2018

SECOND2 SecureMMS

Sikkerhedskoncept for DER

PROJEKT RAPPORT

FORSKEL NO. 2016-1-12400

English scope

SECOND2 shall develop new methods for Access Control and encrypted data communication - which are important elements in a renewable power system with distributed energy resources.

The partners in the project shall make a proof-of-concept for the basic concept of Attribute Based Access Control, to show the possibilities and challenges for the technology. New methods and improvements shall also be developed for the SecureMMS data protocol.

Document no.:	SECOND2 projektrapport
Author:	EURISCO og partnere i SECOND2 projektet
Last revision date:	2018-04-18

Vigtigt vedr. læsning af projektrapporten

Dette dokument er kun en opsummering af de resultater som er frembragt i SECOND2 projektet, så for at få den fulde indsigt og forståelse for projektet frembringelser – henvises til følgende tekniske rapporter på SECOND2 websiten.

- *SECOND2 SecureMMS*
- *SECOND2 ABAC*
- *SECOND2 Security Paper*
- *SECOND2 Security Review*

Dokumenter kan tilsendes via email ved at skrive til: caa@eurisco.dk

Indholdsfortegnelse

Introduktion til SECOND2 projektet

'SECOND2 – Security Concept for DER' er et FoU projekt delvist finansieret af ForskEL (projektnr. 2016-1-12400) og gennemført i peioden 1. marts 2016 til 1. april 2018.

SECOND2 projektets formål er forskning og videreudvikling af eksisterende teknologier for

- ABAC (Attribute Based Access Control)
- SecureMMS (IEC 62351-4) baseret datakommunikation.

Gennem arbejdet i CHPCOM projektet [ForskEL 12095] er et af resultaterne netop behovet for en forbedring af databeskyttelsen i SecureMMS. Kravene for denne forbedring er afstemt internationalt, men metoderne og sikkerhedstest af en praktisk implementering er en mangel i det internationale standardiseringsarbejde, som SECOND2 projektet har haft fokus på.

CHPCOM projektet benyttede også en teknologi for adgangskontrol kaldet RBAC (Role Based Access Control) og denne teknologi ønskes evalueret ift. et udvidet koncept kaldet ABAC (Attribute Based Access Control) – med specielt fokus på følgende elementer:

- ✓ Koblingen imellem ABAC Policy (klar tekst) og XACML (maskinlæsbar tekst) – er det praktisk muligt og hvordan?
- ✓ RBAC som den er defineret i IEC62351-8[1], er den fyldestgørende for fremtidens energisystemer med stort antal DER enheder?
- ✓ Opbygning af 'Proof-of-Concept for et ABAC system til efterprøvning af teknologierne i praksis og ikke mindst som beslutningsgrundlag for de grundlæggende afgræsninger i projektet.

SECOND2 er gennemført med EURISCO som den projektansvarlige virksomhed, samt i et partnerskab med ALS og DONG Energy. Alexandra Instituttet har været tilknyttet projektet som uvildig 3. part for test og sikkerhedsevaluering af det frembragte Proof-of-Concept.

Læs mere omkring SECOND2 projektet på: www.second2.dk

[1] http://iectc57.ucaiug.org/wg15public/default.aspx

Baggrund for ABAC

Adgangskontrol er et af hjørnestenene i datasikkerhed indenfor energisystemet generelt og specielt indenfor datakommunikation mellem distribuerede energiressourcer.

ABAC (Attribute Based Access Control) er en mulig løsning på udfordringen omkring koblingen mellem sikkerhedspolitikker (hvem må få adgang til hvad) og den rent praktisk opsætning og implementering af adgangskontrol for DER.

SECOND2 ønsker med udgangspunkt i en publikation fra NIST (National Institute of Standard and Technology [800-162]) at analysere behov og muligheder for ABAC i forhold til det danske energisystem.

Partnerne i projektet skal frembringe en eksperimentel sandsynliggørelse af muligheder og udfordringer ved ABAC konceptet, samt en beskrivelse og vurdering af forholdene omkring en fremtidig udrulning indenfor større industrielle DER enheder.

Rollebaseret adgangskontrol kan dateres tilbage til 1970'erne, men det var først i 1992 at *Ferraiolo og Kuhn*[2] offentliggjorde en artikel om 'Role Based Access Control' som begreb og som alternativ til den eksisterende Mandatory Access Control (MAC) og Discretionary Access Control (DAC).

