VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

TESTOVÁNÍ BEZPEČNOSTI CHYTRÝCH ELEKTROMĚRŮ

TESTING THE SECURITY OF SMART METERS

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. Ivana Fitere

AUTHOR

VEDOUCÍ PRÁCE — Ing. David Kohout

SUPERVISOR

BRNO 2023

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní program **Informační bezpečnost**

Ústav telekomunikací

Studentka: Bc. Ivana Fitere ***ID:*** 211785

Ročník: 2 ***Akademický rok:*** 2022/23

NÁZEV TÉMATU:

Testování bezpečnosti chytrých elektroměrů

POKYNY PRO VYPRACOVÁNÍ:

Téma práce je zaměřeno na analýzu kybernetické bezpečnosti chytrých elektroměrů a související infrastruktury. Analýza bezpečnosti bude provedena z pohledu protokolu DLMS, Security Suite a komunikačních technologií, které se uvažují pro aktuální výběrové osazovaní v ČR (GSM (mobilní sítě) a NB-IoT a LTE-M technologie).

Výstupem diplomové práce bude návrh bezpečnostního testování, návrh klíčového managementu, návrh typů testů, metodika testů, navrhované nástroje na provádění testů a případně provedení některých praktických testů (útoků) na dodaných chytrých elektroměrech. Druhým výstupem práce bude návrh životního cyklu a procesního managementu klíčů a certifikátů od výroby elektroměru až do instalace (s uvažováním všech procesních úkonů a limitů komunikačních technologií). Třetím výstupem bude laboratorní úloha pro předmět MPC-VDP, kde budou zakomponovány výstupy testování a kde dojde k samotnému praktickému ověření použitelnosti navrhované metodiky.

DOPORUČENÁ LITERATURA:

[1] SM-301-2019: Security requirements for procuring smart meters and data concentrators. European Network for Cyber Security [online]. [cit. 2023-01-26]. Dostupné z: https://encs.eu/resource/sm-301-2019-security-requirements-for-procuring-smart-meters-and-data-concentrators/

[2] NGCOBO T, GHAYOOR F. An overview of DLMS/COSEM and g3-plc for smart metering applications. International Journal on Smart Sensing and Intelligent Systems, 2022. DOI: 10.2478/ijssis-2022-0011

Termín zadání: 6.2.2023 ***Termín odevzdání:*** 19.5.2023

Vedoucí práce: Ing. David Kohout

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Diplomová práca sa venuje problematike bezpečnosti inteligentných elektromerov so zameraním na testovanie týchto zariadení, príklady praktických testov na elektromeroch, životnému cyklu elektromera z pohľadu bezpečnosti a Key Management Systému. V prvej časti sú zhrnuté komunikačné technológie využité v technike vzdialeného odpočtu meradiel, typy testov používaných pri testovaní inteligentných elektromerov, normy, ktoré túto problematiku upravujú a životný cyklus inteligentného elektromera. V druhej sa nachádza návrh Key Management Systému a laboratórna úloha pre študentov, zameraná na simuláciu komunikácie, preskúmanie správ a overenie bezpečnosti.

KĽÚČOVÉ SLOVÁ

DLMS, inteligentný elektromer, testovanie, Key Management Systém, zabezpečenie

ABSTRACT

This thesis studies the topic of smart meters with closer focus on testing of the devices, examples of tests performed on these devices, life cycle of the meter from security and Key Management System perspective. First part summarizes the technologies used in this kind of communication, test types, standards regulating smart metering and description of the life cycle. The second part includes scheme of the Key Management System and laboratory for students, devoted to examination of communication, messages and verifying the security.

KEYWORDS

DLMS, smart meter, testing, Key Management System, security

Vysadené pomocou balíčku `thesis` verzie 4.07; `http://latex.feec.vutbr.cz`

FITERE, Ivana. *Testování bezpečnosti chytrých elektromerů*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2023, 73 s. Diplomová práca. Vedúci práce: Ing. David Kohout

Vyhlásenie autora o pôvodnosti diela

Meno a priezvisko autora:	Bc. Ivana Fitere
VUT ID autora:	211785
Typ práce:	Diplomová práca
Akademický rok:	2022/23
Téma závěrečnej práce:	Testování bezpečnosti chytrých elektroměrů

Vyhlasujem, že svoju záverečnú prácu som vypracovala samostatne pod vedením vedúcej/cého záverečnej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autorka uvedenej záverečnej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto záverečnej práce som neporušila autorské práva tretích osôb, najmä som nezasiahla nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomá následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autorky*

*Autor podpisuje iba v tlačenej verzii.

POĎAKOVANIE

Rada by som sa poďakovala vedúcemu diplomovej práce pánu Ing. Davidovi Kohoutovi, za odborné vedenie, konzultácie a podnetné návrhy k práci. Veľká vďaka patrí taktiež pánovi Ing. Jozefovi Dudiakovi, Ph.D. za spoluprácu, podporu a rady z praxe.

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

V súčastnosti je bezpečnosť elektronickej komunikácie dôležitejšia ako kedykoľvek predtým. Dnes sú bežným javom cielené útoky na prvky kritickej infraštruktúry, či už fyzické alebo kybernetické. Inteligentný elektromer ako zariadenie je nepochybne súčasťou tejto kritickej infraštruktúry, nie len ako jednotlivé zariadenie ale hlavne ako celý systém zložený z tisícov inteligentných elektromerov, ich komunikačných ciest, dátovej a analytickej centrály. Pri téme bezpečnosti inteligentného elektromera teda hovoríme o bezpečnosti všetkých týchto prvkov systému. Vo všeobecnosti by sme bezpečnosť vedeli rozdeliť do následujúcich celkov.

Prvou dôležitou časťou bezpečnosti akýchkoľvek zariadení je bezpečnosť softvéru a hardvéru. Návrh týchto zariadení by mal odpovedať a spĺňať normy a štandardy na ich výrobu a vytvoriť jednotný systém zabezpečených komponent. Je však nesmierne dôležité sa o tieto komponenty aktívne starať a aktualizovať ich tak, aby počas celej svojej životnosti tieto podmienky spĺňali.

Druhým aspektom je fyzická bezpečnosť zariadení. Systémy inteligentných elektromerov by mali byť chránené pred akýmkoľvek fyzickým poškodením alebo neoprávneným prístupom a to správnym umiestnením na bezpečnom mieste a chránené pred vandalizmom, modifikáciou alebo krádežou.

Neodhliadnuteľnou treťou časťou celého systému je forma komunikácie medzi entitami a jej zabezpečenie. Zariadenia sú súčasťou komplexného systému, kde musí fungovať dobrá organizácia a vhodné zabezpečenie. Prevencia pred modifikáciou dát, neoprávnenému prístupu alebo odposluchu patrí medzi najdôležitejšie témy, ktorými sa zaoberá väčšina firiem v dnešnej dobe.

Diplomová práca sa venuje každej z týchto tém vo forme teoretického rozboru, popisu hlavných princípov ochrany, s detailom na Key Management Systém ako kľúčovú časť bezpečnosti. V závere práce je návrh praktických testov bezpečnosti vo forme laboratórnej úlohy, ktorá bude slúžiť na rozšírenie obzoru študentov v oblasti bezpečnosti inteligentného merania.

1 Komunikačné technológie využívané v inteligentnom meraní

Inteligentný merací systém (IMS), známi aj ako Advanced Metering Infrastructure (AMI) je sieť spájajúca koncových užívateľov s riadiacimi centrami energetických spoločností. Toto spojenie prináša mnoho výhod pre obe strany komunikačného reťazca. Zákazníkovi umožňuje nie len prehľad o vlastnej spotrebe ale aj informácie o aktuálnych tarifoch alebo informácie o stavoch v sieti. Najvýraznejšie zmeny sa ale odzrkadlia na strane distribučných spoločností. Nasadenie týchto inteligentných elektromerov umožní takýmto spoločnostiam nielen lepšie a efektívnejšie kontrolovať stav v sieti, ale aj rýchlejšie reagovať na stav zákazníkov. IMS využíva informačné a komunikačné technológie na vytvorenie obojsmerných komunikačných ciest medzi inteligentnými meracími prístrojmi (SM – Smart Meter) a energetickými spoločnosťami na prenos nameraných údajov, oznámení a riadiacich príkazov z centrálnej entity.

Táto kapitola sa zameriava na dve hlavné komunikačné technológie využívané v týchto systémoch a to technológiu PLC (Power-Line Communication) a GSM (Global System for Mobile Communications). V sieťach IMS sa využívajú drôtové aj bezdrôtové technológie. Zatiaľ čo bezdrôtové technológie sú vhodnejšie pre geograficky rozptýlené a všestranné siete, technológie PLC sú preferovanou a nákladovo efektívnou voľbou pre mestské oblasti alebo obytné domy [1].

1.1 Technológia PLC

Technológia G3 PLC nabrala popularity hlavne v posledných rokoch kvôli jej využitiu v rôznych rolloutoch krajín EU ako Nemecko, Francúzsko alebo Taliansko. Táto technológia je plne sebestačná a nezávislá na službách telekomunikačných spoločností. Poskytuje teda služby na svojej vlastnej sieti bez nutných prevádzkových telekomunikačných poplatkov. V súčastnosti tvorí otvorený štandard, ktorý zhlukuje všetky moderné vlastnosti komunikačných sietí a umožňuje prevádzku v drsných podmienkach. Parametre spojenia sa individuálne líšia podľa lokácie, frekvencií a použitých zariadení a tvoria prispôsobenú sadu. Technológia nabrala popularity hlavne vďaka týmto vlastnostiam [2]:

- **robustná komunikácia** – operatívna na nízkom pomere signálu k šumu SNR (Signal-to-noise ratio), schopnosť riešenia nepriaznivých udalostí bez zásahu operátora (selfhealing),
- **dlhé vzdialenosti** – schopná pokryť niekoľko stoviek metrov,
- **vysoká rýchlosť prenosu dát** – vyhovuje zvýšeniu požiadaviek na prenos,

- **silné zabezpečenie** – ochrana dát na jednotlivých vrstvách,
- **podpora rozvoja** – end-to-end IP komunikácia, podpora IPv6,
- **medzinárodný štandard** – ITU (International Telecommunication Union), zhodný s IEEE (Institute of Electrical and Electronics Engineers) a Cenelec.

1.1.1 Štandardy pre technológiu PLC

K prenosu dát používa technológia PLC frekvenčnú moduláciu, ktorá ju kategorizuje do troch základných skupín [1]:

- Ultra-narrowband PLC (UNB-PLC),
- Narrowband PLC (NB-PLC),
- Broadband PLC (BPL).

Typy PLC technológií

UNB-PLC	- používa frekvecie pod 3 kHz - schopná prenášať informácie na dlhšie trasy bez použitia opakovačov - použiteľná však iba na nízke prenosové rýchlosti
NB-PLC	- používa frekvencie od 3 do 500 kHz (v Európe do 150 kHz) - podporuje iba prenos do 500 kbps - schopná pokryť rozsah až 2 km - použitie v kontrolných, dozorných a diaľkových aplikáciách vrámci Smart Grid
BPL	- používa frekvencie od 1 do 250 MHz - podporuje prenos do 500 Mbps - kvôli nemožnosti interoperability je táto technológia menej vhodná a preferovaná na použitie v inteligentnom meraní - dátový prenos je limitovaný na pár stoviek metrov

Z predošlej tabuľky je patrné, že najvhodnejšou technológiou pre inteligerntné meranie je technológia Narrowband PLC (NB-PLC). Je rozdelená do dvoch skupín podľa prenosovej rýchlosti na [1]:

- Low data rate (LDR) – nízka prenosová rýchlosť,
- High data rate (HDR) – vysoká prenosová rýchlosť.

1.1.2 G3 PLC

G3-PLC je technológia, ktorá ako už bolo spomínané ponúka najnižšie celkové náklady na vlastníctvo a totálnu nezávislosť od telekomunikačných operátorov. Umožňuje spoľahlivú komunikáciu vysokými rýchlosťami na veľké vzdialenosti cez existujúce vedenia. Funkcie a možnosti G3-PLC boli vyvinuté na riešenie náročných výziev komunikácií po silových rozvodoch.

G3-PLC spĺňa tieto požiadavky vďaka vlastnostiam, ako je sieťový smerovací protokol na určenie najlepšej cesty medzi vzdialenými sieťovými uzlami, „robustný“ režim na zlepšenie komunikácie v podmienkach hlučného kanála a odhad kanála na výber optimálnej modulačnej schémy medzi susednými uzlami. uzly. Navyše jeho podpora IPv6, ktorá umožňuje jednoduchú integráciu rôznych aplikačných profilov, pridáva vysokú všestrannosť a posúva G3-PLC aj do budúcnosti [2].

Transportná a sieťová vrstva

Komunikačný model G3 PLC je optimalizovaný na každej vrstve aby vyhovoval svojmu charakteru. V časti sieťovej vrstvy sa o komunikáciu stará hlavne protokol TCP (Transmission Control Protocol), no v dokumentácii sa spomína aj protokol UDP (User Datagram Protocol). Oba tieto protokoly majú ako obvykle mnoho výhod i nevýhod. Medzi najdominantnejšie povahy protokolu UDP patrí jeho rýchlosť, čo do komunikačného kanálu prináša nespoľahlivosť vo forme nespojitého kanálu. G3 PLC však umožňuje použitie i protokolu TCP, čo do spojenia prináša spoľahlivý kanál a dôveryhodnosť. Dokumentácia G3 PLC však so spoľahlivosťou dát počíta už na vyšších vrstvách, preto podľa nej už nie je nutné vytvárať dôveryhodný kanál na vrstve sieťovej. Dokumentácia k protokolu G3 PLC sa taktiež zameriava na použitie IPv6 oproti IPv4, keďže sa tento protokol považuje za budúci štandard a predpokladá sa že bude podporovať budúce nové aplikácie. Štandardná veľkosť UDP/IPv6 hlavičky je 48 bytov, no to by v tomto prípade zkompromitovalo rýchlosť prenosu. Namiesto tejto veľkej hlavičky sa používa menšia, zkompresovaná, ktorej kompresia prebehne na linkovej vrstve [2, 3].

Linková vrstva

Linková vrstva sa v protokole G3 PLC skladá z dvoch podvrstiev:

1. Adaptation sublayer (adaptačná podvrstva),
2. MAC sublayer (MAC podvrstva).

Je to práve adaptačná podvrstva, ktorá komprimuje UDP/IPv6 hlavičku ako bolo spomenuté v predošlej podkapitole. Táto kompresia je možná vďaka špecifikácii 6LoWPAN, internetový protokol IP aj na tie najmenšie zariadenia, čo im aj napriek

ich obmedzeným schopnostiam umožňuje spracovávať zapojiť sa do internetu vecí. 6LoWPAN zkomprimuje hlavičku z 48 bytov na 5 bytov.
Na linkovej vrstve sa taktiež využíva protokol LOADng, ktorý slúži na vyhľadanie cesty ak uzol nepozná žiadnu cestu k ďalšiemu uzlu [3].

Fyzická vrstva

Fyzická vrstva protokolu G3 PLC bola definovaná troma rôznymi európskymi výbormi a to CENELEC, FCC a ARIB. V dnešnej dobe sa však najčastejšie používa špecifikácia fyzickej vrstvy od CENELEC (European Committee for Electrotechnical Standardization – Európsky výbor pre normalizáciu v elektrotechnike).
Existujú 3 módy prenosu v G3 PLC:

- Normal mode – normálny mód,
- Robust mode – robustný mód,
- Super Robust mode – super robustný mód.

