User Guide – M7 2FA

Two-Factor Authentication (2FA)

Author	SEMOpx
Date	08/03/2024
Version	Version 1.23

Contents

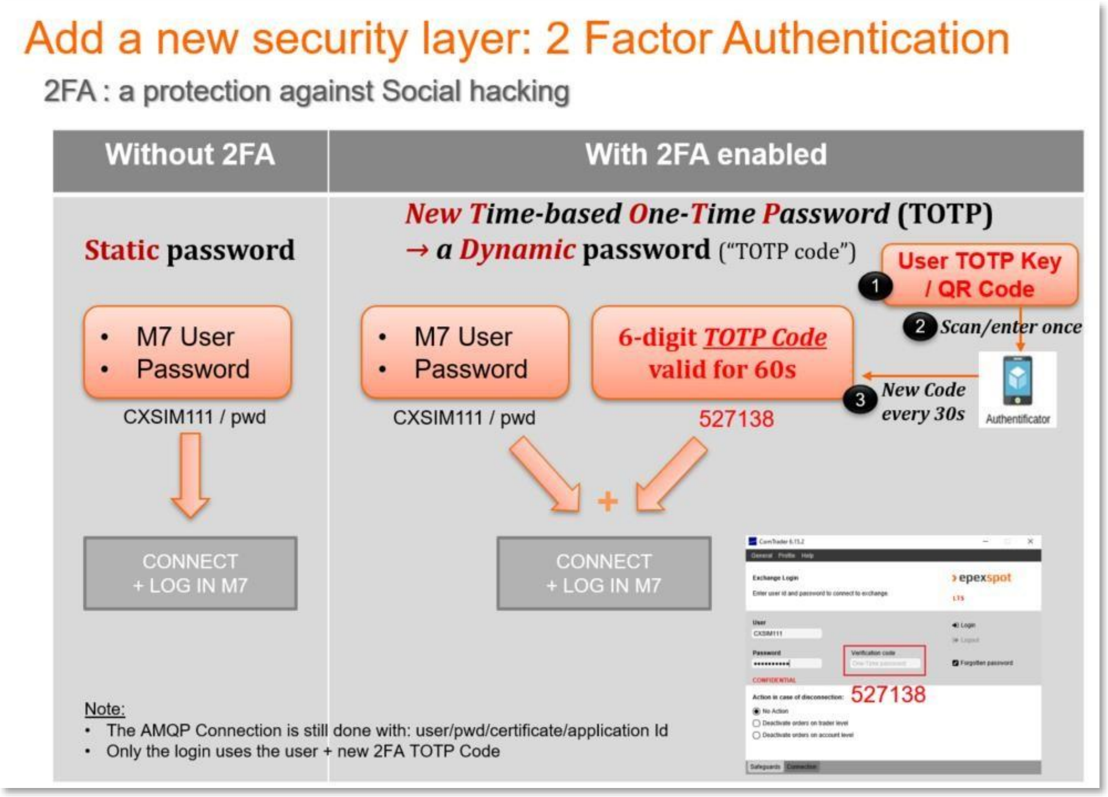
User summary

In compliance with the industry security standards, **the Two-Factor Authentication (2FA),** is introduced to **add one layer of security to your user account:**

- optional with M7 6.15 since 13 June 2023,
- **mandatory as of M7 6.17 in Q1 2024.**

This ***T**ime-based **O**ne-**T**ime **P**assword* **(TOTP) 2FA** consists in asking users to **provide when logging in:**

1. **their usual username (CX...) and password** (current situation),
   - this password can be considered as "static"
   - Note: technically speaking the password only needs to be provided with when establishing a connection with one of our API servers, not with the Login Request).
2. **a NEW 6-digits "authentication code"**, time-based,
   - meaning it **will change every 30 seconds**,
   - will be **valid for 60 seconds** (for the current 30-second period and the next one), so that a code generated at the very end of a 30-second period still works by the time it reaches M7,
   - and will be given by an **Authenticator App** on your smartphone or for API automated applications calculated by an **algorithm** (the public "TOTP" algorithm) .



Add a new security layer: 2 Factor Authentication

2FA : a protection against Social hacking

Without 2FA	With 2FA enabled
Static password	***New Time-based One-Time Password* (TOTP)** **→ *a Dynamic* password** ("TOTP code")

Note:

- The AMQP Connection is still done with: user/pwd/certificate/application Id
- Only the login uses the user + new 2FA TOTP Code

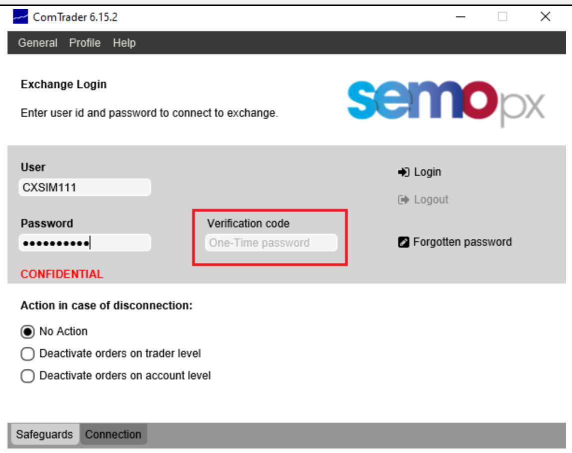
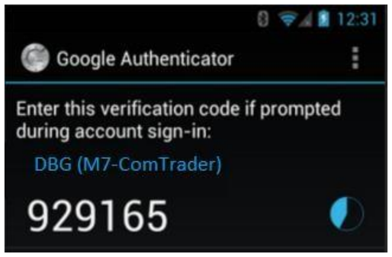
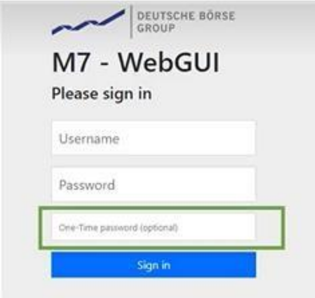
This guide describes the 2FA principles and the related procedures you need to follow to be able to:

- enable this 2FA for each desired user (since optional with M7 6.15):
  - via ComTrader, the Web GUI **or via the M7 API**
- generate the required elements (*QR code* for smartphone and *TOTP Key* for automated API apps) for you to generate this new *Authentication Code* that will change every 30 seconds and be able to log in with your user:
  - in ComTrader,
  - in the WebGUI with a report user,
  - in the M7 API.
- re-generate them in needed, for instance if lost.

The last FAQ section covers related M7 topics (*Password Policy*, *API certificates*) **and specific 2FA questions** (e.g. *What is the validity of my QR code or TOTP Key?, Which application or API library should I use to generate TOTP codes?,* etc.).

Please refer as well to **our 2FA Video Tutorial** that can be downloaded from the SEMOpx Website.

How do I log in with 2FA once Enabled?

User Type	New Login Interface	How to get this new code?
ComTrader **users**	 ComTrader 6.15.2 General Profile Help **Exchange Login** Enter user id and password to connect to exchange. **User** CXSIM111 **Password** •••••••••• Verification code: One-Time password Login Logout Forgotten password CONFIDENTIAL **Action in case of disconnection:** ● No Action ○ Deactivate orders on trader level ○ Deactivate orders on account level Safeguards Connection	1. Download a TOTP **Authentication app** on your smartphone (e.g. Google Authenticator, Microsoft Auth) Authentificator 2. **Enable TOTP in ComTrader 6.17** 3. **Scan** the ComTrader **QR Code with your app** ➔ **4. The app will generate a TOTP *Verification Code,* changing every 30 seconds.**  12:31 Google Authenticator Enter this verification code if prompted during account sign-in: DBG (M7-ComTrader) 929165 For report users: please check below the "Change password" webGUI procedure.
Report users (XML reports: TC540, TC810, etc.)	 DEUTSCHE BÖRSE GROUP M7 - WebGUI Please sign in Username Password One-Time password (optional) Sign in	
API users	Login Request with a new ***authVerificationCode*** attribute. AMQP connections are not affected. Example for an API user for which TOTP has been enabled in ComTrader 6.17: <LoginReq xmlns="http://www.deutsche-boerse.com/m7/v6" user="CXSIMXXX" force="true" disconnectAction="NO" **authVerificationCode="84498"**> **Manual API apps** with a GUI showing a Login panel **can mimic the ComTrader login panel** (users can then follow the ComTrader process above, while the app sends the enriched Login Request with the new code) **or store a "TOTP Key"** in a secured way to generate at each login a new 30-second valid "TOTP Verification Code".	**Automated API apps** will have to store the user TOTP Key and **implement the public TOTP algorithm** (or use public libraries) to generate a new TOTP verification code at each login. ComTrader **or an API request/response** will give a user **TOTP Key** (see below), required as an input of the TOTP algo to generate this new 6-digit verification code in real time. Optional in 6.15, mandatory in 6.17.

How to enable 2FA in 6.17 and get a user QR Code/TOTP Key?

Once M7 6.15 is delivered, **2 FA is by default disabled for all users.**

Though still optional in 6.15, we encourage you to activate it by following the below procedure.

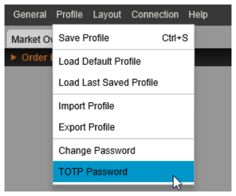
<table>
<tr><th>User Type</th><th>How do I activate/enable 2 FA for my user in ASIM? (or later in PROD)</th></tr>
<tr><td>

ComTrader

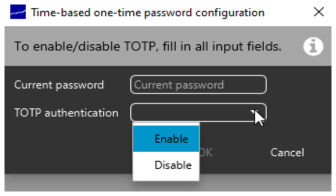
users

</td><td>

- Once logged in ComTrader, go to the menu **>Profile>TOTP Password**:



- A new panel pops-up:
  - select "Enable" after having input your current user password (the one you used to log in), and click on "OK":



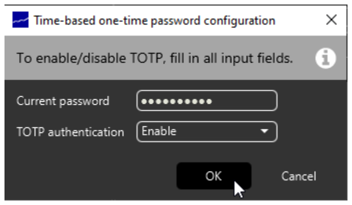
Time-based one-time password configuration

To enable/disable TOTP, fill in all input fields.

Current password: Current password

TOTP authentication: Enable / Disable

Cancel



Time-based one-time password configuration

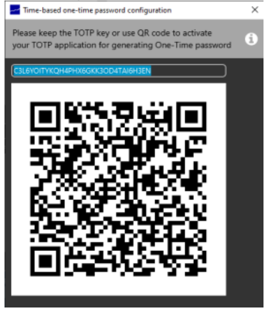
To enable/disable TOTP, fill in all input fields.