I 2004 publiserede ANSI (American National Standard Institute) dokumentet [INCITS 359-2004] og IEC (International Electrotechnical Commission) i 2011 dokumentet [IEC TS 62351-8:2011] omhandlende Role-based Access Control [RBAC] indenfor Power system management.

RBAC er nu en international teknisk specifikation med veldefinerede roller som f.eks.: OPERATOR, INSTALLER, SECAUDIT, VIEWER m.m. – men der er internt i standardiseringsgruppen også en del diskussioner omkring behovet for mere fleksible adgangsparametre, som f.eks. tidsafgrænsning og geografiske adgangsbegrænsninger, kaldet 'Area-of-Responsibility' [AoR], hvilket går i retning af begrebet 'Attribute Based Access Control' [ABAC].

Figur 1 Hvad er ABAC?

[2] http://csrc.nist.gov/groups/SNS/rbac/documents/ferraiolo-kuhn-92.pdf

ABAC er i henhold til Gartner[3], den teknologi for adgangskontrol som i 2020 vil være dominerende med en udbredelse på op til 70% - men ABAC indenfor energisystemer og kritisk infrastruktur er ikke tilstrækkeligt veldokumenteret og afprøvet i praksis.

Resultaterne fra CHPCOM projektet [ForskEL: 12095] har bl.a. vist at RBAC er nødvendig, men også at der i praksis er andre attributter end rollen der kan indgå i adgangskontrollen. Alt afhængigt af den aktuelle 'Policy' kan bestemte tidsperioder, CVR-nummer, IP-adresser og geografiske områder også indgå som attributter for den nødvendige adgangskontrol.

Koncepttegning for ABAC

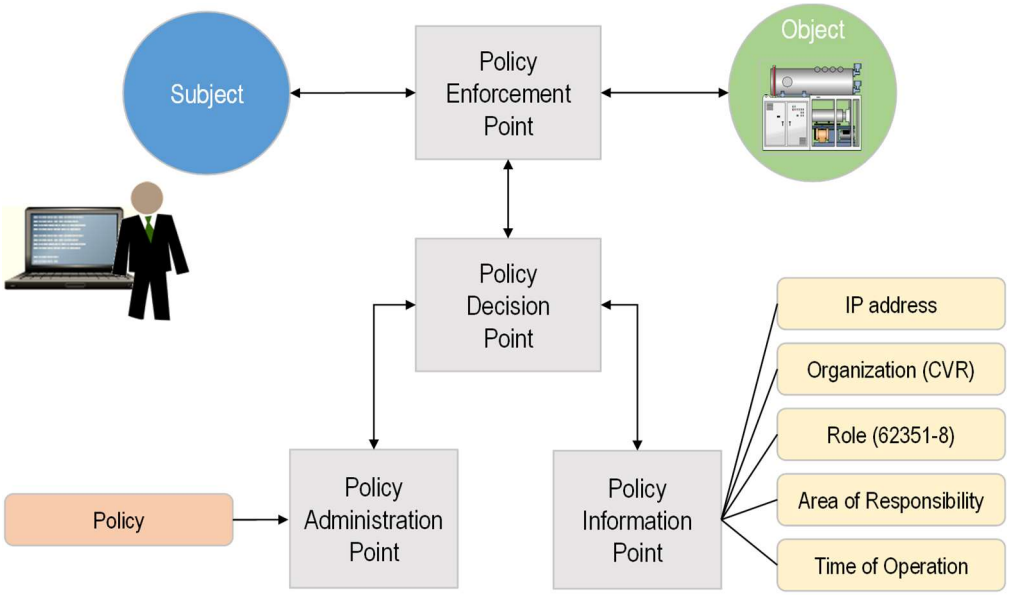
Det grundlæggende koncept som ønskes efterprøvet, består i opbygning af et 'Proof-of-Concept' i henhold til nedenstående funktionstegning.

En person eller et system (Subject) skal have adgang til et motorgeneratoranlæg (Object) gennem 'Policy Enforcement Point' (PEP).

En Policy i klar tekst, f.eks. 'Hans Jensen fra Elhandel A/S skal have adgang til produktionsplanerne fra anlæg 3 på Andeby kraftvarmeværk' – indlæses via 'Policy Administration Point' (PAP) i 'Policy Decision Point' (PDP) via XACML formatet som en 'Digital Policy' (DP) for videre behandling.

