Vedlegg 1 – HAN Personvern – et tillegg til utredningen «AMS + HAN – om å gjøre sanntid måledata tilgjengelig for forbruker»

LILLEAKER 10.OKTOBER 2017

NORSK ELEKTROTEKNISK KOMITE – LARS IHLER

Oppsummering og konklusjon

Når forbruker ber om å få åpnet HAN-porten for lesing av egne forbruksdata skal nettselskapet informere kunden om at ved åpning vil tilstrekkelig personvern sikres ved at

- nettselskapet tilbyr kryptering av data på HAN-porten eller
- at kunden selv bekrefter at tilstrekkelig fysisk sikring av målerens HAN-port er tilstede, dog skal nettselskapet som et første tiltak sikre utvendige og felles skap med lås og mulighet for installasjon av egen lås, i henhold til NEK 399

I begge tilfeller skal nettselskapet vurdere om øvrige åpne grensesnitt i AMS-måleren skal skrus av, forutsatt at kunden selv ikke har behov for tilgang til dem.

Innholdsfortegnelse

AMS-HAN – hvordan oppnå tilfredsstillende personvern?

Bakgrunn

Som en videreføring av rapporten «AMS – HAN utredning NEK 20150122» har NEK på oppdrag fra NVE utarbeidet beskrivelse og retningslinjer for håndtering av personvern ved bruk av AMS-målerens HAN-port. Denne beskrivelsen er et vedlegg til den opprinnelige utredningen fra 20150122.

NEK, NVE og Datatilsynet har hatt en dialog med flere møter og samtaler om muligheter og begrensninger i personvernet knyttet til bruk av AMS-målerens HAN-port. Målerleverandørene og representanter for nettselskapene har bidratt, og beskrivelsen representerer således løsninger som tilfredsstiller alle parter.

Begrunnelse fra Datatilsynet

Det understrekes at alle kunder, i henhold til avregningsforskriften, skal kunne be om tilgang til relevant informasjon om eget forbruk gjennom AMS-målerens HAN-port. Sikkerheten i grensesnittet skal ifølge NEKs opprinnelige anbefaling baseres på NEK IEC 62056-7-5. Videre skal grensesnittet være inaktivt ved installasjon. Kundene bestemmer selv om og når grensesnittet skal benyttes.

NVEs brev av 27.juni 2016 beskriver hvilken informasjon om eget forbruk som nettselskapet skal gjøre tilgjengelig på HAN-porten om og når forbrukeren ber om det. Selv om AMS-målerne også har andre grensesnitt, så er det HAN-porten denne beskrivelsen angår. HAN-porten vil kunne gi raskere og mer tidsriktig informasjon om strømforbruket enn det som blir tilgjengelig via ElHub.

Personopplysningsloven og personopplysningsforskriften stiller krav til informasjonssikkerhet og tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig. Informasjonen om strømforbruket er ikke sensitive personopplysninger, men trenger en viss beskyttelse. Enten via fysisk beskyttelse eller kryptering. I tilfeller der måleren er plassert utenfor boligen vil fysisk beskyttelse kunne være vanskelig å få til, siden informasjonen fra HAN-porten i alle fall skal ut av det skap eller rom måleren står i. Dette gjelder også ved overføring via ukryptert trådløs overføring.

Datatilsynet skriver i brev, datert 16.06.2017:

«Over HAN-grensesnittet utleveres løpende informasjon om strømforbruket i en husstand.

Informasjonen gitt over HAN-grensesnittet er å anse som personopplysninger siden de forteller noe om den enkelte, jf personopplysningsloven § 2 punkt 1. Med innføringen av AMS, går man til en løsning hvor det nå kan kommuniseres personopplysninger via et grensesnitt som ikke fantes før.»

«De dataene som leveres over HAN grensesnittet er ikke sensitive personopplysninger, men er heller personopplysninger som trenger en viss beskyttelse om det så er via fysisk beskyttelse eller kryptering.»

«For å tilfredsstille kravet til informasjonssikkerhet i personopplysningslovens § 13 og sikring av konfidensialitet i personopplysningsforskriftens § 2-11 er beskyttelse nødvendig. Denne beskyttelse kan enklest ivaretas ved å følge NEKs forslag til løsning på hvordan man oppnår tilfredsstillende personvern for AMS-HAN. Løsningen går på at kunden selv ber om at datastrøm blir aktivert og at kunden selv velger om datastrømmen skal være kryptert.»