Current password: ••••••••••

TOTP authentication: Enable

OK Cancel

- After having clicked on "OK", ComTrader displays:
  - **A secret "TOTP Key"** = C3L6YOITYKQH4PHX6GKK3OD4TAI6H3EN (to be copied for a later use by API apps for this user),
  - **a QR Code** (that contains this TOTP Key).

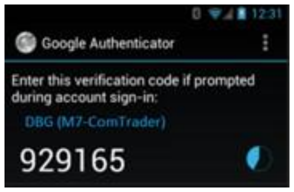


Time-based one-time password configuration

Please keep the TOTP key or use QR code to activate your TOTP application for generating One-Time password

C3L6YOITYKQH4PHX6GKK3OD4TAI6H3EN

- **If using ComTrader, or a manual API app with a GUI user:**
  - **scan this QR code** with your phone authenticator app: it will generate a new 6-digit code every 30 seconds, valid for 60 seconds (see the FAQ section for more details).



Google Authenticator

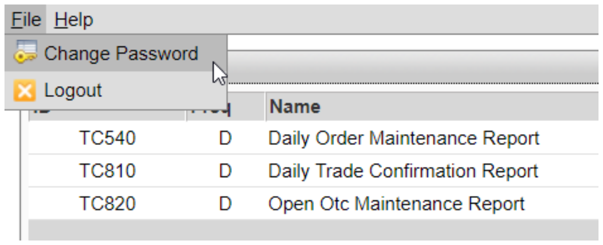
Enter this verification code if prompted during account sign-in:

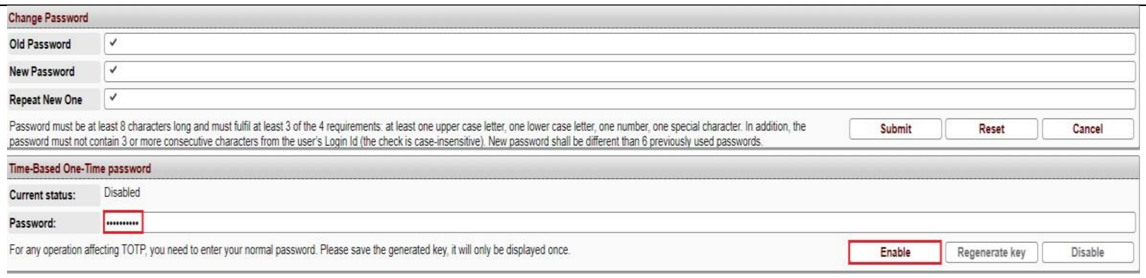
DBG (M7-ComTrader)

929165

- **If using an automated API app:**
  - store the TOTP key string for a later usage by your API app. This will be one input of the TOTP algo, the 2nd being the current timestamp.
  - Note: This TOTP Key works exclusively for this very user.

</td></tr>
</table>

API users	- **API users** can either use ComTrader or use **API messages to enable 2FA and get their TOTP key**: ○ **TotpPwdReq**, proving: ▪ the user current password, ▪ totpEnabled = true/false ○ **TotpPwdResp**, containing the TOTP key (“secret”) Please note that the TotpPwdReq message can be used as well to: - request a new TOTP key if you think the current one has been compromised, or if periodically required by your internal security policy (please note you must be already logged in to send this request, meaning that if 2FA is already activated you must have the last TOTP Key to be able to generate a new one ; if not please consult the “TOTP Key lost” procedure below), - disable 2FA during the optional phase if required, in a test environment (ASIM/XSIM) or in PROD. Example: <?xml version="1.0" encoding="UTF-8"?> <**TotpPwdReq** xmlns="http://www.deutsche-boerse.com/m7/v6" currentPwd="Test0101" totpEnabled="true"> <StandardHeader marketId="EPEX"/> </TotpPwdReq> <?xml version="1.0" encoding="UTF-8"?> <**TotpPwdResp** xmlns="http://www.deutsche-boerse.com/m7/v6" secret="SHIXQZ7AG5HJTSSDLS2P55F2J6LO4UDJ"> <StandardHeader marketId="EPEX"/> </TotpPwdResp> The System Info Response message contain the TotpPwdReq inquiry request limit rate: - Once per minute and 10 times per hour (rolling time windows): - <RequestLimit message="TotpPwdReq" duration="60" rate="1"/> - <RequestLimit message="TotpPwdReq" duration="3600" rate="10"/> Please check DFS180 6.17.357 of higher and the 6.17 XSD file for more details.
TC report users	**For Report user**, log in the Web GUI, and selec the **>File>Change password** menu:  Name TC540 D Daily Order Maintenance Report TC810 D Daily Trade Confirmation Report TC820 D Open Otc Maintenance Report - This leads you to a page that in its lower part gives you the possibility to **Enable the 2FA** for the logged in report user: ○ Input your user current password ○ Click on *Enable*



Change Password

Old Password ✓

New Password ✓

Repeat New One ✓

Password must be at least 8 characters long and must fulfil at least 3 of the 4 requirements: at least one upper case letter, one lower case letter, one number, one special character. In addition, the password must not contain 3 or more consecutive characters from the user's Login Id (the check is case-insensitive). New password shall be different than 6 previously used passwords.