Normálny a robustný mód je využívaný na prenos dát, super robusný mód na prenos kontrolného rámca (FCH), ktorý obsahuje dôležité informácie na demoduláciu celého dátového rámca. Modulácie použité v týchto typoch komunikácií sú DBPSK, DQPSK a D8PSK. Pri robustnom a super robustnom móde je to DBPSK a pri normálnom sa využíva akákoľvek z trojice [2, 3].

Bezpečnosť prenosu dát

Dáta sú pred predaním na komunikačný kanál upravené, aby nedošlo k narušeniu ich integrity. Po predaní dát zo všetkých predošlých vyšších vrstiev sa na fyzickej vrstve dáta prvotne prevedú scramblerom, ktorý náhodne prehodí poradie dát. Časti dát následne prejdú kódovacím Reed-Solomon (RS) mechanizmom. Následuje skrátenie, určitý počet dátových symbolov je v kodéri vynulovaných, tie sa neprenesú, a potom sa znova vložia do dekodéra [4, 5]. Zakódované dáta sa prejdú blokovým a repetitívnym kódovacím kanálom. Na zabránenie výskytu oneskorení sa na koniec a začiatok sekvencie pridá prefix. V poslednom kroku sa signál dostane do bloku, kde sa signál saturuje na požadovanú frekvenciu a následne je poslaný. V skratke sa dá prechod signálu analogicky charakterizovať ako [1]:

1. scrambler,
2. Reed-Solomon,
3. shortening,
4. kódovací kanál,
5. pridanie prefixu,
6. saturácia signálu,
7. zaslanie signálu.

1.1.3 Architektúra siete G3-PLC

Architektúra sietí inteligentných meradiel sa štandardne definuje ako sieť s koordinátorom, ktorý zostavuje sieť, komunikuje a riadi otrokom (ďalej slave), ktorí sa do siete pripájajú. Zariadenia slave sa do siete prvotne musia prihlásiť svojím identifikátorom, frekvenčným pásmom a inými dôležitými parametrami. Ak sa zariadeniu slave podarí pripojiť, v sieti sa od teraz bude môcť správať nie len ako koncové zariadenie ale aj ako opakovač (repeater). Táto schéma dovolí celému systému fungovať viac dynamicky. Ak sa jedena z trás medzi zariadeniami stane nefunkčnou, stále je možné sa vďaka alternatívnym cestám dostať do cielenej stanice. [7]

1.2 Technológia PRIME

Protokol PRIME bol vyvinutý spoločnosťou PRIME Alliance, ktorá bola vedená španielskym poskytovateľom energie. Táto technológia pokrýva rozsah frekvencií 42-89 kHz. Najnovšia verzia protokolu je verzia 1.4.

1.2.1 Architektúra siete PLC-PRIME

Komunikačné vrstvy protokolu sa skladajú z troch hlavných častí a to z [8]:

- konvergenčná vrstva CL – táto vrstva klasifikuje dátový prenos so správnou MAC vrstvou, mapuje rôzne typy dát do dátových jednotiek MAC a prevádza funkcie kompresie hlavičiek,
- vrstva MAC – zaručuje prístup k zdieľanému médiu, alokáciu šírky pásma a taktiež vytvorenie a udržiavanie spojenia,
- fyzická vrstva PHY – pomocou ortogonálneho multiplexu s kmitočtovým delením (OFDM) odosiela a prijíma MPDU medzi susednými uzlami.

Obrázok 1.1 naznačuje základnú štruktúru vrstiev.

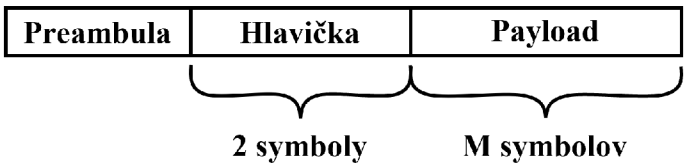
Obr. 1.1: Proces prechodu PPDU fyzickou vrstvou.

Fyzická vrstva

Schéma vysielača prvotne spočíva v prijatí MPDU fyzickou vrstvou od vrstvy MAC následné vygenerovanie fyzického rámca. Proces spracovania hlavičky a PPDU je následovný [8]:

1. Do hlavičky fyzickej vrstvy sa pridá CRC.
2. Prebehne konvolučné zakódovanie (hlavička PHY je vždy zakódovaná), ak je dovolená voliteľná časť FEC.
3. Nasleduje scrambler, ktorý je aplikovaný ako na hlavičku tak aj na PPDU, bez ohľadu na to či je FEC povolené alebo nie.
4. Ak je FEC povolená nasleduje preklad výstupu scramblera.
5. Ďalej sa bity modulujú troma rôznymi spôsobmi podľa schém:
   - DBPSK – Differential Binary Phase Shift Keying,
   - DQPSK – Differential Quaternary Phase Shift Keying,
   - D8PSK – Differential Eight-Phase Shift Keying.
6. Nasleduje OFDM, ktorý sa skladá z rýchlej fourierovej transformácie (IFFT) a generátora cyklického prefixu.

Výstupom schémy je rámec fyzickej vrstvy, ktorý tvorí preambula, hlavička a datové pole (payload). Rámec je na obrázku 1.2 [8].



Obr. 1.2: Rámec PHY.

Vrstva MAC

Táto vrstva môže byť chápaná ako stromová štruktúra s dvoma typmi uzlov [8]:

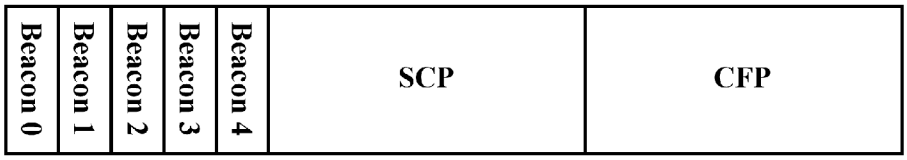
- základný uzol – base node,
- služobný uzol – service node.

Základný uzol je koreňom celej štruktúry a správa sa ako hlavný bod sieťovej komunikácie prvkov podsietí. V jednej podsieti môže existovať iba jeden základný uzol.

Služobný uzol je konármi a listami stromovej štruktúry. Prvotne sú vo funkčnom stave odpojenia (disconnected) a preform registračný proces, ktorý spočíva v zaslaní kontrolného paketu do základného uzla za účelom prihlásenia do podsiete. Služobné uzly majú v podsieti práve dve funkcie:

- udržiavať konektivitu k podsieti (k ich aplikačnej vrstve),
- prepínať dáta iných uzlov na udržanie konektivity.

Rámec MAC z jedného alebo viacerých beaconov, žiadneho alebo jedného kusu dát z predošlých vyšších vrstiev. Formát rámca je zobrazený na obrázku 1.3.



Obr. 1.3: Rámec MAC.

Bezpečná funkcionalita sa na MAC vrstve poskytuje chránením súkromia, autentifikáciou a integritou dát cez bezpečnú správu kľúčov a zabezpečenou metódou pripojenia. Výmena paketov pri komunikácii prebieha až po dohodnutí bezpečnostného profilu (Security profile). Security profiles môžu zatiaľ naberať dve rôzne úrovne 0 a 1. Štandard do budúcich verzií počíta s nasadením vyšších bezpečnostných profilov.

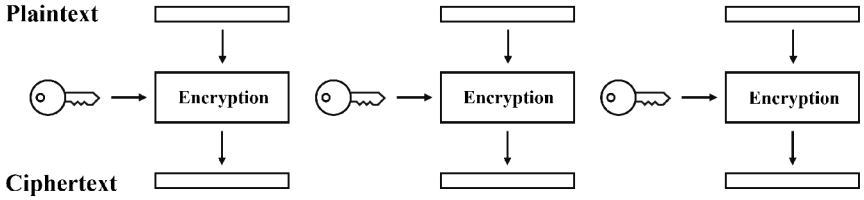
Security profile 0
Táto forma zabezpečenia je využitá v prípadoch, kde bezpečnosť nie je v danom použití potrebná alebo ide o scenáre kde je bezpečnosť poskytnutá vyššou vrstvou.

Security profile 1
Security profile 1 je založený na šifrovacom štandarde AES-128. Jeho charakter je špecifikovaný v niekoľkých bodoch:

- **ochrana súkromia** je zaručená šifrovaním a utajením šifrovacieho kľúča,
- **autentifikácia** je zaručená tým, že každý uzol má svoj vlastný tajný kľúč, ktorý pozná iba samotný uzol a základný uzol (Base node),
- **integrita** dát je zaručená tým, že CRC je šifrované [8].

Kryptografia

V špecifikácii PRIME na vrstve MAC je využitý šifrovací protokol AES. V móde ECB, čiže v režime kódovej knihy je možné túto kryptografickú funkciu použiť na rad rôznych činností ako generovanie hashov, digitálny podpis alebo generovanie prúdu kľúčov na šifrovanie i dešifrovanie [9]. Jedná sa o blokovú šifru, kde je text rozdelený do blokov o veľkosti 128 bitov. Ak je posledný blok textu menší ako 128 bitov, na doplnenie sa k nemu pridá padding. Nákres šifry je na obrázku 1.4 [8, 9].
Všetky typy MAC dát používajú daný vyjednaný bezpečnostný profil. Uzol Base sa po prijatí požiadavku na dohodu o bezpečnosti môže rozhodnúť či profil príjme alebo odmietne. To môže nastať práve v prípade, keď vyhodnotí nedostatočnú formu zabezpečenia pre daný typ spojenia. Z odporúčaní dokumentácie vyplýva, že by sa na začiatku registrácie vždy použil najvyšší podporovaný bezpečnostný profil, a až po doporučení uzla Base ju znížiť na požadovanú hodnotu. Základné a služobné uzly používajú hlavné typy kľúčov zhrnutých v tabuľke 1.1.



Obr. 1.4: AES-ECB.

Tab. 1.1: Tabuľka kľúčov využívaných v uzloch na vrstve MAC [8].

Typ kľúča	**Využitie kľúča**
Initial Working Key	Kľúč použitý na šifrovanie polí v registračnom pakete.
Working Key	Kľúč použitý na šifrovanie unicastových dát prenášaných medzi základným a služobným uzlom.
Subnetwork working key	Kľúč zdielaný celou podsieťou. Kvôli ochrane kľúča sa nikdy neprenáša žiadnym fyzickým kanálom. Používa sa na šifrovanie: • broadcastových dát a kontrolných paketov na vrstve MAC, • multicastových dát, • unicastových dát, prenášané cez priame pripojenia.
Master Keys	Kľúč MK1 počíta Device Secret Key (DSK) a kľúč MK2 zas Key Diversifier (KDIV). Master Keys sú pod správou základného uzla.
Device Secret Key	Každý služobný uzol má vlastný DSK, ktorý je doň pri výrobe vložený manuálne a jeho životnosť je rovná životnosti uzla.
Key Diversifier	Kľúč charakteristický pre základný uzol, nie je však fixný a počas životnosti uzlu s môže meniť.
Unique Secret Key	USK sa používa na odvodenie Working Key. USK sa zase vypočíta aplikáciou AES na Key Diversifier s použitím Device Secret Key ako generátora. Kľúč sa generuje podľa rovnice $USK = AES_{enc}(DSK,KDIV)$.

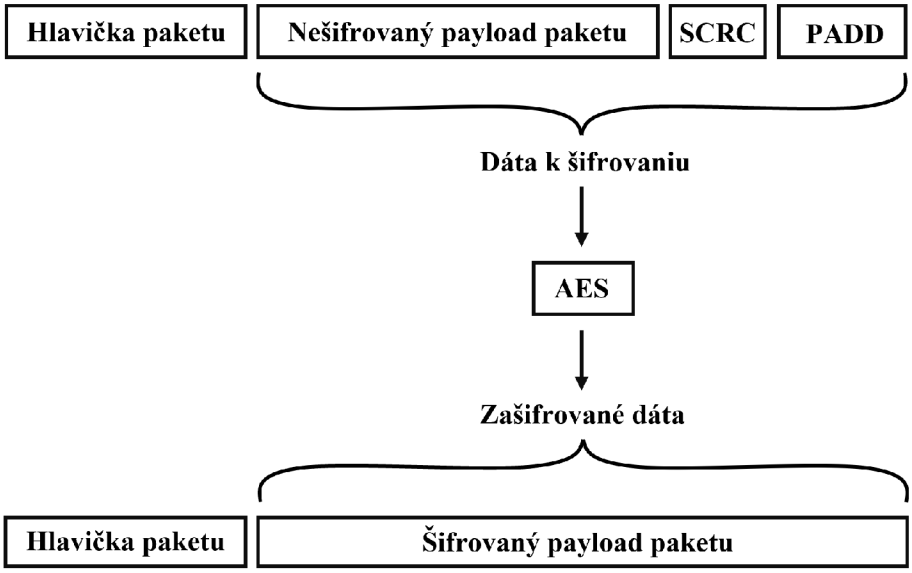
Šifrovanie v Security Profile 1

Spojenie S bezpečnostným profilom 1 zasiela bezpečný CRC takzvaný SCRC (secure CRC) s každým paketom. SCRC je vypočítaná z nešifrovanej časti payload. Po zašifrovaní poskytuje integritu a dôveryhodnosť pri dešifrovaní na strane prijímateľa.

Výpočet SCRC spočíva v súčine zvyšku po delení modulo 2 polynómu generátora

$$g(x) = x^8 + x^2 + x + 1 \tag{1.1}$$

z polynómu x^2 a nešifrovaného payloadu paketu. 128 bitové bloky sú postupne zašifrované použitím AES s príslušným kľúčom. Výsledkom je zašifrovaný payload ako na obrázku 1.5.



Obr. 1.5: Šifrovanie v Security profile 1.

Konvergenčná vrstva

Konvergenčná vrstva klasifikuje a asociuje prenos so správnymi spojeniami pre MAC vrstvu. Poskytuje taktiež prístup k základným funkciám MAC a o prideľovanie šírky pásma [6].

1.3 Technológia LTE-M

Pri vývine a implementácii inteligentných meradiel sa skúmalo niekoľko kandidátskych komunikačných techník, vrátane komunikácií po elektrickej sieti (PLC) spomínanej v predošlej kapitole. Hlavným obmedzením PLC je jeho znížená rýchlosť prenosu dát a značné rozdiely v charakteristikách kanálov PLC medzi krajinami alebo regiónmi v rámci rovnakej krajiny. Je tomu tak v dôsledku rôznych praktík zapojení a záťaží pripojených k systémov. Preto sú bezdrôtové komunikácie pre inteligentný merací systém vnímané ako alternatívne riešenie. S existujúcou mobilnou

sieťovou infraštruktúrou nie je potrebné budovať iné formy komunikačných kanálov a ako pri technológii PLC je možné využívať už vybudovanú sieť.
V dnešnej dobe sa mobilné komunikačné siete vyvinuli nie len z hľadiska pokrytia alebo rýchlosti dát ale aj z hľadiska bezpečnosti a preto majú vysoký potenciál nahradiť fyzické a optické. Je tiež faktom že sa cena týchto služieb postupne celosvetovo znižuje a preto sa táto technológia stáva čím ďalej tým populárnejšou [10]. Táto technológia sa využíva najmä pri selektívnej inštalácii meradiel, kde ide o roztrúsenú polohu zákazníkov.

