

1. Introduksjon

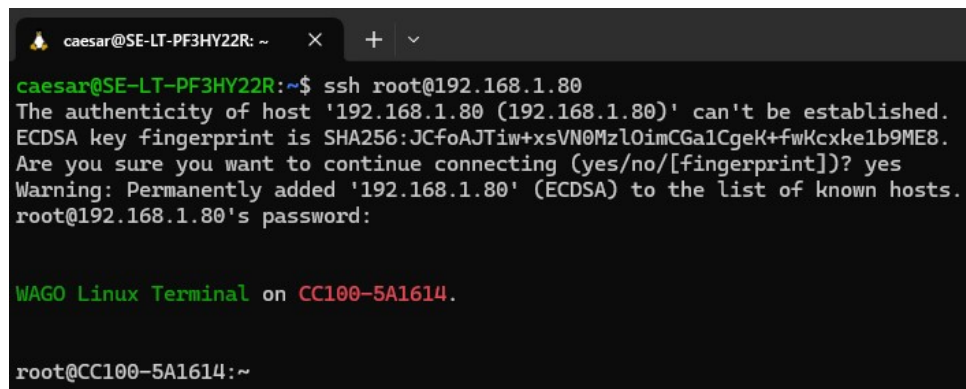
Dette dokumentet er en praktisk veiledning for brukere og driftsansvarlige som skal implementere, bruke og vedlikeholde løsningen for sikker kommunikasjon mellom WAGO CC100 PLS og Ignition SCADA ved hjelp av Tailscale VPN og OPC UA.

2. Forutsetninger

- WAGO CC100 med Linux-basert firmware
- Tilgang til Tailscale-konto
- Ignition SCADA installert
- SSH-tilgang til PLS
- Bash-skript for installasjon og oppdatering

3. Installere Tailscale på PLS

1. Koble til PLS med SSH



```
caesar@SE-LT-PF3HY22R: ~  
caesar@SE-LT-PF3HY22R:~$ ssh root@192.168.1.80  
The authenticity of host '192.168.1.80 (192.168.1.80)' can't be established.  
ECDSA key fingerprint is SHA256:JCfoAJTiwxVN0MzLOimCGalCgek+fwKcxkelb9ME8.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.1.80' (ECDSA) to the list of known hosts.  
root@192.168.1.80's password:  
  
WAGO Linux Terminal on CC100-5A1614.  
  
root@CC100-5A1614:~
```

Figur 1 Innlogging til PLS

Standard brukernavn og passord på wago pls

Brukernavn: root

Passord: wago

2. Hent installasjonsskriptet

```
wget https://raw.githubusercontent.com/espenbo/Sikker-kommunikasjon-og-sertifikath-andtering-i-byggautomasjon-med-Tailscale-og-OPC-UA/refs/heads/main/Skript/InstallTailscale.sh
```

Sluttbrukerveiledning: Automatisert OPC UA-sertifikathåndtering



DRI119

```
root@CC100-5A1614:~# wget https://raw.githubusercontent.com/espenbo/Sikker-kommunikasjon-og-sertifikath-andtering-i-byggautomasjon-med-Tailscale-og-OPC-UA/refs/heads/main/Skript/InstallTailscale.sh
--2025-04-18 13:54:54-- https://raw.githubusercontent.com/espenbo/Sikker-kommunikasjon-og-sertifikath-andtering-i-byggautomasjon-med-Tailscale-og-OPC-UA/refs/heads/main/Skript/InstallTailscale.sh
Resolving raw.githubusercontent.com... 185.199.110.133, 185.199.109.133, 185.199.111.133, ...
Connecting to raw.githubusercontent.com|185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18901 (18K) [text/plain]
Saving to: 'InstallTailscale.sh'

InstallTailscale.sh          100%[=====] 18.46K  --.-KB/s  in 0.03s

2025-04-18 13:54:56 (654 KB/s) - 'InstallTailscale.sh' saved [18901/18901]

root@CC100-5A1614:~#
```