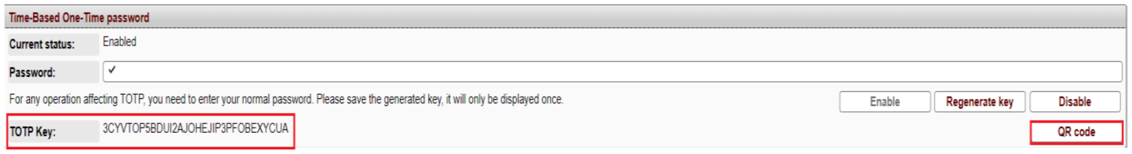
Time-Based One-Time password

Current status: Disabled

Password: ••••••••••

For any operation affecting TOTP, you need to enter your normal password. Please save the generated key, it will only be displayed once.

- **A new TOTP Key gets generated.**
- The page gives you as well the possibility to **generate a new QR code:**



Time-Based One-Time password

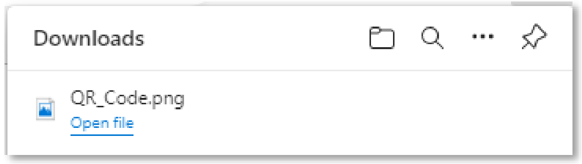
Current status: Enabled

Password: ✓

For any operation affecting TOTP, you need to enter your normal password. Please save the generated key, it will only be displayed once.

TOTP Key: 3CYVTOP5BDUI2AJOHEJIP3PFOBEXYCUA

- If you click on "QR code" a **new QR code image file** is downloaded by your browser:



○ **Then please use the TOTP key or scan the QR code as explained above**, depending on how you connect retrieve your TC reports (manual GUI log in versus automated app).

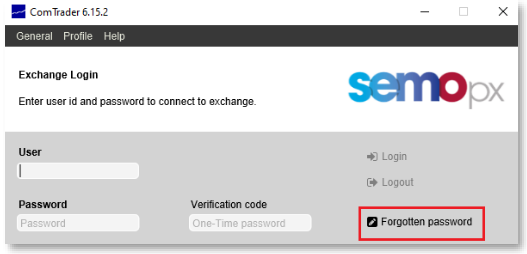
How to get a new TOTP Key or QR code if I lose it? (recovery procedure)

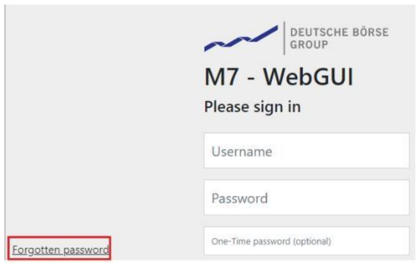
The below ***Forgotten Password* procedure** is applicable for all users : ComTrader, Report users and API users.

By the TOTP security standard, the secret "TOTP key" is:

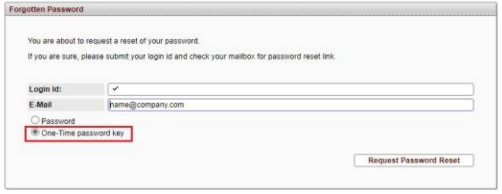
- Personal: unique for each User
- only retrievable by the intended user when enabling 2 FA.
  - Neither SEMOpx nor the user will be able to retrieve it afterwards in case the TOTP Key or QR code has not been not noted down or was lost / forgotten)
  - The "forgotten password" procedure will need to be followed

- **Launch ComTrader (for ComTrader or API users), OR open the Web GUI (for report users) and click on the "Forgotten password" link** (without filling anything)**:**





- The **"Forgotten password webGUI"** now contains a new option to **request a new TOTP Key/QR Code:**


Forgotten Password

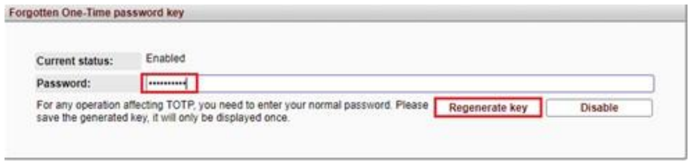
You are about to request a reset of your password.

If you are sure, please submit your login id and check your mailbox for password reset link.

Login Id: ✓
E-Mail: name@company.com

○ Password
● One-Time password key

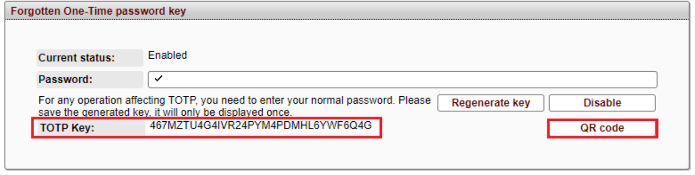
- When clicking on **"Request Password Reset",** M7 sends to the e-mail address a link, valid for 1 hour. Clicking on it leads you to a new page where you can **regenerate your user TOTP Key** :
  - Enter your current user password
  - Click on "Regenerate key"


Forgotten One-Time password key

Current status: Enabled
Password: ••••••••••

For any operation affecting TOTP, you need to enter your normal password. Please save the generated key, it will only be displayed once.

- **A new TOTP Key gets generated.** The page gives you as well the possibility to generate a new QR code:


Forgotten One-Time password key

Current status: Enabled
Password: ✓

For any operation affecting TOTP, you need to enter your normal password. Please save the generated key, it will only be displayed once.