Metodeudviklingen og 'Proof-of-Concept' for managementsystemet til administration af DP'erne er et af de mest omfattende og kritiske elementer af projektets aktiviteter.

Informationer (attributter) fra en række kilder samles i 'Policy Information Point' (PIP) og danner basis for hvorvidt den definerede Policy giver 'Subject' adgang til 'Object'



Figur 2 ABAC koncepttegning

[3] http://objectsecurity-mds.blogspot.dk/2014/04/attribute-based-access-control-abac.html

Baggrund for SecureMMS

Den anbefalede standard[4] for sikker dataoverførsel indenfor elsystemer har i den nuværende version en række sikkerhedsproblemstillinger.

Grundlæggende drejer det sig om at den sikrer autenticitet, men ikke integritet, og derfor kan der potentielt manipuleres med data i et 'proxy scenarie'. I tilgift giver den ikke beskyttelse "end-to-end" i situationer, hvor en forbindelse går over mellemliggende systemer, som er en konfiguration, som forekommer i elsystemer. Her er autenticitet, integritet og hemmeligholdelse (kryptering) af vital betydning.

Den nærmere specificering af problemstillingen er veldokumenteret i et internt dokument[5] i IEC TC57 WG15 gruppen, hvilket af sikkerhedsmæssige og ophavsretslige grunde ikke er vedlagt denne rapport.

Forskningsmæssigt er der tale om metodeudvikling af en avanceret specifikation, som tillader "end-to-end" autenticitet, integritet og kryptering af selve dataindholdet. Da Danmark er i front med udvikling og implementering af SecureMMS, er der her brug for at klargøre danske ønsker og krav. Erik Andersen fra Andersen's L-Service har en indgående indsigt i hvad planerne er for næste udgave af den underliggende internationale standard. Metoden vil basere sig på udvidet brug af Open Systems Interconnection (OSI) standarder og af Recommendation ITU-T X.509, som er den grundlæggende specifikation for "public-key infrastructure" (PKI)

Forskningsmæssigt er der også tale om at analysere behovet for nye og mere effektive krypteringsmetoder.

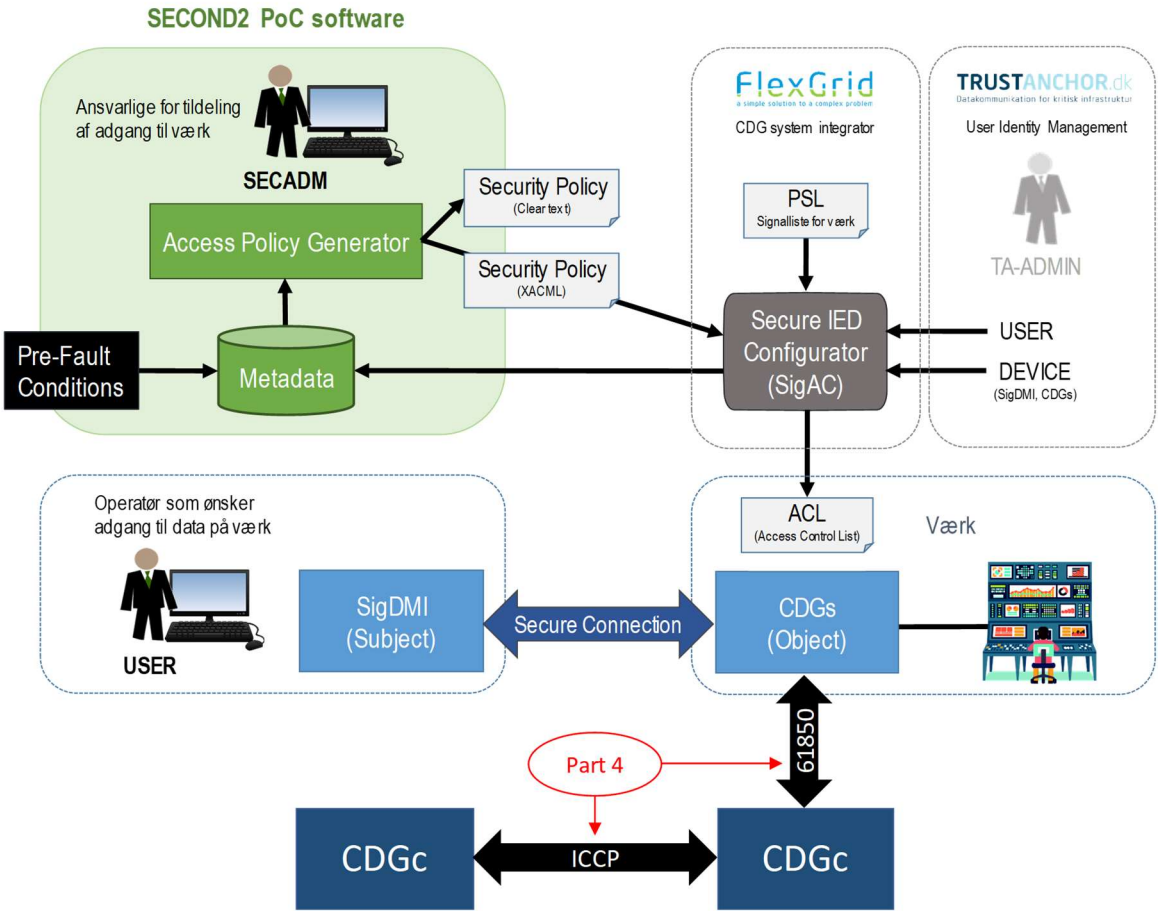
En væsentlig del af metodeudviklingen vil bestå i opbygning af et 'Proof-of-Concept' system, som kan sandsynliggøre at den udviklede metode er sikker.

