Forstudierapport:   
**Automatisert OPC UA-sertifikathåndtering**

A white rectangular object next to a black screen

Description automatically generated

Figur 1: Illustrasjon av Wago PLS og HMI skjem. Hentet fra wago.com

Forstudierapport skrevet av Espen Klippenberg Bø

Dato:12.02.2025

Innhold

[1. Introduksjon til dokumentet 4](#_Toc190289473)

[2. Begrepstabell 5](#_Toc190289474)

[3. Presentasjon av bedriften 7](#_Toc190289475)

[4. Presentasjon av Byggautomasjon 8](#_Toc190289476)

[4.1. Hva er byggautomasjon 8](#_Toc190289477)

[4.2. Oversikt over vanlige deler i et SD-anlegg 8](#_Toc190289478)

[4.2.1. KNX 8](#_Toc190289479)

[4.2.2. OPC UA 8](#_Toc190289480)

[4.2.3. SCADA 8](#_Toc190289481)

[4.2.4. SD-Anlegg 8](#_Toc190289482)

[5. Bakgrunn for prosjektet 10](#_Toc190289483)

[5.1. Prosjektmål 10](#_Toc190289484)

[5.2. Effektmål 10](#_Toc190289485)

[5.3. Resultatmål 10](#_Toc190289486)

[5.4. Prosessmål 11](#_Toc190289487)

[5.4.1. Samarbeid og kommunikasjon 11](#_Toc190289488)

[5.4.2. Læringsmål og kompetansebygging 11](#_Toc190289489)

[5.4.3. For å sikre fremdrift og struktur i prosjektet. 11](#_Toc190289490)

[6. Prosjektets omfang 12](#_Toc190289491)

[6.1. Avdekke utfordringene 12](#_Toc190289492)

[6.2. Evaluering av relevante produkter og metoder 12](#_Toc190289493)

[6.3. Implementering og testing 13](#_Toc190289494)

[6.4. Kommunikasjon og samarbeid 13](#_Toc190289495)

[6.5. Ønsket løsning for henting av nye sertifikater 13](#_Toc190289496)

[6.6. Arbeidsoppgaver 13](#_Toc190289497)

[6.7. **Avgrensninger** 14](#_Toc190289498)

[6.8. Fremdriftsplan og milepæler 15](#_Toc190289499)

[6.9. Forventede resultater 15](#_Toc190289500)

[7. Interessenter og rammebetingelser 16](#_Toc190289501)

[7.1. Interessentanalyse 16](#_Toc190289502)

[7.1.1. Ekstern 17](#_Toc190289503)

[7.1.2. Intern 17](#_Toc190289504)

[7.2. Rammebetingelser 17](#_Toc190289505)

[7.3. OPC UA og rollen den har i automasjonssystemer 17](#_Toc190289506)

[7.3.1. Sikkerhetsmekanismer i OPC UA 18](#_Toc190289507)

[7.3.2. Hvorfor OPC UA brukes i byggautomasjon 18](#_Toc190289508)

[7.3.3. Sammenheng mellom OPC UA og dette prosjektet 19](#_Toc190289509)

[8. Kritiske suksessfaktorer 20](#_Toc190289510)

[8.1. Suksessfaktorer 20](#_Toc190289511)

[8.2. Informasjonsbehov 21](#_Toc190289512)

[9. Risikoanalyse 22](#_Toc190289513)

[9.1. Beskrivelse av risikoer og tilhørende tiltak 22](#_Toc190289514)

[9.1.1. Manglende teknisk støtte 23](#_Toc190289515)

[9.1.2. Forsinkelse i prosjektleveranse 23](#_Toc190289516)

[9.1.3. Kompatibilitetsproblemer 23](#_Toc190289517)

[9.1.4. Begrenset tilgang til verktøy og programvare 23](#_Toc190289518)

[9.1.5. Manglende kompetanse i spesifikke teknologier 23](#_Toc190289519)

[9.1.6. Tidspress på grunn av parallelle oppgaver 23](#_Toc190289520)

[9.1.7. Oppsummering 23](#_Toc190289521)

[10. Kost/nytte-analyse 24](#_Toc190289522)

[10.1. Kostnader tilknyttet prosjektet 24](#_Toc190289523)

[10.2. Nytte prosjektet kan tilføre byggautomasjonsbedriftene 24](#_Toc190289524)

[11. Retningslinjer og standarder 26](#_Toc190289525)

[11.1. Krav til dokumentasjon 26](#_Toc190289526)

[11.2. Krav til kvalitetsgjennomganger 27](#_Toc190289527)

[11.3. Krav til standarder og metoder 27](#_Toc190289528)

[11.4. Verktøy 29](#_Toc190289529)

[11.5. Endringshåndtering 29](#_Toc190289530)

[12. Prosjektorganisering 30](#_Toc190289531)

[13. Anbefaling om videre arbeid 30](#_Toc190289532)

[14. Referanser 31](#_Toc190289533)

**Revisjonshistorie**

|  |  |  |  |
| --- | --- | --- | --- |
| Dato | Versjon | Beskrivelse | Forfattere |
| <23/01/25> | <0.1> | Første versjon | Espen Klippenberg Bø |
| <08/02/25> | <0.2> | Andre versjon | Espen Klippenberg Bø |
| <10/02/25> | <0.3> | Tredje versjon | Espen Klippenberg Bø |
| <12/02/25> | <1.0> | Fjerde versjon | Espen Klippenberg Bø |

# Introduksjon til dokumentet

Jeg er ansatt i Storm elektro AS, det er et firma som leverer elektro og automasjonstjenester. Jeg jobber som prosjektingeniør innenfor byggautomasjon, der jeg jobber utvikling av nye systemer, infrastruktur, drift av infrastruktur, programmering og idriftsettelse.

Denne forstudierapporten har som hensikt å kartlegge rammer og forutsetninger for et prosjekt om automatisert oppdatering og distribusjon av OPC UA-sertifikater i byggautomasjonsnettverk.

# Begrepstabell

|  |  |
| --- | --- |
| API | Et grensesnitt som lar ulike programmer eller systemer kommunisere og utveksle data på en standardisert måte. (application programming interface) |
| BACnet Secure Connect (BACnet/SC) | En sikker kommunikasjonsprotokoll for bygningsautomasjon som bruker TLS-kryptering for å beskytte datautveksling mellom enheter i BACnet-nettverk over IP. |
| Byggautomasjon | Integrert styring, overvåkning og optimalisering av tekniske systemer i bygg, som ventilasjon, varme, lys og sikkerhet, for å sikre energieffektiv drift og et optimalt inneklima. |
| CA-tjenester | Systemer som utsteder, verifiserer og administrerer digitale sertifikater for å sikre autentisering og kryptering i elektronisk kommunikasjon. |
| Databaser | Strukturerte systemer for lagring, organisering og søk av data, som gjør det mulig å effektivt håndtere og gi tilgang til store mengder informasjon. |
| Driftsansvarlige | Personer som overvåker og styrer den daglige driften av tekniske installasjoner, som ventilasjon, varme og sikkerhetssystemer, for å sikre optimal ytelse og stabilitet. |
| Eiendomsforvaltere | Administrerer og vedlikeholder bygninger og tekniske systemer, og er ansvarlige for økonomisk og operasjonell forvaltning av eiendommer for eiere eller investorer. |
| Eiendomseiere | Enkeltpersoner eller selskaper som eier bygninger og infrastruktur, og har økonomisk og strategisk interesse i effektiv drift, vedlikehold og sikkerhet av sine eiendommer. |
| HMI | Brukerinterfacer for å vise data og kontrollere systemet. Lokal skjerm. (human-machine interface) |
| IIoT | Et nettverk av sammenkoblede enheter, maskiner og sensorer som samler inn, utveksler og analyserer data i sanntid for å optimalisere produksjon, drift og vedlikehold. |
| IT-ansvarlige | Har ansvaret for drift, vedlikehold og sikkerhet av IT-infrastruktur, inkludert nettverk, servere og datasystemer, for å sikre stabil og sikker digital drift. |
| KNX | En global standard for bygningsautomasjon som gir enkel kommunikasjon mellom ulike produsenter og systemer som belysning, varme, persienner og sikkerhet. |
| KNX Secure | |  | | --- | |  |   En sikkerhetsutvidelse for KNX- protokollen som benytter AES-128-kryptering for å sikre kommunikasjon mellom KNX-enheter mot uautorisert tilgang og manipulasjon. |
| OPC UA | En standardisert kommunikasjonsprotokoll for sikker og plattformuavhengig datautveksling mellom industrielle systemer, sensorer og IT-systemer. |
| OT | Refererer til systemer og maskinvare som brukes for å overvåke, styre og automatisere industrielle prosesser, inkludert byggautomasjon, produksjonsanlegg og kritisk infrastruktur. |
| OT-ansvarlige | Personer eller team som har ansvar for drift, vedlikehold og sikkerhet av OT-systemer, med fokus på å sikre stabil, effektiv og sikker drift av industrielle kontrollsystemer og automatiseringsnettverk. |
| PKI-basert | Et system for administrasjon av digitale sertifikater og krypteringsnøkler, som sikrer autentisering, integritet og konfidensialitet i elektronisk kommunikasjon. |
| PLS | En programmerbar logisk styring er en datamaskin som brukes i industrien for å automatisere oppgaver som produksjon og kontroll av for eksempel nivåer i siloer/tanker. PLSen har tatt over oppgavene som hundrevis eller tusenvis av releer gjorde i industrien før og kan programmeres til å gjøre det samme. |
| SCADA | Større overvåkningssystemer som samler og analyserer data fra flere bygningskomponenter. (supervisory control and data acquisition) |
| SD-anlegg | Et system for overvåking, styring og automatisering av tekniske installasjoner i bygg. Består ofte av SCADA-system, ventilasjonsanlegg, PLS-er, sensorer osv. (Sentral driftskontroll anlegg) |
| Sensorer | Måler data som temperatur, luftkvalitet, lysstyrke og trykk. |
| Sikkerhetsansvarlige | Fagpersoner som har ansvaret for å beskytte IT-systemer, bygningsautomasjon og fysiske anlegg mot uautorisert tilgang, cyberangrep og andre sikkerhetsrisikoer. |
| Systemintegratorer | Fagpersoner som designer, implementerer og vedlikeholder automasjonsanlegg som inneholder PLS, HMI, KNX, ventilasjonsanlegg, varmeanlegg og sensorer. |
| Varmesentraler | Sentrale anlegg som produserer og distribuerer varme til et bygg, ofte ved hjelp av varmepumper, fjernvarme eller el/olje-kjeler. |
| Ventilasjonsanlegg | Systemer som regulerer luftkvaliteten i et bygg ved å styre tilførsel og utskifting av luft. |

