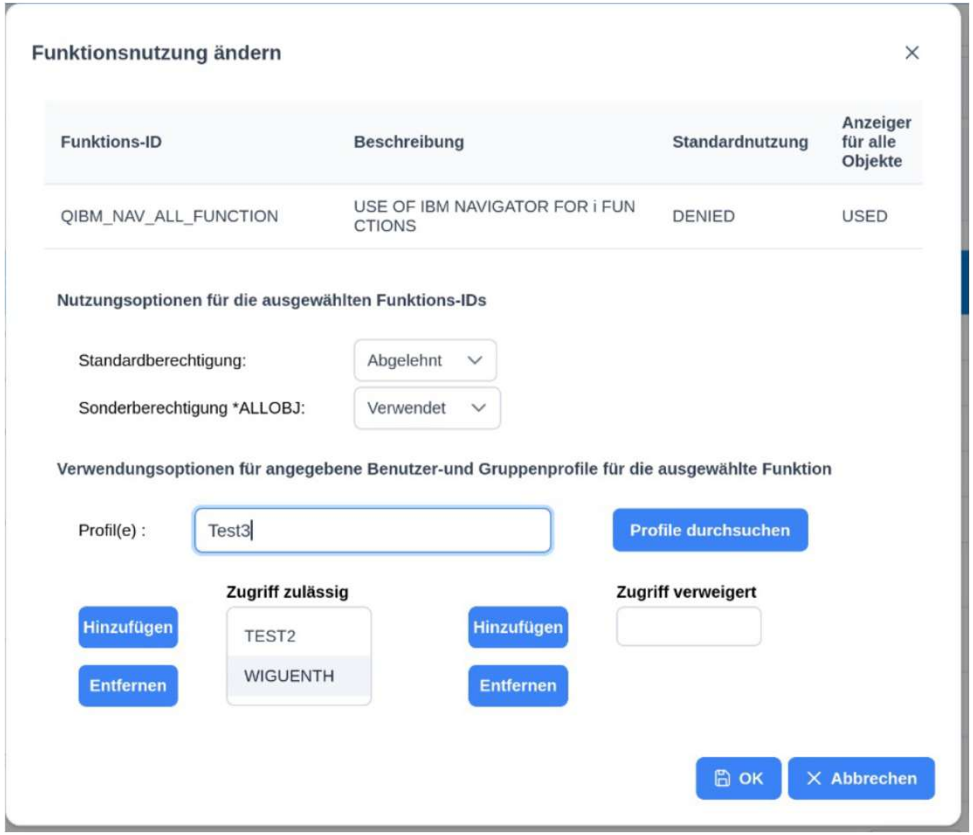
QIBM_NAV_ALL_FUNCTION

Adjusting the Permission When the Functional Error Is Reported



QIBM_NAV_ALL_FUNCTION

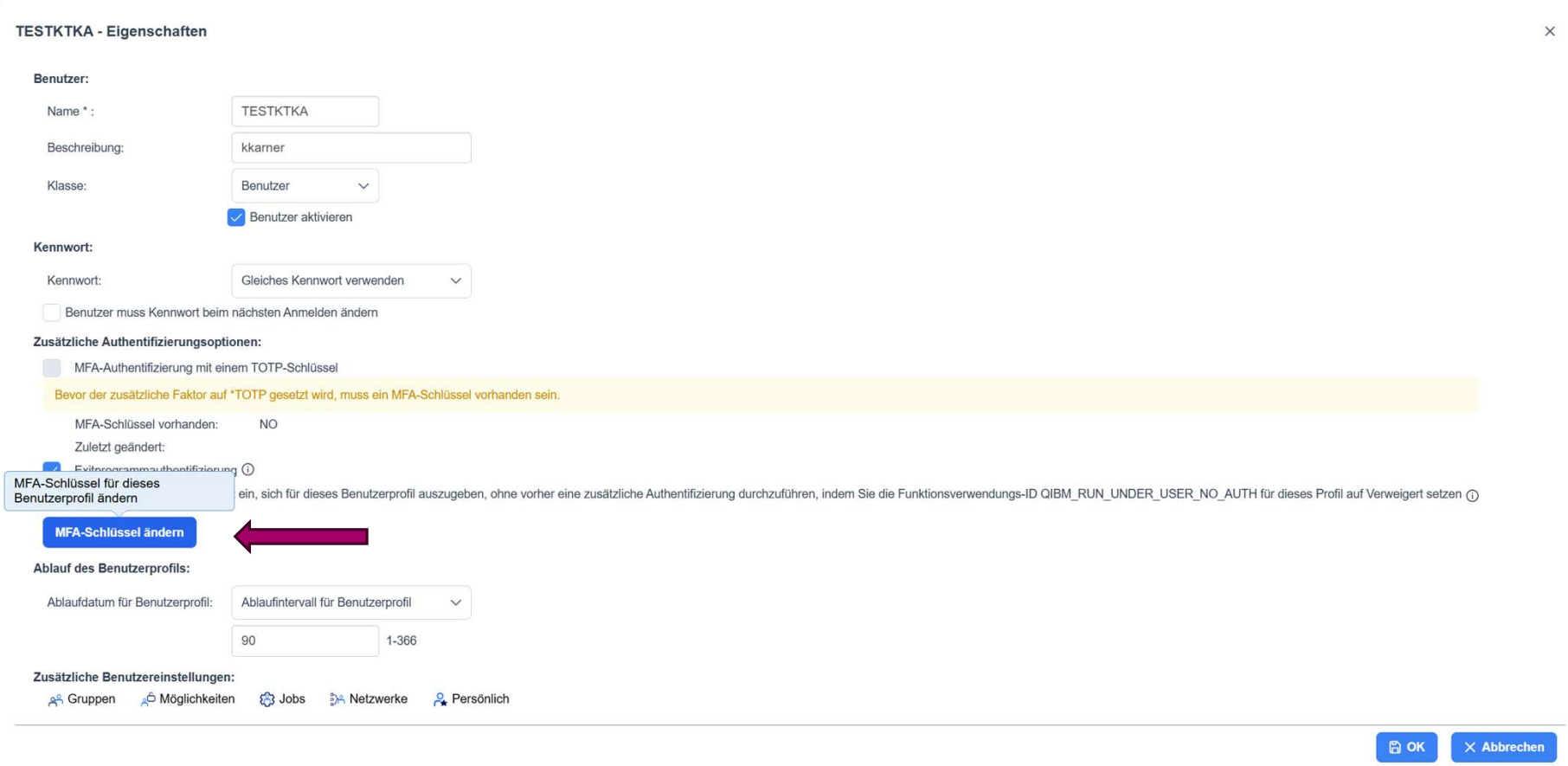
Adjusting Permission via Navigator or WRKFCNUSG