1.3.1 Výhody využitia technológie LTE

Pri komunikácii inteligentných elektromerov so sieťou sú kľúčové najmä charakteristiky ako [16, 10]:

- dostať sa k veľkému objemu informácií od meradla čo najefektívnejšie- regulácie momentálne vyžadujú 15 minútové odpočty údajov o profile zákazníka navrhujú sa ale už aj 5 minútové a dokonca 1 minútové odpočty,
- umožnenie odpočtu z meradiel, ktoré nemajú jednoduchý terénny prístup,
- diaľkové ovládanie zariadení na rôzne účely,
- vzdialená konfigurácia a aktualizácia firmvéru a softvéru,
- primeraná až nízka latencia, takže zber informácií a kontaktovanie pár desiatok tisíc zariadení naraz je možné vykonať bez toho, aby sa muselo čakať na žiadosť a odpoveď.

Spoľahlivosť a pokrytie

Fungovanie na existujúcich mobilných sieťach udržiavaných mobilnými operátormi, ktorí majú veľký záujem o bezpečnú, spoľahlivú a neustálu prevádzku siete [14]. Mobilné siete využívajú globálne štandardy, a preto sú vysoko kompatibilné so širokou škálou zariadení a aplikácií, pričom sa vyhýbajú zablokovaniu jedným dodávateľom.

Medzi technológie, ktoré sú momentálne dostupné patria hlavne 2.5G, 3G, 4G, 5G LTE Cat 1, 5G LTE Cat M1 a 5G NB IoT [16].

Staršie technológie ako 2.5G a 3G sú do dnešného dňa v niektorých štátoch ešte stále dostupné. Ich charakteristiky ako šírka pásma, 100kps a menej alebo latencia okolo 100 m/sec sú pre využitie v inteligentnom meraní dosť nepraktické hlavne kvôli zvyšujúcemu sa objemu prenášaných dát. Životnosť elektromerov sa taktiež odhaduje na 10-15 rokov, čo takisto tejto technológii nehrá do karát.

4G bolo pri vývoji optimalizované hlavne na streaming cez mobilné dáta s charakteristickou širokopásmovou službou sťahovania od 19 do 36 Mbps. Latencia sa tiež vzťahuje na charakter technológie pohybujúca sa okolo 50 msec, čo je o polovicu

menšie ako jej predchodca. Momentálne sa bežne stretneme s rolloutom elektromerov s podporou 4G. Nie sú však najefektívnejším využitím technológie, najmä v hustejších mestských obytných zónach.

Poslednou možnosťou je technológia 5G, ktorá bola zostrojená práve pre aplikácie IoT. Je teda najlepšou voľbou pri použití zariadení komunikujúce cez mobilné siete [16, 17].

Nákladová efektívnosť a jednoduchosť

Inštalácia a nasadenie sú veľmi jednoduché. Na rozdiel od PLC zariadení komunikujú mobilné zariadenia nezávisle od iných a pridanie alebo odstránenie meradla nemá vplyv na celkovú topológiu a stabilitu celej siete. Pri pridávaní nového meradla môže začať okamžite komunikovať a pred spustením komunikácie nie je potrebné čakať na dokončenie okolitých inštalácií [14]. S viacerými poskytovateľmi na jednom mieste si zariadenie taktiež môže vybrať alebo prepnúť sa na najspoľahlivejšiu alebo najefektívnejšiu sieť.

Zaistenie budúcnosti

Nové technológie LTE sú súčasťou stratégii a implementácie sietí 5G. To zabezpečuje spotrebiteľa, že komunikačná technológia bude zabezpečená počas celej životnosti elektromera.

2 Bezpečnostné testovanie inteligentných elektromerov

Moderné infraštruktúry v oblasti merania elektriny ovplyvňujú spôsob výroby, ceny a hlavne spotrebu elektrickej energie. Naprieč celému svetu sa v dnešnej dobe prehá-ňajú rôzne inovačné projekty a nové technológie na rozvoj inteligentných sietí. Sektor energetiky sa v súčastnosti značne mení. So zmenami prirodzene prichádzajú avšak aj nové prekážky a výzvy. Jednou z takýchto prekážok pri nových technológiách je umožnenie protivníkom manipulovať so sieťou, pretože sa žiaľ stále do siete nasa-dzujú nové zariadenia a technológie s malou alebo žiadnou skutočnou implementácie bezpečnosti.
Elektromery založené na digitálnych technológiách sú jednou z najdôležitejších častí nášho elektrického systému hlavne kvôli svojej schopnosti merania spotreby elektriny na rôznych úrovniach v mechanizme distribúcie energie. Okrem tohto umožňujú tak-tiež hodnotenie výkonu alebo odhad strát v systéme ale aj určenie výnosov verejných služieb. K dosiahnutiu týchto účelov je dôležité otestovať kvalitu a spoľahlivosť elek-tromera, aby dôveryhodne a presne zaznamenával dáta. Testovanie meradiel môže predchádzať poruchám a zabezpečuje dlhú životnosť bez zníženia výkonu [11].

2.1 Európske normy a vyhlášky upravujúce inteligentné meracie systémy

V Českej republike sa tejto problematike venujú dve dôležité normy a vyhlášky:

- norma NÚKIB – Doporučení v oblasti kryptografických prostředků: Minimální požadavky na kryptografické algoritmy,
- vyhláška č. 359/2020 Sb. – Vyhláška o měření elektřiny.

Norma NÚKIB doporučuje kryptografické požiadavky vo dvoch rozdeleniach a to na algoritmy schválené a dostatočné. Vo vyhláške č. 359/2020 Sb. sa okrem rozdele-nia a termínov inštalácie meradiel taktiež nachádza kapitola s technickými a kryp-tografickými minimálnymi požiadavkami na rozhranie elektromera pre komunikáciu s inými prvkami infraštruktúry.

Medzi najznámejšie európske doporučenia patrí:

- norma ENCS,
- štandard DSMR.

V norme ENCS nájdeme doporučenia na sieťovú komunikáciu, rozdelenie typov sie-ťovej architektúry alebo technické požiadavky na jednotlivé prvky. Štandard DSMR je dokument poskytujúci sprievodné normy pre holandské systémy AMM. Jedná sa

o meradlá elektriny, tepla, plynu, vody a teplej vody [20]. Tento štandard nabral popularity aj u českých dodávateľov vďaka jeho univerzálnosti a priehľadnosti.

2.2 Testy podľa IEC a ANSI

Štandardy IEC (International Electrotechnical Commission) a ANSI (American National Standards Institute) popisuje a upravuje veľké množstvo technológií ako i generovanie a distribúcia elektriny, čo zahŕňa aj inteligentné meradlá. V Európe sa o príslušenstvo na meranie elektrickej energie, tarify alebo regulátory záťaže stará IEC komisia 13 (TC 13 – Technical Committee). Pracovný rozsah tejto skupiny pokrýva všetky meracie zariadenia pre všetky možné aplikácie. V súčasnosti je k dispozícii viac ako 30 noriem a technických správ zahŕňajúcich túto problematiku . Normy TC 13 poskytujú spoľahlivý základ pre špecifikácie, typové overenia a akceptačné testy. Medzi takéto testy patria napríklad [23]:

- typový a akceptačný test IEC 62052–11 zahŕňa mechanické, klimatické a elektrické aspekty aspekty, aby sa zabezpečila robustnosť a bezpečnosť meradiel,
- typový a akceptačný test IEC 62054–11 a 4–21 – špecifikujú konkrétne požiadavky na prijímače ripple control receiver a časové spínače,
- typový a akceptačný test IEC 60514 a 61358 – špecifikujú postupy akceptačných skúšok.

2.3 Nástroje testovania

V dnešnej dobe existuje množstvo nástrojov, pomocou ktorých možno sledovať alebo otestovať elektromery. Medzi najznámejšie a najefektívnejšie nástroje patria podľa [40] následujúce:

- Kali Linux ako operačný systém ponúka viacero nástrojov vhodných na testovanie komunikácie, ktorá prebieha medzi elektromerom a dátovou centrálou. Sledovanie sieťovej komunikácie nám umožňujú aplikácie ako Nmap, GreenBone alebo arpspoof,
- HPing3 slúži ako sieťový nástroj na zasielanie vlastných paketov,
- Avalanche tvorí hardvérový tester imitujúci entity v sieti. Funguje ako koncové zariadenie na oboch stranách klienta a servera,
- DLMS Conformance Test Tool .

2.3.1 DLMS Conformance Test Tool

Conformance Test Tool, skrátene CTT, je aplikácia, ktorá automatizovane prevádza pre-definované testy na zariadeniach, ktoré implementujú špecifikáciu DLMS/CO-

SEM. CTT umožňuje vykonávať individuálne testy pre danú konkrétnu vrstvu alebo testovacie sady všetkých testov pre danú vrstvu. Pre skompletizovanie Conformance Testu (CT) je nutné previesť všetky testy [19].

Medzi základné vlastnosti CTT patria hlavne [19]:

- účelom CTT je otestovať, či je možné server prevádzkovať s klientom, vyhovujúcim štandardu DLMS/COSEM,
- testovanie serverov nástrojom CTT je limitované testovaním iba objektov COSEM a ich atribútov a metód. To znamená, že triedy výrobcu nespadajú pod toto testovanie,
- Testovanie serverov nástrojom CTT je limitované testovaním funkcionality servera v takom zmysle, v akom je uvedený na komunikačnom rozhraní.
- Testy môžu byť vykonané pomocou použitia priameho spojenia ako:
  - optický kábel,
  - optická sonda,
  - RS-232/RS-485.
- Testy CT môžu byť vykonané výrobcom alebo treťou stranou s minimálnym zásahom človeka.

2.4 Prehľad testov na inteligentných meradlách

2.4.1 Reliability assesment test

Test posúdenia spoľahlivosti je nadizajnovaný na detekciu zlyhania súčiastok v inteligentnom elektromeri. Je faktom, že v množine inštalovaných elektromerov často dochádza k zbytočným opravám a vysokej miere nepotrebnej údržby. Dlhá životnosť meradla je dôležitá ako i pre poskytovateľa tak i pre spotrebiteľa. Je teda dôležité aby meradlá zodpovedali kvalitnému vývoju už od začiatku výroby.

Odhalenie zraniteľností, vývoj správneho procesu a zaistenie správnosti na korektné testovanie spočíva v týchto krokoch [21]:

1. zber dát z nefunkčnej časti systému,
2. analýza chyby – nájdenie ultimátneho zdroja nefunkčnosti,
3. vytvorenie mechanizmu chyby a simulovanie stresu na komponentu,
4. použitie testu a odhalenie pôvodu.

Testy tohto typu potvrdzujú, že sa v produkčnom procese elektromerov niečo zanedbáva. Podľa dokumentu [21] ide o proces spájkovania malých komponent, počas ktorého s veľkou pravdepodobnosťou nie sú splnené tieto základné predpoklady:

- vhodná teplota,
- electrical static discharge protection,

- ochrana pred vlhkom.

Niektorí výrobcovia inteligentných elektromerov hlásia takmer 80 % chybných častí podrobené funkčným testom, ktoré súvisia so zlým spájkovaním.

Podľa procesu analýzy zraniteľností v súlade s krokmi spomenuté vyššie sa medzi komponenty s najfrekventovanejšími poruchami zaradili komponenty v tabuľke 2.1.

Tab. 2.1: Typické chyby a mechanizmus zlyhania podľa [21].

Typ modulu	**Mechanizmus zlyhania**
Komunikácia	Termálna expanzia zapríčiní otvorený spoj, absorpciu vlhka a elektrickú poruchu. Tranzistor: absorpcia vlhka spôsobuje rozptyl elektródy.
Meranie energie	Čipový rezistor: korózia alebo kontaminácia spôsobuje elektrickú poruchu. Meradlo: vlhkosť spôsobuje posun parametrov.
Display	LCD: vlhkosť spôsobuje poškodenie polarizátora a nedostatočné spájkovanie spôsobuje nestabilné spojenie čo vedie k mechanickému poškodeniu.
Kontrolná a spracujúca jednotka	MCU: absorpcia vlhkosti spôsobuje úniky, elektrostatický výboj (ESD) spôsobil elektrický stres (EOS). Relé: korózia, oxidácia a elektromigrácia spôsobuje zlyhanie.
Alarm chýb	LED: vlhkosť spôsobuje únik, mechanické a termálne expanzie vedú k elektrickej poruche.
Meranie času	Batéria: nízke hodnoty vlastnej kapacity, úniky elektrolytu a vlhkosť spôsobuje degeneráciu a poruchu. Oscilátor: nekvalitné spájkovanie a kontaminácia vedie k nefunkčnosti.

2.4.2 Test odolnosti

Tento test sa venoval skúmaniu reakcie jednofázových elektromerov na zmenu teploty prostredia. Zmena teploty sa môže značne odzrkadliť na funkcionalite komponent elektromera a keďže práve toto zariadenie funguje vďaka spolupráci všetkých komponent. Pri nefunkčnosti alebo chybe v čo i len jednej komponente, je funkcia elektromeru nepresná a nemôže 100% naplniť svoju úlohu [22].

Cieľom testu bolo simulovať teplotu prostredia a sledovať odozvu jednotlivých komponent. Zvyšovanie teploty nenastalo do momentu, pokiaľ sa jeden z komponent nedostal do bodu nefunkčnosti. Proces a princíp testu je nasledovný:

1. prvotne testované objekty prejdú súborom výkonnostných testov aby sa zistila ich kvalifikácia na samotné testovanie,

2. do testovania sa zapojí aj online monitorovanie trendov a zmien, ktoré sa objavia počas testu,
3. konečné testy by vždy mali byť zhodnotené a spracované pri izbovej teplote a dáta by mali byť zaznamenávané v reálnom čase.

výsledkom testu bolo lineárne stúpanie chyby spolu so zvyšovaním teploty. Zo všetkých testovaných komponent v meradle na zvyšovanie teploty najhoršie reagoval LCD display, ktorého funkcionalita začala ubúdať pri 90 °C. Úplná nefunkčnosť prišla v dosiahnutej teplote 100 °C [22].

2.4.3 Multistresová metóda akcelerovaných testov životnosti pre inteligentné elektromery

Hlavnou úlohou akcelerovaných testov životnosti (Accelerated Life Tests – ALT) je zvyšovanie levelov environmentálneho stresu na zariadenia v krátkom časovom intervale. Táto metóda vznikla hlavne kvôli zrýchleniu procesu testovania čo má priamy vplyv na cenu testovania. Medzi hlavné časti testovania patria [25]:

- teplotný stres,
- stres vlhkosti,
- vibračný stres,
- napäťový stres,
- množstevný stres.

Väčšina zlyhaní elektromera je zapríčinená neštandardnou teplotou a vlhkosťou, tvoriacu až 75 % zlyhaní.

Weibullova distribúcia

Weibullova distribúcia patrí medzi najbežnejšie používané typy distribúcie v technikách spoľahlivosti. Medzi jeho hlavné použitia patria modelovanie pevnosti materiálu, času do zlyhania elektronických a mechanických komponentov alebo systémov. Metóda využíva tri typy parametrov [24]. Táto metóda bola vybratá ako najvhodnejší model, ktorý dokáže opísať charakteristiku života inteligentného elektromera.

Life-stress model

Tento model charakterizuje vzťah medzi vonkajším environmentálnym stresom na zariadenie a jeho charakteristikami životnosti. Model bol vytvorený v súlade s percentuálnym rozložením každého typu záťažových stresov spomínaných vyššie. Z týchto predpokladov vyplýva vzťah:

$$AF = \left(\frac{RH_u}{RH_s}\right)^{-n} * e^{\frac{E_a}{k}\left(\frac{1}{T_u}-\frac{1}{T_s}\right)} \tag{2.1}$$

kde:

Obr. 2.1: Proces testovania softvéru 2.1.