# Presentasjon av bedriften

Storm Elektro AS er et autorisert installasjonsfirma etablert i 2001, med hovedkontor i Lerkeveien 2, 1624 Gressvik. Storm Elektro tilbyr et bredt spekter av elektriske tjenester i Oslo, Akershus og Østfold.

Tjenestene omfatter:

* Elektrikertjenester: Alt innen elektroarbeid, inkludert oppussing, sikringsskap og EL-kontroll av boliger.
* Industri: Alt innen elektroarbeider innen industri, inkludert produksjonsbedrifter som Mills, Salatmesteren, Sirkel og Bevi
* Ladestasjoner for el-bil: Levering og montering av ladestasjoner for alle typer el- og hybridbiler.
* Automasjon: Automatikk for bygg og smarthusløsninger.
* Sikkerhet: Installasjon av brannalarmsystemer, innbruddsalarmer, kameraovervåkning og nødlyssystemer.
* Nettverk: Installasjon av fiber, telefoni, datanettverk og trådløs kommunikasjon.
* Energi og miljø: Løsninger for vannbåren varme- og kjøleanlegg samt energivurdering av tekniske anlegg.

# Presentasjon av Byggautomasjon

## Hva er byggautomasjon

Byggautomasjon er systemer for å automatisere og koble sammen styringen av varmeanlegg, lysstyring, ventilasjon, solskjerming, energimåling osv. Sammen med et Scada system for å visualisere og logge informasjonen blir det et SD-anlegg.

SD-anlegg(Sentral driftskontroll anlegg) er et viktig verktøy for å skape smarte, effektive og bærekraftige bygg. Gjennom avansert teknologi og integrerte styringssystemer med sensorer, KNX, PLS-er(programmerbar logisk styring), HMI(human-machine interface) og Scada(supervisory control and data acquisition) som man kan koble mot APIer(application programming interface) levert av andre tjenester, kan man oppnå best mulig drift, lavere energiforbruk og bedre inneklima.

En av de viktige fordelene er energibesparelser. Ved å integrere styring av lys, varme og ventilasjon, kan driftskostnadene reduseres. Ved å analysere historiske bruksdata og sanntidsmålinger, kan systemet også forutsi når behovet for ventilasjon og oppvarming vil øke, og dermed tilpasse energiforbruket. Det sikrer drift med lavest mulig energikostnad, samtidig som inneklimaet holdes på et komfortabelt nivå.

Sikker drift av tekniske systemer er viktig i alle bygg, spesielt i helsebygg og industribygg. Ved hjelp av alarmhåndtering, feildiagnostikk, sanntidsovervåkning og brukertilpassede varslinger, kan potensielle problemer oppdages og løses før de utvikler seg til alvorlige feil. Det reduserer vedlikeholdskostnader og minsker risikoen for driftsstans.

## Oversikt over vanlige deler i et SD-anlegg

### KNX

KNX er en global standard for byggautomatisering der produkter fra forskjellige produsenter kan kommunisere over en felles standard. Vanligvis blir KNX produkter brukt for å styre lys, varme, solavskjerming. Ofte ser du som bruker av bygget produktene som lysbrytere, bevegelse detektorer eller termostater.

### OPC UA

OPC UA (*Open Platform Communications Unified Architecture*) er en global standard for sikker og pålitelig datautveksling mellom ulike systemer og enheter i industri- og byggautomasjon.

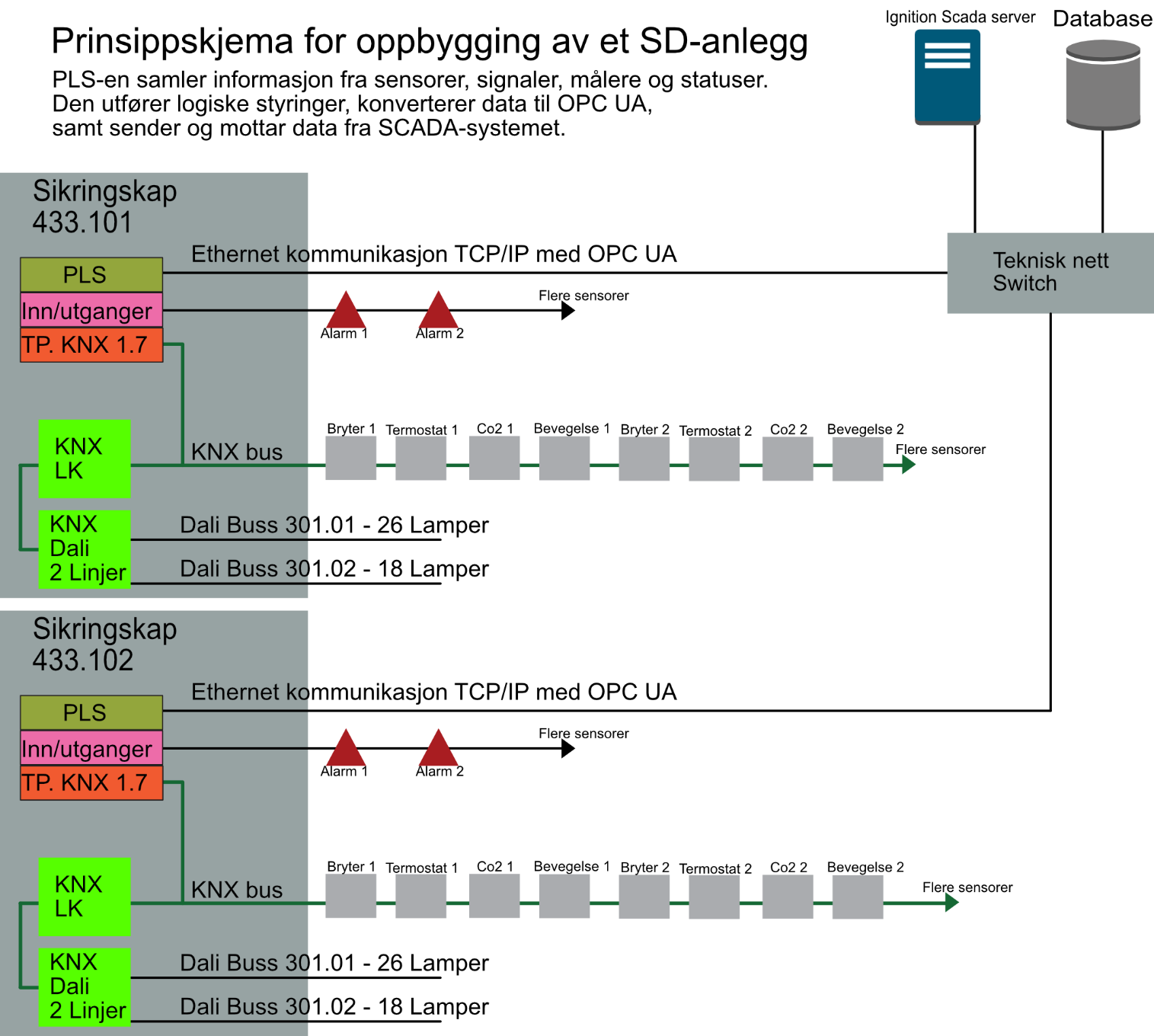
I byggautomasjon brukes OPC UA til å koble sammen KNX, varmesentraler, ventilasjonssystemer, energistyring, sikkerhetssystemer og IoT-enheter i én felles infrastruktur som kan visualiseres i et scadasystem. OPC UA støtter kryptert og autentisert kommunikasjon som sikrer at dataene forblir sikre og beskyttet mot uautorisert tilgang.

### SCADA

SCADA (supervisory control and data acquisition) er for styring, regulering og overvåkning av tekniske installasjoner. Storm elektro bruker Ignition fra Inductivatomation som scadasystem. Det er et webbasert system for visualisering av informasjon fra alle enhetene som er koblet til byggautomasjonsanlegg.

### SD-Anlegg

SD-anlegg(Sentral Driftskontroll) [figur 1]er en fellesbetegnelse på hele systemet som styrer bygget. Et SD-anlegg består da ofte av KNX utstyr, PLSer som bruker OPC UA og et scadasystem for å visualisere og logge data.