TOTP Key: 467MZTU4G4IVR24PYM4PDMHL6YWF6Q4G

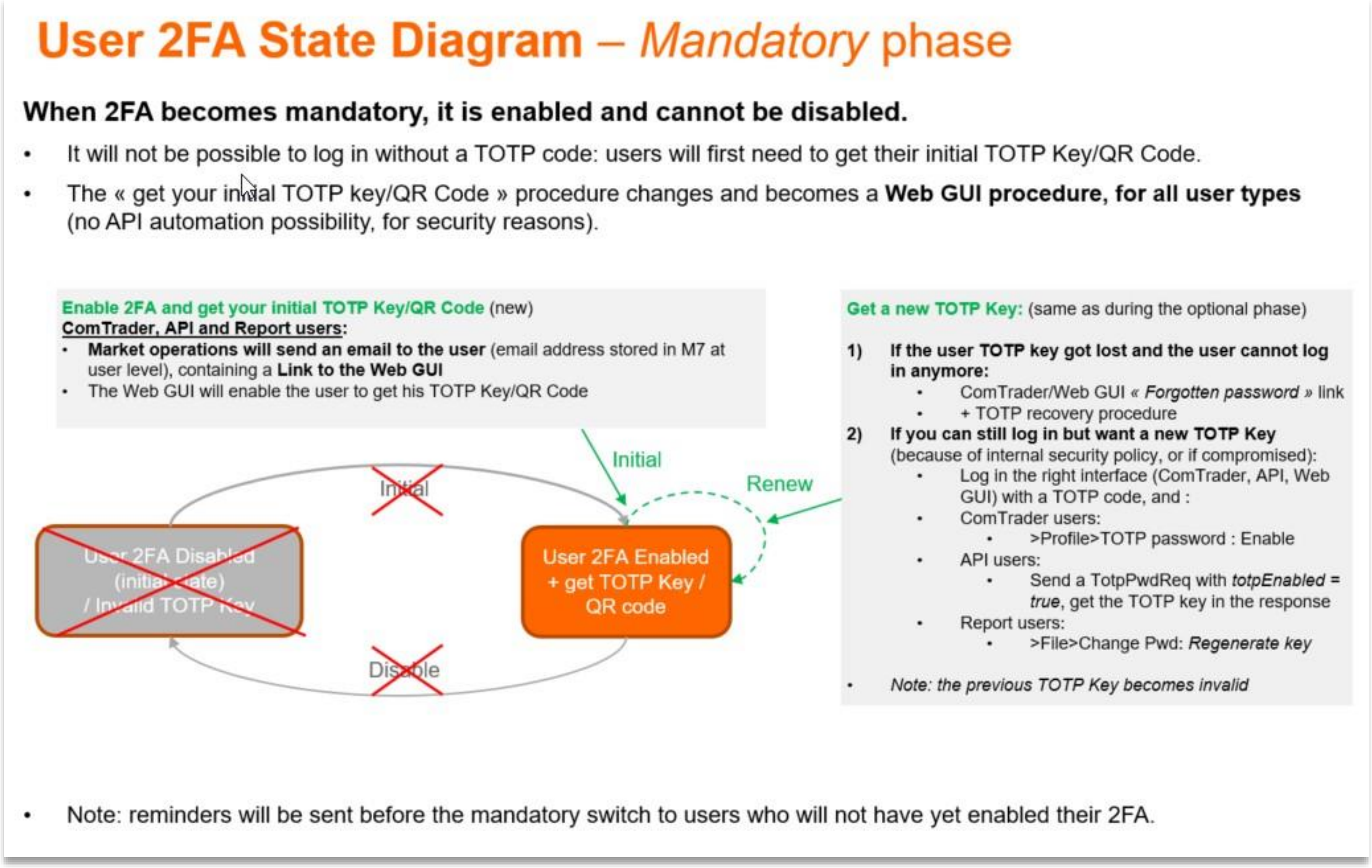
- If you click on "QR code" a **new QR code image file** is downloaded by your browser: [redacted]

Note for the testing period in ASIM:
please make sure that your email is registered in ASIM for your tested user so you can receive the required link :
do not hesitate to contact our Market Operation team at marketops@ops.semopx.com to adjust your user setup if required, so you can receive all emails sent by M7.

M7 6.17 MANDATORY PHASE

Once 2FA becomes mandatory (M7 6.17 release), 2FA will be enabled by default:

- **There will not be any possibility to disable 2FA.**
- **Users will not be able to log in if they are cannot provide a TOTP code:**
  - All users who would not have already enabled 2FA and collected their TOTP Key/QR code, or users created after the "2FA mandatory switch" will have to **use a Web GUI procedure** that will be provided later with the 6.17 documentation (email received by the end user containing a link redirecting to the M7 Web GUI).
  - Please note that API apps will not be able anymore to use *TotpPwdReq* to get a user first TOTP Key. The request will though still be available to generate a new TOTP key if required.
  - **API apps implementing the "hide the TOTP code" model or hybrid model** (please see the below dedicated section) **will have to be able to store in a secured way the TOTP Key collected by the end user.**



User 2FA State Diagram – *Mandatory* phase

When 2FA becomes mandatory, it is enabled and cannot be disabled.