[4] IEC 62351-4 ed. 1 (IEC TS 62351-4:2007)

[5] UPDATE-Overview of end-to-end security_stf_20140917.pdf

SECOND2 Proof-of-Concept

Det grundlæggende koncept er efterprøvet gennem opbygning af et 'Proof-of-Concept' i henhold til nedenstående funktionstegning.



Alexandra Instituttet, har som uvildig 3. part gennemført et 'Security review' inkl. Praktisk pen-test og code review, for at sikre en gennemgang og evaluering af de frembragte resultater.

Resultaterne er beskrevet i detalier i dokumentet SECOND2 Security Review.

Resultat og konklusioner

Sammenholdes de oprindelige problemstillingen for ansøgningen af SECOND2, men de praktiske resultater i en forenklet form – kan det sammenfattes til følgende.

SECOND2 ønsker med udgangspunkt i publikation fra NIST (National Institute of Standard and Technology [800-162] at analysere behov og muligheder for ABAC i forhold til det danske energisystem.

Ifølge NIST rapporten er det nødvendigt at have en høj grad af fleksibilitet i forhold til dynamisk at kunne ændre i de grundlæggende elementer (subjekter, objekter og deres respektive attributter. m.v.) og i adgangspolitikkerne.

Isoleret set, så er ABAC mekanismen ikke specielt kompleks, men den høje grad af fleksibilitet medfører at der skal etableres ekstra processer til at overvåge og synkronisere ændring i de grundlæggende elementer og i oprettede politikkerne.

Set i forhold til erfaringerne fra CHPCOM og hvordan f.eks de decentrale værker opererer i dag, og kan formodes at gøre det i fremtiden, vil et mindre fleksibelt og dermed mindre komplekst ABAC miljø formodentligt kunne løfte opgaven til fulde.

Fordele ved ABAC

Med ACL og RBAC mekanismerne, som beskrevet i 800-162, kan der specificeres hvilken adgang et system eller et system med en bestemt identitet eller rolle må få.

Med ABAC kan der specificeres mere nuancerede adgangsregler, hvor et system f.eks. kun må få adgang til en ressource indenfor et bestemt tidsrum under bestemte driftsmæssige forhold. Ved at knytte flere eller færre attributter til en ressource eller et subjekt (person/system) kan der defineres mere eller mindre komplekse regler for adgang.

Ulemper ved ABAC

Mens ABAC giver en høj grad af fleksibilitet ved opsætning af adgangsregler, så kan de potentielt mange attributter gøre det vanskeligt at bevare overblikket over indholdet af en politik. Når der yderligere, som beskrevet i 800-162, skal oprettes en politik per ressource, så kan man potentielt set ende med ganske mange politikker for at beskrive f.eks. en persons adgangsrettigheder til et system (f.eks. et kraftvarmeværk) der indeholder mange ressourcer.

Samtidig hermed sker opsætningen af politikker, ifølge 800-162, af andre end dem der ejer ressourcerne, hvorfor der er påkrævet en høj grad af trust på tværs af entiteter. Dette i modsætning til f.eks. RBAC, hvor ejeren af ressourcerne selv kan fastlægge hvilke roller der kan få adgang til hvilke ressourcer.