SD-anlegg(Sentral Driftskontroll) [figur 1]

# Bakgrunn for prosjektet

Stuxnet, er en avansert dataorm som ble oppdaget i 2010. Den var spesielt designet for å infiltrere og sabotere scada systemer. Etter dette angrepet ble fokuset på cybersikkerhet innen automatikkanlegg mye større. Disse anleggene hadde vanligvis vært lokale nettverk som ikke har vært tilkoblet internett. Men Stuxnet hendelsen viste at flere av disse anleggene hadde blitt tilkoblet internett. Økende krav fra kunder som ønsker fjerntilgang til SD-anleggene sine, epost ved alarmer, eller bruk av tjenester som YR sammen med SD-anlegget viste behovet for å øke sikkerhetstiltakene på automasjonsanlegg.

OPC UA (Open Platform Communications Unified Architecture) er en kommunikasjonsprotokoll som brukes i industri og byggautomasjonsanlegg. Det er en standardisert protokoll som sikrer datautveksling mellom systemer som PLS-er, HMI-paneler og SCADA-systemer. Protokollen støtter sertifikater for autentisering og kryptering, men bruk og oppdatering av slike sertifikater i byggautomasjon er ofte manuelle og tidkrevende. Disse sertifikatene bør oppdateres relativt ofte slik at man er sikker på at sertifikatet ikke er forfalsket eller forfalsket. Både i nye anlegg som bygges i dag og eksisterende anlegg er ikke kryptering blitt så mye brukt, anleggene sikres ved at de ikke er tilkoblet internett, de er helt lokale anlegg. Krav og forventninger fra kunder har forandret seg, og nå ønsker kundene og ha tilgang til scada systemene uansett hvor de er. Prosjektet har som mål å finne en effektiv og sikker løsning for automatisering av oppdateringsprosessen.

## Prosjektmål

Byggautomasjonssystemer har blitt mere komplekse, og med økende krav til fjernadgang til SCADA-systemer, integreringer av nye APIer, eller andre tekniske løsninger blir det flere utfordringer rundt sikker datautveksling og autentisering. Prosjektet har som hovedmål å utvikle en metode for automatisert oppdatering av OPC UA-sertifikater i byggautomasjonsnettverk for å sikre kontinuerlig autentisering og kryptering av kommunikasjon mellom enheter.

## Effektmål

Det overordnede effektmålet er å sikre kontinuerlig autentisering og kryptering i byggautomasjonsnettverk ved å automatisere oppdateringen av OPC UA-sertifikater. Ved å fjerne den manuelle prosessen knyttet til sertifikathåndtering, kan systemer oppdateres raskt, dynamisk og sikkert, uten at et menneske må gjøre det manuelt. Det vil redusere sikkerhetsrisikoen, forbedre driftseffektiviteten, og sikre at alle enheter i nettverket alltid har oppdaterte sertifikater.

## Resultatmål

For å oppnå effektmålet vil prosjektet:

* Utvikle og teste en skalerbar og sikker metode for automatisert sertifikathåndtering i byggautomasjonsnettverk.
* Implementere og evaluere løsningen i et simulert automasjonsmiljø med WAGO PLS-er.
* Sikre at sertifikater genereres, distribueres og fornyes uten behov for manuelle oppdateringer.
* Evaluere eksisterende sikkerhetsløsninger, samt implementere en PKI-basert (Public Key Infrastructure) tilnærming for sertifikathåndtering.

For å oppnå dette må løsningen integrere et system for automatisert sertifikatregistrering og fornyelse, som muliggjør:

1. Automatisk generering av sertifikater via en sertifikatautoritet (CA).
2. Distribusjon av sertifikater til enheter i byggautomasjonsnettverket.
3. Automatisk fornyelse og utveksling av sertifikater ved utløpsdato eller når sikkerhetspolicyer krever det.
4. Integrasjon med OPC UA sikkerhetsmekanismer for autentisering og kryptert datautveksling.

## Prosessmål

Prosjektet vil involvere både interne og eksterne interessenter, inkludert veileder, bransjeeksperter og tekniske ressurspersoner. Det er viktig å opprettholde jevnlig kommunikasjon for å sikre at prosjektet utvikles i tråd med forventninger og krav. Jeg ønsker å utvide kompetansen min og bygge nettverk med flere som jobber i dette segmentet, både innen byggautomasjon, OPC UA og cybersikkerhet.

### Samarbeid og kommunikasjon

Prosjektet vil ha fokus på god kommunikasjon og samarbeid mellom alle de involverte partene.

* Regelmessige møter med veileder for å drøfte utfordringer, fremdrift og mulige løsninger.
* Dialog med bransjeeksperter, inkludert representanter fra Storm Elektro og WAGO Norge, for å få innspill til løsningen og dens praktiske anvendelse.
* Bruk av digitale samarbeidsverktøy, som Discord, Teams og e-post for kommunikasjon.

### Læringsmål og kompetansebygging

Et viktig mål for prosjektet er å utvikle en dypere forståelse av OPC UA-sikkerhet, automatisert sertifikathåndtering og byggautomasjonssystemer.

* Utforske teknologier knyttet til PKI og OPC UA, og hvordan disse kan implementeres i praksis.
* Få praktisk erfaring med WAGO PLS-er og deres rolle i industrielle nettverk.
* Bygge videre på et faglig nettverk med personer som arbeider innen byggautomasjon og industriell IT-sikkerhet, for fremtidige samarbeid og erfaringsutveksling.
* Effektiv prosjektgjennomføring

### For å sikre fremdrift og struktur i prosjektet.

* Planlegging av oppgaver og milepæler i et Gantt-diagram, for å visualisere prosjektets tidslinje.
* Kontinuerlig evaluering av resultater for å sikre at prosjektet holder seg innenfor rammene av de tekniske og sikkerhetsmessige kravene.
* Dokumentasjon av arbeidsprosessen, slik at erfaringene fra prosjektet kan deles og videreutvikles i senere arbeid.

Gjennom dette prosjektet ønsker jeg ikke bare å utvikle en teknisk løsning, men også å lære mer om industristandarder, sikkerhetsmekanismer og beste praksis for implementering av OPC UA i byggautomasjon. Samtidig vil jeg bruke muligheten til å utvide kontaktene med bransjeaktører som kan bidra med verdifull innsikt og erfaring.

# Prosjektets omfang

## Avdekke utfordringene

Dette prosjektet skal avdekke utfordringene knyttet til sertifikathåndtering, undersøke og sammenligne ulike løsninger, samt finne en metode som kan automatisere denne prosessen i et testmiljø. Gjennom arbeidet skal svakheter i eksisterende løsninger identifiseres, mulige forbedringer analyseres og hvordan en slik løsning kan tilpasses byggautomasjonssystemer undersøkes. Målet er å vurdere om en automatisert metode kan være sikker, skalerbar og pålitelig nok til å brukes i reelle anlegg.

For å forstå utfordringene knyttet til eksisterende sertifikathåndtering, vil prosjektet først gjennomføre en analyse av nåværende praksis. Dette inkluderer identifisering av utfordringer knyttet til manuell håndtering av OPC UA-sertifikater, samt en gjennomgang av dagens implementering av autentisering og kryptering i byggautomasjonssystemer. Basert på dette vil behovet for automatisering dokumenteres, med fokus på forbedringer som kan øke sikkerheten og effektiviteten.

## Evaluering av relevante produkter og metoder

A diagram of a software

AI-generated content may be incorrect.Neste del blir en evaluering av eksisterende PKI-løsninger, CA-tjenester og automatiserte systemer for sertifikathåndtering. Målet er å prøve å finne en metode som kan fungere i et byggautomasjonsmiljø med WAGO PLS-er. Jeg vil vurdere ulike alternativer og undersøke hvilke løsninger som kan forenkle fornyelse og distribusjon av sertifikater på en sikker og automatisert måte.

Figur 2 viser den manuelle løsningen av sertifikathåndtering som er beskrevet av OPC Foundation.

<https://reference.opcfoundation.org/Core/Part2/v104/docs/8.1.2#_Ref260612420>

[figur 2 manuell sertifikathåndtering]

A diagram of a software application

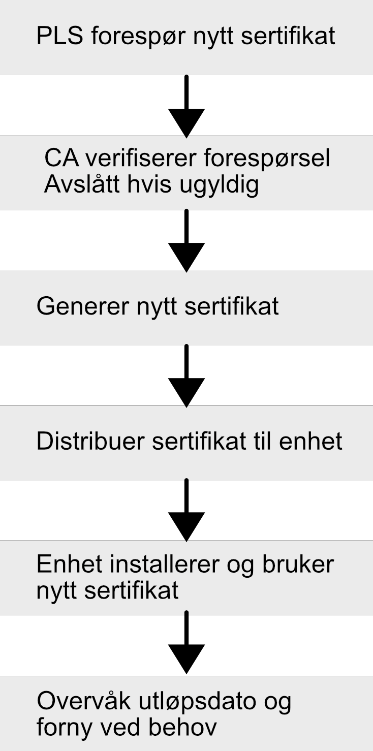
AI-generated content may be incorrect.

**GDS sertifikat håndterer**

Figur 3 viser den automatiserte sertifikathåndteringen som er beskrevet av OPC Foundation.

<https://reference.opcfoundation.org/Core/Part2/v104/docs/8>

[figur 3 den automatiserte sertifikathåndteringen]



## Implementering og testing

Basert på det jeg lærer gjennom analysen og evalueringen, vil jeg prøve å utvikle en prototypeløsning for automatisk registrering og fornyelse av OPC UA-sertifikater som kan brukes i byggautomasjonsanlegg. Løsingen skal testes i et simulert automasjonsnettverk med WAGO PLS-er og SCADA. Målet er å undersøke om løsningen fungerer i praksis, og om den oppfyller kravene til sikkerhet, pålitelighet og skalerbarhet. Hvis resultatene blir bra, kan jeg vurdere hvordan dette kan brukes i reelle byggautomasjonsanlegg.