- RHu je percentuálna relatívna vlhkosť pri použitých podmienkach,
- RHs je percentuálna relatívna vlhkosť pri záťažových podmienkach,
- Tu je teplota v Kelvinoch použitých podmienkach,
- Tu je teplota v Kelvinoch použitých podmienkach,
- k je Boltzmannova konštanta,
- Ea je aktivačná energia v elektrónvoltoch,
- n je konštanta (medzi 1 až 12, typicky n = 3).

Výsledkom testovaní a simulácií sa touto metódou podarilo skrátiť čas životnostných testov až o 50 % na 4,5 dní [25].

2.4.4 Testovanie softvéru

S narastajúcou úrovňou inteligentného merania exponenciálne rastie aj rozsah a zložitosť použitého softvéru. Kľúčovým faktorom sa preto postupne stáva samotný softvér, vysoko ovplyvňuje kvalitu meradiel a jeho spoľahlivosť je pre chod celého systému dôležitá. Životný cyklus elektromerov a ich softvérové metódy sú často skúmané s cieľom vytvorenia všeobecných metód a procesov testovania. Na ich vytvorenie sa skúmajú a analyzujú rôzne zlyhania a chyby v konkrétnych módoch a režimoch, podľa ktorých sa hľadá ich príčina a zdroj. Chyby softvéru sa tvoria už počas procesu vývoja. Typický model testovania softvéru 2.1 vystihuje vzťah medzi vývojom, testovaním, analýzou a dizajnom softvéru.

Ľavá strana charakterizuje fázu vývoja a pravá fázu testovania. Fáza vývoja začína

zhrnutím požiadaviek na softvér, preformulujú sa do detailného návrhu a nakoniec sa vytvorí samotný kód. Po zostavení kódu nasleduje fáza testovania a to testovaním jednotiek, následnou integráciou testovaním systémov a akceptačným testovaním.

Testovací model elektromerov zahŕňa hlavne:

- statické testovanie,
- dynamické white-box testovanie,
- dynamické gray-box testovanie,
- dynamické black-box testovanie.

Statické testovanie zahŕňa analýzu softvérových chýb so zameraním na konkrétne chyby ako napríklad pole mimo hranice, inicializácia premenných alebo pretečenie vyrovnávacej pamäte. Dynamické white-box testovanie sa zameriava na testy logiky kódu. Dynamické gray-box testovanie testuje interný úložný priestor a interakciu rozhraní softvéru elektromera. Tieto testy sa vykonávajú v prostredí polo-fyzikálnej simulácie. Dynamické black-box testovanie je založené najmä na systémovom overení celého zariadenia [37].

Spoločnosti poskytujúce softvérové testovanie

Testovaniu softvérovej časti inteligentných elektromerov sa venuje hŕstka súkromných firiem, ktoré ponúkajú svoje služby za poplatok. Jednou z týchto firiem je firma Critical sofrware, ktorá napríklad ponúka elektronické overovacie skúšky alebo testy zariadení aj sietí na mieru. Ich zákazníkom môže byť ako výrobca týchto zariadení aj energetická spoločnosť či sieťový operátor. Critical sofrware vyvinulo svoje vlastné testovacie prostredie s vlastnými prostriedkami na testovanie so skratkou SMITEn (Smart Meter Integrated Test Environment).

Jednou z ďalších spoločností, ktoré ponúkajú testovanie inteligentných elektromerov je firma UL Solutions, ktorá ponúka testovanie zariadení podľa požiadaviek viacerých regiónov nie len Európy a Ameriky ale aj Ázie, Austrálie alebo Južnej Afriky. UL Solutions ponúka testovanie bezpečnosti elektromerov, vodomerov aj plynomerov na zaistenie splnenia požiadavkov tried presnosti, ako aj požiadavkov na použitie v prípade otrasov, požiarov alebo iných nebezpečných udalostí. V ponuke sú taktiež testy funkcií elektromeru ako elektronické meranie, bezdrôtové alebo diaľkové hlásenie a testovanie ovládačov.

3 Životný cyklus inteligentného elektromera

Inteligentné elektromery v procese výroby podstupujú štyri základné fázy pred odoslaním distribučným spoločnostiam [12]:

- zostavovanie sa začína po prijatí objednávky od distribučnej spoločnosti,
- na kalibráciu sú použité špeciálne a presné kalibračné funkcie,
- zrenie prichádza po kalibrácii všetkých funkcionalít a je dôležité skontrolovať fungovanie komunikácie, odpočtu alebo merania,
- inšpekcia prevádza testovanie meradla,
- prvotná inšpekcia funkcionalít je firmou vyskúšaná na percente zariadení. Počet zariadení sa môže líšiť podľa regulácie v danom štáte, typicky je to okolo 5 %, v Nemecku až 20 %,
- meter sealing spočíva v zapečatení zariadenia aby sa predišlo manipulácii,
- inštalovanie zariadení zákazníkom,
- kontrola počas prevádzky,
- test demontáže,
- demontáž, zničenie a recyklácia zariadenia.

3.1 Životný cyklus z pohľadu distribučnej spoločnosti

Potom ako sa elektromer fyzicky a systémovo zostaví je dôležitá jeho certifikácia. Elektromer podstúpi niekoľko testov a skúšok z ktorých najdôležitejší je test overenia presnosti merania elektrickej energie. Tento test sa prevádza podľa kalibračného protokolu triedy presnosti a preukazuje teda presnosť meradla. Toto overenie robí spravidla výrobca, ktorý meradlu vystaví certifikát. Potom ako elektromer kúpi DS sa toto meradlo, ako aj každé iné, zaregistruje do systému. Po registrácii sa elektromer buď namontuje na nové odberné miesto alebo na miesto staršieho meradla. Proces výmeny týmto spôsobom tj. starý elektromer za nový sa nazýva periodická výmena. Elektromer bude na odbernom mieste pôsobiť po dobu jeho životnosti, ktorú určuje práve certifikát overenia presnosti meradla.

3.1.1 Bezpečnosť

Výrobcovia komponent väčšinou vôbec netušia ako a kde sa ich zariadenia budú používať. Je teda dôležité aby sa počítalo s bezpečným nasadením do siete. Existujú dva spôsoby ako sa táto bezpečnosť zaistí. Je to buď nahraním predom zdieľaných kľúčov PSK (Pre-shared key) do zariadení pri výrobe alebo použitím verejnej správy kľúčov PKI (Pulic key infrastructure).

Pre-shared keys (PSK)
PSK predstavuje najzákladnejšiu úroveň zabezpečenia zariadeniam aj IoT platforme spoločným kľúčom, ktorý bol bezpečne priradený zariadeniu. Považuje sa jedine za základné zabezpečenie, pretože tam existuje riziko ohrozenia dôveryhodných zoznamov.

Pulic key infrastructure (PKI)
Preferovaná a najbezpečnejšia varianta je použitie správy kľúčov, ktorá využíva a pridáva do systému vrstvu s asymetrickou kryptografiou a spája kryptografický podpis s treťou stranou. Použitie tretej strany ponúka oveľa bezpečnejší systém autentifikácie, kde sú údaje generované iba v zariadení a nie sú uložené v žiadnej externej databáze.

Informačná bezpečnosť

Existujúce bezdrôtové a mobilné infraštruktúry musia mať implementované silné a osvedčené bezpečnostné technológie. Tieto bezpečnostné opatrenia zahŕňajú [18]:

- bezpečná konektivita a šifrovanie – nevyhnutnosťou každého komunikačného systému je zabezpečiť doručenie správnej informácie tomu správnemu zariadeniu v správny čas. V prípade prenášania osobných informácií a dátach používaných k fakturácii ceny energie je zaistenie bezpečnosti kľúčové. Bezdrôtové systémy by mali používať silné a overené šifrovacie protokoly,
- detekcia hrozieb,
- autonómna prevádzka – aj napriek odpojeniu meradle od siete by malo byť naďalej schopné vykonávať svoje funkcie.

3.1.2 Dôvera v aktualizácie a bezpečná aktualizácia

Bezpečné aktualizácie sú kľúčovým prvkom v živote elektromera a prispievajú k jeho dlhej životnosti. Pomocou aktualizácií výrobca ponúka dodatočné funkcie pre používateľov aj poskytovateľov služieb. Vzdialené aktualizácie sú tiež účinným prostriedkom ochrany pred najnovšími hrozbami a zraniteľnosťami bez toho, aby bolo nutné prevádzať manuálne aktualizáciu v teréne. Okrem predajcov elektromerov sa môže aktualizovať softvér aj kvôli novým nariadeniam upravovaných v súvisiacom zákone alebo vyhláške, ako aj kvôli chybám a zlepšeniu celkovej funkčnosti [15].

Klient na správy o aktualizáciách čaká. Po prijatí notifikácie overí balík, použije aktualizáciu a vráti sa do pôvodného stavu. Okrem zabezpečenia novej aktualizácie je tiež podstatné, aby sa zariadenie chránilo pred úmyselným vrátením do staršej

verzie firmvéru. Ako všetky iné časti systému, aj aktualizovanie a starostlivosť o firmvér so sebou prináša bezpečnostné hrozby. Niektoré útoky, s ktorými sa môžeme pri aktualizáciách najčastejšie stretnúť sú podľa [15]:

Útok: **Odpočúvanie na komunikačnom kanále s cieľom zachytiť súbor s aktualizáciou**
Možné riešenie: Zabezpečenie aktualizácie tak, aby ju mohli odhaliť iba meradlá, na ktoré je aktualizácia mierená.

Útok: **Útočník v strede komunikácie môže zachytiť a modifikovať aktualizačný súbor s úmyslom poškodenia meradla**
Možné riešenie: Poskytnutie integrity údajov na overenie obsahu súboru aktualizácie.

Útok: **Útočník sa môže tváriť ako predvolená brána a zasielať falošné požiadavky o aktualizáciu elektromeru.**
Možné riešenie: Zaistenie nie len overenia odosielateľa ale aj obsahu jeho žiadostí.

Útok: **Útočník sa zmocní jedného alebo viacerých meradiel a začne nimi predvolenej bráne posielať veľké množstvo žiadostí.**
Možné riešenie: Do systému je potrebné integrovať mechanizmus autentifikácie, ktorý zistí či je požiadavka legitímna alebo nie.

Útok: **Útočník, ktorý odpočúva komunikačný kanál odchytí a znova zašle legitímnu notifikáciu o aktualizácii v jeho zvolený čas a iniciuje falošné sťahovanie**
Možné riešenie: Systém by mal identifikovať a zahadzovať opätovné žiadosti.

3.1.3 Životnosť kľúča

Kryptografia sa väčšinou používa na zaistenie bezpečnosti komunikácie nezabezpečené médium a na ochranu rôznych kritických aplikácií. Kryptografický kľúče zohrávajú dôležitú úlohu v procese kryptografie. Asymetrické nastavenie kľúča, všeobecne známe ako infraštruktúra verejného kľúča (PKI), využíva pár kľúčov (napr. verejný kľúč a súkromný kľúč) na vykonávanie kryptografických operácií. Životnosť kľúča spočíva v:

- generovanie kľúča,
- aktivácia kľúča,
- expirácia kľúča,
- revokácia kľúča,
- zničenie kľúča.

3.1.4 Digitálny certifikát

Existujú sú rôzne typy certifikátov podľa ich použitia. Najdôležitejší certifikát je koreňový certifikát (root certificate), ktorý sa používa sa na podpisovanie iných certifikátov. Ďalším typom certifikátov môže byť serverový certifikát použitý na autentizáciu identity servera alebo klientský certifikát, ktorý identifikuje klientov. Životný cyklus certifikátov je zväčša automatizovaný. Inteligentný elektromer systém požiada o výmenu alebo nový certifikát, ktorý sa následne odkáže na certifikačnú autoritu o vykonanie požiadavku.

Certifikáty vydáva certifikačná autorita a odosielajú sa do brány na distribúciu do elektromerov. Pri vydaní certifikátu bude jeho platnosť obmedzená dátumom exspirácie. Existuje viacero dôvodov prečo by certifikát mal byť vymenený a to napríklad uplynutie platnosti certifikátu, kompromitácia kľúčov alebo zastavenie platieb zákazníkom. Na vykonanie kontrol certifikátov sa vytvárajú zoznamy CRL (Certificate Revocation List – Zoznam neplatných certifikátov) a pravidelne sa zverejňujú. CRL zvyčajne obsahuje sériové čísla všetkých zrušených certifikátov spolu s ich dátumami zrušenia. Toto CRL je podpísané CA a z času na čas sa aktualizuje. Najnovšia verzia zoznamu CRL je sprístupnená všetkým potenciálnym uzlom, ktoré ho budú používať.

Na vrchole hierarchie certifikátov je Root CA (koreňový certifikát), na nižšej úrovni sa nachádza Subordinate CA (vedľajší certifikát), ktorý dostáva certifikáty od Root CA.

3.1.5 Všeobecný návrh Key Management Systému

Napriek tomu, že nasadenie inteligentnej siete má obrovské výhody, existujú kritické obavy o jeho bezpečnosť a súkromie. Najmä ak táto infraštruktúra zodpovedná za zhromažďovanie, analýzu a ukladanie osobných údajov o meraní a poskytovanie ich distribučnej spoločnosti. Zaistenie bezpečnosti inteligentného meradla a chránenie osobných údajov si vyžaduje zodpovedný prístup založený na životnom cykle, ktorý siaha od výroby cez zabudovanie až po samotné používanie [13].

V systéme bezpečnosti AMM figurujú 3 hlavné systémy:

1. KMS – Key Management Systém je systém na manažovanie hesiel a kľúčov – napríklad generovanie nových alebo výmena,
2. HSM – Hardware Security Module je modul na ukladanie kľúčov a certifikátov,
3. HES – Head End System slúži na zber a spracovanie dát z elektromerov pred ich uložením do databázy a následným použitím a validáciou.

Pri **výrobe** elektromera nastanú následujúce kroky:

- do elektromera sa vloží časť hardware – kryptografický modul, ktorý bude slúžiť na generovanie certifikátov a bezpečné úložisko,
- v elektrometri je vygenerovaný súkromný kľúč, ktorý je taktiež uložený v kryptografickom module a tento elektromer neopustí,
- kryptografický modul chráni súkromný kľúč a certifikáty. Taktiež bude exportovať verejný kľúč,
- do elektromera sa vložia kombinácie kľúčov (master key – kľúč slúžiaci na podpis globálnych kľúčov a global key),
- predajú sa certifikačné autority Root CA, Subordinate CA,
- nahrajú sa certifikačné autority Root CA, Subordinate CA,
- informácie vložené do elektromera sú šifrované na základe predom dohodnutého štandardu a podpísané predom dohodnutým certifikátom výrobcu,

Po opustení výroby sa meradlo otestuje a akceptuje autoritou, ktorá zhodnotí či zariadenie spĺňa všetky požiadavky. Skontroluje sa taktiež kombinácia kľúčov, prevedú sa fyzické a metrologické testy. Elektromer sa po úspešnom vložení certifikátov následne dostane do DS, kde sa pri **technickej inštalácii** elektromera:

- dešifruje sa potrebný obsah kryptografického modulu,
- overia a vygenerujú sa nové certifikáty a bezpečne sa uložia do KMS,
- overení sa zoznam neplatných certifikátov (Certificate revocation list – CRL) aby sa predišlo použitiu neplatných certifikátov,
- nasadenie elektromera,
- obnova kľúčov a certifikátov.