Figur 2 Hente bash skript

3. Gjør skriptet kjørbart

```
chmod 700 InstallTailscale.sh
```

```
root@CC100-5A1614:~# ls
InstallTailscale.sh
root@CC100-5A1614:~# chmod 700 InstallTailscale.sh
root@CC100-5A1614:~# ls
InstallTailscale.sh
root@CC100-5A1614:~#
```

Figur 3 Forandre filen til å bli kjørbart

4. Kjør installasjonsskriptet `InstallTailscale.sh`

```
root@CC100-5A1614:~# ./InstallTailscale.sh
[ CURRENT ] Checking if Tailscale is installed...
```

Figur 4 Kjør installasjons skriptet

DRI119

```
-----
| Install Summary
-----
| Target Operating System:      linux
| Target distribution:          ptxdist
| Target distribution version:
| Target Arch:                  armv6
| Section = OS and version:     --
| URL:                          https://pkgs.tailscale.com/stable/
-----

| Install Summary
-----
| Target Operating System:      ptxdist
| Distribution Name:             PTXdist / WAGO-CTL
| Distribution Version ID:       2020.08.0
| Distribution Version Codename: N/A
| Target Arch:                  armv6
| URL:                          https://pkgs.tailscale.com/stable/
-----

[ CURRENT ] Install_binaries_for_armv6
[ CURRENT ] Fetching installation methods from Tailscale...
[ CURRENT ] Found link: tailscale_1.82.5_arm.tgz
[ CURRENT ] Downloading https://pkgs.tailscale.com/stable/tailscale_1.82.5_arm.tgz
[ CURRENT ] Downloading with curl...
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %         0      0     1362k         0  0:00:20  0:00:11  0:00:10 1572k
```

Figur 5 Skriptet finner riktig pakke som skal installeres eller oppdateres

5. Restart PLS

DRI119

```
WAGO Linux Terminal on CC100-5A1614.  
  
root@CC100-5A1614:~ tailscale login  
  
To authenticate, visit:  
  
https://login.tailscale.com/a/194d783801214a
```

Figur 6 Logg inn på Tailscale

6. Logg inn på PLSen og logg inn på Tailscale.

```
tailscale login
```

5. Logg inn på Tailscale med enhetens auth-url (vises ved oppstart)

6. Verifiser at enheten vises i Tailscale admin-panelet

cc100-5a1614 ekb@stormelektro.no	100.120.96.59	1.82.5 Linux 5.15.107-rt62-w04.03.06	Connected	...
-------------------------------------	---------------	---	-----------	-----

Figur 7 PLSen vises nå i Tailscale

Man kan også bruke status for og se alle enheter koblet til tailscale nettet.

```
tailscale status
```

7. Ping en annen enhet.

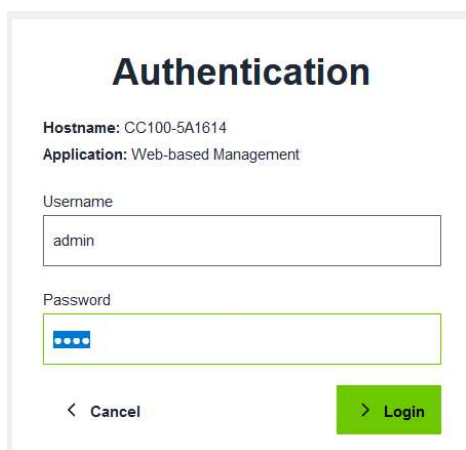
```
root@CC100-5A1614:~ ping 100.101.171.89  
PING 100.101.171.89 (100.101.171.89): 56 data bytes  
64 bytes from 100.101.171.89: seq=0 ttl=64 time=15.096 ms  
64 bytes from 100.101.171.89: seq=1 ttl=64 time=12.487 ms  
64 bytes from 100.101.171.89: seq=2 ttl=64 time=13.542 ms  
^C  
--- 100.101.171.89 ping statistics ---  
3 packets transmitted, 3 packets received, 0% packet loss  
round-trip min/avg/max = 12.487/13.708/15.096 ms  
root@CC100-5A1614:~
```

Figur 8 Ping en annen enhet på nettverket

4. Aktivere sikker kommunikasjon i OPC UA

Man kan bruke OPC UA uten og bruke sikkerhets sertifikater. Når PLSen er koblet til Tailscale nettverket vil all trafikk som går igjennom dette nettet være kryptert. Men kommunikasjon som ikke går over Tailscale nettverket vil ikke være kryptert.