## Kommunikasjon og samarbeid

For å sikre at løsningen er relevant og gjennomførbar i reelle byggautomasjonsanlegg, vil det være tett samarbeid med Storm Elektro og WAGO Norge. Dette innebærer, testing og evaluering i samarbeid med fagpersoner innen byggautomasjon. Prosjektets resultater, utfordringer og anbefalinger vil dokumenteres grundig, slik at løsningen kan videreutvikles og implementeres i operative anlegg.

[figur 4 viser ønsket løsning]

## Ønsket løsning for henting av nye sertifikater

Sikre kontinuerlig autentisering og kryptering i byggautomasjonsnettverk, en løsning som let's encrypt der sertifikater blir hentet og oppdatert automatisk. Prosjektet skal kartlegge utfordringer, evaluere metoden lage en testløsning i et simulert automasjonsmiljø med WAGO PLS-er. Resultatet vil skal være skalerbart og gi en sikker løsning som kan anvendes i moderne byggautomasjonssystemer. Se figur 4 for ønsket løsning.

## Arbeidsoppgaver

For å sikre en strukturert gjennomføring av prosjektet er det definert flere arbeidsoppgaver som skal utføres.

Først kartlegges utfordringer ved dagens manuelle prosesser for OPC UA-sertifikater:

* Identifisering av hvordan sertifikater genereres, distribueres og fornyes manuelt.
* Analyse av potensielle svakheter og sårbarheter i eksisterende praksis.
* Kartlegging av utfordringer knyttet til integrasjon av sertifikater i byggautomasjonsnettverk.
* Evaluering av produkter og metoder for sertifikathåndtering

Neste steg er vurdering av relevante produkter og metoder for automatisert sertifikathåndtering.

* Undersøkelse av eksisterende PKI-løsninger og CA-tjenester.
* Evaluering av hvordan løsninger tilsvarende Let's Encrypt eller andre automatiserte sertifikattjenester kan integreres med OPC UA.
* Sammenligning av tilgjengelige metoder for automatisk sertifikatdistribusjon og fornyelse.
* Design av en automatisert løsning for sertifikathåndtering

Basert på informasjonen fra de to første stegene, er målet å lage en løsning som:

* Sikrer enkel implementering og bruk i byggautomasjonsnettverk.
* Automatiserer prosessen med å registrere, distribuere og fornye OPC UA-sertifikater.
* Er kompatibel med WAGO PLS-er.
* Ivaretar sikkerhetsaspekter som autentisering, kryptering og tilgangskontroll.
* Lage et testmiljø for å simulere et anlegg.

For å validere løsningen vil løsningen testes i et testmiljø bestående av WAGO PLS-er:

* Konfigurering av testoppsett med nødvendig maskinvare og programvare.
* Integrasjon av den automatiserte sertifikatløsningen.
* Evaluering av funksjonalitet, sikkerhet og ytelse gjennom omfattende tester.
* Dokumentasjon av testresultater og forslag til forbedringer.

## **Avgrensninger**

For å sikre at prosjektet har en avgrenset og håndterbar tilnærming, vil jeg fokusere på implementering av en automatisert løsning for OPC UA-sertifikathåndtering innen byggautomasjon. Dette betyr at prosjektet ikke vil se på andre industriprotokoller som BACnet Secure connect, eller KNX Secure. Det er eksisterende OPC UA standarder som benyttes, og prosjektet vil undersøke hvordan sertifikatene kan oppdateres på en sikker og effektiv måte.

Testing av løsningen vil foregå i et simulert miljø med WAGO PLS-er, det betyr at løsningen ikke vil bli testet på et operativt anlegg i denne fasen. Dette sikrer at alle tester og evalueringer kan gjennomføres under kontrollerte forhold før en eventuell videre utrulling.

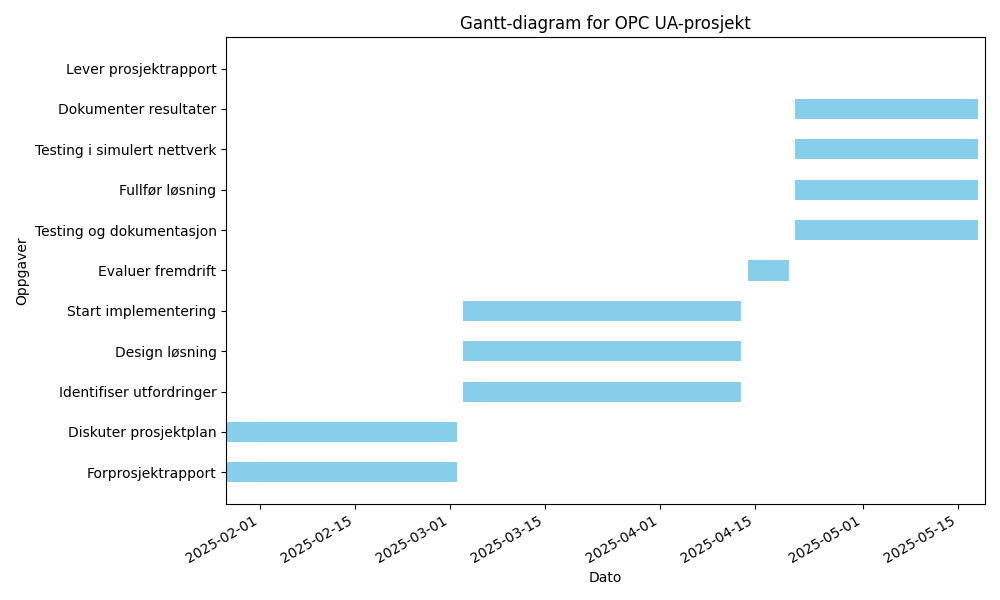
Videre vil prosjektet ikke inkludere sikkerhetsaspekter utenfor sertifikathåndtering. Dette innebærer at mekanismer som brannmurer, VPN eller IAM-systemer ikke vil bli analysert eller implementert som en del av løsningen. I stedet vil prosjektet bygge på eksisterende PKI-løsninger for å håndtere generering, distribusjon og fornyelse av OPC UA-sertifikater. Dette innebærer at en egen sertifikatautoritet (CA) ikke vil bli utviklet, men at allerede etablerte CA-tjenester vil bli integrert for å oppnå sikker og pålitelig autentisering innenfor byggautomasjonssystemer.

For å sikre en fokusert tilnærming til prosjektet er det definert følgende avgrensninger:

* Begrenset til OPC UA-sertifikater: Prosjektet fokuserer utelukkende på håndtering av OPC UA-sertifikater og inkluderer ikke andre sikkerhetsmekanismer som brannmurer, VPN eller IAM-systemer.
* Testmiljø med WAGO PLS-er: Testing vil kun foregå i et simulert miljø med WAGO PLS-er, og det er ikke planlagt testing i operative byggautomasjonsanlegg i denne fasen.
* Ingen endringer i OPC UA-protokollen: Prosjektet vil benytte eksisterende OPC UA-standarder og spesifikasjoner uten å utvikle nye protokoller eller utvide OPC UA-standarden.
* Bruk av eksisterende PKI-løsninger: Det vil ikke bli utviklet en egen sertifikatautoritet (CA), men prosjektet vil integrere eksisterende PKI-løsninger for sertifikathåndtering.

Prosjektet skal ferdigstilles innen uke 21.

## Fremdriftsplan og milepæler



[figur 5 gantt-diagram oversikt tidsbruk

Uke 5–9

- Fullfør forprosjektrapport med fokus på problemstilling, målsetning, metode og ressursplanlegging.

- Diskuter prosjektplan og ambisjonsnivå med veileder.

Uke 10–15

- Identifiser utfordringer i OPC UA-sertifikathåndtering og evaluer mulige løsninger.

- Design en løsning for sertifikathåndtering (struktur og automatisering).

- Start implementering i et simulert miljø, med WAGO PLS-er, linux og Ignition SCADA.

Uke 16

Evaluer fremdrift og gjør justeringer

Uke 17–20

- Testing og dokumentasjon

- Fullfør løsningen.

- Testing i simulert automasjonsnettverk.

- Dokumenter resultatene fra testing og lag rapport

Uke 21 Avslutning

- Lever prosjektrapport innen 20. mai (midnatt).

## Forventede resultater

Ved slutten av prosjektet forventer jeg følgende resultater:

* En fungerende prototype av en automatisert sertifikathåndteringsløsning for OPC UA.
* Dokumentasjon av testresultater, sikkerhetsaspekter og integrasjonsmuligheter.
* En vurdering av implementerbarheten i reelle byggautomasjonsanlegg.

Denne rapporten vil fungere som grunnlag for videre arbeid med å implementere løsningen i faktiske anlegg og kan også bidra til forbedringer av standardisert sertifikathåndtering i byggautomasjon.

# Interessenter og rammebetingelser

## Interessentanalyse

Prosjektet har flere interessenter som vil dra nytte av utviklingen av en automatisert løsning for sertifikathåndtering i OPC UA-baserte byggautomasjonsnettverk. Det vil være systemintegratorer, driftsansvarlige, OT-ansvarlige, eiendomsforvaltere, sikkerhetsansvarlige, it-ansvarlige, eiendomseiere og leverandører av byggautomasjonssystemer.

For systemintegratorer er dette prosjektet interessant fordi det kan redusere kompleksiteten ved implementering av sikre byggautomasjonssystemer. En automatisert løsning for sertifikathåndtering vil gjøre det enklere å integrere OPC UA-sikkerhetsmekanismer uten behov for omfattende manuelle prosesser. Dette kan gi lavere kostnader og raskere idriftsettelse av nye systemer.