- It will not be possible to log in without a TOTP code: users will first need to get their initial TOTP Key/QR Code.
- The « get your initial TOTP key/QR Code » procedure changes and becomes a **Web GUI procedure, for all user types** (no API automation possibility, for security reasons).

Enable 2FA and get your initial TOTP Key/QR Code (new)
ComTrader, API and Report users:
- **Market operations will send an email to the user** (email address stored in M7 at user level), containing a **Link to the Web GUI**
- The Web GUI will enable the user to get his TOTP Key/QR Code

Get a new TOTP Key: (same as during the optional phase)

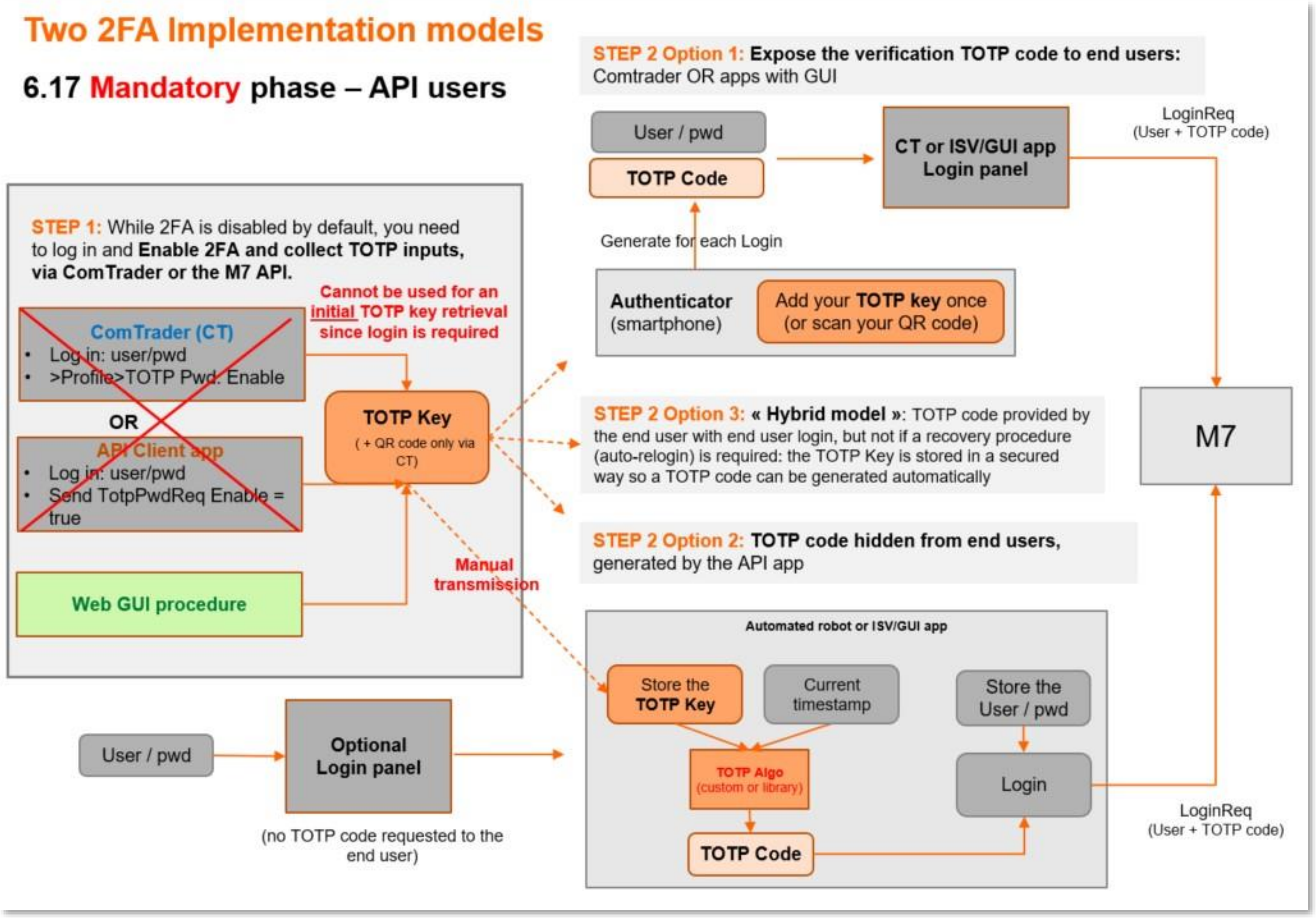
1) **If the user TOTP key got lost and the user cannot log in anymore:**
   - ComTrader/Web GUI « *Forgotten password* » link
   - + TOTP recovery procedure
2) **If you can still log in but want a new TOTP Key** (because of internal security policy, or if compromised):
   - Log in the right interface (ComTrader, API, Web GUI) with a TOTP code, and :
   - ComTrader users:
     - >Profile>TOTP password : Enable
   - API users:
     - Send a TotpPwdReq with *totpEnabled = true*, get the TOTP key in the response
   - Report users:
     - >File>Change Pwd: *Regenerate key*

- *Note: the previous TOTP Key becomes invalid*

~~User 2FA Disabled (initial state) / Invalid TOTP Key~~
~~Initial~~
Initial
Renew
User 2FA Enabled + get TOTP Key / QR code
~~Disable~~

- Note: reminders will be sent before the mandatory switch to users who will not have yet enabled their 2FA.

