Scanduc | 23

# A TOTP implementation

Sture Andersen, Sture ApS

# What’s special about TOTP?

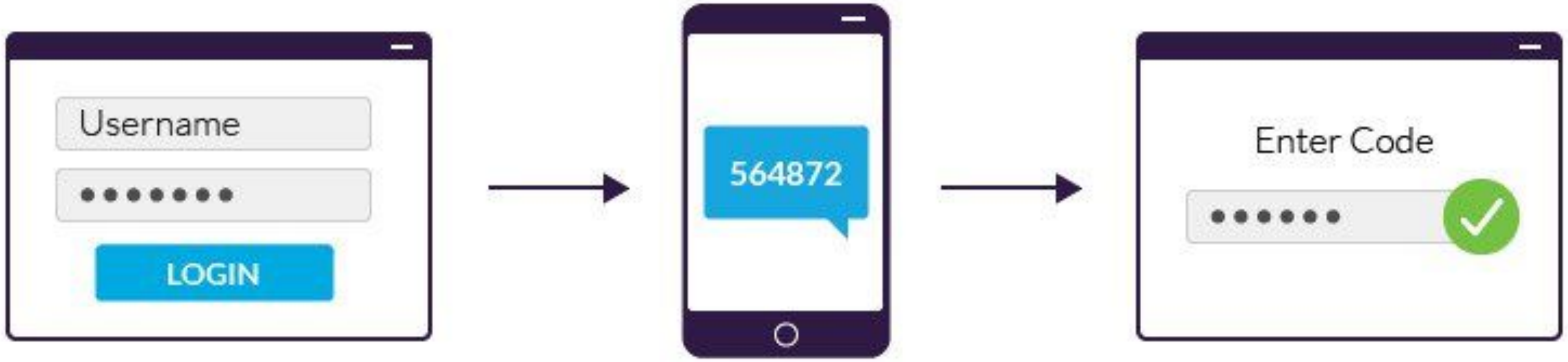
TOTP - or Timed One Time Passwords - make out a subclass of 2-factor authentication systems.

The thing that sets them apart is that TOTP does not involve sending a verification code from the server to a phone or an email account.

Such communications can be tapped. And TOTP can not.

It’s the first “arrow” of the next slide that may be compromised

# Conventional 2-factor



The user enters in their username and password.

An authentication code is sent to the user's mobile device.

The user enters in their authentication code to log into the application.