axians

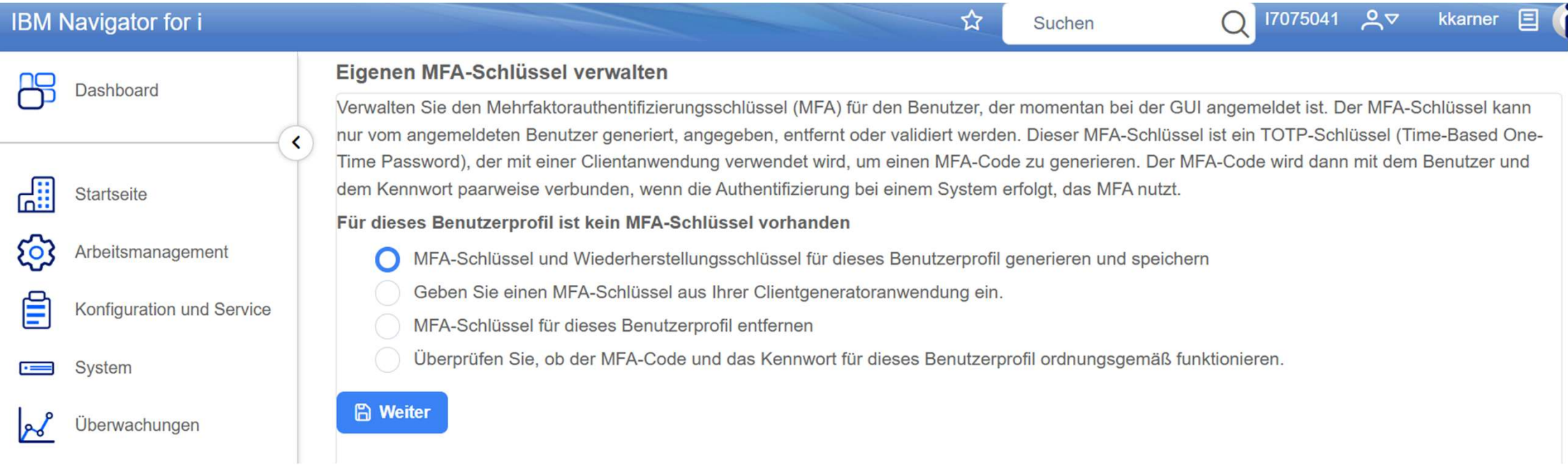
Set up MFA keys

IBM i Navigator, creating the MFA key by users



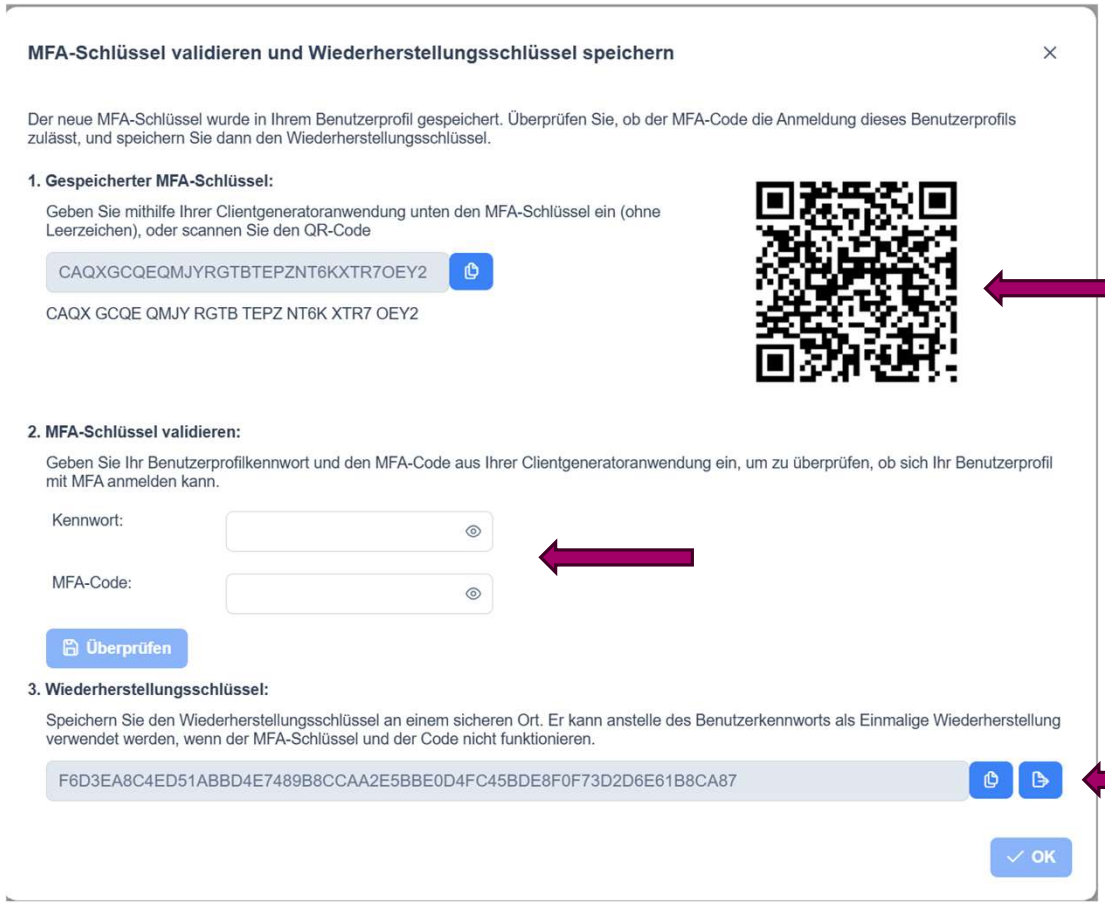
Set up MFA keys

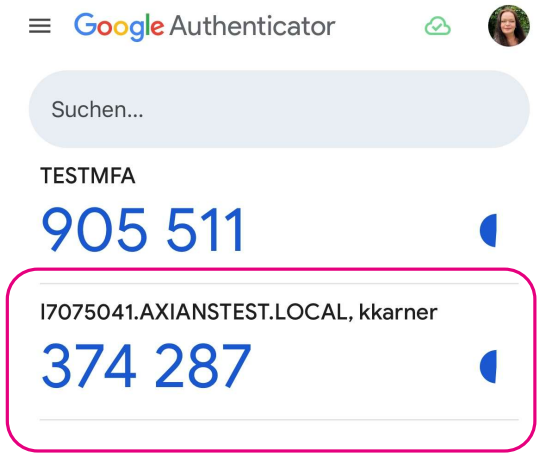
IBM i Navigator



Set up MFA keys

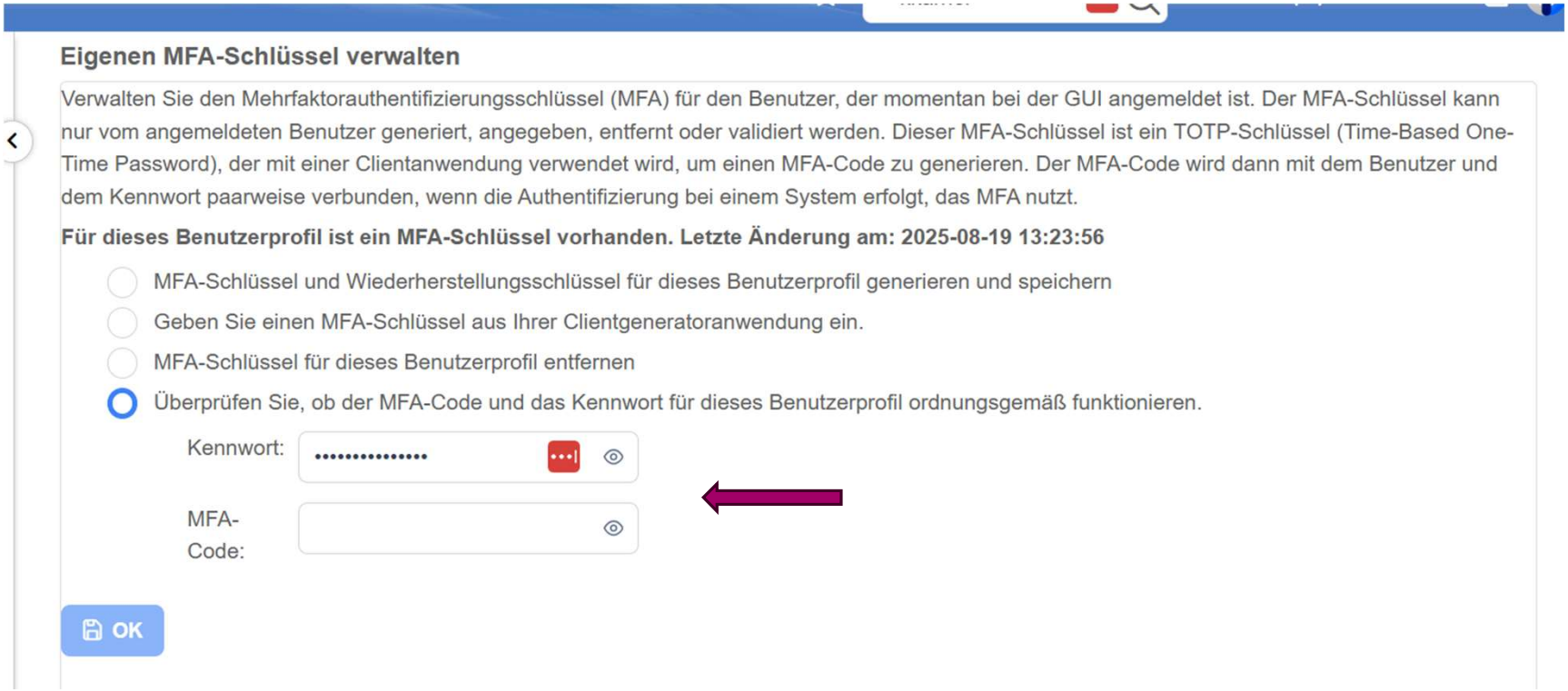