Once 2FA becomes mandatory: API apps can only acquire the initial TOTP key “manually” (retrieved by the end user, via a Web GUI procedure).



Two 2FA Implementation models

6.17 Mandatory phase – API users

STEP 1: While 2FA is disabled by default, you need to log in and **Enable 2FA and collect TOTP inputs, via ComTrader or the M7 API.**

~~ComTrader (CT)~~
- ~~Log in: user/pwd~~
- ~~>Profile>TOTP Pwd: Enable~~

~~OR~~

~~API Client app~~
- ~~Log in: user/pwd~~
- ~~Send TotpPwdReq Enable = true~~

Cannot be used for an initial TOTP key retrieval since login is required

STEP 2 Option 1: Expose the verification TOTP code to end users: Comtrader OR apps with GUI

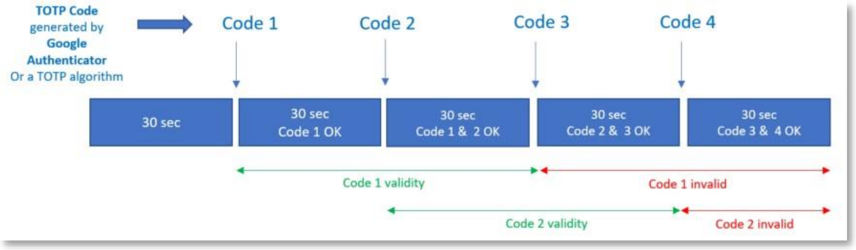
STEP 2 Option 3: « Hybrid model »: TOTP code provided by the end user with end user login, but not if a recovery procedure (auto-relogin) is required: the TOTP Key is stored in a secured way so a TOTP code can be generated automatically

STEP 2 Option 2: TOTP code hidden from end users, generated by the API app

(no TOTP code requested to the end user)

FAQ

QUESTION	ANSWER
- ***How does this 2FA fit with the password policy, currently deactivated in PROD?***	- This 2FA security policy will impact the password policy : the constraints on new password remains but **the automatic user password expiry every 90 days will NOT be re-activated in PROD** since 2FA becomes mandatory as of M7 6.17.
- ***Will API certificates still be required once 2 FA is mandatory with M7 6.17?***	- Yes, API certificates per API application will still be required.
- **What is the difference between these codes: between a TOTP Key (or a QR code) and a TOTP verification code?**	- The TOTP Key or the QR code must be requested only once (though then can be generated again if lost). - They are used to generate a real time TOTP code, required when logging in, on top of your usual user/password. - Manual users who need to type their TOTP code when logging in will use an authenticator app: they will scan once the QR Code and then only use the app. ○ QR code -> scan it once -> then use the app to get your TOTP code to log in - Automated API apps will to be fed with the TOTP key, so they can use it an TOTP algo input , combined with the current timestamp. ○ TOTP Code = function (TOTP secret key, current time)
- ***Which application or API library should I use to generate TOTP codes?***	- The TOTP code can be generated using **the known and public TOTP algorithm**. - For app with a manual log in panel, either one of the industry-standard authentication applications (authenticators like *Google Authenticator, Microsoft Auth*) can be used. - For automated API apps: customers can implement their own algorithm based on the TOTP “norm”, or use public libraries.
- **On which standards does 2FA rely?**	- The Open Authentication Initiative community agreed with the following specifications for the TOTP algorithm, also used by the google authenticater and specified in these RFCs: https://www.rfc-editor.org/rfc/rfc6238 (as an extension of https://www.rfc-editor.org/rfc/rfc4226)
- ***With M7 6.17, can I enable 2 FA for all my users at once?***	- No, the activation (enabling 2 FA) is personal, and thus must be done user per user. - No mass activation is possible with M7 6.17.
- ***What is the validity of the TOTP Key and the QR code?***	- Neither the TOTP Key nor the QR Code (which contains as well the TOTP Key) expires automatically. - They become invalid only if you generate a new one.
- ***What is the validity of each TOTP verification code?***	- The validity of the 6-digit code generated by the Authenticator (i.e. length of the window in which the code, in combination with the correct User Password and User Name is accepted by M7) is **valid for a maximum of 60 seconds** (for the current 30-second period and the next one), so that a code generated at the very end of a 30-second period still works by the time it reaches M7.

<table>
<tr>
<td></td>
<td>


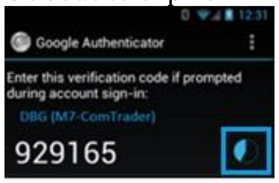
- Once logged in, the User will not be asked anymore to provide the TOTP code. This is also valid for API connections – if the connection drops and the User is considered disconnected, then a new login with a TOTP code is required.
</td>
</tr>
<tr>
<td>

- ***With M7 6.14, my user becomes invalid/revoked when I enter a wrong password 5 times in a row. Is this rule affected by 2FA?***
</td>
<td>

- As of M6.17, 2FA each wrong verification code is counted.
</td>
</tr>
<tr>
<td>

- **If I experience an AMQP disconnection, or if I am logged out, do I need to enter again a TOTP code when I re-log in?**
</td>
<td>