# Authenticator app

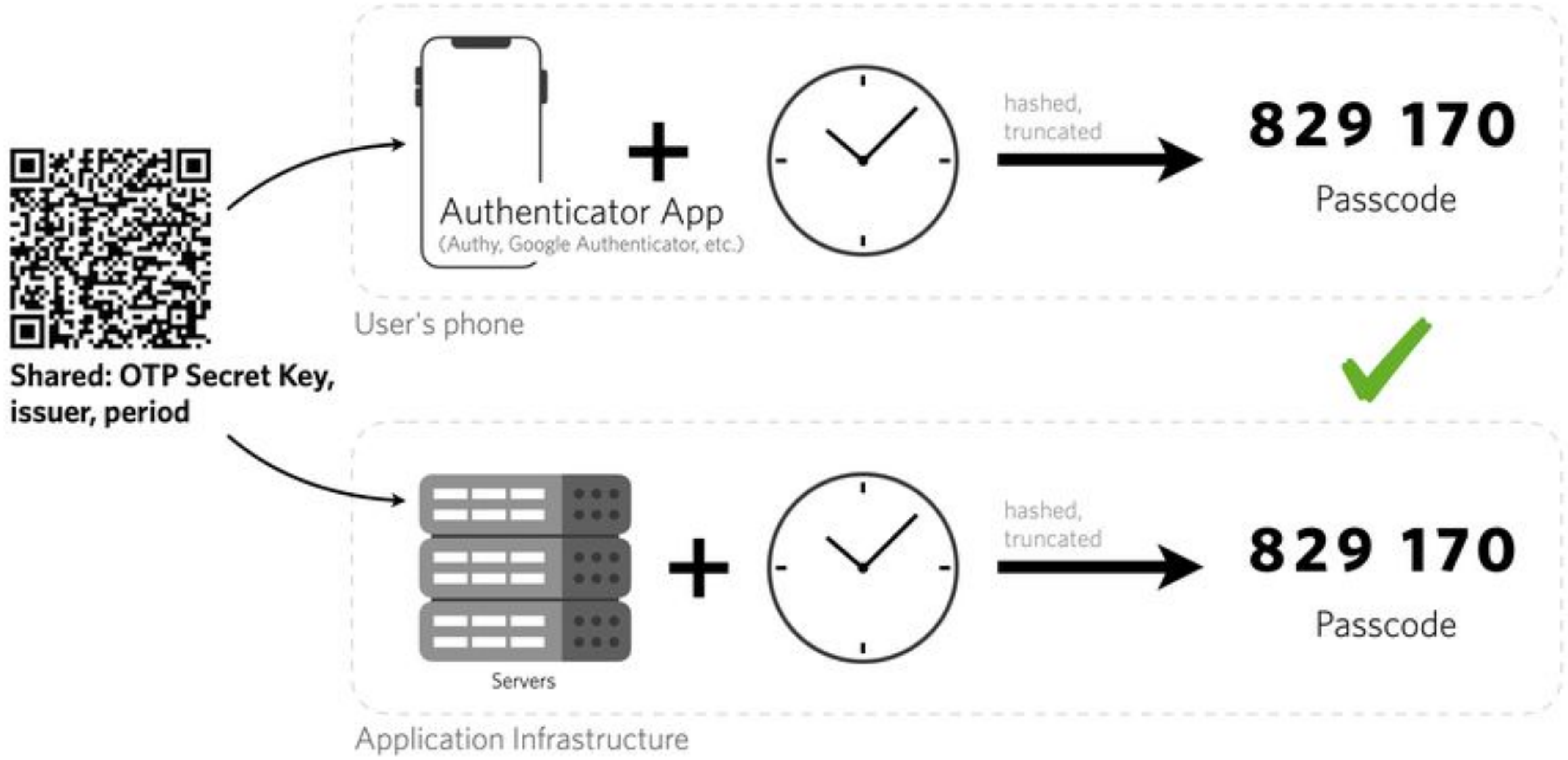
For TOTP verification an "authenticator" app must be installed on the users phone. You can get such an app from Microsoft or Google or the one I have is called FreeOTP. They are all the same and can be used interchangeably - and they are all free.

Such an app and your DF app agrees on a "secret" by way of a QR code.

This is what is depicted to the left in the graphics on the next slide.

After the secret has been shared the authenticator app is able to generate codes that the app can verify without talking to each other again. This is what's indicated by the rest of the graphics next slide.