IBM i Navigator





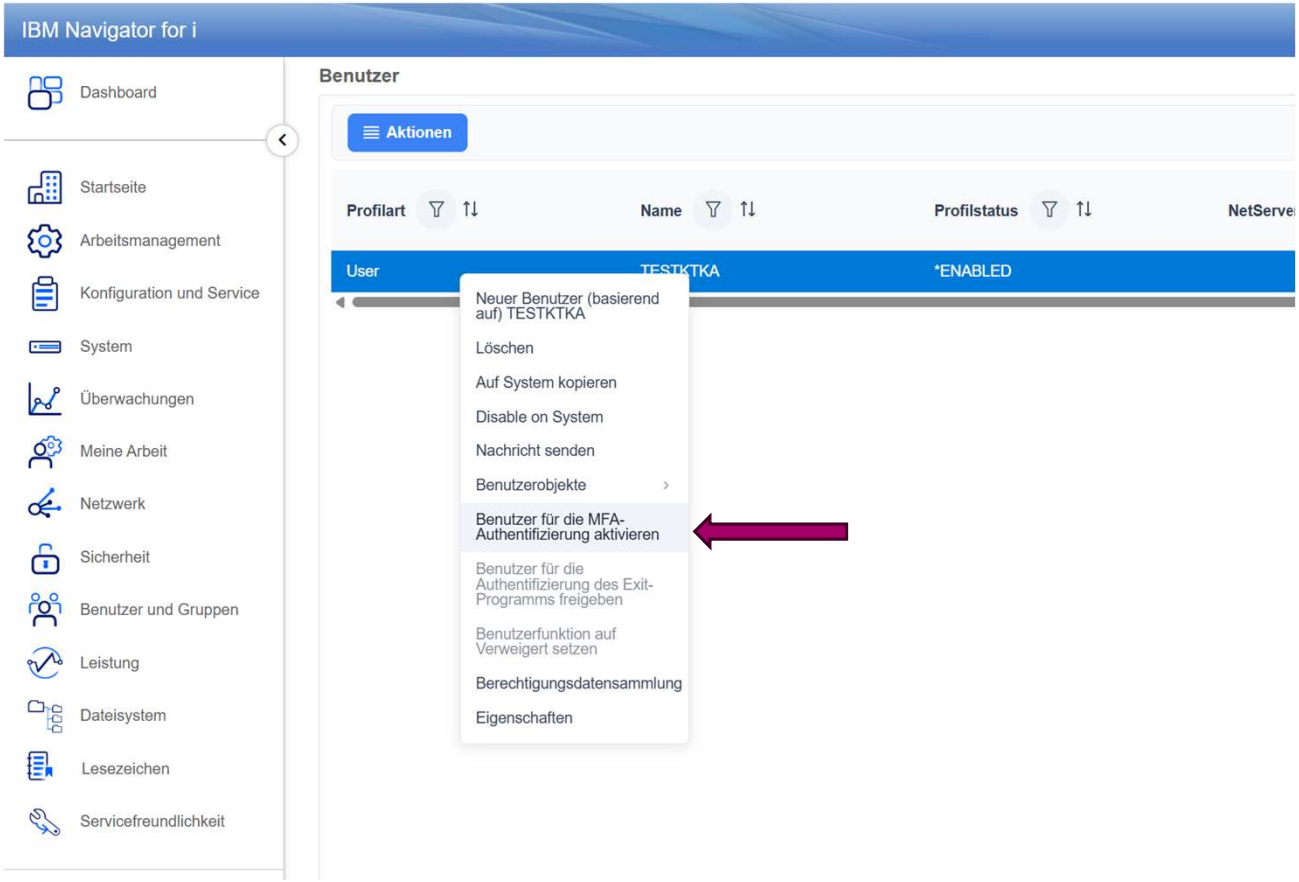
Validate MFA key

IBM i Navigator



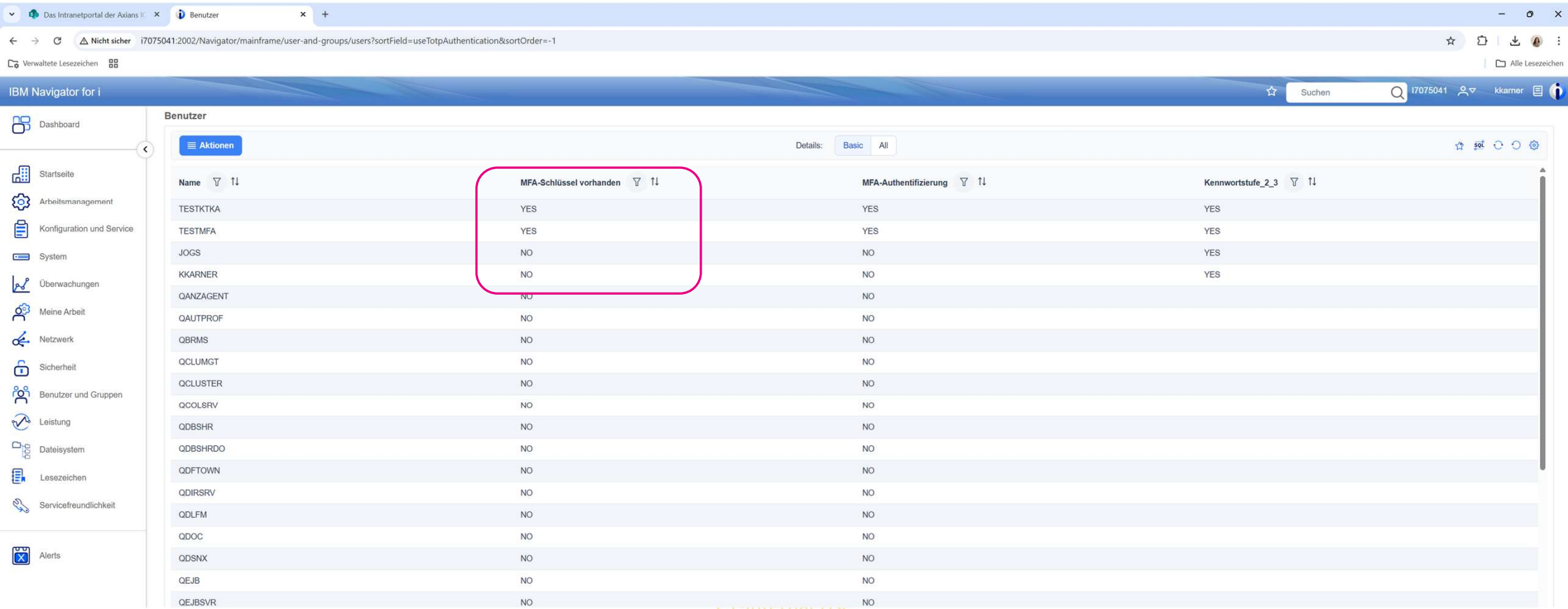
Enable MFA by SYSADMIN

IBM i Navigator



CHGUSRPRF

Activate TOTP, user by user



Name	MFA-Schlüssel vorhanden	MFA-Authentifizierung	Kennwortstufe_2_3
TESTKTKA	YES	YES	YES
TESTMFA	YES	YES	YES
JOGS	NO	NO	YES
KKARNER	NO	NO	YES
QANZAGENT	NO	NO	
QAUTPROF	NO	NO	
QBRMS	NO	NO	
QCLUMGT	NO	NO	
QCLUSTER	NO	NO	
QCOLSRV	NO	NO	
QDBSHR	NO	NO	
QDBSHRDO	NO	NO	
QDFTOWN	NO	NO	
QDIRSRV	NO	NO	
QDLFM	NO	NO	
QDOC	NO	NO	
QDSNX	NO	NO	
QEJB	NO	NO	
QEJBSVR	NO	NO	