De mange politikker gør det nødvendigt med et ekstra management- og overvågningslag, som sikrer at politikkerne bliver korrekt udvekslet mellem de forskellige entiteter i ABAC miljøet. Alt i alt, så opnås den højere grad af fleksibilitet på bekostning af et betydeligt mere komplekst setup.

SECOND2 skal gennem analyse og praktisk afprøvning, frembringe en forbedring af konceptet for den eksisterende SecureMMS dataprotokol.

Indledningsvis blev følgende hovedelementer fremhævet og projektet har udfærdiget afklaringer som beskrevet under hvert enkelt hovedelement.

Analysér den anvendte kryptografi som den er beskrevet i IEC 62351-4:2018; lever den op til nuværende standarder?

Den anvendte kryptografi i IEC 62351-4:2018 er meget udbredt i den kryptografiske verden og anses bredt for at være tilstrækkelig til brug for sikker kommunikation anno 2018.

E2E-Security stiller to Elliptic Curve Diffie-Hellman algoritmer til rådighed for udveksling af kryptografiske nøgler. Disse kurver er secp256r1 eller bedre kendt som NIST P-256 og brainpoolP256r1. NIST P-256 er blandt andet anvendt i TLS 1.3 som standard. Flere er dog begyndt at søge væk fra NIST P-256, da denne kurve anvender konstanter der er mistænkt for at være udvalgt af NSA specifikt for at svække dets sikkerhed. Derfor er det udmærket, at E2E-Security giver mulighed for at anvende brainpoolP256r1 som alternativ.

E2E-Security bruger som standard AES til kryptering, som er en af de mest anerkendte og anvendte kryptografiske algoritmer inden for symmetrisk kryptering. Yderligere giver E2E-Security mulighed for at anvende AES-128 eller AES-256, hvor AES-256 udover at være klassificeret til tophemmelige dokumenter, også vil være sikker overfor en teoretisk quantum computer mange år ud i fremtiden.

Efter rettelsen fra IEC TC57 WG15 der forøgede public Diffie-Hellman maksimum nøgle størrelse, fra 256 til MAX, betyder det at IEC 62351-4:2018 understøtter muligheden for at supportere nye algoritmer i fremtiden, hvis svagheder skulle findes i de på indeværende specificererede algoritmer.

Undersøg eventuelle faldgruber en udvikler kan støde på, under implementeringen af E2E-Security

Oftest, når det kommer til sikkerheds huller, er det ikke den anvendte standard eller kryptografi, som fejler. I stedet er det implementeringsspecifikke fejl som ender med at kompromittere systemet. Derfor er det vigtigt at sætte fokus på eventuelle faldgruber en udvikler potentielt kan støde på.

E2E-Security tillader brug af AES-CBC. Dette cipher er blevet droppet af den nye TLS 1.3 standard, for at forårsage for mange implementeringsfejl. AES-CBC er i stedet blevet erstattet af ciphers, der er lige så sikre, men ikke lægger op til fejl i samme grad.

Udvikleren skal yderligere være opmærksom på kun at anvende ICV algoritmen, der blev udvekslet under association establishment og ikke anvende den som ligger i alle afsendte data pakker, til andet end at tjekke, at den stemmer overens med den aftalte ICV algoritme under association establishment. Den afsendte ICV algoritme kunne med fordel fjernes fra ”data transfer” fasen for at undgå denne problemstilling, da den kun er tilstede til debug formål; men da den er en del af den nuværende standard, skal den inkluderes.

Undersøg om E2E-Security’s A+ og AE+ profiler lever op til sine egne ”Security threats countered” som beskrevet i IEC 62351-4:2018

I den tidligere IEC TS 62351-4:2007, er de identificerede trusler beskrevet for A-profilen ikke endegyldigt modvirket, hvorved A-profilen i sidste ende, hvis anvendt alene, vil resultere i en usikker kommunikation. Derfor er det vigtigt at tjekke, at den nye IEC 62351-4:2018 rent faktisk beskytter mod de trusler som den hævdes at gøre.

De identificerede trusler som A+ og AE+ sikrer mod, bygger på de tre kryptografiske sikkerhedsprincipper ”Autenticitet”, ”Integritet” og ”Fortrolighed”. Dette betyder, at så længe E2E-Secruity lever op til disse kryptografiske principper, lever disse to profiler også op til de beskrevne trusler.