Driftsansvarlige og eiendomsforvaltere har et direkte behov for robuste sikkerhetsløsninger i byggautomasjon. Med økende krav til fjernovervåkning og sentral styring av tekniske systemer, blir sikker autentisering og kryptering stadig viktigere. Automatisering av sertifikathåndtering vil bidra til økt driftssikkerhet, redusert risiko for menneskelige feil og bedre kontroll over sikkerhetsnivået i anleggene.

Sikkerhetsansvarlige, it-ansvarlige og OT-ansvarlige i organisasjoner som benytter OPC UA i byggautomasjon vil også ha stor interesse av prosjektet. Tradisjonelt har byggautomasjonsnettverk vært isolert fra internett, men med økende digitalisering og fjernaksess er det nødvendig med moderne sikkerhetsløsninger. Automatisering av sertifikathåndtering vil gi en mer forutsigbar og pålitelig sikkerhetsstruktur som beskytter systemene mot uautorisert tilgang.

Eiendomsforvaltere og eiendomseiere har en økonomisk og strategisk interesse i prosjektet, da en sikker og effektiv drift av byggautomasjonssystemer kan bidra til reduserte driftskostnader og økt energieffektivitet. Ved å implementere en løsning for automatisert sertifikathåndtering kan eiendomseiere sikre at byggets tekniske systemer opererer på en stabil og sikker måte, samtidig som de oppfyller krav til cybersikkerhet og nye sikkerhets krav.

For eiendomsforvaltere er dette også viktig fra et risikostyringsperspektiv, da moderne bygg i økende grad er koblet til internett og dermed utsatt for potensielle cyberangrep. Ved å automatisere sikkerhetsprosesser som sertifikathåndtering, reduseres faren for uautorisert tilgang og systemfeil, noe som kan beskytte byggets tekniske infrastruktur og minimere behovet for akutt vedlikehold. Dette øker ikke bare påliteligheten, men også bygningens langsiktige verdi og attraktivitet på markedet.

Leverandører av byggautomasjonssystemer kan også dra nytte av prosjektet ved å tilby OPC UA-løsninger med innebygd støtte for automatisk sertifikathåndtering. Dette vil forbedre konkurranseevnen deres og gjøre produktene mer attraktive for kunder som ønsker sikre og vedlikeholdsvennlige løsninger.

### Ekstern

|  |  |  |
| --- | --- | --- |
| Interessent | Suksesskriterier | Bidrag til prosjektet |
| Storm Elektro | En sikker og enkel løsning for sertifikater | Tid og muligheter |
| WAGO Norge | Kompatibilitet med deres produkter  Et godt gjennomført prosjekt | Teknisk støtte og verktøy |
| Veileder Wago Norge ved Thomas Sandberg | Et godt dokumentert og gjennomført prosjekt | Veiledning og kvalitetssikring |

### Intern

|  |  |
| --- | --- |
| Aleksander Tandberg, TISIP | Veiledning |
| Espen Klippenberg Bø | Utvikling, testing, drift |

## Rammebetingelser

Prosjektet skal ferdigstilles innen uke 21, og løsningen som utvikles må følge etablerte standarder og spesifikasjoner fra OPC Foundation og relevante leverandører innen byggautomasjon. Dette innebærer at løsningen må være kompatibel med OPC UA-spesifikasjonene, spesielt innen sikkerhet, sertifikathåndtering og interoperabilitet med eksisterende systemer.

Prosjektet gjennomføres av en person, noe som medfører begrenset tid og kapasitet. Dette innebærer at omfanget må tilpasses ressursene som er tilgjengelige, både når det gjelder utvikling, testing og dokumentasjon. Det kan derfor være nødvendig å prioritere spesifikke aspekter av løsningen, for eksempel å teste en begrenset mengde utstyr eller fokusere på en spesifikk metode for sertifikathåndtering.

Tilgangen til maskinvare og programvare er også en viktig faktor. Prosjektet har mulighet til å teste på WAGO PLS-er, men det er begrenset tilgang til andre systemer som benyttes i operative byggautomasjonsanlegg. Prosjektet ønsker i størst mulig grad å bruke gratis eller åpen kildekode-verktøy, men det kan bli nødvendig å teste løsninger med tidsbegrensede demoer eller lisensierte programmer.

For å sikre at prosjektet kan gjennomføres innen tidsrammen, vil arbeidsmengden styres nøye, og løsningen vil bli testet i et kontrollert simuleringsmiljø før eventuelle vurderinger for praktisk implementering i reelle anlegg.

## OPC UA og rollen den har i automasjonssystemer

I motsetning til eldre OPC-standarder som var avhengige av Windows-baserte teknologier (DCOM), er OPC UA designet for å fungere på tvers av ulike plattformer, inkludert Windows, Linux og PLS systemer. Det gjør den til en av de mest brukte standard for IIoT (Industrial Internet of Things) og automasjonssystemer.

OPC UA brukes i forskjellige sektorer, inkludert produksjonsindustri, kraftforsyning, vann- og avløpssystemer, transport, farmasøytisk industri og byggautomasjon. Standardens fleksibilitet og omfattende sikkerhetsmodell gjør den ideell for integrasjon mellom ulike systemer og teknologier.

### Sikkerhetsmekanismer i OPC UA

En av de viktigste fordelene med OPC UA er sikkerhetsmodellen.

Standarden inkluderer:

* Autentisering og tilgangskontroll – OPC UA støtter bruk av sertifikater og identitetsbasert autentisering, slik at kun autoriserte enheter og brukere får tilgang til systemet.
* Kryptering – Kommunikasjon mellom OPC UA-klienter og -servere beskyttes gjennom TLS (Transport Layer Security) for å forhindre avlytting og manipulering av data.
* Signering av meldinger – Alle meldinger som sendes via OPC UA, kan signeres digitalt for å sikre at innholdet ikke er blitt endret under overføring.
* Sikkerhetsnivåer – OPC UA tillater forskjellige sikkerhetsnivåer, avhengig av hvilke krav systemet har. Dette gir fleksibilitet i konfigurasjonen av sikkerhetsinnstillinger.

Bruken av PKI (Public Key Infrastructure) og OPC UA’s sikkerhetsmodeller krever at løsningen overholder retningslinjene for sertifikathåndtering beskrevet i OPC UA Part 12 – Discovery & Global Services. (https://reference.opcfoundation.org/GDS/v105/docs/)

Dette inkluderer prosesser for generering, distribusjon, fornyelse og tilbakekalling av sertifikater, som sikrer at alle enheter i systemet er verifisert og beskyttet.

### Hvorfor OPC UA brukes i byggautomasjon

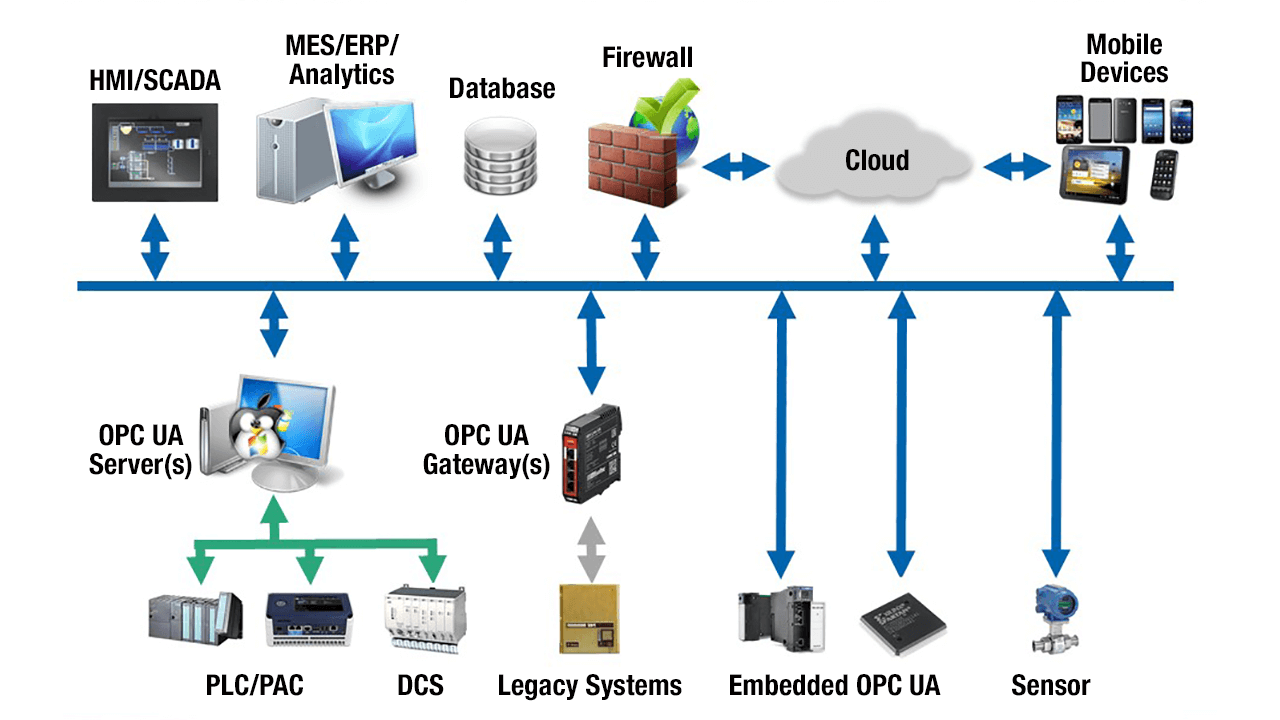
Byggautomasjonssystemer er avhengige av kommunikasjon mellom ulike enheter som PLS-er, HMI-paneler, SCADA-systemer, sensorer og aktuatorer. OPC UA gjør det mulig å integrere disse systemene på en standardisert måte, uavhengig av produsent eller underliggende teknologi.