MFA is active

Entering the second factor or recovery key

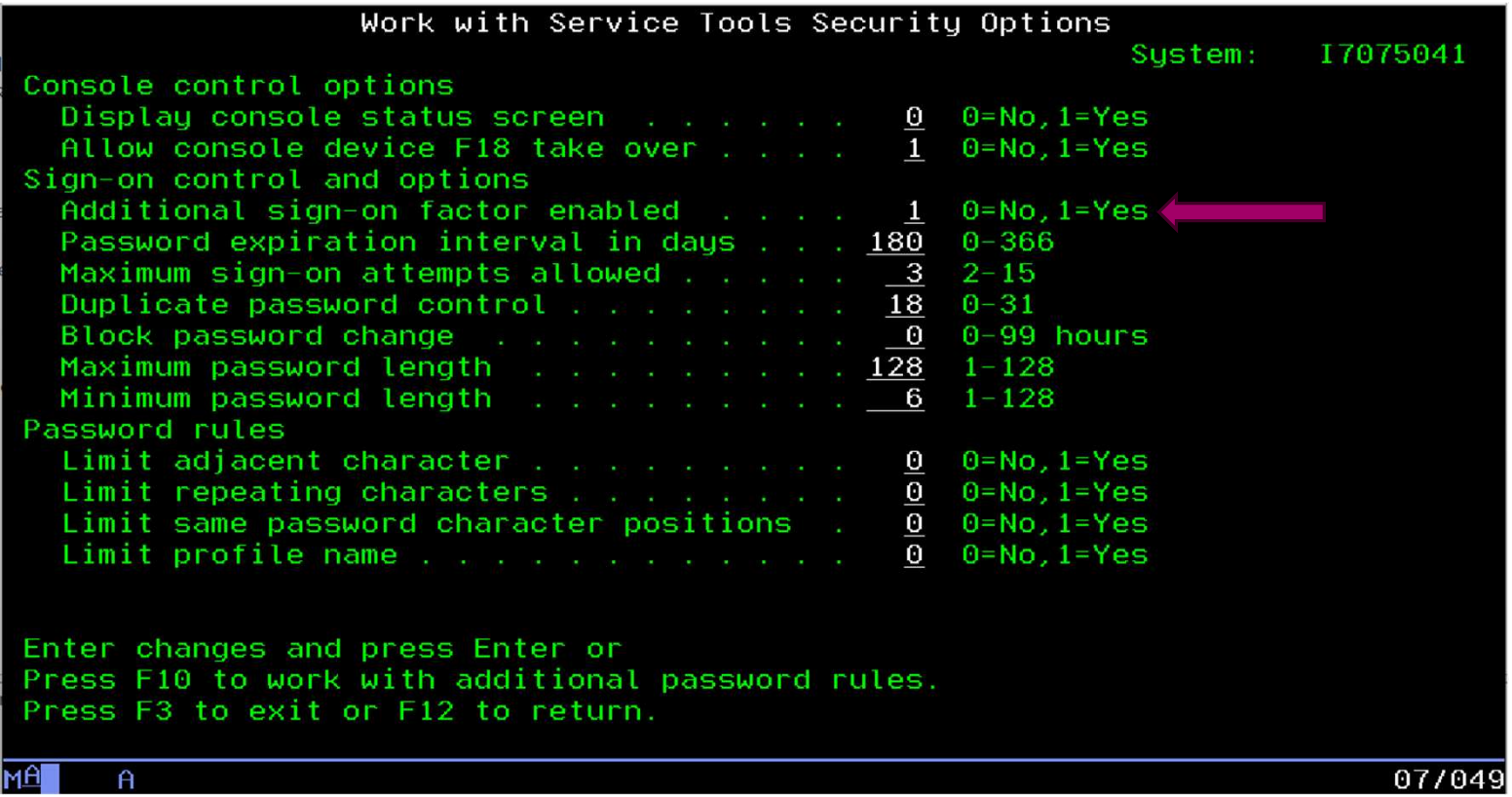
SST/DST MFA

Regardless of the implementation MFA on IBM i

- System values QDATE, QTIME and QTIMZON must be correct
- Use of NTP (Network Time Protocol) recommended
- No period for the validity of the TOTP value, so a token is required every time you log in
- Function also available in a restricted state