Platnosť certifikátov sleduje KMS a ich životnosť je obmedzená počtom použití alebo časovo. Certifikát elektromera má životnosť cca 10-15 rokov. Global a master kľúče zväčša 2-4 roky. Ak je nutné vytvoriť nový, elektromer vygeneruje nový pár kľúčov a s verejným kľúčom zašle žiadosť a vygeneruje sa nový certifikát. Certifikát pre elektromer vygeneruje PKI. Po tom ako elektromer a systém bezpečne obdrží nový certifikát, starý sa dostane do štádia revokácie a následne sa zničí. Výmena kľúčov prebieha po ich expirácii. Neide však o faktickú expiráciu, tá nikdy nenastane. Ak nastane situácia expirácie certifikátu na vrchole hierarchie (Subordinate CA alebo Root CA), certifikáty v nižšej úrovni sa taktiež vymenia.
Správy DLMS budú podpísané kľúčmi HES, zašifrované a zabezpečené autentikačným tagom:

- HES zašle správu HSM k podpisu,
- správa sa doručí a elektromer overí podpis,
- elektromer vytvorí odpoveď, ktorú podpíše certifikátom alebo privátnym kľúčom elektromera,

- HES správu prijme a odošle KMS na overenie.

Pri likvidácii a periodickej výmene elektromera sa počíta s tým, že neobsahuje žiadne informácie, ktoré by vedeli ovplyvniť chod celého systému a ostatných zariadení. Elektromer je teda po dobe jeho životnosti vyradený z centrálnej databázy systému a vymenený za nový. V prípade núteného odstavenia elektromera z dôvodu jeho čiastočnej nefunkčnosti sa zariadenie môže diagnostikovať a opraviť alebo nanovo nasadiť po uvedení do prvotného továrenského nastavenia. V mnoho prípadoch sa však oprava elektromerov z finančných dôvodov neuskutočňuje a na miesto vadného elektromera sa nasadí nový.

4 Metodika

Metodika uvádza funkčné a kvalitatívne požiadavky na bezpečnosť inteligentných meradiel, dátových koncentrátorov ako aj požiadavky na bezpečné vývojové procesy u dodávateľa. Tieto požiadavky sa aplikujú na obstarávanie a prevoz nový inteligentných meradiel alebo dátových koncentrátorov, nie na staré systémy.

4.1 Metodika bezpečnosti ENCS

Dokument od European Network for Cyber Security (ENCS) definuje požiadavky na bezpečnú komunikáciu od inteligentných elektromerov a dátových koncentrátorov k centrálnemu systému. Nedefinujú bezpečnosť centrálneho systému ako takého [26]. Táto metodika rozlišuje tri typy spojenia systému:

1. priame spojenie medzi elektromerom a centrálnym systémom,
2. spojenie medzi elektromerom a centrálnym systémom pomocou dátového koncentrátora, ktorý dáta zbiera a zasiela centrálnemu sytému,
3. spojenie medzi elektromerom a centrálnym systémom pomocou východzej brány, ktorá slúži iba ako prechod. Neobsahuje žiadne bezpečnostné prvky.

4.1.1 Požiadavky na inteligentný elektromer

Komponenty, na ktoré sa kladú požiadavky vrámci meradla sú zhrnuté v tabuľke 4.1.

Tab. 4.1: Komunikačné rozhrania inteligentného elektromera [26].

Typ rozhrania	**Popis požiadavkov**
Display	Fyzický displej, ktorý informuje zákazníka by mal byť iba read-only.
Rozhranie zákazníka	Komunikačný port, cez ktorý sa môžu odosielať informácie o zákazníkovi, malo byť iba read-only.
Rozhranie Multi-Utility	Voliteľné rozhranie, ktoré pripája iné meradlá (voda, plyn, teplo).
Rozhranie údržby	Rozhranie, ktoré môžu technici použiť lokálne ako prístup k inteligentnému meradlu.
Rozhranie LAN	Pripojenie na východziu bránu alebo dátový koncentrátor väčšinou cez PLC alebo mobilnú sieť.
Rozhranie WAN	Pripojenie na centrálny systém väčšinou cez mobilnú sieť.

4.1.2 Požiadavky na dátový koncentrátor

Komponenty dátového koncentrátora sú zhrnuté v tabuľke 4.2.

Tab. 4.2: Komunikačné rozhrania dátového koncentrátora [26].

Typ rozhrania	Popis požiadavkov
Rozhranie údržby	Lokálne prístupné pre servisných inžinierov buď cez Ethernet, sériový alebo USB port.
Rozhranie LAN	Pripojenie na elektromer väčšinou cez PLC alebo bezdrôtovú sieť.
Rozhranie WAN	Pripojenie na centrálny systém väčšinou cez mobilnú sieť.

4.1.3 Požiadavky na východziu bránu

Komponenty východzej brány sú rovnaké ako pri dátovom koncentrátore.

4.1.4 Požiadavky na bezpečnosť

Protokoly a služby

Protokoly a služby by mali spĺňať hlavne tieto požiadavky:

- zariadenia by mali podporovať iba tie komunikačné protokoly a sieťové služby, ktoré potrebuje na splnenie svojich funkčných požiadaviek,
- zariadenia nesmú používať služby alebo aplikácie, ak sú pre ne známe zraniteľnosti,
- je doporučené prevádzať penetračné testy a skenovanie prostredia na vyhodnotenie týchto dvoch predošlých požiadavkov.

Hardvérové porty

Hardvérové porty by mali spĺňať požiadavky ako:

- zariadenie by navonok malo odhaľovať iba tie hardvérové porty, ktoré potrebuje na splnenie svojich funkčných požiadavok,
- zariadenie by malo mať všetky ladiace porty na doske plošných spojov vypnuté, aby ich nebolo možné použiť na čítanie alebo zápis do pamäte,
- je doporučené prevádzať penetračné testy a skenovanie portov na vyhodnotenie týchto dvoch predošlých požiadavkov.

Užívateľské profily

Profily na zariadení musia spĺňať tieto požiadavky:

- zariadenie by malo obsahovať iba také užívateľské profilov, ktoré potrebuje na splnenie svojich funkčných požiadavok,
- je doporučené prevádzať penetračné testy a skenovanie profilov na vyhodnotenie predošlej požiadavky.

4.1.5 Požiadavky na kryptografiu

Kryptografické algoritmy

Požiadavky na kryptografické algoritmy zahŕňajú:

- zariadenie by malo na zabezpečenie svojej funkčnosti používať iba tie kryptografické algoritmy a parametre, ktoré sú v súlade s doporučenými postupmi a národnými predpismi,
- zariadenie nesmie používať proprietálne kryptografické algoritmy,
- implementované algoritmy a parametre by mali byť súčasťou dokumentácie,
- je doporučené prevádzať penetračné testy algoritmov na vyhodnotenie predošlých požiadavkov.

Generovanie náhodných čísel

Na generovanie náhodných čísel sú kladené tieto požiadavky:

- zariadenie by malo pri generovaní náhodných čísel pre bezpečnostné funkcionality používať iba kryptografické generátory náhodných čísel zo zdrojov ako AIS 20, AIS31 alebo FIPS 140-2,
- je doporučené prevádzať funkčné testy algoritmov na vyhodnotenie predošlého požiadavku.

4.1.6 Integrita dát

Autenticita správ

- Zariadenie by malo kryptograficky overiť pravosť všetkých údajov aplikačnej vrstvy, ktoré dostane z rozhraní nižšie.
- Ak zariadenie nemôže overiť pravosť údajov, odmietne ich alebo ich zahodí.
- Zariadenie musí autentizovať všetky údaje aplikačnej vrstvy, ktoré odosiela z nižších rozhraní. Netýka sa to údajov, ktoré nie je možné autentifikovať.

Potvrdzovanie vstupov

- Zariadenie by malo potvrdzovať všetky prijaté dáta.

- Je doporučené prevádzať penetračné testy spolu s testami, ktoré overujú či je zariadenie schopné spracovať správy s pridaním fuzzingu.

Podpisovanie firmvéru

Pri podpisovaní firmvéru by zariadenie malo spĺňať tieto požiadavky:

- zariadenie by pred použitím aktualizácie firmvéru malo overiť jej digitálny podpis,
- zariadenie by malo odmietnuť firmvér práve vtedy keď zistí že bol upravený alebo ak jej digitálny podpis overiť nemôže,
- zariadenie by malo odmietnuť firmvér, ak je číslo jeho verzie nižšie ako číslo aktuálne nainštalovaného firmvéru,
- je doporučené prevádzať testy na overenie inštalovaných firmvérov s platným podpisom a vyššími číslami verzie ako aj či je firmvér s neplatným podpisom alebo nižším číslom verzie odmietnutý.

4.1.7 Dôvernosť dát

Dôvernosť správ

- Zariadenie by malo šifrovať všetky údaje aplikačnej vrstvy, ktoré prijíma na rozhraní nižšie s výnimkou údajov, ktoré sa nedajú odoslať šifrovane.
- Zariadenie by malo zašifrovať všetky dáta aplikačnej vrstvy, ktoré odošle na nižších rozhraniach okrem dát, ktoré sa nedajú zašifrovať.
- Je doporučené prevádzať testy na overenie správnej aplikácie šifrovania alebo prípadné použitie nižších techník bezpečnosti komunikačných protokolov.

4.1.8 Riadenie prístupu

- Zariadenie by malo oddeľovať role užívateľov vytvorením rôznych účtov pre každú rolu.
- Zariadenie by malo umožňovať priradenie individuálnych prihlasovacích údajov a kľúčov každej role aby sa predišlo možnosti autentifikácie jednej role ako role inej alebo odpočúvaniu komunikácií iných rolí.
- Zariadenie by malo umožňovať naviazanie rolí na jednotlivé rozhrania.
- Zariadenie by malo byť schopné zabrániť útokom zneužitia privilégií.

5 Key Management System

Táto časť práce bola konzultovaná s distribučnou spoločnosťou. K zaručeniu bezpečnej komunikácie a služieb je za potreby aj v energetickom sektore vytvoriť zabezpečený systém, ktorý bude spoľahlivo prenášať dáta od meradla až k distribučnej spoločnosti. Základom celého systému je:

- KMS (Key Management System),
- PKI (Public Key Infrastructure).

5.1 Životný cyklus

5.1.1 Public Key Infrastructure

PKI je entita vybudovaná v rámci Key Management Systému energetickou spoločnosťou. Štandardom pre tento systém sú eliptické krivky. Kryptografia s využitím verejného kľúča sa v dnešnej dobe stala štandardom pre bezpečnú komunikáciu cez internet ale aj iné komunikačné médiá, ako sú mobilné siete alebo siete Wi-Fi. Eliptické krivky majú v porovnaní s technikami verejných kľúčov omnoho lepší výkon a vyššiu bezpečnosť čo viedlo k rýchlemu získaniu uznania a popularity. V dokumentácii k štandardu DLMS sa konkrétne v Green Booku nachádzajú doporučenia na typ eliptických kriviek. Tabuľka 5.1 rozlišuje typ krivky pre rôzné úrovne zabezpečenia. Krivky odporúča organizácia NIST (National Institute of Standards and Technology), ktorá sídli v americkom ministerstve obchodu, ktorej úloha spočíva v pomáhaní rôznym inštitúciám správne pochopiť, spravovať, znižovať riziko kybernetickej bezpečnosti a chrániť ich siete a údaje. Tohto cieľa sa snažia dosiahnuť vydávaním štandardov.

Tab. 5.1: Eliptické krivky podľa štandardu DLMS/COSEM.

Security suite	**Názov krivky**
Security suite 0	-
Security suite 1	Krivka od NIST P-256
Security suite 2	Krivka od NIST P-384

P-256

Elliptic Curve Digital Signature Algorithm (ECDSA) P-256 charakterizuje nasledujúca rovnica [27]:

$$y^2 = x^3 - 3x + b \, mod \, q \tag{5.1}$$

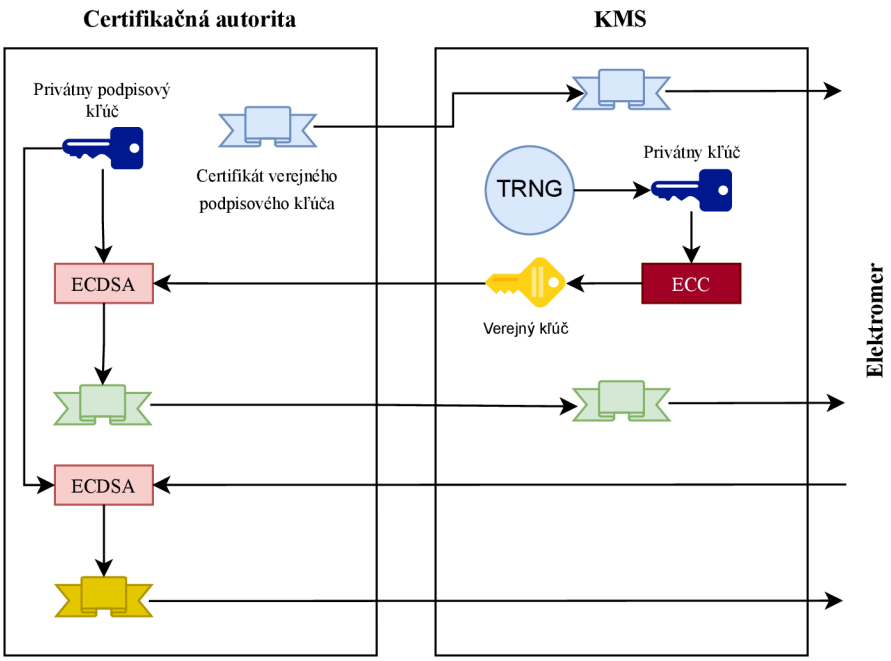
P-384

P-384 je eliptická krivka, ktorú NSA (National security agency) odporúča používať, pokiaľ nebudú štandardizované postkvantové metódy. Poskytuje 192 bitovú bezpečnosť, zatiaľ čo bežnejšie používané krivky poskytujú 128 bitov. P-384 charakterizuje následujúca rovnica [27]:

$$y^2 = x^3 - 3x + b \tag{5.2}$$

PKI s dôveryhodnou certifikačnou autoritou

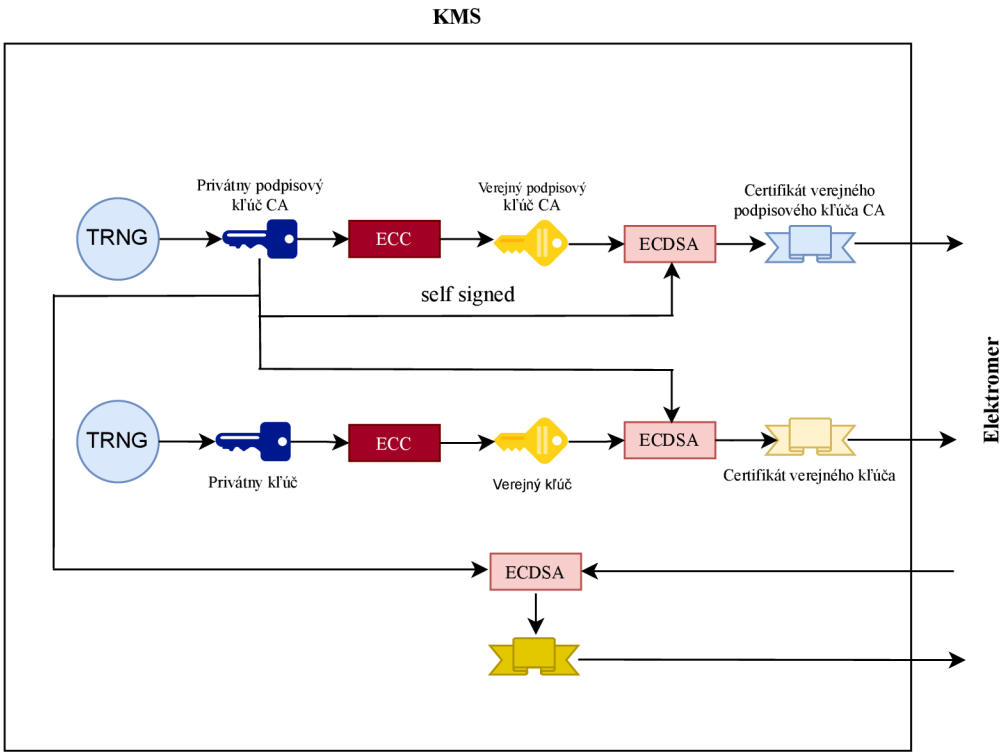
V tomto prípade distribučná spoločnosť spolupracuje s dôveryhodnou certifikačnou autoritou, ktorá vlastní svoj privátny podpisový kľúč a nikomu ho nikdy nezdelí. K tomuto privátnemu kľúču je vygenerovaný kľúč verejný, ktorý sa v podobe certifikátu dostane do KMS a následne do elektromera. Koreňový certifikát by sa do zariadení mal vkladať počas výroby a táto kópia verejného kľúča sa bude nachádzať v každom z nich. Týmto krokom sa zaistí to, že elektromer v budúcnosti príjme iba tie certifikáty, ktoré sú podpísané práve týmto privátnym kľúčom. Štandard DLMS nedefinuje presný alebo preferovaný čas vloženia koreňového certifikátu do zariadenia, mal by iba predchádzať akýmkoľvek iným, ktoré sa do zariadenia plánujú nasadiť. Tento certifikát je nemenný a platí počas celej životnosti elektromera. KMS následne vygeneruje svoj vlastný podpisový pár kľúčov, ktorý bude využiteľný napríklad pri podpise komunikácie vo výmene kľúčov počas Diffie-Hellman protokolu. Verejná časť tohto páru sa zašle pomocou správy CSR (Certification signing request) certifikačnej autorite, ktorá ho svojím privátnym kľúčom podpíše, vytvorí certifikát a zašle naspäť KMS, ktorý to distribuuje elektromeru. V samotnom elektromery sa taktiež vygeneruje pár kľúčov s rovnakým účelom ako podpisovanie dát alebo dočasných DH kľúčov. Verejný kľúč sa taktiež v certifikačnej autorite podpíše a vo forme certifikátu sa vráti naspäť do meradla. Tento scénar charakterizuje obrázok 5.1.



Obr. 5.1: Public Key Infrastructure s certifikačnou autoritou.

PKI bez certifikačnej autority

Majiteľom privátneho podpisového kľúča je samotná energetika a spolu so svojím párom verejného podpisového kľúča sa obe nachádzajú v KMS. Certifikát verejného podpisového kľúča sa vygeneruje technikou self signed, čiže podpisom verejného kľúča kľúčom privátnym. Generovanie ostatných kľúčov sa realizuje ako v predošlom prípade iba s tým rozdielom, že sú podpisované vrámci KMS a distribuované do elektromerov. Elektromer rovnako vygeneruje svoj podpisový pár, zašle verejný kľúč do KMS, kde sa vytvorí certifikát a vráti sa do elektromeru. Výhodou tejto techniky bez použitia certifikačnej autority je jej cena. Distribučná spoločnosť nemusí platiť externej certifikačnej autorite za jej služby. Obrázok 5.2 zobrazuje túto schému PKI.



Obr. 5.2: Public Key Infrastructure bez certifikačnej autority.

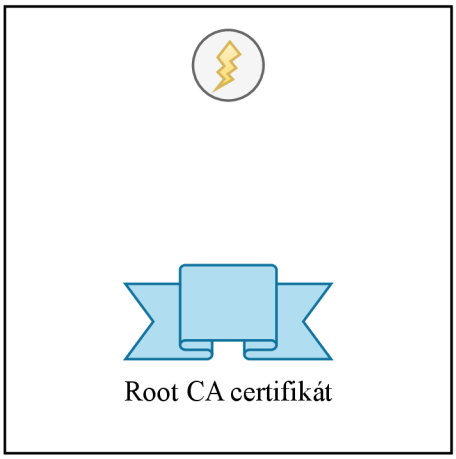
Model dôvery

Pre systémy inteligentných meradiel založených na protokole DLMS/COSEM, by mali využívať kryptografiu s verejným kľúčom, rôznymi pármi verejných a súkromných kľúčov a certifikáty verejných kľúčov. **Certifikát verejného kľúča** spája verejný kľúč s identitou určitého subjektu. **Certifikát** je digitálne podpísaný certifikačnou autoritou. Na poskytovanie a správu certifikátov slúži infraštruktúra Public Key Infrastructure, ktorá pozostáva z certifikačných autorít vydávajúce certifikáty použité koncovými entitami. Prvý certifikát z celého reťazca certifikátov musí byť opretý o dôveryhodnú certifikačnú autoritu, zvyčajne Root CA. Všetky certifikáty majú v systéme predurčenú dobu platnosti. Tieto certifikáty môžu byť po ukončení ich platnosti nahradené. Server musí pred použitím certifikátu skontrolovať nasledovné:

- syntax certifikátu,
- atribúty vrámci certifikátu,
- kontrola validity a platnosti certifikátu,
- dôveryhodná cesta certifikátu k jeho autorite,
- podpis vydavateľa certifikátu.

Výroba

Energetická spoločnosť poskytne výrobcovi meradla koreňový certifikát certifikačnej autority Root CA. Pri výrobe je tento certifikát vložený do elektromera, nie je možné ho vymazať ani modifikovať. Certifikát obsahuje informácie o vydávateľovi, žiadateľovi, jeho platnosti, verejný kľúč a podpis. Tento certifikát bude slúžiť na overovanie podpisov ostatných certifikátov cez Root CA, ktoré budú v budúcnosti inštalované do elektromera. Týmto bude dosiahnuté faktu, že elektromer bude akceptovať iba tie certifikáty, ktoré boli podpísané Key Management Systémom príslušnej energetickej spoločnosti alebo poprípade nadriadenou autoritou. Tento certifikát je **neodstraniteľný** a má **neobmedzenú platnosť**. Stav elektromera je naznačený na obrázku 5.3.

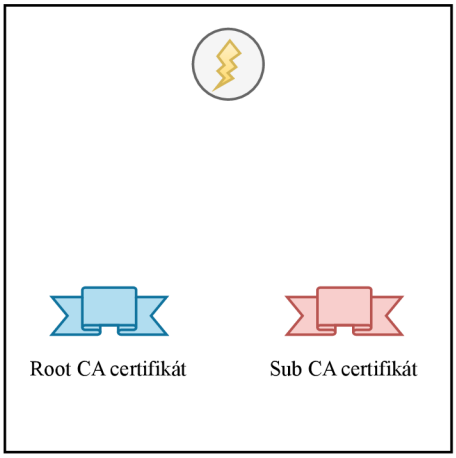


Obr. 5.3: Vloženie Root CA do elektromera.

Inštalácia

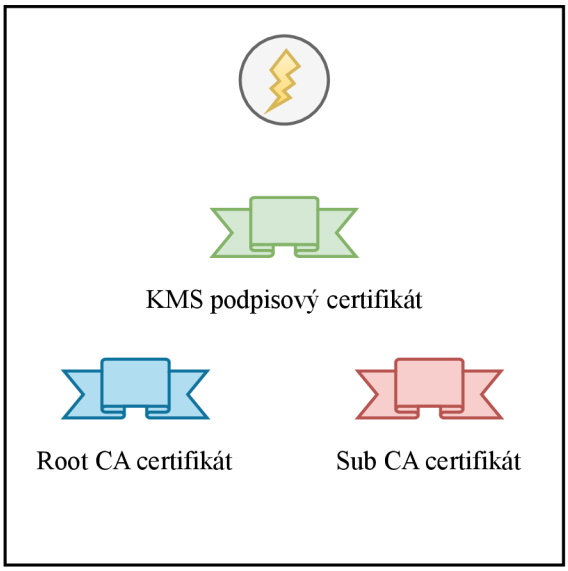
Po inštalácii má elektromer zatiaľ iba koreňový certifikát čo znamená že komunikácia nie je zabezpečená a vytváranie vyššie zabezpečených asociácií nie je doposiaľ možné. V elektromeri sa nevyskytujú žiadne kľúče.

KMS následne vygeneruje svoj pár kľúčov Sub CA a importuje verejnú časť vo forme certifikátu do elektromera, ako je zobrazené na obrázkuu 5.4. V elektromeri sa táto dvojica overí pomocou predošle vloženého certifikátu Root CA. Certifikáty tvoria iba verejnú časť kľúčového páru. Ku každému existuje kľúč privátny, ktorý je uložený iba v KMS distribučnej spoločnosti a v nadriadenej certifikačnej autorite. Privátny kľúč nikdy tieto entity neopustí.



Obr. 5.4: Vloženie certifikátu Sub CA.

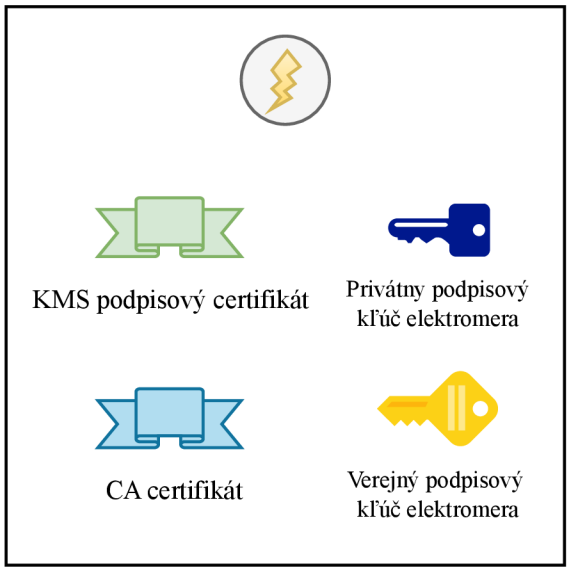
V ďalšom kroku KMS vygeneruje svoj podpisový pár kľúčov a verejnú časť vo forme certifikátu vloží do elektromera. V elektromeri sa tento certifikát overí pomocou certifikátu podradenej certifikačnej autority Sub CA, pretože vydavateľom je teraz už KMS, nie certifikačná autorita. Tento certifikát slúži k tomu, aby KMS mohlo pomocou privátneho kľúča niečo podpísať tak, aby bol elektromer pomocou tohto certifikátu schopný overiť že je to skutočne podpísané KMS. Všetky tri doposiaľ prítomné certifikáty je vidieť na obrázku 5.5.



Obr. 5.5: Vygenerovanie podpisového páru.

KMS vyvolá v elektromeri generovanie podpisového páru kľúčov. Aby existoval aj podpisový certifikát elektromeru, ktorým si KMS vie overiť správnosť komunikácie od elektromera, elektromer vygeneruje svoj vlastný privátny kľúč pomocou generátora náhodných čísel, ku ktorému sa dopočíta kĺúč verejný. Situácia v elektromeri

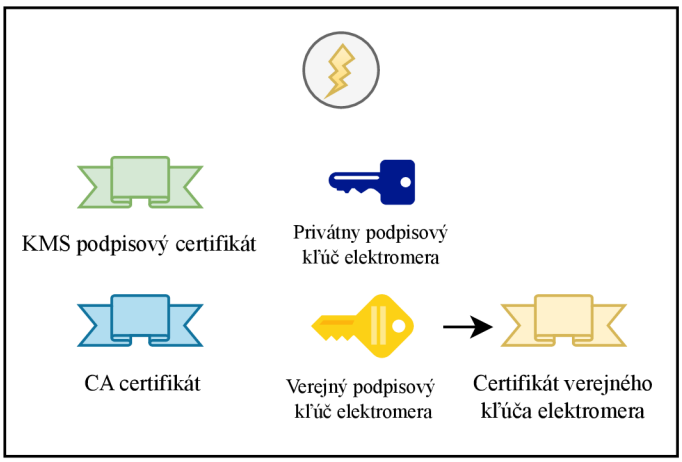
je zobrazená na obrázku 5.6.



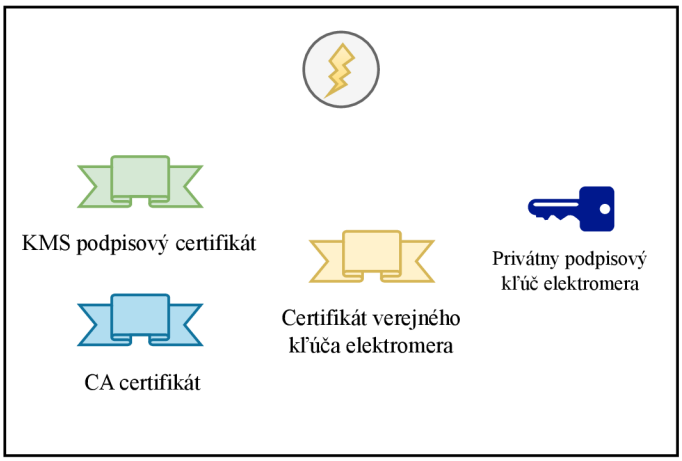
Obr. 5.6: Vygenerovanie podpisového páru kľúčov.

KMS vyvolá v elektromeri žiadosť o vystavenie certifikátu pre vygenerovaný verejný kľúč, ktorá sa nazýva CSR (Certificate Signing Request).

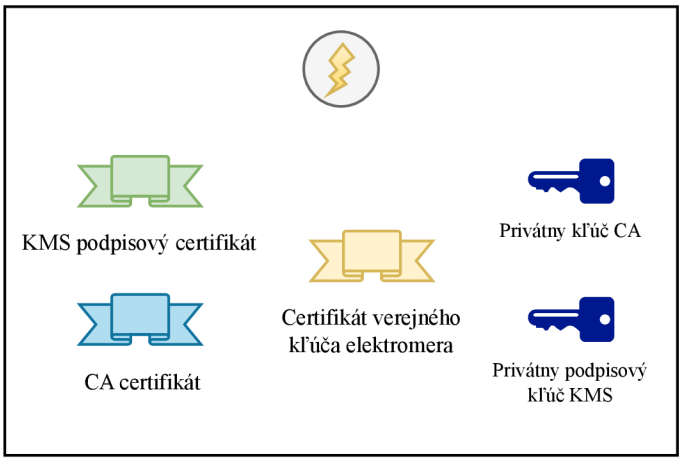
KMS následne na základe žiadosti CSR od elektromeru vygeneruje certifikát požadovaného podpisovaného verejného kľúča elektromeru a privátnym kľúčom Sub CA ho podpíše. Vyrobený certifikát sa importuje naspäť do elektromera, ako naznačuje obrázok 5.7. Na obrázku 5.8 a 5.9 je zhrnutý všetok kryptografický materiál.



Obr. 5.7: Vygenerovanie certifikátu podpisového páru kľúčov.