Datatilsynet presiserer i et senere brev, datert 18.09.2017, at ved fysisk sikring «må det også tas hensyn til innebygd personvern, slik at sikkerheten på en enkel måte kan ivaretas.»

Leverandørenes innspill

De tre leverandørene Aidon, Kaifa og Kamstrup er alle innstilt på å kunne levere data på kryptert form på HAN-porten dersom dette skulle bli et krav. Kaifa-målerne er allerede forberedt i henhold til NEK IEC 62056-7-5. Kamstrups målere krypterer på alle grensesnitt og kan tilpasses samme standard. Aidon bekrefter at de vil kunne kryptere i henhold til NEK IEC 62056-7-5 dersom kravet om kryptering gjøres gjeldende.

Det finnes forskjellige krypteringsalgoritmer og Kaifa ytret ønske om bruk av nøkler som krypteres i henhold til det symmetriske krypteringssystemet AES 128. Aktuelle krypteringsalgoritmer er beskrevet nærmere i NEK ISO/IEC 18033-serien, og spesielt beskrives AES 128 i NEK ISO/IEC 18033-3:2010.

Leverandørene bekrefter at alle nødvendige endringer i målerne som følge av et krav om kryptering kun vil dreie seg om oppdatering av programvare. All programvare lastes ned via kommunikasjonsgrensesnittet som nettselskapene benytter for avlesing av kWh-verdier.

Alle leverandørene er av den oppfatning at de største kostnadene med kryptering vil knytte seg til infrastrukturen for håndtering av krypteringsnøkler og kundenes aksept for åpning av HAN-porten. Man kan tenke seg flere modeller for denne infrastrukturen, for eksempel en sentral løsning som forvalter alle kunder, med deres aksepter, og om data på HAN-porten skal krypteres eller ikke. Alternativt kan nettselskapet selv forvalte infrastrukturen. Ved kryptering må systemet også lagre informasjon om krypteringsnøkler.

Et løsningsalternativ med fysisk sikring av måleren innebærer ingen ekstra tilpasninger eller tillegg fra målerleverandørenes side.

Ansvarsforhold

Grensesnittet mellom nettselskap og kunde er klart definert i den første «AMS – HAN utredningen» og i denne forbindelsen er det viktig å gjenta at data som kommer ut av HAN-porten er kundens. Det er også kundens ansvar hva som skjer med dataene videre. Dersom tredjepart skal bearbeide dataene videre må kunden sørge for at det inngås tilfredsstillende avtale om den videre databehandlingen hos tredjepart. Dette gjelder uavhengig av kryptering eller ikke. Dersom data fra HAN-porten er kryptert må tredjepart få tilgang til krypteringsnøkkel før forbruksdata kan bearbeides.

Dersom kunden ønsker å aktivere ukrypterte data på HAN-porten skal nettselskapet be kunden om en bekreftelse på at AMS-måleren og HAN-porten er fysisk sikret. Enten ved at måleren er i kundens bolig eller ved at den er fysisk sikret i eget eller felles skap utenfor eierens bolig. Merk at det er nettselskapets ansvar at utvendige og felles skap minimum er låsbare i henhold til NEK 399 for sikring av HAN-porten. Det tilrådes samme sikring for alle skap, også de som er bygget før NEK 399 ble gjort gjeldende i 2014. I det tilfelle at kunden selv bekrefter at tilstrekkelig fysisk sikring er tilstede kan nettselskapet velge å åpne HAN-porten uten selv å foreta fysisk sikring.

Nettselskapet bør vurdere å skru av AMS-målerens øvrige åpne grensesnitt, som display og lysdiode, når HAN-porten åpnes, forutsatt at kunden selv ikke har behov for tilgang til dem. Kunden vil nå få full tilgang på data som tidligere bare kunne leses i display og/eller ved avlesing av blinkende lysdiode.

