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

LILLEAKER 15.FEBRUAR 2018

NORSK ELEKTROTEKNISK KOMITE

Oppsummering og konklusjon

Når forbruker ber om å få åpnet HAN-porten for lesing av egne forbruksdata bør nettselskapet informere kunden om at ved åpning vil kundens data beskyttes enten ved at

- nettselskapet velger å tilby kryptering av data på HAN-porten eller
- at nettselskapet ber kunden om en bekreftelse på at tilstrekkelig fysisk sikring av målerens HAN-port er tilstede, enten ved at måleren er i kundens egen bolig eller at den står i et låsbart skap eller rom, eventuelt i låsbare fellesskap eller fellesrom sammen med andre kunders målere. Låsing med bruk av nøkkel nr. 20, trekantnøkkel som ikke kan anvendes i kabelskap eller tilsvarende er minimum nivå av tilstrekkelig sikring. Dersom fysisk sikring ikke er tilstede, vil nettselskapet være ansvarlig for å etablere dette.

Dersom kunden selv velger å motta ukrypterte data via HAN-porten, selv om nettselskapet tilbyr kryptering, er kunden ansvarlig for fysisk sikring. Nettselskapene kan av praktiske grunner velge å la en tredjepart utføre arbeidet med administrasjon av kundeaksepter og forvaltning av krypteringsnøkler. Eksempler på tredjeparter er strømleverandører og driftspartnere.

Innholdsfortegnelse

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 rapporten 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 disse partene.

Etter høringsrunde som ble avsluttet i november 2017 er flere endringer og presiseringer tatt inn. De viktigste presiseringene har med ansvarsforhold å gjøre.

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. Vi viser til NVEs brev av 27. juni 2016 for en nærmere vurdering av dette. Sikkerheten i grensesnittet bør 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 rapporten angår. HAN-porten vil kunne gi raskere og mer kontinuerlig informasjon om strømforbruket enn det som blir tilgjengelig via Elhub.

Måleverdier om strømforbruk er å anse som personopplysninger. 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.»

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, Nuri/Kaifa og Kamstrup er alle innstilt på å kunne levere data på kryptert form på HAN-porten dersom dette skulle bli et krav. Nuri/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 Nuri/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 har bekreftet 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 bør krypteres eller ikke. Alternativt kan eksempelvis strømleverandøren, nettselskapet eller driftsoperatør 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. Da har kunden dataene selv og de er derfor ikke lenger regulert under personopplysningsloven. Selve grensesnittet er imidlertid nettselskapets ansvar. Dersom kunden ønsker å dele dataene med en tredjepart er det opp til kunden hvordan dette gjøres. Dette gjelder uavhengig av kryptering eller ikke. Dersom data fra HAN-porten er kryptert må krypteringsnøkkel registreres i utstyr fra kunden eller tredjepart før forbruksdata kan bearbeides.

Fra et elsikkerhetsperspektiv er boligeier ansvarlig for sikring av skap. Fra et personvernperspektiv er nettselskapet ansvarlig for å sikre data i måler, inklusive grensesnitt.

Datatilsynet har ikke et krav om at kunden skal kunne sikre måler med egen lås. Dersom en kunde anskaffer egen lås for å øke sikkerhetsnivået må denne dekkes av kunden. Andre aktører med behov må fortsatt ha tilgang.

Alle målere skal i utgangspunktet av elsikkerhetshensyn være fysisk sikret i kundenes låsbare skap eller rom. Ved åpning av HAN-porten kan det likevel vise seg at sikring ikke er tilfredsstillende.

Dersom kunden ønsker å aktivere HAN-porten og nettselskapet ikke tilbyr krypterte data, bør nettselskapet be kunden om en bekreftelse på at AMS-måleren og HAN-porten er fysisk sikret før porten kan åpnes. Enten ved at måleren er i kundens bolig eller ved at den er fysisk sikret i eget eller felles låsbart skap utenfor eierens bolig. I siste instans bør det likevel være nettselskapets ansvar å verifisere eller etablere sikring hvis kunden ikke gjør det.

Dersom kunden selv velger å motta ukrypterte data via HAN-porten, selv om nettselskapet tilbyr kryptering, er kunden ansvarlig for fysisk sikring. Her må kunden bekrefte at måleren er plassert i adgangskontrollert område, og dermed fysisk sikret, før HAN-porten kan åpnes.

Dersom det må etableres fysisk sikring så anbefales låsing i henhold til NEK 399-1:2014.

Nettselskapet bør i alle tilfeller sørge for at nødvendig infrastruktur for håndtering av kundenes aksept og eventuell forvaltning av krypteringsnøkler ivaretas. Enten ved at nettselskapet selv, strømleverandør, driftsoperatør eller annen tredjepart tilbyr løsning. En naturlig følge av dette vil være at de utførende partene også vil ivareta kundesupport for håndtering av aksepter og eventuelle krypteringsnøkler for HAN-porten.

Informasjon til kunde

Nettselskapene bør på en lettfattelig måte informere kundene om muligheter, begrensninger og ansvarsforhold som gjør seg gjeldende ved åpning og bruk av HAN-porten I tillegg bør nettselskapene informere om at de er ansvarlig for at det benyttes fysisk eller logisk sikring (sistnevnte ved kryptering)». Vi anbefaler at det som et minimum informeres om:

- Hvilke data som strømmes på HAN-porten
- At det er kunden selv som eier data som strømmes ut HAN-porten
- At data om forbruk anses som personopplysninger som trenger en viss beskyttelse
- At kunden bør være bevisst på sikker dataoverføring fra HAN-porten, spesielt ved bruk av trådløs overføring. Wi-fi, Z-wave, Zigbee og Bluetooth kan eventuelt nevnes som eksempler på teknologier som gir tilstrekkelig sikring
- At det er kunden selv som har ansvaret for hvordan han/hun ønsker å behandle data fra HAN-porten videre
- At kunden bør ha et bevisst forhold til tredjeparts behandling av data fra HAN-porten hvis den leses av tjenester på internett eller i skyen
- Eventuell informasjon om tjenestetilbydere
- På hvilken måte nettselskapet sikrer personvernet og at kunden må bekrefte at måleren er fysisk sikret før HAN-porten kan åpnes hvis metode med fysisk sikring velges. Tilsvarende bekreftelse kreves hvis nettselskapet tilbyr kryptering og kunden likevel ønsker ukryptert datastrøm.