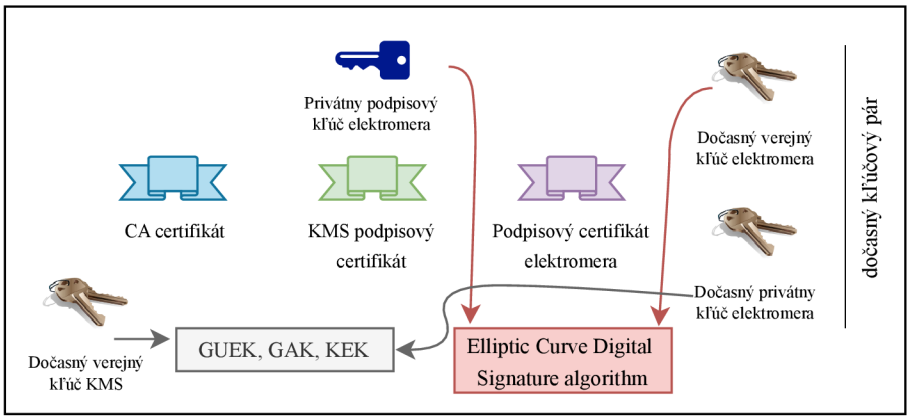
Obr. 5.8: Kľúče a certifikáty v elektromeri.



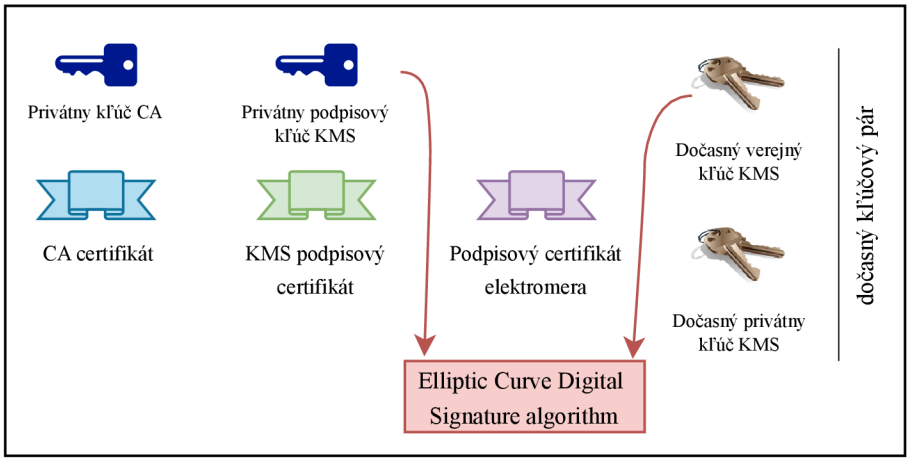
Obr. 5.9: Kľúče a certifikáty v KMS.

Generovanie a výmena kľúčov pomocou ECC Diffie Hellman

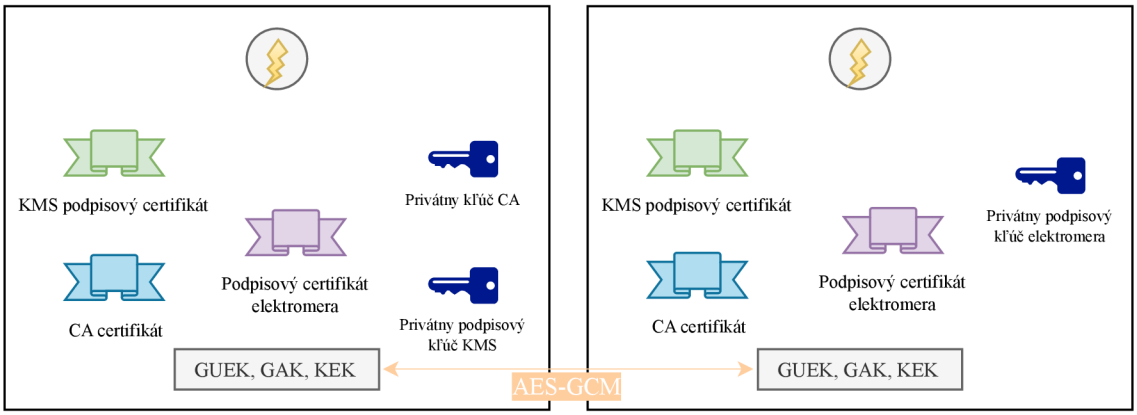
KMS v prvom kroku vygeneruje svoj dočasný privátny kľúč a dopočíta k nemu verejnú časť. Ten podpíše pomocou svojho podpisového privátneho kľúča a odošle ho do elektromera. Obrázok 5.10 a 5.11 naznačuje prípravu kryptografického materiálu pre AES-GCM. Elektromer overí, že dočasný verejný kľúč je skutočne od KMS a následne vygeneruje svoj dočasný kľúčový pár. Ako je vidieť na obrázku 5.10, zariadenie už má všetko k tomu, aby odvodilo symetrický kľúč, ktorý tvorí súčin privátneho dočasného kľúča elektromera a dočasného verejného kľúča KMS. Na oboch stranách prebehne vytvorenie kľúčov GUEK, GAK a KEK. Od tejto chvíle môžu pomocou protokolu AES-GCM elektromer a KMS komunikovať zabezpečene, ako je zobrazené na obrázku 5.12. Dočasné kľúče vytvorené pre túto reláciu sa zničia.



Obr. 5.10: Príprava kľúčov pre AES-GCM na strane elektromera.



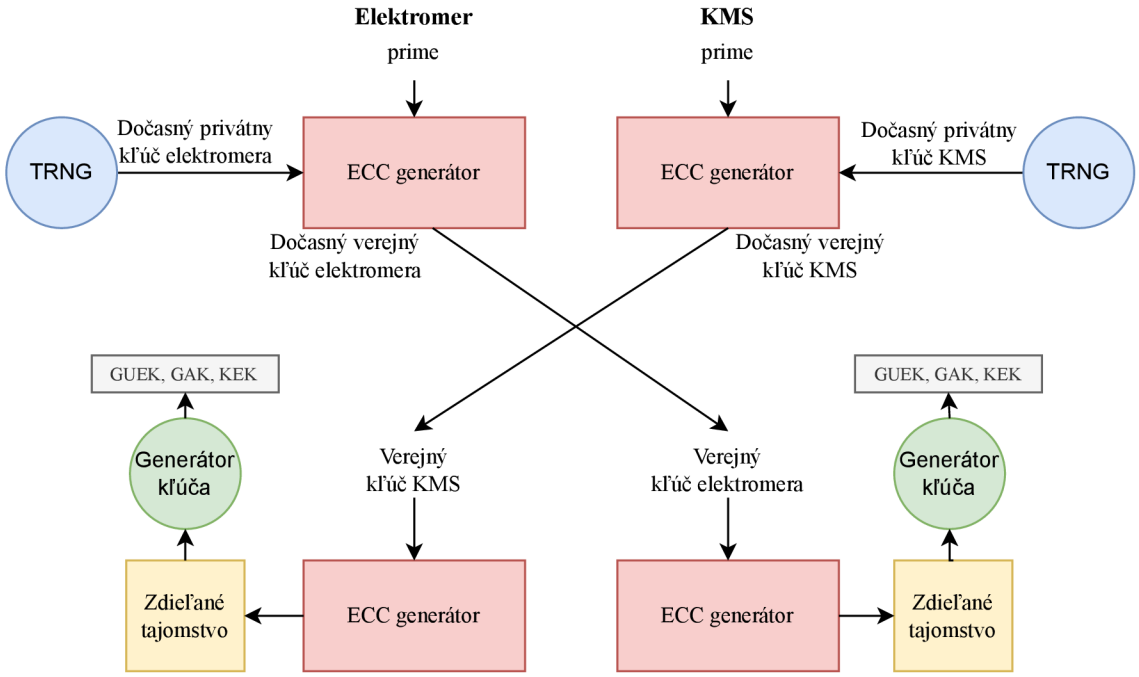
Obr. 5.11: Príprava kľúčov pre AES-GCM na strane KMS.



Obr. 5.12: Komunikácia pomocou AES-GCM.

Priebeh ECC Diffie Hellman

Generátorom náhodných čísel sa na oboch stranách tj. na strane elektromera aj KMS vytvorí dočasný privátny kľúč, ktorý sa vloží do generátoru eliptických kriviek. Ich kombináciou získame dočasný verejný kľúč, ktorý sa zašle protiľahlej strane. Strana elektromera skombinuje svoj dočasný privátny kľúč s verejným kľúčom KMS a týmto krokom vytvorí zdieľané tajomstvo. Z tohto tajomstva sa následne vygenerujú kľúče GUEK, GAK a KEK pre AES-GCM. Kľúče kvôli závislosti nie sú vytvorené v jednom procese ECDH ale viacerých. Dočasné kľúče po ukončení tohto procesu obe strany zničia. Priebeh protokolu je zobrazený na obrázku 5.13



Obr. 5.13: Ustanovenie kĺúčov pomocou Elliptic Curve Diffie Hellman.

5.1.2 Kryptografický materiál

Ako bolo spomenuté v predošlých schémach, jedné z najdôležiteších komponentov celého systému sú kľúče:

- GUEK – Global Unicast Encryption Key,
- GAK – Global Authentication Key,
- KEK – Key Encryption Key.

Kľúč GUEK je globálna kľúč, používaný v niekoľkých inštanciách AA (Application Association) opakovane vytvorených medzi tými istými partnermi [34]. Kľúč Master key (KEK) šifruje iný kľúč (zvyčajne šifrovacie kľúče prevádzky) na prenos alebo ukladanie. Takto sa poskytne ochrana dôvernosti týchto kľúčov. Kľúč GAK

sa môže použiť v kombinácii s inými modulmi na generovanie zdieľaného *kex nonce* [35]. Symetrické kľúče majú v systéme 256 bitov a kľúče v certifikátoch zas 2048 až 3072 bitov. Kľúče zhŕňa tabuľka 5.2.

Tab. 5.2: Kľúče použité pri komunikácii.

Symetrické kľúče

Globálne statické kľúče AES	- GUEK, GAK, KEK - Výmena pre Diffie Hellmana - Transport kľúča KEK - Tieto kľúče majú neobmedzenú platnosť - Sú rýchle
Dočasné AES kľúče	- Sú časovo obmedzené - Využívajú sa iba pre otvorené asociácie - Zaniknú po uzavretí spojenia

Asymetrické kľúče

Pár podpisových kľúčov	- Slúži na digitálny podpis dát - Použije sa na podpis dočasných verejných kľúčov pri výmene GUEK, GAK a KEK
Pár kľúčov Diffie Hellman	- Slúži na výmenu krátkodobých GUEK, GAK pre tretie strany

Kde je uložený kryptografický materiál

Každý elektromer má vo svojom hardware procesor a externú flash. Procesor sa skladá z jadra, RAM, TRNG a FLASH. Privátne nesymetrické kľúče a symetrické kľúče GUEK, GAK a KEK sú uložené v pamäti FLASH. Certifikáty verejných kľúčov sa nachádzajú v externej FLASH. Ďalšou, bezpečnejšou variantou by boli zariadenia Trusted Platform Module (TPM), ktorý plní úlohu bezpečného kryptoprocesoru. Tento typ procesoru sa zväčša používa pri výkonnejších a drahších zariadeniach, preto tento modul netvorí štandardnú výbavu elektromera pri obmedzených rozpočtoch energetických spoločností.

5.2 AES Galois Counter Mode

AES Galois/Counter Mode v skratke AES-GCM implementuje kódovanie a dekódovanie v súlade so štandardom NIST. Spracováva 128-bitové bloky a je programovateľný pre 128, 192 a 256 bitové dĺžky kľúčov. GCM je režim pre šifrovacie blokové šifry so symetrickým kľúčom a je ideálny na ochranu údaje v paketoch, pretože

má nízku latenciu a minimálnu prevádzkovú réžiu [32]. O šifrovanie datových rámcov sa v protokole DLMS/COSEM stará práve tento algoritmus. GCM poskytuje zaručenie dôveryhodnosti údajov pomocou variácie režimu *Counter mode* operácie pre šifrovanie. GCM taktiež zaručuje pravosť dôverných údajov pomocou univerzálnej hashovacej funkcie, ktorá je definovaná cez binárne pole Galois. Služba GCM môže tiež poskytnúť dodatočnú záruku overenia dáta, ktoré nie sú zašifrované [33]. Tento algoritmus má 4 hlavné vstupy [31, 33]:

- **tajný kľúč EK** (Encryption Key),
- **inicializačný vektor IV** (Initialization Vector),
- **dáta** vo forme plaintext,
- **dodatočné dáta na autentizáciu ADD** (Additional Authenticated Data), ktoré obsahujú informácie o forme zabezpečenia.

5.3 Veľkosti kľúčov

K veľkosti kľúčov algoritmov, ktoré sa využívajú v kryptografii sa v Českej republike vyjadruje Národný úrad pre kybernetickú a informačnú bezpečnosť (NÚKIB). Veľkosti kľúčov sú v tabuľke 5.3. Európska únia konkrétne nevymädzuje veľkosti ani typ používaných kľúčov, kryptografických algoritmov a šifier.

5.3.1 Vyhláška č. 359/2020 Sb. o měření elektřiny

Vyhláška číslo 359/2020 vydaná dňa 13. augusta 2020 spolu so Zákonom o energetike druhy meracích zariadení upravuje niekoľko aspektov merania ako umiestnenie meracích zariadení, spôsob vyhodnocovania a určovania množstva odoberanej elektriny ale aj bezpečnostné požiadavky pre meradlá merania typu C, ktoré sú zhrnuté v tabuľke 5.4 [36].

5.4 Menežment certifikátov

5.4.1 Obstaranie serverov s dôveryhodnou autoritou

Každý z aktívnych serverov by mal mať ujasnenú jeho dôveryhodnú autoritu (anglicky *trust anchor*), ktorou sa budú overovať certifikáty. Dôveryhodnými entitami môžu byť certifikáty koreňovej Root CA), certifikáty Sub-CA alebo priamo dôveryhodné kľúče CA. Server môže byť vybavený viac ako jednou dôveryhodnou entitou. Podľa [31] sú naň kladené následujúce požiadavky:

- dôveryhodná autorita musí byť umiestnená na serveri Out-of-band,
- jej certifikáty sú uložené spolu s inými certifikátmi,

Tab. 5.3: Tabuľka noriem podľa NÚKIBu [30]. Prevzaté z [39].

Symetrické algoritmy		
Kategória	**Schválené**	**Dostatočné**
Blokové a prúdové šifry	AES keys 128,192,256 b Twofish keys 128 až 256 b Serpent keys 128,192,256 b Camellia keys 128,192,256 b SNOW 2.0 SNOW 3G keys 128 a 256 b ChaCha20 key 256 b	3DES key 112 b Blowfish key > 128 b Kasumi key 128 b
Metódy šifrovania	CCM EAX OCB1 a OCB3 (OCB3 > OCB1) GCM (nonce:96 b, tag:128 b) ChCha20 Poly1305 s kľúčom < 256 GB Schémy typu *Encrypt-then-MAC*	CTR OFB CBC a CBC-CS) CFB
Metódy ochrany identity	HMAC s hašovacou funkciou EMAC CMAC UMAC (tag:64 b)	HMAC-SHA1 CBC-MAC-X9.19
Asymetrické algoritmy		
Algoritmy digitálneho podpisu	DSA key ≥ 3072 b s podgrupou ≥ 256 b EC-DSA key ≥ 256 b RSA-PSS key ≥ 3072 b EC-Schnorr key ≥ 256 b	DSA key 2048 b EC-DSA key 224 b RSA-PSS key 2048 b EC-Schnorr key 224 b
Algoritmy pre procesy s kľúčmi	DH key ≥ 3072 b s podgrupou ≥ 224 b ECDH key ≥ 256 b ECIES-KEM key ≥ 256 b PSEC-KEM key ≥ 256 b ACE-KEM key ≥ 256 b RSA-OAEP key ≥ 3072 b RSA-KEM key ≥ 3072 b	DH key 2048 b ECDH key 224 b ECIES-KEM key 224 b PSEC-KEM key 224 b ACE-KEM key 224 b RSA-OAEP key 2048 b RSA-KEM key 2048 b
Algoritmy hashovacích funkcií		
Funkcie SHA2, SHA3	SHA-256, SHA3-256 SHA-384, SHA3-384 SHA-512, SHA3-512 SHA-512/256, SHA3-512 SHAKE-128, SHAKE-256	SHA-224,SHA-512/224 SHA3-224 RIPEMD-160
Iné funkcie	Whirpool BLAKE2	

Tab. 5.4: Tabuľka požiadavok na bezpečnosť pre meradlá merania typu C [36].