# Timed One Time Password (TOTP)



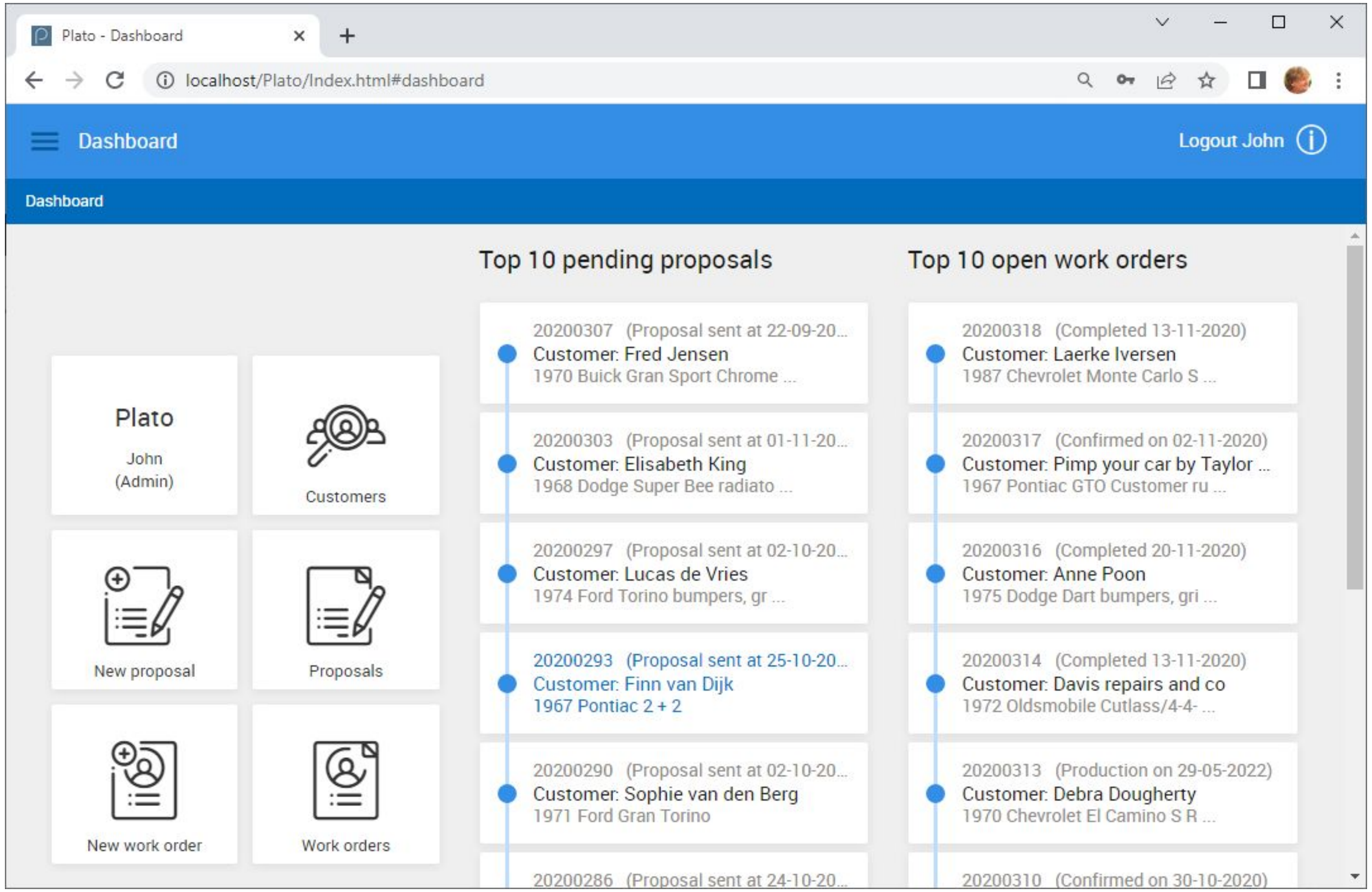
# Meanwhile: the Plato sample app

As you may recall Dataflex 20.0 was followed by a Plato sample app that showcased handling orders for a small chrome plating business.

This app featured the use of an access control library called SecMod.

You may look at this presentation as a preview of the next version of SecMod that should appear shortly after the release of DF 23

# Plato sample application



Top 10 pending proposals

20200307 (Proposal sent at 22-09-20...
Customer: Fred Jensen
1970 Buick Gran Sport Chrome ...

20200303 (Proposal sent at 01-11-20...
Customer: Elisabeth King
1968 Dodge Super Bee radiato ...

20200297 (Proposal sent at 02-10-20...
Customer: Lucas de Vries
1974 Ford Torino bumpers, gr ...

20200293 (Proposal sent at 25-10-20...
Customer: Finn van Dijk
1967 Pontiac 2 + 2

20200290 (Proposal sent at 02-10-20...
Customer: Sophie van den Berg
1971 Ford Gran Torino

20200286 (Proposal sent at 24-10-20...

Top 10 open work orders

20200318 (Completed 13-11-2020)
Customer: Laerke Iversen
1987 Chevrolet Monte Carlo S ...

20200317 (Confirmed on 02-11-2020)
Customer: Pimp your car by Taylor ...
1967 Pontiac GTO Customer ru ...