Dette gir flere fordeler:

* Interoperabilitet – OPC UA gjør det mulig for enheter og systemer fra forskjellige leverandører å kommunisere uten behov for spesialtilpassede protokoller.
* Skalerbarhet – Standarden er utviklet for både små og store systemer, noe som gjør den egnet for alt fra enkeltstående bygg til store industrikomplekser.
* Fremtidssikkerhet – OPC UA er en aktivt vedlikeholdt standard som stadig forbedres, ved å implementere den sikres langsiktig kompatibilitet med nye systemer og teknologier.
* Integrasjon med sky- og IIoT-løsninger – OPC UA kan kobles til skybaserte tjenester for fjernovervåkning og dataanalyse, noe som gir mulighet for prediktivt vedlikehold og avansert energistyring.

### Sammenheng mellom OPC UA og dette prosjektet

For å oppnå høy sikkerhet og kompatibilitet med etablerte systemer, skal prosjektet bruke OPC UA sin dokumentasjonen og benytte eksisterende verktøy og bibliotek fra OPC Foundation, wago som automatikk leverandør og andre produkter eller programmer ved behov. Det skal sikre en effektiv løsning for automatisert sertifikathåndtering, som kan implementeres i både nye og eksisterende byggautomasjonsanlegg.

Ved å følge OPC UA-standardene og sikre en god sertifikathåndtering, vil prosjektet bidra til økt sikkerhet og effektivitet i byggautomasjonssystemer. Dette vil også legge til rette for enklere integrasjon med tredjepartsløsninger og fremtidige utvidelser av systemene. Ettersom fjernaksess til byggautomasjonssystemer blir stadig viktigere, gir OPC UA en sikker plattform for kryptert kommunikasjon i moderne bygg.

<https://iebmedia.com/wp-content/uploads/2020/12/opc-ua-fig2.png>

[figur 6 viser et prinsippskjema over et SD-anlegg med OPC UA]

# Kritiske suksessfaktorer

## Suksessfaktorer

For at prosjektet skal lykkes, er det avgjørende å identifisere og ivareta flere faktorer som vil påvirke resultatet. Det vil være valg av riktige tekniske løsninger, støtte fra relevante interessenter, automatisering av prosesser og en grundig testfase i et kontrollert miljø.

En av de viktigste forutsetningene for at det skal bli en suksess er kompatible verktøy og metoder. Sånn at løsningen skal kunne integreres i eksisterende byggautomasjonsnettverk, må teknologiene som benyttes være i samsvar med OPC UA-standardene. Det innebærer at alle verktøy, biblioteker og systemkomponenter må være kompatible med de sikkerhets- og kommunikasjonsprotokollene som OPC Foundation har definert. Dersom løsningen ikke tilfredsstiller disse kravene, kan det føre til utfordringer ved bruk av løsningen i installasjoner som er i produktsjon.

Dette prosjektet krever tett samarbeid med eksterne aktører for å sikre at løsningen utvikles i henhold til reelle behov. Dersom støtte og veiledning fra eksperter innen OPC UA, PKI og byggautomasjon ikke er tilgjengelig gjennom prosjektperioden, kan det oppstå tekniske utfordringer som forsinker eller hindrer gjennomføringen.

For at løsningen skal bli brukt, må den være automatisert og kreve minimalt med manuell håndtering. Tradisjonell sertifikathåndtering i OPC UA-systemer er ofte manuell, noe som kan føre til feilkonfigurasjoner og sikkerhetshull. Ved å utvikle en automatisert løsning kan man sikre at systemene alltid har gyldige sertifikater, uten at driftspersonell trenger å utføre tidkrevende vedlikeholdsoppgaver. Automatisering bidrar også til bedre sikkerhet, ettersom risikoen for menneskelige feil reduseres betydelig.

Videre må løsningen være enkel å gjennomføre i eksisterende anlegg. En løsning som krever omfattende tilpasninger eller store endringer i infrastrukturen, kan føre til høyere kostnader noe sluttkunden ikke ønsker. Derfor må implementeringen være modulær og fleksibel, slik at den kan tilpasses ulike systemarkitekturer uten omfattende endringer. Dokumentasjon og brukerveiledning er også viktig for å sikre at teknisk personell enkelt kan sette opp og administrere løsningen.

Den siste avgjørende suksessfaktor er at løsningen gjennomgår en vellykket testing i et simulert miljø. Før løsningen kan tas i bruk i operative anlegg, må den evalueres i et kontrollert testoppsett hvor alle funksjoner verifiseres. Testfasen må inkludere scenarier som simulerer reelle utfordringer, som utløp av sertifikater, autorisasjonsfeil og nettverksforstyrrelser. Dersom løsningen er stabilt og sikkert under disse forholdene, vil det øke sjansen for at det kan gjennomføres i installasjoner som er i produksjon.

Om prosjektet er en suksess avhenger av en kombinasjon av teknisk kvalitet, brukervennlighet, støtte fra bransjeaktører og grundig testing. Ved å oppfylle disse kriteriene sikrer vi at løsningen ikke bare er teknisk solid, men også praktisk gjennomførbar og verdifull for drift av moderne byggautomasjonssystemer.

## Informasjonsbehov

For at prosjektet skal oppnå de ønskede resultatene og kunne implementeres i automasjonssystemer, er det viktig at all relevant informasjon blir grundig dokumentert og tilgjengelig for alle interessenter. Storm Elektro og WAGO Norge er de viktigste interessentene i dette prosjektet og ønsker detaljert informasjon om utviklingen, implementeringen og testresultatene. Dette innebærer teknisk dokumentasjon og praktiske retningslinjer for hvordan løsningen kan integreres i eksisterende og nye anlegg.

Siden prosjektet kan gi verdi for hele byggautomasjonsbransjen, ønsker jeg å gjøre informasjonen tilgjengelig for flere. Prosjektresultatet blir publisert på github under min bruker sammen med kildekode, dokumentasjon og testresultater. Jeg håper at løsningen kan videreutvikles av andre aktører i automasjonsmiljøet, slik at eventuelle svakheter kan identifiseres og forbedringer kan foreslås.

For at løsningen skal kunne brukes av andre må dokumentasjonen inneholde trinnvise instruksjoner for oppsett, beskrivelse av hvilke tekniske krav som må være oppfylt, og eventuelle sikkerhetsanbefalinger knyttet til OPC UA-sertifikathåndtering. Dette inkluderer oppsett av sertifikatautoritet (CA), sertifikatdistribusjon, automatisert fornyelse og validering. Informasjonen må også inkludere anbefalinger om vedlikehold av sertifikater i større systemer.

En annen viktig del av informasjonsbehovet er knyttet til sikkerhet og samsvar med standarder. OPC UA har strenge sikkerhetskrav, og det er essensielt at løsningen er utviklet i henhold til spesifikasjonene definert av OPC Foundation. Dette betyr at løsningen må overholde retningslinjer for kryptering, autentisering, og meldingssignering, slik at datautvekslingen forblir sikker.

Ved å sørge for at all relevant informasjon blir dokumentert og gjort tilgjengelig for andre, håper jeg at løsningen ikke bare blir en teoretisk mulighet, men også en praktisk forbedring i byggautomasjonssystemer.

# Risikoanalyse

## Beskrivelse av risikoer og tilhørende tiltak

For å få en god gjennomføring av prosjektet er det viktig å identifisere hvilke mulige risikoer som finnes før vi starter eller som kan oppstå underveis. Også må det planlegge hvilke tiltak som kan gjennomføres for å redusere eller eliminere de forskjellige risikoene. Risikoanalysen fokuserer på tekniske, organisatoriske og eksterne faktorer som kan ha innvirkning på prosjektets fremdrift og resultat.

Risikoanalysen skal identifiserer mulige utfordringer som kan påvirke prosjektets gjennomføring og resultat. Hver risiko vurderes med hensyn til sannsynlighet og konsekvens, og nødvendige tiltak skal planlegges for å minimere negative effekter.

Risiko = Konsekvens \* Sannsynlighet

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Konsekvens | Veldig høy | 5 | 10 | 15 | 20 | 25 |
| Høy | 4 | 8 | 12 | 16 | 20 |
| Medium | 3 | 6 | 9 | 12 | 15 |
| Lav | 2 | 4 | 6 | 8 | 10 |
| Veldig lav | 1 | 2 | 3 | 4 | 5 |
|  | Veldig lav | Lav | Medium | Høy | Veldig høy |
| Sannsynlighet | | | | | |

[figur 7 konsekvens tabell]

En systematisk tilnærming til risikoanalyse innebærer en vurdering av sannsynlighet og konsekvens for hver identifisert risiko. Dette gir en kvantifiserbar forståelse av hvilke utfordringer som er mest kritiske, og hvilke tiltak som bør iverksettes for å minimere deres påvirkning.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Risiko | Sannsynlighet | Konsekvens | Før tiltak | Tiltak | Sannsynlighet | Konsekvens | Etter tiltak |
| Manglende teknisk støtte | Høy(4) | Medium(3) | 12 | Tidlig kontakt med leverandører | Veldig Lav(1) | Medium(3) | 3 |
| Forsinkelse i prosjektleveranse | Medium(3) | Høy(4) | 12 | Justere tidsplan og prioritere oppgaver | Lav(2) | Medium(3) | 6 |
| Kompatibilitetsproblemer | Medium(3) | Veldig høy(5) | 15 | Teste løsningen grundig i simulert miljø | Lav(2) | Medium(3) | 6 |
| Begrenset tilgang til verktøy og programvare | Medium(3) | Høy(4) | 12 | Undersøke og evaluere gratis og kommersielle alternativer tidlig i prosjektet | Veldig Lav(1) | Lav(2) | 2 |
| Manglende kompetanse i spesifikke teknologier | Medium(3) | Høy(4) | 12 | Prioritere opplæring og samarbeid med eksperter | Lav(2) | Lav(2) | 4 |
| Tidspress på grunn av parallelle oppgaver | Høy(4) | Høy(4) | 16 | Effektiv tidsplanlegging og regelmessige statusmøter | Lav(2) | Medium(3) | 6 |

[figur 8 Tabellen gir en oversikt over sentrale risikoer i prosjektet, samt tiltak for å redusere deres innvirkning]

### Manglende teknisk støtte

Siden prosjektet avhenger av tilgang til informasjon og veiledning fra leverandører som Storm Elektro og WAGO Norge, kan manglende teknisk støtte føre til forsinkelser eller feil i implementeringen. For å redusere denne risikoen har jeg tatt kontakt med leverandørene tidlig for å sikre nødvendig veiledning og teknisk bistand gjennom hele prosjektperioden.