1. Logg inn på nettsiden til PLSen



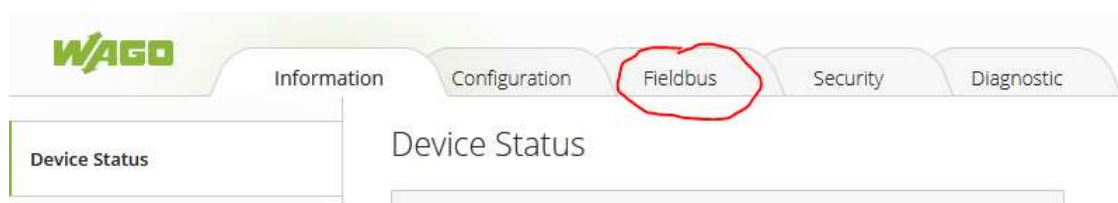
The image shows a web-based authentication form titled "Authentication". It displays the hostname "CC100-5A1614" and the application "Web-based Management". There are input fields for "Username" (containing "admin") and "Password" (masked with dots). At the bottom, there are two buttons: a green "Login" button and a grey "Cancel" button with a left arrow.

Figur 9 Innlogging nettsiden til PLS

Brukernavn: admin

Passord: wago

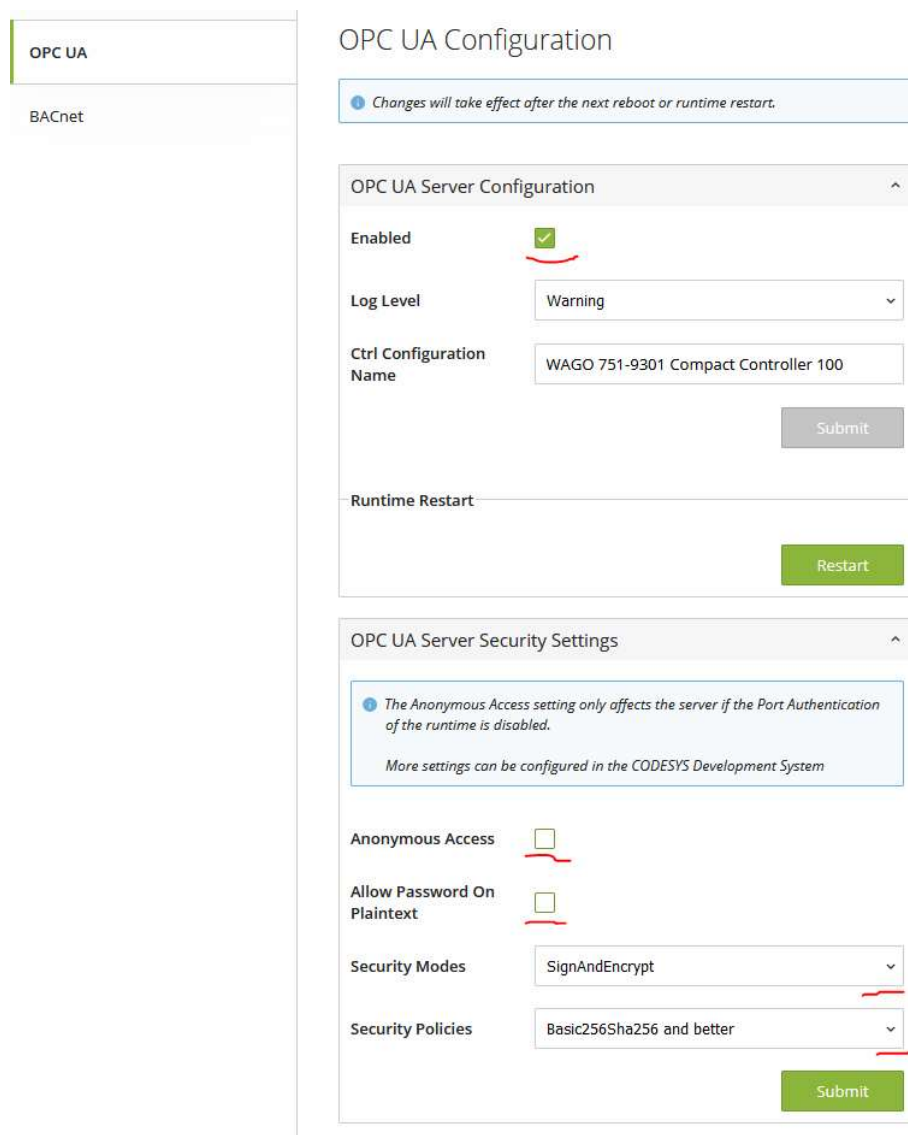
3. Velg Fieldbus



Figur 10 Velg Fieldbus

DRI119

4. Velg hvilken sikkerhetsfunksjoner som skal være minimum på PLSen og pass på at OPC UA er 'Enable'