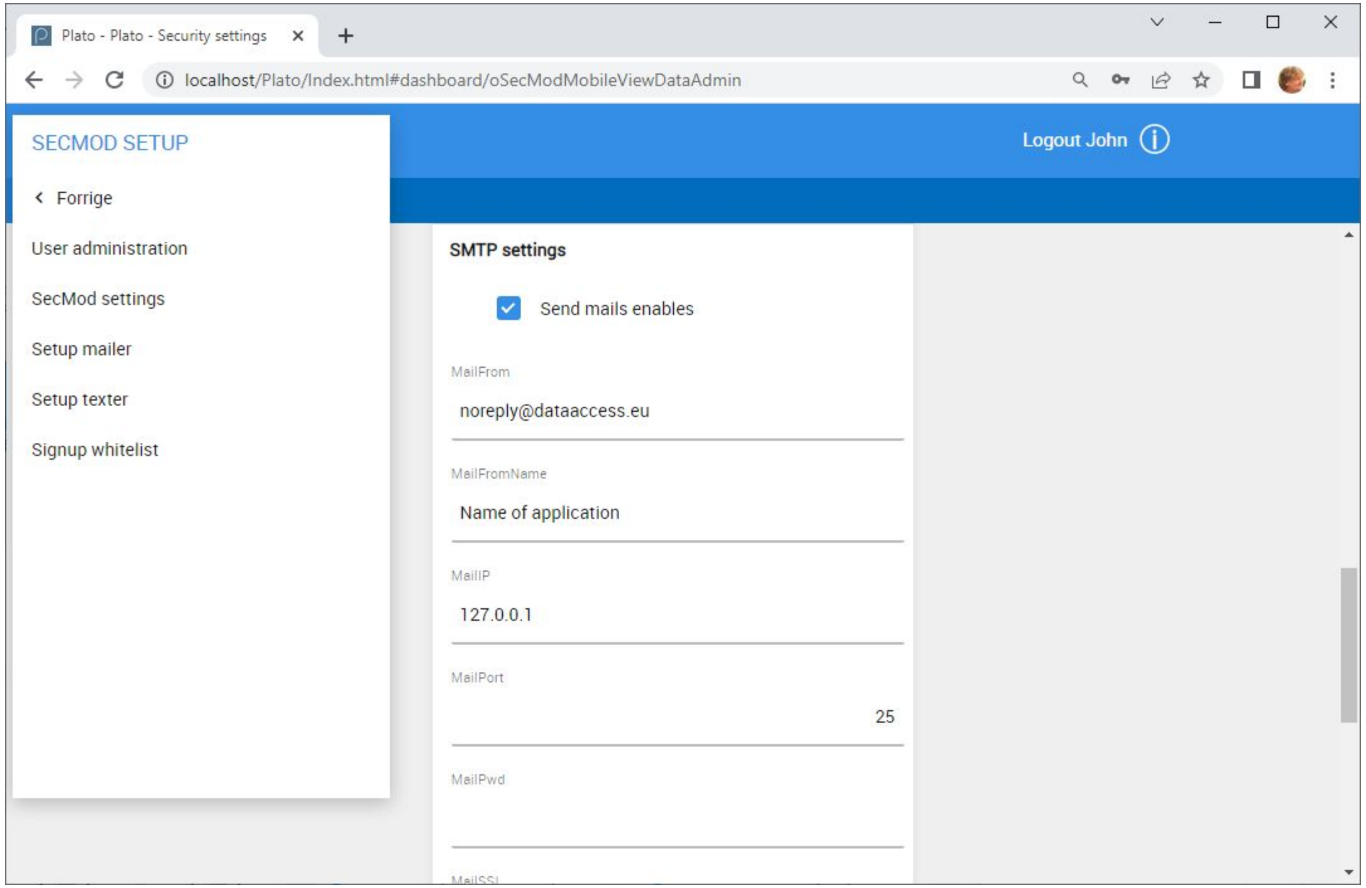
20200316 (Completed 20-11-2020)
Customer: Anne Poon
1975 Dodge Dart bumpers, gri ...

20200314 (Completed 13-11-2020)
Customer: Davis repairs and co
1972 Oldsmobile Cutlass/4-4- ...

20200313 (Production on 29-05-2022)
Customer: Debra Dougherty
1970 Chevrolet El Camino S R ...