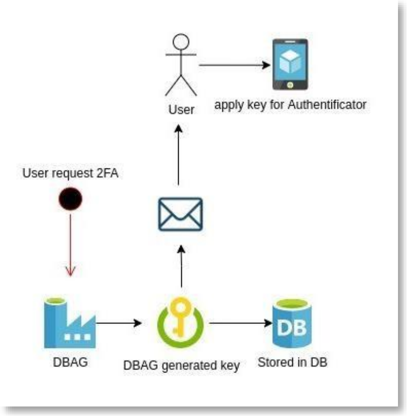
- Yes, each time a new login is required (including after an AMQP connection loss), a new TOTP code must be input.
- This code changes every 30 seconds, but is valid for 60 seconds : during these 60 seconds the same code can be re-used to log in as many times as needed (for APIs in the respect of the LoginReq limit per minute).
- Your authenticator app will display code changes on your phone screen and usually gives a rough indication of the remaining number of seconds (framed in blue below): you see when the TOTP code is about to expire:


12:31
Google Authenticator
Enter this verification code if prompted during account sign-in:
DBG (M7-ComTrader)
929165

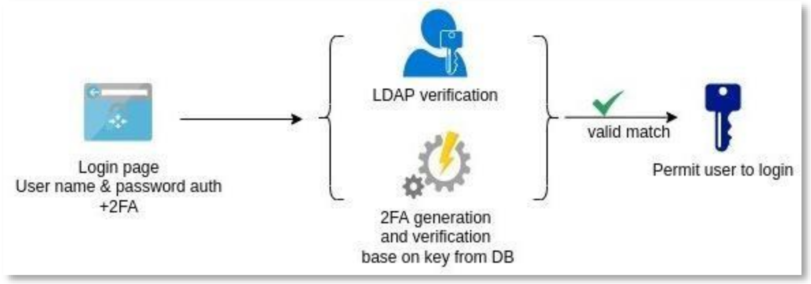
- Reminder: in case an API app experiences an AMQP disconnection without having been able to send a Logout Request, M7 detects this loss within the next 20 to 40 seconds and logs your user out for “INACTIVITY” : please refer to the M7 API FAQ for more details.
</td>
</tr>
<tr>
<td>

- **How does it work on M7 side?**
</td>
<td>

- M7 stores the generated TOTP Key in its database:



- When a user logs in with its user/password and the new TOTP verification code, M7 generates as well a TOTP code (based on the same TOTP Key and its current
</td>
</tr>
</table>

	timestamp) and compares it with the one provided : if they match, the user is authenticated and gets logged in:  Login page User name & password auth +2FA LDAP verification 2FA generation and verification base on key from DB valid match Permit user to login
- **Is it possible that my TOTP code gets refused while correct at the moment it was generated?**	- Indeed, the TOTP algorithm divides the time elapsed since 00:00:00 UTC on 1 January 1970 into 30 seconds interval. - As a result, this code changes every 30 seconds, but is valid for 60 seconds : during these 60 seconds the same code can be re-used to log in as many times as needed. - If, for whatever reason, the TOTP code calculated by M7 does not match the one sent by the client application, the following error is sent in the private response queue as a response to the Login Request and the user cannot not log in: <?xml version="1.0" encoding="UTF-8"?> <ErrResp xmlns="http://www.deutsche-boerse.com/m7/v6"> <StandardHeader marketId="EPEX"/> <Error err="Auth error" errCode="0"/> </ErrResp> - As a result, your API app must be ready to try to relog in with a new TOTP code.
- **Does 2FA apply to Read only users as well?**	- Yes, 2FA applies to all users and apps (RO or R/W).
- **Does the TOTP Key expires after a period?**	- No, the TOTP Key remains valid until a new one is generated.
- **Do I get logged out after a certain time with the introduction of 2FA?**	There is no change at all regarding the “logged in” status of users once they use 2FA: - Once you have logged in with your user/password and the new “verification code”, there is no expiry after x hours : as long as you are logged in you do not need to enter the verification code again. - You only need to input this additional code when you need to log in, and the moments when you are required to log in are not affected by this 2FA compared to today. - But if you log out, even for a second, then a TOTP code will be required for your next login.
- **What is the maximum length of the TOTP key?**	As per the XSD file, the TOTP key can have a maximum of 64 characters.

Glossary

Term	Description
2FA	Two-Factor Authentication. Also referred to as multi-factor authentication. Instead of just using a password, one other mean of user authentication is required to add another layer of security, in order to prevent unauthorized users from gaining access to a user account with nothing more than a stolen password.
TOTP	Time-based One-Time Password. Sometimes referred to as "OTP". "Time-based" means that the password is valid for a short time (in our case 30 seconds), when usual user passwords can be considered as "static" (though they have their own life cycle with a potential expiry date, they do not change "spontaneously").
TOTP Algorithm	Public cryptographic algorithm that generates a one-time password (OTP): • that uses the current time as a source of uniqueness in combination with a static secret key, • used as a standard in many industries 2FA systems.
TOTP Key	Or "OTP Key" or "Secret Key". The static "secret" key given by ComTrader/webGUI, required to be able to generate a TOTP verification code.
TOTP Verification Code	Or "OTP Verification Code" Or "TOTP code" Or "TOTP authentication code" Or "2nd password" The new code changing every 30 seconds, but valid for 60 seconds, that users need to be able to log in M7, on top of their usual user/password combination, when 2FA is enabled for this user. This code is a function of a secret Key and current time. TOTP Code = function (TOTP secret key, current time)