OPC UA Configuration

Changes will take effect after the next reboot or runtime restart.

OPC UA Server Configuration

Enabled ☒

Log Level Warning

Ctrl Configuration Name WAGO 751-9301 Compact Controller 100

Submit

Runtime Restart

Restart

OPC UA Server Security Settings

The Anonymous Access setting only affects the server if the Port Authentication of the runtime is disabled.

More settings can be configured in the CODESYS Development System

Anonymous Access ☐

Allow Password On Plaintext ☐

Security Modes SignAndEncrypt

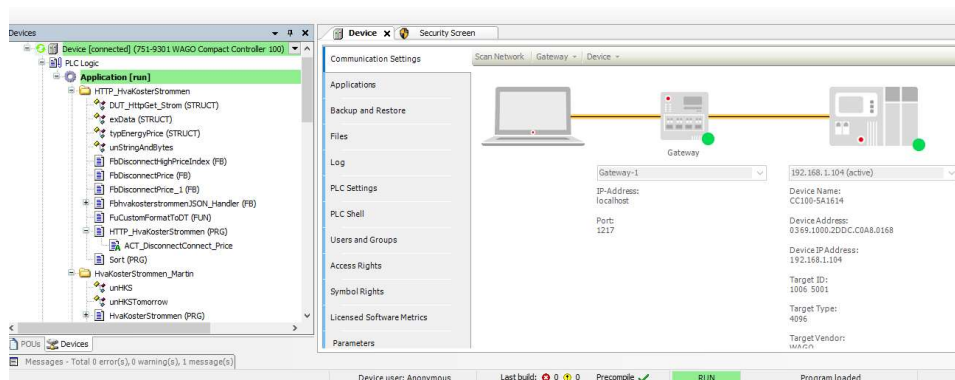
Security Policies Basic256Sha256 and better