### Forsinkelse i prosjektleveranse

Prosjektet har en fastsatt tidsramme, og forsinkelser kan oppstå på grunn av uforutsette tekniske eller organisatoriske utfordringer. Dette kan påvirke kvaliteten på leveransen. For å håndtere denne risikoen har jeg utarbeidet en tidsplan med tydelige milepæler og prioritetsoppgaver, sånn at eventuelle forsinkelser kan håndteres tidlig.

### Kompatibilitetsproblemer

Byggautomasjon involverer flere ulike systemer og protokoller, og det er en risiko for at den utviklede løsningen ikke fungerer sømløst med eksisterende utstyr. Dette kan føre til feil eller behov for omfattende tilpasninger. For å redusere denne risikoen vil løsningen testes grundig i et simulert miljø med WAGO PLS-er.

### Begrenset tilgang til verktøy og programvare

Prosjektet har som mål å finne løsninger som ikke krever store investeringer i kommersiell programvare. Men det kan være nødvendig med enkelte programmer som er kostbare eller kreve lisenser. Jeg skal prøve å finne programmer som er open source eller tilgjengelig i demo versjoner.

### Manglende kompetanse i spesifikke teknologier

OPC UA, PKI og byggautomasjon er tekniske fagfelt som krever spesialisert kunnskap. Hvis prosjektet møter utfordringer på grunn av manglende kunnskap om disse teknologiene, kan det føre til feil eller lite effektiv gjennomføring. For å prøve og hindre dette vil jeg ta tidlig kontakt med eksperter og lese dokumentasjon som finnes.

### Tidspress på grunn av parallelle oppgaver

Prosjektet må gjennomføres samtidig med andre aktiviteter, noe som kan føre til tidspress. For å redusere denne risikoen vil det legges vekt på effektiv tidsplanlegging, prioritere prosjektarbeid og regelmessige statusmøter.

### Oppsummering

En grundig risikoanalyse og forebyggende tiltak skal hjelpe til med å sikre en stabil og forutsigbar prosjektgjennomføring. Ved å adressere de mest kritiske utfordringene tidlig i prosjektet kan risikoen for forsinkelser, tekniske problemer og ressursbegrensninger minimeres. Gjennom god planlegging, opplæring og tett samarbeid med interessenter skal det sikres at prosjektet leverer en fungerende løsning for automatisk sertifikathåndtering i OPC UA-baserte byggautomasjonssystemer.

# Kost/nytte-analyse

Prosjektet gjennomføres som en del av et skoleprosjekt, utgiftene vil være tid som brukes utvikling, testing og prosjektskriving. Også vil prosjektet kreve PLSer og programvare.

## Kostnader tilknyttet prosjektet

* Arbeidstid: Estimert tid til skoleprosjektet er 300 timer. 200 timer går til utvikling og implementering, mens 100 timer benyttes til testing, dokumentasjon og forbedringer.
* Maskinvare: WAGO PLSer Compact Controller CC 100 for å utføre testing. Listepris per stk 5 345 kr eks.mva
* Programvare: Prosjektet har som mål å bruke gratis eller open-source programvare. Det kan bli behov for testlisenser eller demoer fra kommersielle aktører. Lisenser for den type software ligger på 50 000 – 100 000 kr eks.mva.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Kostnader | Timer | Kost per time | Antall | Pris per stk | Totalt |
| Arbeidstid | 300 | 250 |  |  | 75 000 |
| Maskinvare |  |  | 2 | 5 345 | 10 690 |
| Programvare |  |  |  |  | 0 |
|  |  |  |  |  |  |
| Total sum | | | | | 85 690 kr |

## Nytte prosjektet kan tilføre byggautomasjonsbedriftene

Løsningen som utvikles kan gi både kvantifiserbare og ikke-kvantifiserbare fordeler.

Kvantifiserbar nytte

* Reduserte driftskostnader: Automatisering av sertifikathåndtering vil fjerne behovet for manuell oppdatering, som kan spare opptil 7,5–15 timer per system per år. En ingeniør som ofte gjør denne jobben, koster fra 1 400-1 700 kr eks. mva timen.
* Mindre nedetid: Automatisk fornyelse av sertifikater reduserer risikoen for feil eller utløpte sertifikater, noe som kan spare bedrifter for betydelige kostnader knyttet til driftsstans. Driftsstans kan koste fra noen tusen til flere hundre tusen alt etter hvilke type bygg som stanser. Må beboerne flyttes? De ansatte sendes hjem? Produksjonen stopper? Jeg tar et utgangspunkt på 200 000 kr.
* Bedre ressursutnyttelse: Teknisk personell kan bruke tiden sin på andre viktige oppgaver fremfor manuelle oppdateringer.

Ikke-kvantifiserbar nytte

* Økt sikkerhet: Kontinuerlig oppdaterte sertifikater reduserer risikoen for sikkerhetsbrudd og uautorisert tilgang.
* Forbedret omdømme: Firmaet vil kunne tilby en mer pålitelig og moderne løsning, noe som kan styrke konkurransefortrinnet.
* Økt kundetilfredshet: En sikker og stabil løsning vil gi sluttbrukerne trygghet om at systemene oppfyller dagens sikkerhetsstandarder.
* Redusert arbeidsbelastning: Automatiseringen vil redusere behovet for manuelt arbeid og risikoen for menneskelige feil.
* Mulighet for gjenbruk: Løsningen kan videreutvikles og brukes i andre prosjekter eller tilpasses ulike byggautomasjonsmiljøer.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Kostnader | Timer | Kost per time | Antall | Pris per stk | Totalt |
| Arbeidstid | 7,5 | 1 400 |  |  | 10 500 |
| Drifts stopp |  |  | 1 | 200 000 | 200 000 |
|  |  |  |  |  |  |
| Total sum | | | | | 200 500 kr |

Når man sammenligner kostnadene med potensielle fordeler, viser analysen at investering i en automatisert løsning for sertifikathåndtering kan gi betydelige besparelser på sikt. Prosjektet vil ikke bare redusere manuelle driftskostnader, men også forbedre sikkerheten og driftssikkerheten i byggautomasjonsnettverk. Spesielt når løsningen brukes i flere bygg. Da vil både driftskostnadene synke og sikkerheten bli bedre. Sjansen for driftsstans på grunn av feil eller utgåtte sertifikater vil også bli mye mindre.

# Retningslinjer og standarder

Prosjektet må forholde seg til en rekke retningslinjer og standarder som Tisip ønsker at følges i prosjektet. Dette kapittelet gir en oversikt over hvilke dokumenter som er planlagt produsert, hvilke formater de skal leveres i, og hvilke krav for gjennomgang som skal gjøres.

## Krav til dokumentasjon

All dokumentasjon skal være detaljert, godt strukturert og tilgjengelig for interessenter. Følgende dokumenter skal produseres i prosjektperioden:

Dokumenter:

* Forstudierapport:
  + Ferdigstilles: Uke 9
  + Format: .pdf
* GanttDiagram:
  + Ferdigstilles: Uke 9
  + Format: .py .png
* Prosjektrapport:
  + Ferdigstilles: Uke 21
  + Format: .pdf
  + Med vedlegg:
    - Timeliste
      * Format: .pdf
    - Møteinnkallinger
      * Format: .png
    - Tegninger/ diagrammer som systemarkitektur og sertifikathåndtering
      * Format: Format: .png .svg eller pdf
    - Linker
      * Format: pdf
    - Script program
      * Format: Usikker på ferdig resultat kan bli bash script, python. .sh/.py
    - Sluttbrukerveiledning som beskriver hvordan løsningen kan brukes og vedlikeholdes
      * Format: .pdf
* Github
  + Ferdigstilles: Uke 21
  + Alle dokumenter fra prosjektet
  + Format: .md, .pdf .svg .png .sh .py

All dokumentasjon skal publiseres på GitHub for å sikre enkel tilgang og deling med eksterne interessenter. I tillegg til tekniske spesifikasjoner skal det utarbeides en testdokumentasjon som beskriver testmiljø, testprosedyrer og resultater. Dokumentene skal gjennomgås og revideres for å sikre at de oppfyller krav til kvalitet og fullstendighet.