20200310 (Confirmed on 30-10-2020)

# SecMod in Plato



**SMTP settings**

☑ Send mails enables

MailFrom: noreply@dataaccess.eu

MailFromName: Name of application

MailIP: 127.0.0.1

MailPort: 25

MailPwd:

MailSSL

# SecMod library recapture

- Access control to replace the standard “webappuser/webappsession”.
- 2-factor login by email or text messaging
- “I forgot my password”
- Sign up new user
- User activity logging
- Self signup (with optional whitelisting)
- User administration UI (Web or Windows interface)

Currently, if you want to quickly create a new web application you are pretty much limited to the webappuser/webappsession system that the Studio inserts by default.

The SecMod library is meant to let you create new applications with a more capable and complete access control embedded from the beginning. I higher starting point if you like.

# Demo

# Lift-off

I have created a workspace called ApplicationStubSecmodTOTP. It’s an empty application that I have prepared with the all stuff needed for having TOTP access control:

- Create new workspace
- Add SecModTOTP library
- Create new webapp to set up AppHtml folders and more
- Run SQL script to create SecMod tables
- Run *SQL Connect Wizard* to add tables to *filelist.cfg*
- Copy over a few source files (listed on next slide)

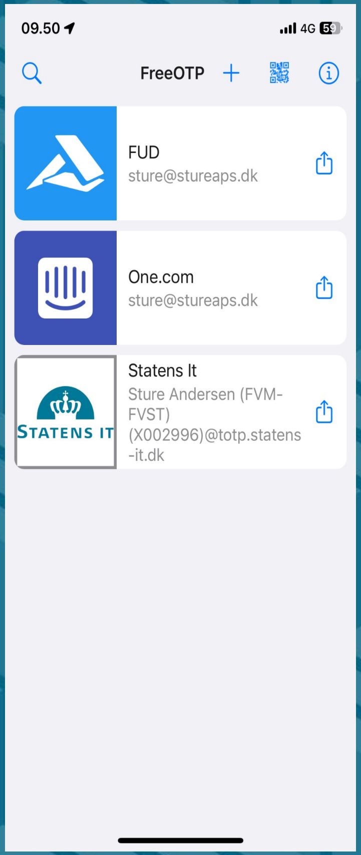
# 3 source files and how they were edited

- WebApp.src
  - Language setup for SecMod
  - 2 menu items added (Change Password and User Administration)
  - Add **`Use`** of relevant SecMod panels
  - Augmentation of GetLoginView function (to enable pw-reset deep linking)
- oSecModConfig.pkg
  - A package that configures some basic things about SecMod
  - First thing: how SecMod send e-mails and text messages
  - For emails it can use a SMTP server or it can send via the SQL server or - as here - it can use a service out there called Gateway API
  - Setting up of “roles” (just dummy roles: “frontdesk”, “finance”, “management”)
- SessionManager.pkg
  - Not noteworthy - we skip it

# First light

- Compile and run  =>  no users, can’t login
- Run windows util instead and setup email server
- Run webapp again and click “sign up new user” (sends confirmation mail)
- Login as new user and scan resulting QR code with authenticator
- Show “I have forgotten my password” feature
- Finally show all the user-admin interface (both in webapp and windows “backoffice”)
- Now you have a worthy starting point for your new webapp.