Submit

Figur 11 Oppsett av OPC UA server i PLSen

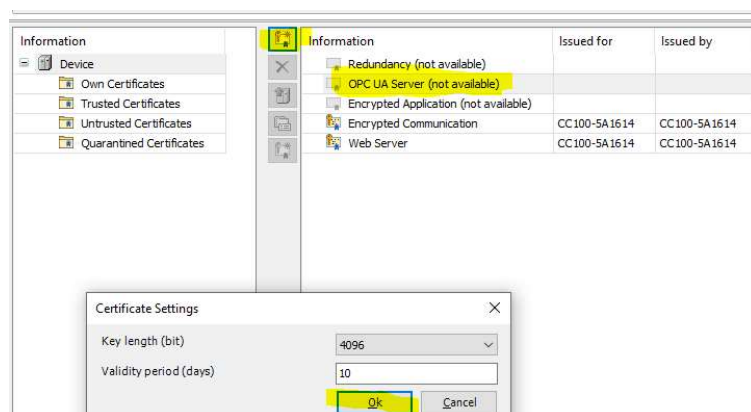
DRI119

5. Koble seg til PLSen



Figur 12 Koble seg til PLSen

6. Generer sertifikat i Codesys for OPC UA-serveren



Figur 13 Oppsett av sikkerhets sertifikat til PLSen i Codesys 3.5

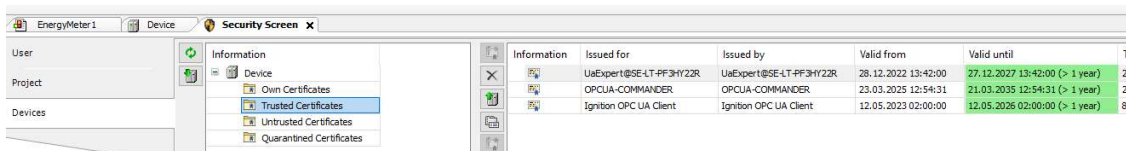
DRI119

7. Hent ut sertifikatet som du lagde, slik at det kan legges inn på klienten. uaExpert eller Ignition.



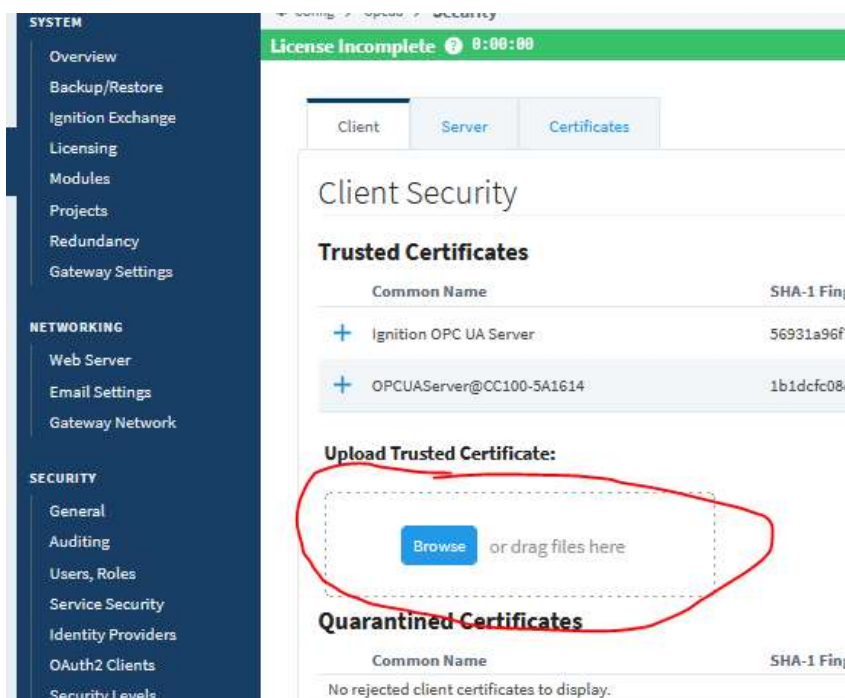
Figur 14 Hent ut sertifikat

8. Legg til klientens sertifikat i PLSens 'Trusted Certificates'



Figur 15 Legg sertifikater fra klienter i Trusted

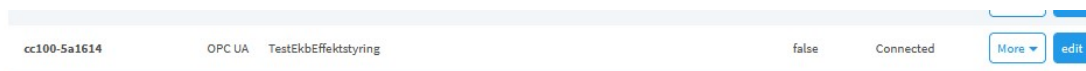
9. Legg til PLSens sertifikat i klientens 'Trusted Certificates'