SST/DST MFA

Setup



SST

Option 8 = Service Tools Server Security and Devices

Option 5 = Security options of the service tools

DST

Option 5 = Work with DST

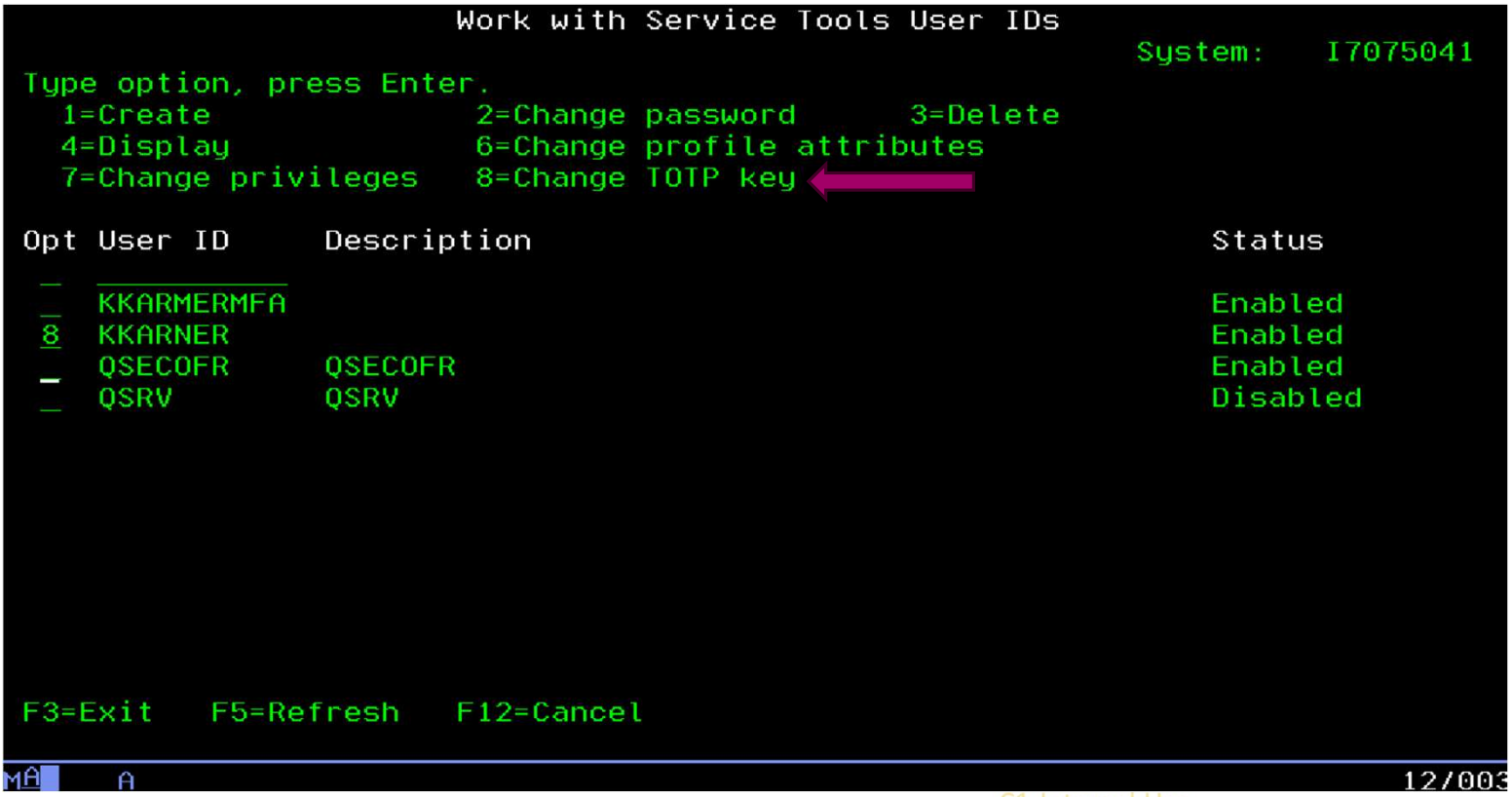
Option 4 = Safety data

Option 7 = Utilities security options

DSPSSTSECA for testing

SST/DST MFA

User Setup



SST

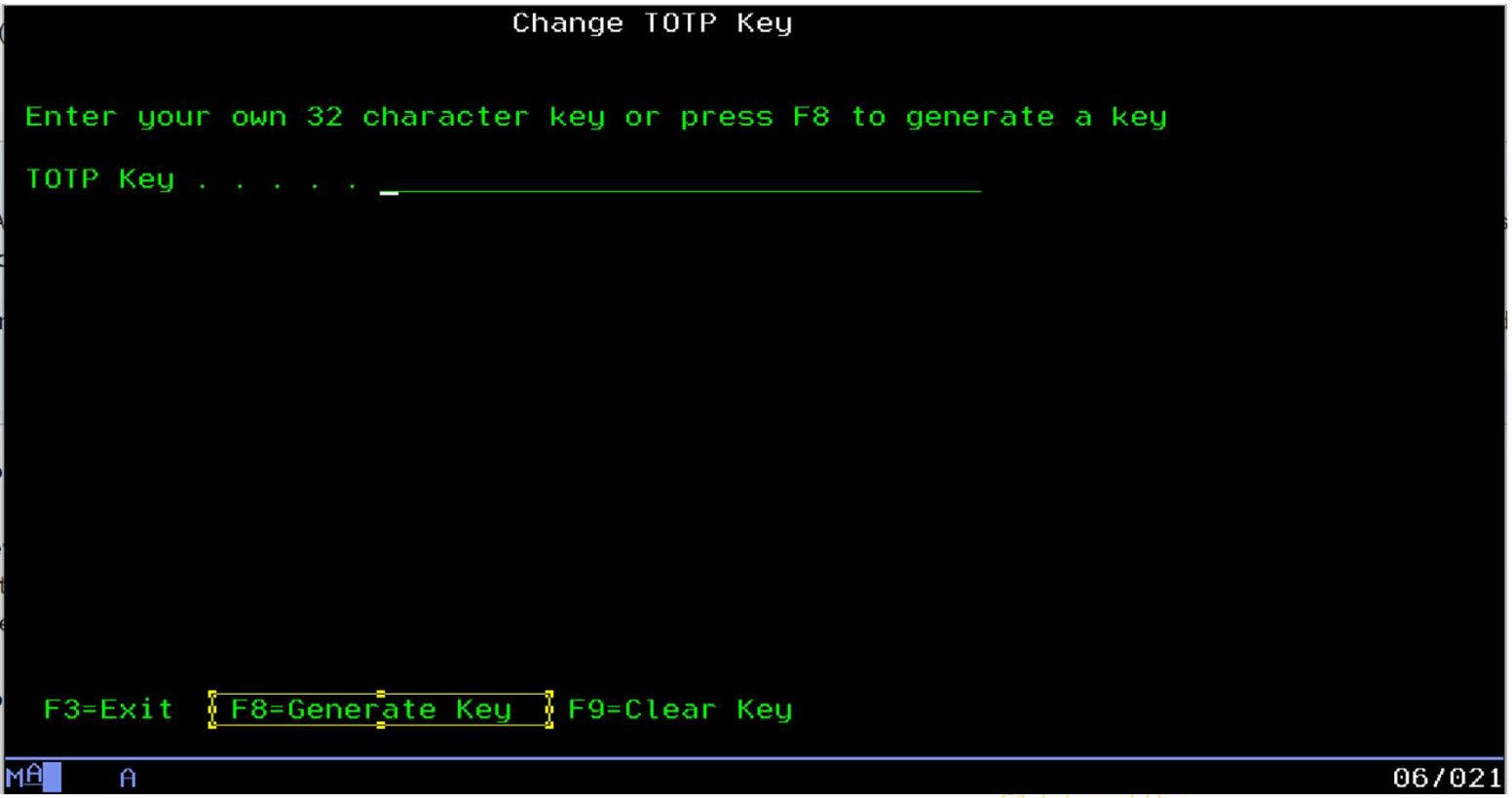
Option 8 = Service Tools Server Security and Devices