Løsningsalternativ A – informasjonssikkerhet ved kryptering

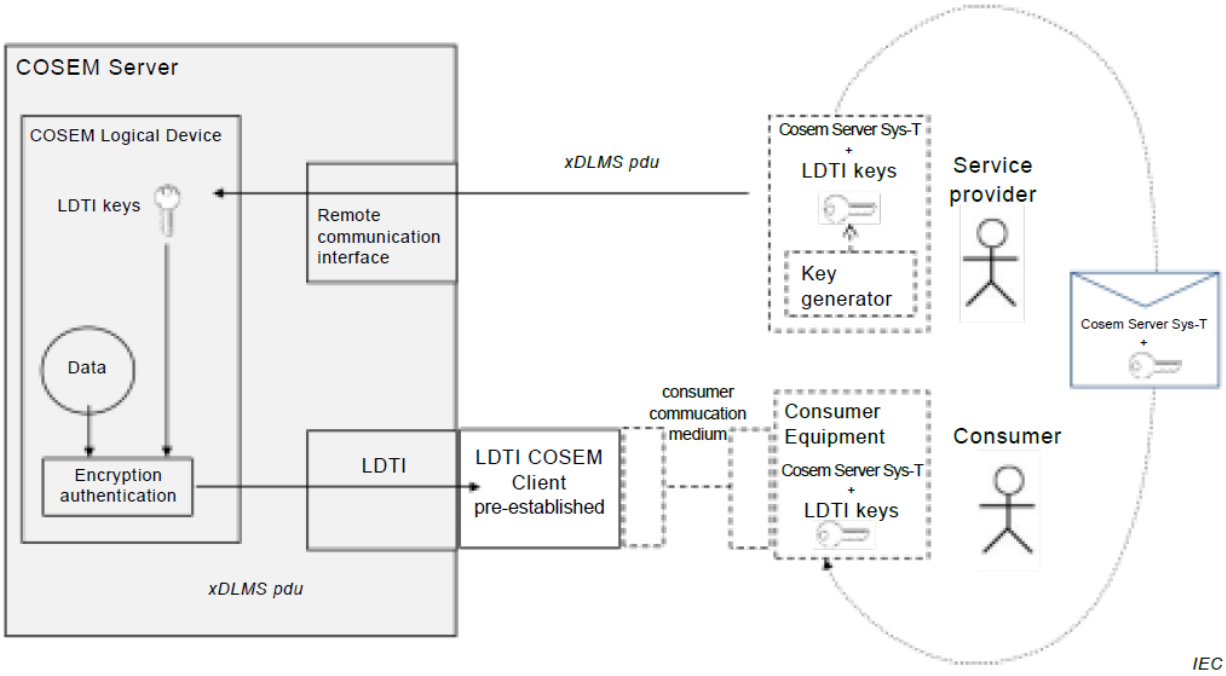
NEKs forslag til løsning på åpning og aktivering av HAN-port med kryptering oppsummeres som følger:

Forbruker må logge seg på kundeside og be om aktivering av datastrøm som vil føre til at krypteringsnøkkel (passord) vil bli sendt til valgt måler.

Forbruker får utdelt nøkkel for dekryptering (passord), enten på kundesiden eller ved at den vil bli sendt på SMS, e-post eller tilsvarende.

Dekrypteringsnøkkel (passord) må legges inn i enhet som skal lese datastrøm (HAN-enhet).

Løsningen er i tråd med beskrivelsen i NEK IEC 62056-7-5, slik figuren nedenfor skisserer.



I figuren tilsvarer COSEM Server den sentrale programvaren i AMS-måleren og LDTI er Local Data Transmission Interface, eller HAN-porten i AMS-måleren. Øvrige forkortelser og begreper er beskrevet i eget tillegg.

For ordens skyld gjentas data som skal strømmes på HAN-porten så snart den er åpnet. Dette er beskrevet i detalj i brev fra NVE, datert 27.09.2016, ref 2016603500-6.

Frekvens = 2,5 sekund (*)

- Aktiv effekt (kW) (= import)

Frekvens = 10 sekunder

- OBIS liste versjon, Måler ID og målertype
- Aktiv effekt (kW) x 2 (= import og eksport)

- Reaktiv effekt (kVAr) x 2
- Strøm (A) x 3 (L1, L2 og L3)
- Spenning (V) x 3 (alle faser)

Frekvens = 1 time

- Aktiv energi (kWh) x 2 (= import og eksport)
- Reaktiv energi (kVArh) x 2
- Klokke og dato

(*) Frekvensen for uttak av aktiv effekt kan endres til maksimalt 10 sekunder om det foreligger begrensninger som hindrer en høyere oppdateringsfrekvens.