A+: Masquerade during association establishment end-to-end. (Autenticitet)

Masquerade under association establishment, er et forsøg på at udgive sig for at være en, man ikke er. A+ kommer dette problem til livs ved brug af X.509 certifikatsigneringen, hvorved kun den klient/server, som kan generere en valid signatur til det anvendte certifikat, vil blive anset for at være ejer af det medbragte certifikat. Selve certifikatet anvendes til identifikation af hvem afsenderen er.

A+: Unauthorized modification (tampering) both for the handshake phase and for the data transfer phase by use of digital signatures and integrity check values (ICVs) end-to-end (Integritet)

På samme måde som der sikres mod masquerade angreb under association establishment, sikres det også at det ikke er muligt at ændres på de afsendte data. Dette opnås ved at alle parametre er en del af den generede signatur. Derved vil en ændring af en eller flere parameter føre til at signaturen beregnet af modtageren ikke længere stemmer overens med den i kommunikationen medsendte signatur.

For dataoverførsel anvender E2E-Security integrity check values (ICV’s) til at forhindre, at beskeder kan ændres uden at det kan detekteres. ICV er genereret ud fra nøgler der blev udvekslet under association establishment. Derved arver ICV den sikkerhed, som disse nøgler blev generet under. I E2E-Security’s tilfælde betyder dette at ingen andre end klienten eller serveren kan generere beskeder som er kryptografisk gyldige.

A+: Replay countered through the use of time, association ID and sequence numbers (Integritet)

Både timestamp, sequence number og association id er påkrævet for alle sendte pakker. Kombinationen af alle tre parameter skal tjekkes for alle afsendte pakker. Hvis det detekteres at en pakke tidligere har brugt den samme kombination, vil pakken blive afvist som et forsøg på at gennemføre et replay angreb. Disse parametre er alle beskyttet af pakkens signatur og det vil derfor ikke være muligt for en angriber at ændre disse i et forsøg på at omgå E2E-Security’s replay detektering.

AE+: Theft or misuse of information by use of confidentiality (encryption) end-to-end (Fortrolighed)

AE+ er en udvidelse af A+ og vil derfor have de samme egenskaber, plus noget mere.

AE+ sikrer, at hele data pakken er beskyttet af kryptering. Dette betyder at så længe der ikke sendes afslørende information under association establishment, vil AE+ sikre at ingen data kan aflæses af uvedkommende.

Implementer ”Proof-of-Concept” system til validering og efterprøvning af E2E-Security’s design specifikation

E2E-Security prototypen blev implementeret med udgangspunkt i A+ profilen i Java og C, med henblik på at teste sikker kommunikation via IEC 61850.

Implementering af fejldetektering påviste en problemstilling i forhold til de kriterier, der blev brugt til at afbryde association establishment. Da det eneste kriterie var at tidsstempel ikke måtte være ens, betød dette, at serveren ikke måtte acceptere to eller flere samtidige association establishment forsøg, hvis deres tidsstempler var ens. Dette er nu blevet løst af IEC TC57 WG15 ved tilføjelse af et association id, som skal være unikt for alle forbindelser mellem en given klient til den samme server.

Under implementeringen blev der identificeret nogle problemstillinger i forhold til ASN.1 specifikationen, hvor mere hensigtsmæssige valg kunne træffes (relateret til længde og frivillighed af parametre). Disse ændringer havde til formål at forenkle strukturen, og gøre implementering nemmere og mere entydig. Disse ændringsforslag er allerede blevet inkorporeret i IEC 62351-4:2018 af IEC TC57 WG15.

Udover diverse punkter nævnt tidligere, blev der ikke fundet nogle større fejl eller mangler som skulle adresseres, før E2E-Security succesfuldt kunne testes i eksisterende setups med IEC 61850.

Et andet vigtig resultat fra SECOND2 har været det arbejde der er udført i IEC TC57 WG15 og ITU-T på baggrund af resultaterne beskrevet i rapporterne ovenfor. Der er dog tale om resultater som er frembragt i en koncensus-proces med andre eksperter fra andre nationalkommiter end Dansk Standard og derfor ikke direkte dokumenterbar.

For at få det fulde udbytte af resultaterne, anbefales det at læse de egentlige aflevering i form af disse 4 dokumenter.

- SECOND2 SecureMMS
- SECOND2 ABAC
- SECOND2 Security Paper
- SECOND2 Security Review