Option 1 = Service Tools User IDs

Option 8 = Change TOTP key

SST/DST MFA

User Setup



SST

F8 = Generate Key

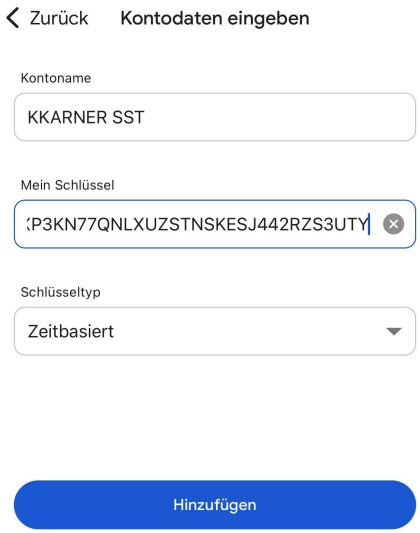
axians

SST/DST MFA

User Setup

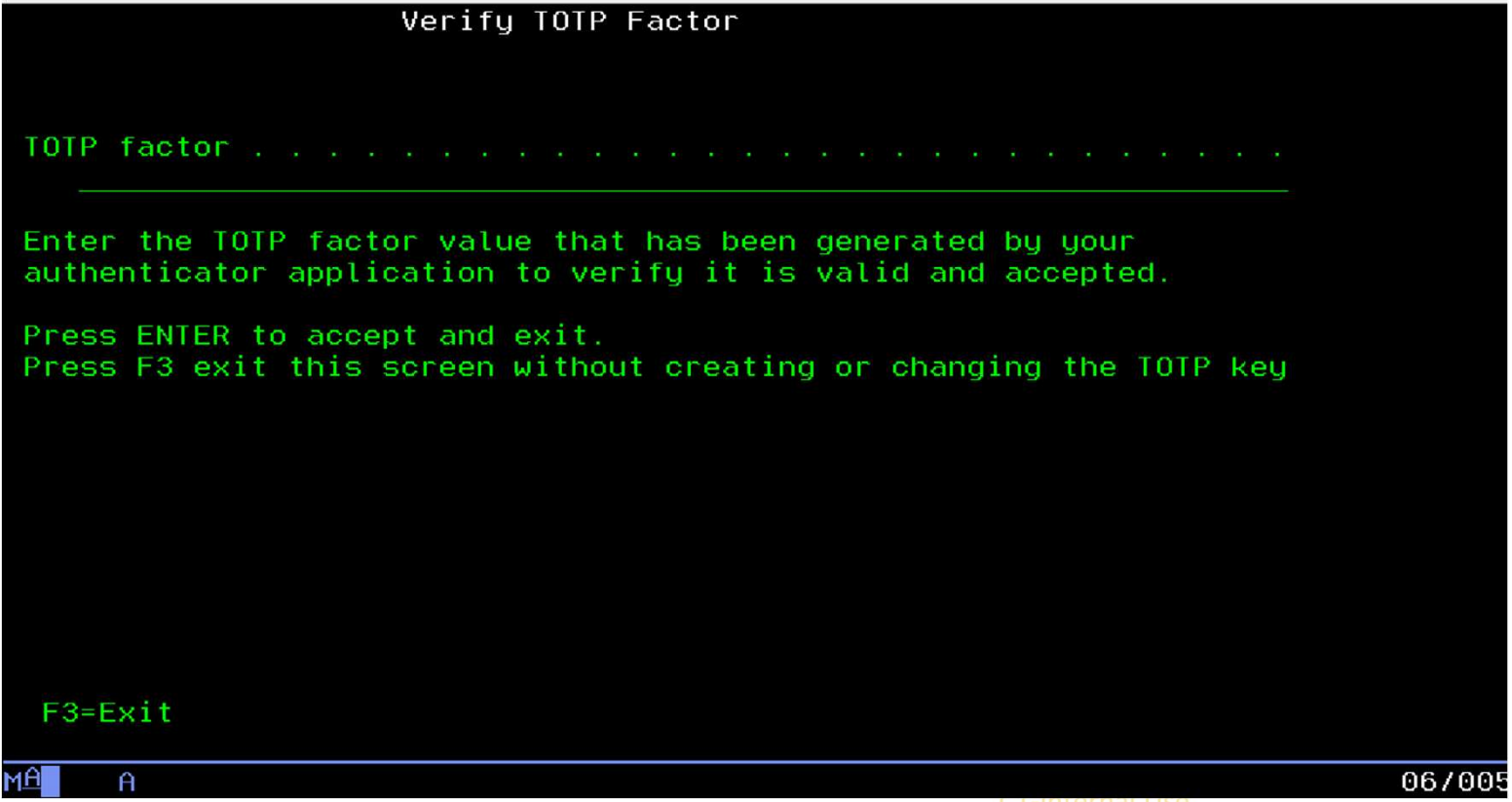
```
                              TOTP Key


TOTP key:
    KXP3 KN77 QNLX UZST NSKE SJ44 2RZS 3UTY
Copy and paste version:
    KXP3KN77QNLXUZSTNSKESJ442RZS3UTY
Recovery key:
    BBDH6HF2A736GCAA6F76ACA42262B7D7E9776A96B2289C6EB4HC332B52HAEE2B


This key must be entered into your TOTP generator client
application, without the blanks.

Save the recovery key for this TOTP key in a safe place.

Press ENTER to verify the key and accept.



 F3=Exit

MA  A                                                        01/001
```