Valg av krypteringsalgoritme

Siden dataene som skal krypteres har fast lengde, benyttes et synkront krypteringssystem. Algoritmen AES-128, Advanced Encryption Standard med blokkstørrelse på 128 bit, skal anvendes. Både målerleverandører som skal kryptere og tredjepartsleverandører som skal dekryptere må forholde seg til denne algoritmen. Mer her: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

Algoritmen beskrives i NEK ISO/IEC 18033-3:2010.

Administrasjon av kunder, kundeaksepter og krypteringsnøkler

Under skisseres en mulig løsning for administrasjon av kundenes åpning av HAN-porten og tilhørende krypteringsnøkler. Merk at krypteringsnøkkel for HAN-porten skal være unik for HAN-porten. Den skal således ikke kunne benyttes for andre grensesnitt i AMS-måleren. Rapporten tar ikke stilling til hvem som skal tilby disse tjenestene, men enkelte nettselskap har allerede en løsning på plass.

Tjenestetilbyder/HAN-sentral som vist i figuren over skal i denne sammenhengen kunne betjene følgende funksjoner (use cases):

- Kunden skal kunne logge seg inn på «Minside» og få tilgang til sine målepunkter
- Alle endringer skal varsles på sms/epost.
- Hvert målepunkt identifiseres ved Målepunkt ID og har som et minimum informasjon om
    - HAN-port status = Åpen/Lukket
    - Krypteringsnøkkel/passord
    - Dato/tidspunkt for sist nedlastede nøkkel
- Kunden skal kunne åpne/lukke HAN-port. Ved «Åpne» genereres krypteringsnøkkel. For håndtering og generering av nøkler vises det til standarden NEK IEC 62351-9 «Cyber security key management for power system equipment»
- Dato/tidspunkt for aktivering/nedlasting må kunne velges. Melding med nøkkel sendes Nettselskap når tiden er moden.
- Kunden skal kunne be om generering av ny nøkkel. Dato/tidspunkt for aktivering/nedlasting må kunne velges. Melding med nøkkel sendes Nettselskap for aktivering/nedlasting til kundens måler når tiden er moden.
- Ved bytte av måler eller når kunde flytter må håndtering av HAN-porten tas inn i eksisterende prosesser der Nettselskap og ElHub er involvert i dag. HAN-porten må skrus av når kunde flytter og HAN-portens status må videreføres ved målerbytte.

Nettselskap skal i denne sammenhengen utføre disse funksjonene:

- Kundens HAN-port skal kun åpnes/lukkes basert på melding med krypteringsnøkkel fra tjenestetilbyder/HAN-sentral.

HAN-sentral må ha grunnlagsdata om målere, kunder og nettselskap. Kundene må tilbys et enkelt grensesnitt for administrasjon av sine målere.

Løsningsalternativ B – informasjonssikkerhet ved fysisk sikring

NEKs forslag til løsning for fysisk sikring av AMS-måleren kan benyttes i de tilfellene der kryptering ikke er tilgjengelig fra nettselskapets side, eller at kunden selv har valgt ukryptert datastrøm. I tilfellene der datastrømmen er kryptert og øvrige åpne grensesnitt på måleren skrus av, er det ikke nødvendig med fysisk sikring utover den som allerede er tilstede for å sikre personvern av data over HAN-porten.

Dersom nettselskapet ikke tilbyr kryptering av datastrømmen på HAN-porten skal selskapet sørge for at fysisk sikring er tilstede. Fysisk sikring i tilfelle kunden selv velger å motta ukrypterte data via HAN-porten, selv om nettselskapet tilbyr kryptering, er kundens ansvar. Her må kunden bekrefte at måleren er plassert i adgangskontrollert område, og dermed fysisk sikret, før HAN-porten kan åpnes.

I 2014 kom standarden «NEK 399 Tilknytningspunkt for el- og ekomnett». Anlegg som er bygget etter denne standarden er godt forberedt for tilstrekkelig fysisk sikring av tilhørende målere. Alle tilknytningsskap som er bygget etter NEK 399 vil kun være tilgjengelig for bygningseier, boligeiere, elnett- og ekomnetteiere med trekantnøkkel forskjellig fra nøkler som brukes til kabelskap. I tilfeller med fellesskap kan bygningseier låse tilknytningsskap med egen nøkkel for å sikre egne målerdata og sikre uautorisert tilgang. Som et siste tiltak skal det kunne ettermonteres et låsbart deksel for hver enkelt elmåler.