## Authenticator app

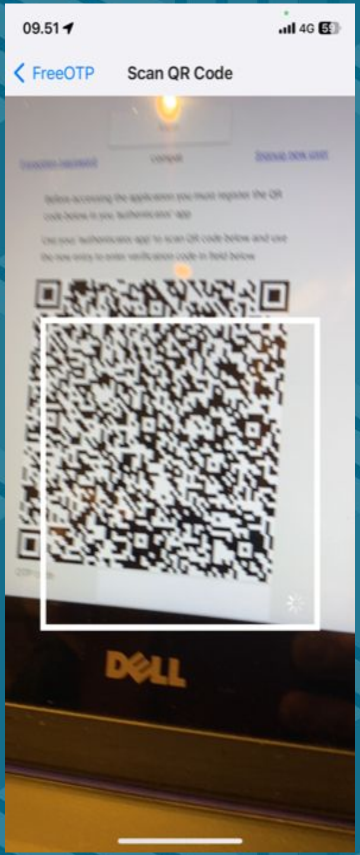


FUD
sture@stureaps.dk

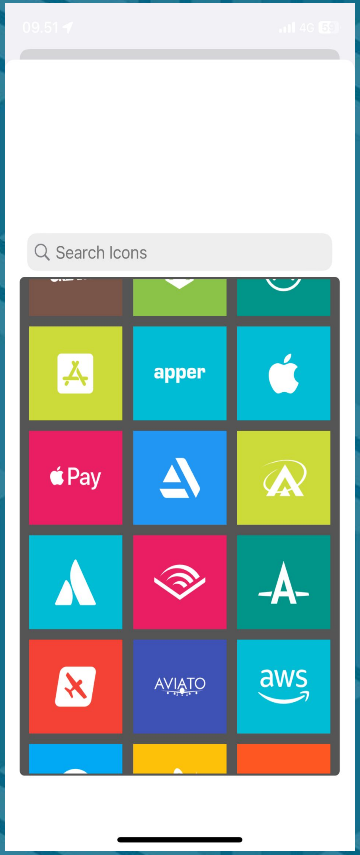
One.com
sture@stureaps.dk

Statens It
Sture Andersen (FVM-FVST)(X002996)@totp.statens-it.dk

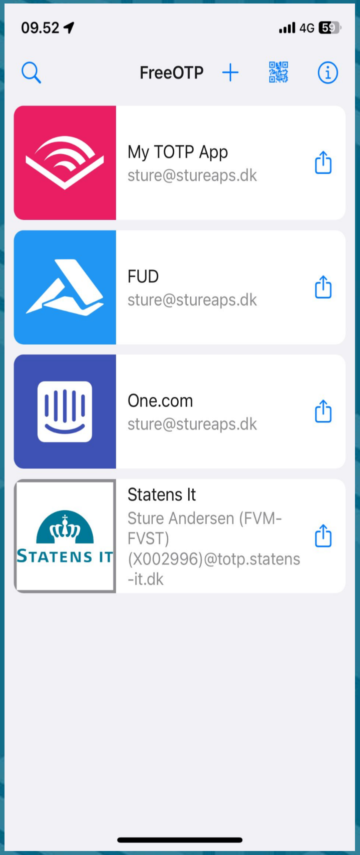
## 'My TOTP App'



## Select icon



## Your app added



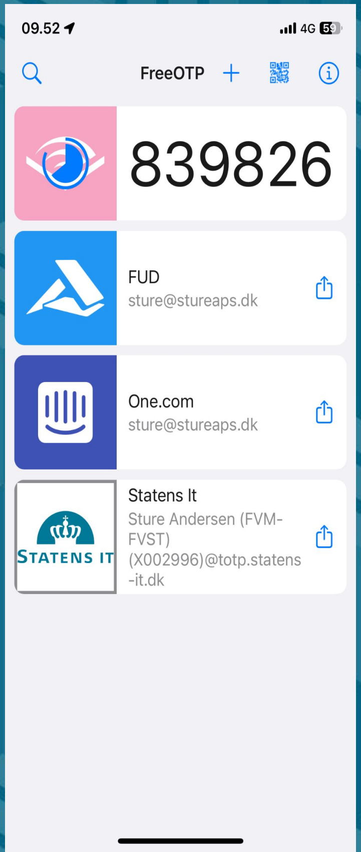
My TOTP App
sture@stureaps.dk

FUD
sture@stureaps.dk

One.com
sture@stureaps.dk

Statens It
Sture Andersen (FVM-FVST)(X002996)@totp.statens-it.dk

## Querying current code



839826

FUD
sture@stureaps.dk

One.com
sture@stureaps.dk

Statens It
Sture Andersen (FVM-FVST)(X002996)@totp.statens-it.dk

# Outlook

Next version of Plato to have the TOTP enabled version of SecMod set up by default. And I expect that version of Plato to arrive not long after DF 2023.

# Thank you

happy jazz ever after