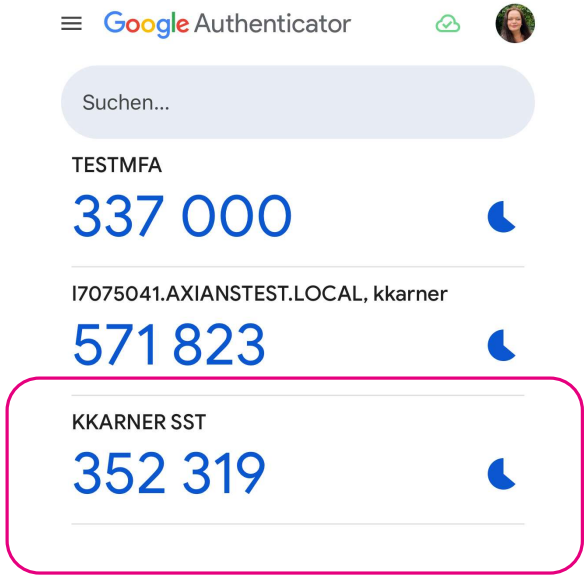
Add to Authenticator as usual



SST/DST MFA

User Setup





SST/DST MFA

User Setup

```
                    Display Service Tools User ID
                                                          System:   I7075041
  Service tools user ID name . . . . . :  KKARNERMFA

  Previous sign-on . . . . . :  04.09.25    13:46:30
  Password verification not valid . . . . . :  0
  Status . . . . . :  Enabled
  Date password last changed . . . . . :  04.09.25
  System date password expires . . . . . :  03.03.26
  User date password expires . . . . . :  None
  Password is set expired . . . . . :  No
  TOTP key exists . . . . . :  Yes
  Authentication method . . . . . :  TOTP

  Linked user profile . . . . . :  TESTMFA
  Description . . . . . :  MFA TEST




  F3=Exit    F5=Display privileges    F12=Cancel
MA    A
```

```
                    Anmelden mit STRSST (Start Service Tools)

                                                  SYSTEM: I7075041

  Benutzer-ID f. Service-Tool. _________
  Kennwort f. Service-Tools .

  Zusätzlicher Faktor. . . . . .
  ____________________________________________________________________




Hinweis: Groß-/Kleinschreibung von Kennwort muss beachtet werden.

F3=Beenden      F9=Kennwort ändern          F12=Abbrechen
MA    A                                                          07/033
```

Interfaces without a second factor

Solutions

- Password with attached MFA key
- A colon serves as a separation between password (:) and MFA value
- Example: ssh testusr@ibmiktka my$ecretPassw0rd:123456
- ODBC or JDBC interfaces:
  If passwords are stored in configuration files or used in automated jobs, an administrator must review these settings and update them if necessary, see Redbook IBM i 7.6 Features and Functions

Host Connection Servers

- Problem: ACS/Navigator can establish a large number of individual host-server connections
  - Depending on whether a stored PWD is used in the client
  - User with Saved Interval Required (TOTPOPTITV)
- Solution: New Host Connection Server
  - As a front-end for existing host servers
  - Requires TLS, uses port 9480
  - Persistent TOTP/MFA authenticated connection, all subsequent host-server connections are established through this connection
- ACS 1.1.9.7, Navigator, DCM and other tools use HCS, also works without an optional interval.

QIBM_RUN_UNDER_USER_NO_AUTH
Function Usage ID (CHGFCNUSG)

- Problem
  - The ability to perform actions as a different user profile based only on the permission for that user profile is contrary to MFA principles.
  - IBM i's built-in MFA TOTP implementation enables this password bypass due to widespread usage
- IBM i Solution
  - Optional blocking of applications that bypass the entry of credentials for a user
  - A user's entry in (QIBM_RUN_UNDER_USER_NO_AUTH) prevents that user profile from being the target of a "Run Under" operation.
  - Use is recommended with an MFA/TOTP user profile QIBM_RUN_UNDER_USER_NO_AUTH does not require a TOTP/MFA configuration for the user or the system

QIBM_QSY_AUTH (*REGFAC)

Single authentication exit point (WRKREGINF)

- Problem
  - The MFA-TOTP implementation built into IBM i may not work with existing enterprise-level MFA solutions used by the customer
- IBM i Solution
  - The new authentication exit QIBM_QSY_AUTH provides the ability to invoke an exit program during authentication processing for all applications that perform a corresponding operation.
  - The exit program is given information that can be used to perform additional checks, and it can return a success or failure indicator.
  - A deployed exit program could generate an **out-of-band push notification** to a phone that requires a fingerprint to continue.
  - For more information, see the *REGFAC authentication method section in the IBM documentation

Regulations and standards

Requiring the implementation of MFA (EU and International)

- GDPR (General Data Protection Regulation) (EU)
- PSD2 (Revises Payment Services Directive) (EU)
- ISO/IEC 27001 (Global Information Security Standard) (EU)
- NIST 800-171 & NIST 800-53 (Government & Contractors) (US)
- CMMC (Cybersecurity Maturity Model Certification) (Defense Contractors) (US)
- GLBA (Gramm-Leach-Bliley Act) (Financial Institutions) (US)
- PCI DSS (Payment Card Industry Data Security Standard) (Payment Processing) (US)
- HIPAA (Health Insurance Portability and Accountability Act) (Healthcare) (US)

Links

- Password level
  https://www.ibm.com/docs/en/i/7.5.0?topic=changes-considerations-changing-qpwdlvl-from-2-3-4
- MFA on IBM i
  https://www.ibm.com/docs/en/i/7.6.0?topic=security-multi-factor-authentication-mfa
- TLS Configuration
  https://www.ibm.com/docs/en/i/7.6.0?topic=security-system-tls
- IBM 7.6 Features and Functions
  https://www.redbooks.ibm.com/abstracts/sg248588.html
- Using IBM Navigator for I to manage MFA
  https://www.ibm.com/support/pages/using-ibm-navigator-i-manage-mfa
- QIBM_RUN_UNDER_USER_NO_AUTH Function Usage ID
  https://www.ibm.com/docs/en/i/7.6.0?topic=mfam-qibm-run-under-user-no-auth-function-usage-id
- SST/DST MFA
  https://www.ibm.com/docs/en/i/7.6.0?topic=concepts-service-tools-multi-factor-authentication-mfa

axians

Your contact

Katharina Karner

katharina.karner@axians.at

+43(0)664 / 851 3875

www.axians.at

VINCI ENERGIES