Når AMS-målernes HAN-porter åpnes vil mindretallet av målerne i Norge være installert i skap som er bygget etter NEK 399. Skap som ikke er bygget i henhold til NEK 399 vil ha forskjellige behov for løsninger til sikring av HAN-porten.

NEKs tilrådning er at det i alle tilfeller med utvendige og felles tilknytningsskap foretas en oppgradering slik at låsing er i tråd med NEK 399. I skrivende stund pågår utarbeidelse av NEK 399:2017, og her har det kommet innspill om at låsing bør skje med bruk av systemnøkkel. Dersom dette blir endelig krav i NEK 399 anbefaler vi tilsvarende tiltak for fysisk sikring av HAN-porten.

Ved trådløs overføring mellom skap og bolig tilrådes kryptering for tilstrekkelig sikring.

Fordeler og ulemper med de to løsningene

Tabellen under lister noen sentrale og viktige punkter til hjelp i vurderingen av hvilken løsning som er best egnet.

Løsning	**Fordel**		**Ulempe**
Kryptering av data på HAN-port	Tilfredsstillende personvern av forbruksdata		Tilgang på tjenester kan i en oppstartsperiode bli mindre enn ønsket
	Vern av øvrige data som strømmes på HAN-porten, også fremtidige		Kostnader

	Ikke behov for fysisk sikring av HAN-porten utover eksisterende sikring		
	Ikke behov for kryptering fra kundens side		
Fysisk sikring av HAN-port ved låsing av utvendige og felles skap	Tilfredsstillende personvern av forbruksdata		Kan medføre behov for kryptering av kommunikasjon fra HAN-port i fellesskap til bolig
	Vern av øvrige data som strømmes på HAN-porten, også fremtidige		Skap må ha nok plass til å kunne plassere trådløs ruter og/eller eventuelt krypteringsutstyr til alle målerne i skapet
	Ikke behov for kryptering fra nettselskapets side		Kostnader
	De to grensesnittene optisk port og display beskyttes like godt som HAN-porten		Oppgradering av gamle utvendige og felles skap er påkrevet

Kost-nytte analyse

Som en del av denne utredningen er det foretatt en kost-nytte analyse, basert på risiko og tiltak for reduksjon av risiko i de anbefalte løsningsalternativene.

Løsningsalternativ A, kryptering, vil i svært varierende grad medføre ekstra kostnader for nettselskapene. Innhentede data viser at for selskap som ikke har noen løsning på plass kan kostnadene beløpe seg til ca. kr. 10 pr anlegg, forutsatt at kostnadene fordeles på samtlige kunder.

Nytten av dette tiltaket er god, forutsatt at kunden ikke installerer en løsning som dekrypterer data i utvendige eller felles skap før videre trådløs eller åpen kommunikasjon, samt at nettselskapet kan deaktivere øvrige åpne grensesnitt i måleren. Nytten er på den annen side ikke så god hvis markedet i hovedsak tilbyr dataoverføringsløsninger med kryptert eller på annen måte tilstrekkelig beskyttet kommunikasjon. Her vil det i de fleste tilfellene være unødvendig med kryptering på HAN-porten.

Løsningsalternativ B, fysisk sikring ved lås av utvendige og felles skap, medfører ekstra kostnader som antas å ligge i samme størrelsesorden som for løsningsalternativ A, men er ikke verifisert.

Nytten ved dette tiltaket er god i og med at alle målerne og deres grensesnitt i skapet blir låst, men forutsetter at kunden selv installerer utstyr som krypterer data før videre trådløs eller åpen kommunikasjon.

Referanser/Kilder

1. AMS – HAN utredning NEK 20150122
2. NEK IEC 62056-7-5
3. NVEs brev av 27.06.2016

4. Avregningsforskriften
5. Personopplysningsloven
6. NEK ISO/IEC 18033-3:2010
7. NVEs brev av 27.09.2016, ref. 2016603500-6
8. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
9. NEK IEC 62351-9
10. NEK 399 Tilknytningspunkt for el- og ekomnett