## Krav til kvalitetsgjennomganger

For å sikre at prosjektet leverer en stabil og god løsning, skal det gjennomføres kvalitetsgjennomganger i flere faser. Kvalitetsgjennomgangene skal sikre at løsningen oppfyller spesifikasjonene, at dokumentasjonen er fullstendig, og at prosjektet holder seg innenfor rammene av etablerte standarder.

Følgende kvalitetsgjennomganger vil bli utført:

* Samtaler med veileder
  + Regelmessige møter for å evaluere fremdriften og sikre at prosjektet følger planlagt kurs.
* Tekniske gjennomganger
  + Jevnlige evalueringer med eksperter fra Storm Elektro og WAGO Norge for å sikre at løsningen er kompatibel med bransjestandarder og krav.
* Dokumentasjonsgjennomgang
  + Prosjektets dokumentasjon vil bli gjennomgått for å sikre at den er klar, korrekt og følger gjeldende krav og retningslinjer.
* Sluttvurdering og verifikasjon
  + En endelig kvalitetsgjennomgang før implementering for å verifisere at alle spesifikasjoner og krav er oppfylt. Dette inkluderer testing av funksjonalitet, sikkerhet og brukervennlighet.

## Krav til standarder og metoder

A diagram of a computer process

AI-generated content may be incorrect.Prosjektet vil følge flere etablerte standarder og metoder for utvikling, dokumentasjon og kvalitetssikring. Dette skal sikrer at løsningen er i samsvar med industripraksis og kan brukes i eksisterende systemer uten store tilpasninger.

* OPC UA-standarder
  + OPC UA spesifikasjoner fra OPC Foundation skal brukes som grunnlag for sikker kommunikasjon og sertifikathåndtering. Denne standarden
  + Spesifikke deler av standarden som omhandler autentisering, kryptering og sertifikathåndtering vil være sentrale.
  + Figur viser kommunikasjon imellom OPC UA server og OPC UA klient.

<https://www.opc-router.com/what-is-opc-ua/>

[figur 9 OPC UA Client/Server]

* PKI (Public Key Infrastructure)
  + Prosjektet vil følge retningslinjer for PKI for å sikre korrekt sertifikathåndtering, herunder generering, fornyelse og tilbakekalling av sertifikater.

A diagram of a key system

AI-generated content may be incorrect.

Prosessen for opprettelse av sertifikater er basert på asymmetrisk kryptering og fungerer som følger:

* En privat nøkkel opprettes, og den tilhørende offentlige nøkkelen beregnes.
* Sertifikatutstederen (CA) ber om identifiserende attributter fra eieren av den private nøkkelen og verifiserer denne informasjonen.
* Den offentlige nøkkelen og identifiserende attributter kodes inn i en Certificate Signing Request (CSR).
* CSR signeres av eieren av den private nøkkelen for å bevise eierskap til nøkkelen.
* Den utstedende CA-en validerer forespørselen og signerer sertifikatet med sin egen private nøkkel.

<https://www.keyfactor.com/education-center/what-is-pki/>

[figure 10 Sertifikat håndtering]

* Utviklingsmetoder
  + Prosjektet vil bli utviklet stegvis med testing av forskjellige løsninger og evaluering for å finne den beste metoden.
  + Best practices for sikkerhet: Løsningen vil implementeres med fokus på sikkerhetsprinsipper for å sikre robusthet og pålitelighet.
* Dokumentmaler og verktøy
  + Alle dokumenter vil skrives i Microsoft Word og eksporteres til pdf.
  + Diagrammer, flytskjemaer og systemarkitekturen vil bli laget i affinity designer 2. Filene blir eksportert i svg. .png .pdf etter hva det skal brukes til og enkel tilgjenglighet for leseren
  + Jeg lagde et enkelt Python skript for å visualisere et Gantt-diagram som viser fremdriftsplanen. Skript i .py fil, bilde i .png. Lagt inn i forstudierapporten.
  + Skript og testing mot PLS vil bruke, ssh, bash, vi, nano, vscode og andre terminalprogrammer.
  + Verktøy for OPC UA og PLS-programmering.
    - UaExpert: Dette er et avansert verktøy for å overvåke og feilsøke OPC UA-kommunikasjon. Det lar brukeren inspisere dataoverføringer, sertifikater og sikkerhetsinnstillinger for å sikre riktig implementering av OPC UA.
    - CODESYS 3.5: Et kraftig utviklingsmiljø for programmering av PLS-er (Programmerbare Logiske Styringer). CODESYS 3.5 støtter OPC UA og gir mulighet for integrasjon av industrielle kommunikasjonsprotokoller, inkludert sikkerhet og sertifikathåndtering.

## Verktøy

* Kommunikasjons verktøy
  + Outlook
  + Discord
  + Teams
* Gantt
  + Python
* Dokumentasjon/rapport
  + Microsoft Word
* Diagrammer, flytskjemaer og systemarkitekturen
  + Affinity designer 2
* Terminal linux
  + Bash
  + Ssh
  + Nano
  + VI
  + VSCode
* OPC UA program og PLS program
  + Uaexpert
  + Codesys 3.5

Retningslinjene og standardene skal sikrer at prosjektet blir godt dokumentert og at løsningen blir så godt dokumentert at andre kan bruke det videre.

## Endringshåndtering

Trinn ved endringshåndtering

1. dokumenter endringens innhold
2. analyser konsekvensene for prosjektet
3. beregne eventuell kost/nytte
4. godkjennelse og aksept
5. logg endringen
6. juster planene
7. informer interessentene
8. gjennomfør endringen

# Prosjektorganisering

* **Prosjektleder**: Espen Klippenberg Bø.
* **Oppdragsgiver**: Storm Elektro AS, v/Erling Berg Johansen.
* **Ressurspersoner**: WAGO Norge, **Thomas Sandberg**.
* **Veileder**: TISIP fagskole v/Aleksander Tandberg. Wago Norge v/Thomas Sandberg.

# Anbefaling om videre arbeid

Etter en gjennomgang av prosjektet, anbefaler jeg å fortsette arbeidet med å utvikle og dokumentere en enkel og brukervennlig løsning for automatisk sertifikathåndtering i OPC UA-baserte byggautomasjonsanlegg. Prosjektet viser at det er fordeler ved å automatisere denne prosessen, både i form av økt sikkerhet, redusert risiko for driftsstans og mer effektiv drift av anleggene.

Videre arbeid bør ha følgende fokusområder:

Videreutvikling og testing av løsningen: Løsningen må utvikles og testes grundig i et testmiljø.

Enkelt og brukervennlig: Sertifikathåndteringen bør gjøres så enkel og automatisert som mulig, sånn at den kan brukes ut uten omfattende manuelle tilpasninger.

Evaluering av skalerbarhet: Løsningen bør testes for å vurdere hvordan den kan tilpasses større installasjoner med flere bygg og ulike systemleverandører.

Samarbeid med industripartnere: Videre samarbeid med aktører som Storm Elektro og WAGO Norge er viktig for å sikre at løsningen gir praktiske verdi og kan brukes i produksjon.

Prosjektet kan utvikle en skalerbar, sikker og praktisk løsning som kan som forbedrer sertifikathåndteringen i OPC UA-anlegg. Dette vil ikke bare gi fordeler for de aktuelle anleggene, men også kunne fungere som en modell for fremtidige automatiseringsløsninger i byggautomasjon.

# Referanser

1. OPC Foundation – OPC UA Specification
   * Kilde: <https://reference.opcfoundation.org/>
   * Beskrivelse: OPC UA-spesifikasjonen.
2. OPC Foundation – OPC UA Specification Part 2: Security Model
   * Kilde: <https://reference.opcfoundation.org/Core/Part2/v105/docs/>
   * Beskrivelse: OPC UA-spesifikasjonen som beskriver sikkerhetsmodellen, inkludert autentisering, kryptering og sertifikathåndtering.
3. A Beginner’s Guide to OPC
   * Kilde: <https://opcconnect.opcfoundation.org/2017/12/a-beginners-guide-to-opc/>
   * Beskrivelse: Grunnlegende informasjon om hva OPC UA er og hvordan det kan brukes.
4. WAGO Norge
   * Kilde: <https://www.wago.com/no>
   * Beskrivelse: Informasjon om PLS-er og automasjonssystemer som brukes i testmiljøet for dette prosjektet.
5. Keyfactor – Public Key Infrastructure (PKI)
   * Kilde: <https://www.keyfactor.com/education-center/what-is-pki/>
   * Beskrivelse: En guide til hvordan PKI fungerer, inkludert sertifikathåndtering, signering og autentisering.
6. OPC Router – What is OPC UA?
   * Kilde: <https://www.opc-router.com/what-is-opc-ua/>
   * Beskrivelse: Grunnleggende forklaring av OPC UA-protokollen, dens bruksområder og fordeler.
7. Let's Encrypt – Automatisert sertifikathåndtering
   * Kilde: <https://letsencrypt.org/>
   * Beskrivelse: Informasjon om gratis og automatisert sertifikathåndtering for sikker autentisering og kryptering.
8. Stuxnet og cybersikkerhet i industrielle kontrollsystemer
   * Kilde: <https://en.wikipedia.org/wiki/Stuxnet>
   * Beskrivelse: En analyse av hvordan Stuxnet påvirket sikkerhetskravene til industrielle kontrollsystemer, inkludert OPC UA og byggautomasjon.
9. OPC UA Security Model for Administrators

* Kilde: OPC UA Security Model for Administrators V1.00
* <https://opcfoundation.org/wp-content/uploads/2014/05/OPC-UA_Security_Model_for_Administrators_V1.00.pdf>
* Beskrivelse: En teknisk gjennomgang av sikkerhetsmekanismene i OPC UA, inkludert håndtering av sertifikater, tilgangskontroll og datakryptering.