Figur 16 Last opp sertifikat til Ignition server

DRI119

10. Verifiser at 'Sign & Encrypt' fungerer mellom SCADA og PLS



Figur 17 Status på kommunikasjon til Ignition server

5. Oppdatere HTTPS-sertifikater automatisk

1. Koble til PLS med SSH

```
caesar@SE-LT-PF3HY22R: ~  
caesar@SE-LT-PF3HY22R:~$ ssh root@192.168.1.80  
The authenticity of host '192.168.1.80 (192.168.1.80)' can't be established.  
ECDSA key fingerprint is SHA256:JCfoAJTiw+xsVN0MzloimCGalCgeK+fwKcxke1b9ME8.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.1.80' (ECDSA) to the list of known hosts.  
root@192.168.1.80's password:  
  
WAGO Linux Terminal on CC100-5A1614.  
  
root@CC100-5A1614:~
```

Figur 18 Innlogging til PLS

Standard brukernavn og passord på wago pls

Brukernavn: root

Passord: wago

2. Hent installasjonsskriptet

```
wget https://raw.githubusercontent.com/espenbo/Sikker-kommunikasjon-og-sertifikath-andtering-i-byggautomasjon-med-Tailscale-og-OPC-UA/refs/heads/main/Skript/update_tailscale_certificates.sh
```

```
<-kommunikasjon-og-sertifikath-andtering-i-byggautomasjon-med-Tailscale-og-OPC-UA/refs/heads/main/Skript/update_tailscale_certificates.sh  
--2025-04-18 15:10:06-- https://raw.githubusercontent.com/espenbo/Sikker-kommunikasjon-og-sertifikath-andtering-i-byggautomasjon-med-Tailscale-og-OPC-UA/refs/heads/main/Skript/update_tailscale_certificates.sh  
Resolving raw.githubusercontent.com... 185.199.108.133, 185.199.111.133, 185.199.110.133, 185.199.109.133  
Connecting to raw.githubusercontent.com|185.199.108.133|:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 5923 (5.8K) [text/plain]  
Saving to: 'update_tailscale_certificates.sh'  
  
update_tailscale_certificates.sh 100%[=====]  
2025-04-18 15:10:08 (286 KB/s) - 'update_tailscale_certificates.sh' saved [5923/5923]  
root@CC100-5A1614:~
```

Figur 19 Hente update_tailscale_certificates.sh

DRI119

3. Gjør skriptet kjørbart

```
chmod 700 update_tailscale_certificates.sh
```

```
root@CC100-5A1614:~# ls
installTailscale.sh      output.txt      tailscale_1.82.5_arm  tailscale_1.82.5_arm.tgz  update_tailscale_certificates.sh
root@CC100-5A1614:~# chmod 700 update_tailscale_certificates.sh
root@CC100-5A1614:~# ls
installTailscale.sh      output.txt      tailscale_1.82.5_arm  tailscale_1.82.5_arm.tgz  update_tailscale_certificates.sh
root@CC100-5A1614:~#
```