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 kundesiden hos selskapet som nettselskapet har satt til å forvalte krypteringsnøklene. Her ber kunden om aktivering av datastrøm som vil føre til at krypteringsnøkkel blir sendt til valgt måler.

Forbruker får utdelt nøkkel for dekryptering fortrinnsvis ved at nøkkelen sendes elektronisk direkte til kundens tredjeparts utstyr. Tredjepartsutstyret kobles til slutt til kundens HAN-port. Dekrypteringsnøkkelen må alternativt legges inn manuelt i enhet som skal lese datastrømmen fra HAN-porten.

Løsningen er i tråd med beskrivelsen i NEKs anbefaling fra 2014 (ver 2) og NEK IEC 62056-7-5, med mediaspesifikk kommunikasjonsprofil i henhold til Annex D.

Sikkerhetsløsningen er i henhold til DLMS Security suite 0 (symmetriske nøkler), også nærmere beskrevet i NEK IEC 62056 serien og DLMS UA Coloured books.

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, bør 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 bør være unik for HAN-porten. Den bør således ikke kunne benyttes for andre grensesnitt i AMS-måleren. Krypteringsnøklene bør deles på en måte som er passende for maskinlesing.

Rapporten tar ikke stilling til hvem som skal tilby disse tjenestene, men eksempelvis har enkelte nettselskap allerede en løsning på plass. Tilbyder kan være nettselskapet selv, strømleverandør, driftsoperatør, eller annen tredjepart.

Tjenestetilbyder/HAN-sentral bør i denne sammenhengen kunne betjene følgende funksjoner (use cases):

- Kunden bør kunne identifisere seg på tjenestetilbyderens nettside og få tilgang til sine målepunkter
- Alle endringer bør 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.
- Dato/tidspunkt for aktivering/nedlasting av nøkkel må kunne velges. Tjenestetilbyder sørger for sikker aktivering/overføring til måler og tredjeparts utstyr hos kunden.
- Kunden bør kunne be om generering av ny nøkkel.
- Ved bytte av måler eller når kunde flytter bør håndtering av HAN-porten tas inn i eksisterende prosesser, herunder: HAN-porten må skrus av når kunde flytter og HAN-portens status må videreføres ved målerbytte.
  Kundens HAN-port bør kun åpnes/lukkes basert på melding fra tjenestetilbyder/HAN-sentral. Denne meldingen bør i størst mulig grad være lik for alle målere, men i mangel av et standard format og muligheter i de forskjellige målerne oppfordres bransjen til selv å søke en best mulig løsning her.

Tjenestetilbyder bør ha grunnlagsdata om målere, kunder og nettselskap. Kundene må tilbys et enkelt grensesnitt for administrasjon av sine målere.

Det er avgjørende å ivareta sikker transport av nøkler ved implementering av løsning. I tillegg bør det være enkelt for kundene å forholde seg til bruk av nøkler og nedlasting til tredjeparts utstyr.

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 er det ikke nødvendig med fysisk sikring utover den som allerede er tilstede.

Dersom nettselskapet ikke tilbyr kryptering av datastrømmen på HAN-porten bør selskapet be kunden om en bekreftelse på at fysisk sikring er tilstede. Kunden må bekrefte at måleren er plassert i adgangskontrollert område, og dermed fysisk sikret, før HAN-porten kan åpnes. Med adgangskontrollert

område forstås at det innenfor et begrenset område er et begrenset og kjent antall personer som har tilgang.

I 2014 kom standarden «NEK 399-1 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 399-1:2014 vil kun være tilgjengelig for bygningseier, boligeiere, elnett- og ekomnetteiere med nøkkel nr. 20, trekantnøkkel forskjellig fra nøkler som brukes til kabelskap eller tilsvarende.

Når AMS-målernes HAN-porter åpnes vil mindretallet av målerne i Norge være installert i skap som er bygget etter NEK 399-1:2014. Skap som ikke er bygget i henhold til NEK 399-1:2014 vil ha forskjellige behov for løsninger til sikring av HAN-porten.

NEKs tilrådning er at det i alle tilfeller med utvendige og fellesskap for målere foretas en oppgradering slik at låsing er i tråd med NEK 399-1:2014.

Det er i alle tilfeller med fysisk sikring viktig at nettselskapenes rett til fri adgang til måler sikres.

Ved trådløs overføring mellom skap og bolig tilrådes kryptering for tilstrekkelig sikring. Denne sikringen er det tredjeparts leverandør av utstyr som kan ha ansvaret for. Anerkjente og etablerte metoder som anses å gi tilstrekkelig sikring er blant andre wi-fi, Z-wave, Zigbee og Bluetooth.

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 at kunden må kryptere 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 kan være 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, vil kunne medføre totale ekstra kostnader i samme størrelsesorden som for kryptering. Her vil imidlertid kundene selv i større grad direkte måtte ta den ekstra kostnaden. Nytten er god ved 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. DLMS UA Coloured books
10. NEK 399-1:2014 Tilknytningspunkt for el- og ekomnett