Figur 20 Gjør skriptet kjørbart

4. Kjør `update_tailscale_certificates.sh` på PLS

```
./update_tailscale_certificates.sh
```

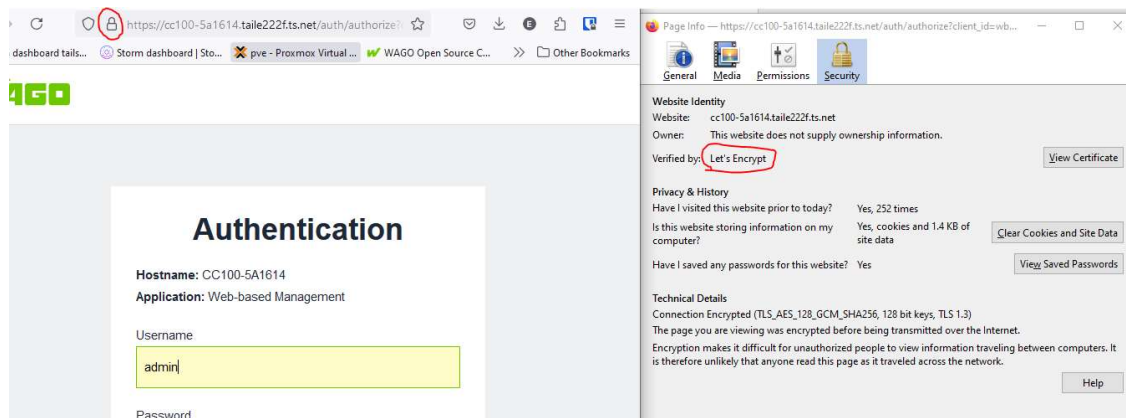
```
root@CC100-5A1614:~# ./update_tailscale_certificates.sh
Detected Tailscale DNS Name: cc100-5a1614.tailnet222f.ts.net
Certificate expires soon or is expired, renewing...
Wrote public cert to cc100-5a1614.tailnet222f.ts.net.crt
Wrote private key to cc100-5a1614.tailnet222f.ts.net.key
Symlinks created and verified:
lrwxrwxrwx 1 root root      58 Mar 26 22:01 /etc/certificates/cc100-5a1614.tailnet222f.ts.net.crt -> /var/lib/tailscale/certs/cc100-5a1614.tailnet222f.ts.net.crt
lrwxrwxrwx 1 root root      58 Mar 26 22:01 /etc/certificates/keys/cc100-5a1614.tailnet222f.ts.net.pem -> /var/lib/tailscale/certs/cc100-5a1614.tailnet222f.ts.net.pem
Reloading lighttpd server...
[ INFO ] lighttpd: reload
lighttpd: stopping
Duplicate array-key ''
lighttpd: starting
[ INFO ] lighttpd: reload done
Certificate update completed successfully!
root@CC100-5A1614:~#
```

Figur 21 Hente sertifikater eller oppdatere dem

5. Scriptet vil hente gyldig sertifikat fra Tailscale og plassere det riktig

6. Webserveren (lighttpd) restartes med nytt sertifikat

7. Test tilgang til https://<plsen>.tailnet-yourdomain.ts.net



Figur 22 Test at sikkerhetssertifikatene fungerer. Husk man må være koblet til Tailscale nettverket

DRI119

8. Legg til automatisk oppdatering av sertifikater i crontab

```
crontab -e
```

```
* * * * * /usr/sbin/logrotate -s /var/log/logrotate.status /etc/logrotate.conf
0 5 */14 * * /usr/local/bin/update_tailscale_certificates.sh >> /var/log/tailscale_cert_update.log 2>&1
```

Figur 23 Oppsett av cron

Sjekk logg med

```
tail -f /var/log/tailscale_cert_update.log
```

```
root@CC100-5a1614:~# tail -f /var/log/tailscale_cert_update.log
Detected Tailscale DNS Name: cc100-5a1614.tailnet222f.ts.net
Certificate expires soon or is expired, renewing...
Symlinks created and verified:
lrwxrwxrwx 1 root root 58 Mar 26 22:01 /etc/certificates/cc100-5a1614.tailnet222f.ts.net.crt -> /var/lib/tailscale/certs/cc100-5a1614.tailnet222f.ts.net.crt
lrwxrwxrwx 1 root root 58 Mar 26 22:01 /etc/certificates/keys/cc100-5a1614.tailnet222f.ts.net.pem -> /var/lib/tailscale/certs/cc100-5a1614.tailnet222f.ts.net.pem
Reloading lighttpd server...
Certificate update completed successfully!
```

Figur 24 Sjekk logg for https sertifikater

6. Vedlikehold og overvåking

- Sjekk Tailscale dashboard for tilkoblingsstatus
- Kjør `tailscale status` for lokal status
- Verifiser gyldighet av sertifikater periodisk med `tailscale cert`

7. Feilsøking

- Hvis OPC UA-feil oppstår, dobbeltsjekk at sertifikater er riktig plassert
- Ved manglende VPN-tilkobling, kjør `tailscale up` på nytt
- Sjekk loggene i `/var/log/lighttpd/` for HTTPS-relaterte feil
- Sjekk `/var/log/tailscale_cert_update.log`

8. Oppdatering av skript

Scriptene er utformet for enkel oppdatering. Endringer kan gjøres med en teksteditor, men husk å teste etter modifikasjoner.