Zaistenie dôvernosti a integrity	Bloková šifra GCM Bloková šifra CCM
Zaistenie dôvernosti	Bloková šifra AES-256
Zaistenie integrity	Digitálny podpis DSA 3072 Digitálny podpis EC-DSA-256 Digitálny podpis RSA 3072 Hash SHA2-256 Hash SHA3-256 Mód pre ochranu integrity CMAC Mód pre ochranu integrity HMAC
Management s kľúčami	DH-3072 ECDH-256
Generátor náhodných bitov	HMAC DRBG pre SHA2 a SHA3 Hash DRBG pre SHA2 a SHA3

- môže dôjsť k ich exportovaniu, nemôžu však byť importované alebo odstránené,
- dôveryhodné kľúče certifikačnej autority nemožno exportovať.

Ďalšie certifikáty

Server môže byť vybavený ďalšími certifikátmi certifikačnej autority, ktoré sa použijú na overenie digitálnych podpisov na certifikátoch koncových zariadení. Na tento účel slúži metóda *import_certificate* objektu Security setup.

5.4.2 Pridelenie bezpečnosti serveru

Pridelením bezpečnosti je myslené zaobstaranie asymetrických kľúčových párov a príslušných certifikátov verejných kľúčov.

6 Laboratórna úloha

V tejto časti práce bude demonštrovaná praktická implementácia komunikácie medzi dvoma entitami, elektromerom a dátovou centrálou. Komunikácia môže prebiehať v nešifrovanej i šifrovanej podobe medzi klientom (elektromerom) a serverom (dátovou centrálou), ktorú umožňuje protokol DLMS/COSEM.

6.1 Teoretický úvod

6.1.1 DLMS/COSEM

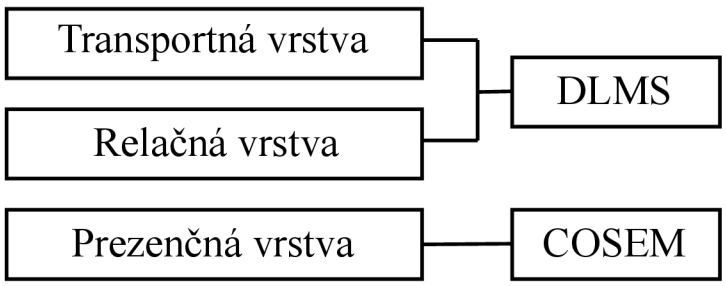
DLMS štandard bol adaptovaný Medzinárodnou elektrotechnickou komisiou- International Electrotechnical Commission (IEC) do štandardov typu IEC 62056. DLMS/COSEM protokol je využiteľný v rôznych oblastiach merania a to:

- meranie spotreby elektriny,
- meranie spotreby plynu,
- meranie spotreby vody a tepla.

Protokol sa skladá z troch hlavných častí:

- DLMS – Device Language Message Specification,
- COSEM – Companion Specification for Energy Metering,
- OBIS – Object Identification System.

Úlohou DLMS je poskytnúť interoperabilitu prostredia pre štruktúrované modelovanie a výmenu údajov z meradiel. DLMS model je modelovaný do tried rozhraní, ktoré slúžia ako štruktúra pre dáta. Je schopné komunikovať s elektromerom a čítať dostupné funkcionality a dáta. Časť COSEM slúži pre tvorbu objektov. Oddelenie aplikačnej vrstvy od transportnej naznačenej na obrázku 6.2 v budúcnosti umožní rýchlu a efektívnu výmenu použitých komunikačných technológií. Aj tento protokol teda do svojej implementácie aplikuje univerzálnosť, jednú z najdôležitejších myšlienok pri vývoji nových protokolov a technológií.



Obr. 6.1: Separácia aplikačnej vrstvy od transportnej.

Protokol je špecifikovaný v štyroch knihách rozdelených na:

- Green Book – obsahuje komunikačné modely a procesy komunikácie,
- Blue Book – špecifikuje systém OBIS priraďovanie objektov,
- Yellow Book – definuje procesy testovania a výber vhodných nástrojov,
- White Book – definuje pojmy.

Koncept bezpečnosti DLMS je podopretý niekoľkými mechanizmami, ktoré sa navzájom dopĺňajú. **Autentifikácia entít** zaistí, že výmena dát môže prebehnúť iba medzi entitami, ktoré prešli vhodnou autentifikáciou a potvrdením identity. **Prístup založený na roliach** zaručí že prístup k objektom COSEM je zaručený iba pre klientov so správnym prístupovým profilom. **Ochrana správ** zaisťuje, že údaje uchovávané objektom COSEM môžu byť prístupné iba prostredníctvom vhodne zabezpečených správ. **Ochrana dát** prichádza v úvahu počas prenosu senzitívnych alebo kritických dát, ktoré vyžadujú samostatnú ochranu. Protokolom DLMS/COSEM poskytuje tri základné vrstvy triády CIA:

- zaistenie dôvernosti – obmedzenie prístupu k informáciám,
- zaistenie integrity – ochrana proti modifikácii zničeniu dát,
- zaistenie dostupnosti – zabezpečenie včasného a spoľahlivého prístupu.

6.1.2 Identifikátory

Všetky entity (klient, servery, tretie strany) majú unikátny identifikátor, ktorý sa priradí atribútu system title a je nemenný. Požiadavky na system title sú jedinečnosť a dĺžka 64 bitov (prvé 3 oktety sú ID výrobcu, ostatných 5 oktetov je výnimočné číslo) a často sa jedná o časť sériového čísla.

6.1.3 COSEM triedy a objekty

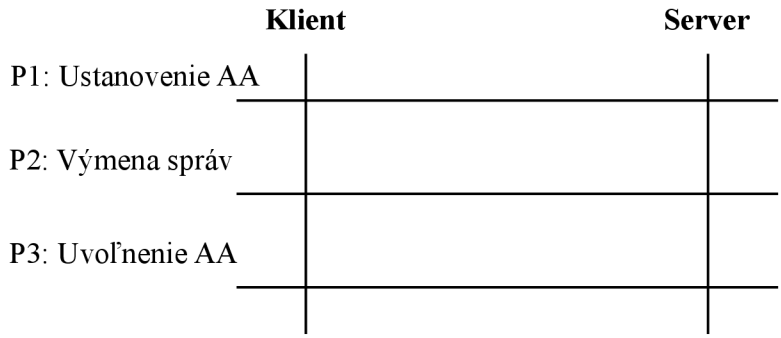
Každý objekt tvoria atribúty a metódy. Atribúty predstavujú vlastnosti objektu a jej hodnota môže ovplyvniť správanie objektu. Prvý atribút v každom objekte je *logical_name* a tvorí jednu časť identifikácie objektu. Objekty môžu ponúkať množstvo metód na preverovanie alebo úpravu hodnôt atribútov. Objekty, ktoré medzi sebou zdieľajú spoločnú charakteristiku sú zovšeobecnené ako trieda rozhrania, ktorú identifikuje *class_id*. Protokol umožňuje výrobcom pridávať do akýchkoľvek objektov proprietárne metódy a atribúty [38].

6.1.4 Priebeh spojenia

Priebeh spojenia (relácie) má 3 fázy:

- Aplication Association (AA) – vytvorenie spojenia medzi klientom a serverom,
- výmena správ,

- uvoľnenie AA a ukončenie spojenia.



Obr. 6.2: Priebeh spojenia.

6.1.5 Bezpečnosť

DLMS delí bezpečnosť na autentizáciu dvoma úrovňami: Low Level Security a High Level Security.

Low Level Security

V tomto prípade prebieha jednostranná autentifikácia klienta pomocou hesla, ktoré meradlo pozná. Po úspešnom prijatí hesla sa iniciuje spojenie. Priebeh spojenia [39]:

1. prebehne výmena informácie o spôsobe a začiatku komunikácie,
2. klient serveru odošle heslo a dodatočné dáta (napr. identifikátory strán).
3. server overí, či heslo odpovedá,
4. ak je heslo správne, začne sa spojenie,
5. ak je heslo nesprávne, spojenie je odopreté.

High Level Security

V tomto prípade prebieha obojstranná autentifikácia na strane klienta aj servera pomocou náhodne vygenerovaných postupností. Priebeh spojenia:

1. Klient zašle výzvu CtoS.
2. Server odpovedá na výzvu svojou žiadosťou StoC.
3. Klient spracuje $f(\text{StoC})$ v odpovedajúcom autentifikačnom móde.
4. Správu odošle serveru.
5. Server skontroluje klientovu odpoveď $f(\text{StoC})$.
6. Ak je výsledok správny akceptuje jeho autentifikáciu a odošle klientovi $f(\text{CtoS})$.
7. Klient skontroluje prijatú správu $f(\text{CtoS})$.
8. Pri správnom výsledku autentifikuje server.

O výber autentizačného mechanizmu sa stará parameter mechanism_id, ktorý môže naberať hodnoty 0-7. Zabezpečenie správ sa riadi úrovňami Security Suite, ktoré môžu nabrať hodnoty 0, 1 a 2. Algoritmy, ktoré sú využívané úrovňami Security Suite sú zhrnuté v tabuľke 6.1.

Tab. 6.1: Úrovne Security Suite a použité algoritmy.

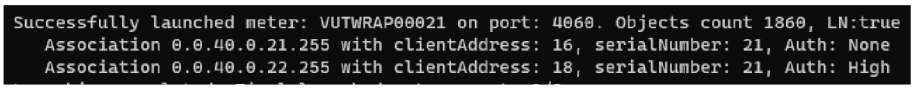
Mechanizmus	**Security suite 0**	**Security suite 1**	**Security suite 2**
Šifrovanie	AES-GCM-128	AES-GCM-128	AES-GCM-256
Digitálny podpis	x	ECDSA P-256	ECDSA P-384
Hash	x	SHA-256	SHA-384
Ustanovenie kľúča	x	ECDH P-256	ECDH P-384
Prenos kľúča	AES-256	AES-128	AES-256

6.2 Úloha

Praktická ukážka DLMS/COSEM komunikácie je demonštrovaná v simulačnej aplikácii DATEL[1], čítači DLMS správ Gurux a paketovom analyzátore Wireshark. Aplikácia ponúka 8 simulovaných elektromerov typu HDLC a WRAPPER, v úlohe sa bude využívať elektromer typu Wrapper. Pri analýze paketov v programe Wireshark sa použije skript *wrapper-dlms.lua*[2].

6.2.1 Komunikácia bez šifrovania/ autentizácie

Pri spustení aplikácie je v konzole vidno pripojenie oboch typov elektromera a ich základné informácie (viz obrázok 6.3). Na demonštráciu prvého typu komunikácie bez šifrovania a bez autentizácie bude použitý prvý elektromer typu Wrapper s názvom *Wrapper*.



Obr. 6.3: Pripojenie elektromerov.

K spusteniu elektromera dôjde kliknutím pravého tlačítka na elektromer *Wrapper*, inicializovaním OBIS kliknutím na *Init Obis* (krúžok pri názve naberie oranžovú farbu) a následným znova kliknutím pravého tlačítka na elektromer *Wrapper* a otvorenie klienta kliknutím na *Manual klient*. K analýze priebehu spojenia sa využije

[1] https://ieeexplore.ieee.org/document/9896543/
[2] https://github.com/matousp/dlms-analysis

program Wireshark so skriptom *wrapper-dlms.lua*. Pakety sa budú analyzovať v rozhraní Loopback a využije sa filter *tcp.port == 4060*, keďže v terminálovom okne vidíme využitie TCP portu 4060 (viz obrázok 6.3). V klientskom okne sa elektromer pripojí kliknutím na tlačítko *Connect*. Status elektromera sa zmení z oranžovej farby na zelenú, čo indikuje aktívne pripojenie na server a úspešné neviazané DLMS spojenie. Vo Wiresharku sa objavia prvé správy, k zobrazeniu správ DLMS je potrebné aktivovať skript kliknutím pravého tlačítka na okno Wiresharku, vybratie zložky *Decode As* pridanie prekladu na TCP port 4060 a v poslednom políčku vybratie DLMS-WRAPPER. Niektorým správam sa zmení protokol TCP na protokol DLMS. V zachytenej komunikácii sa nachádzajú práve dve správy s protokolom DLMS. Prvou správou je DLMS AARQ Association Request (viz obrázok 6.4) a druhou je správa DLMS AARE Association Response: accepted (viz obrázok 6.5). Tieto dve správy slúžia na vytvorenie spojenia medzi elektromerom a serverom. V detaile správy je vidieť, že ide o nešifrovanú komunikáciu.

```
DLMS Wrapper over TCP
    Header: Uninterpreted Data Sequence (8 bytes)
DLMS/COSEM
    Type: AARQ Association Request (0x60)
    Length: 29
    ApplicationContextName: 2.16.756.5.8.1.1 (LN Referencing, Without Ciphering)
  UserInformation: xDLMS-Initiate.request
      DedicatedKey: False(0)
      ResponseAllowed: False(0)
      ProposedQualityOfService: False(0)
      ProposedDLMSversionNumber: 6
      ProposedConformance: 5f1f0400ffffff
      ClientMaxReceivedPDUsize: 65535
```

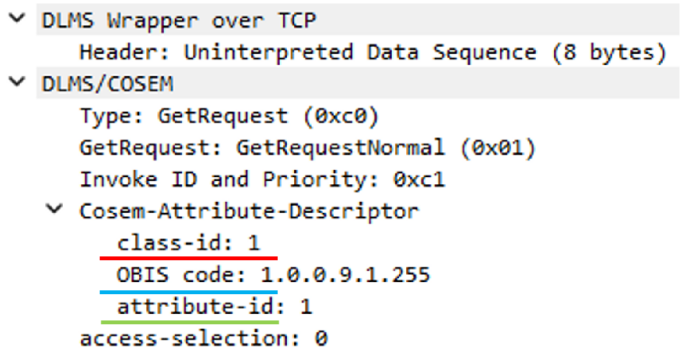
Obr. 6.4: Žiadosť o uskutočnenie pripojenia.

```
DLMS Wrapper over TCP
    Header: Uninterpreted Data Sequence (8 bytes)
DLMS/COSEM
    Type: AARE Association Response (0x61)
    Length: 41
    ApplicationContextName: 2.16.756.5.8.1.1 (LN Referencing, Without Ciphering)
    AssociationResult: accepted (0)
    ResultSourceDiagnostic: null (0)
  UserInformation: xDLMS-Initiate.response
      NegotiatedQualityOfService: 0
      NegotiatedDLMSversion: 6
      ProposedConformance: 5f1f0400421e5d
      ClientMaxReceivedPDUsize: 65535
```

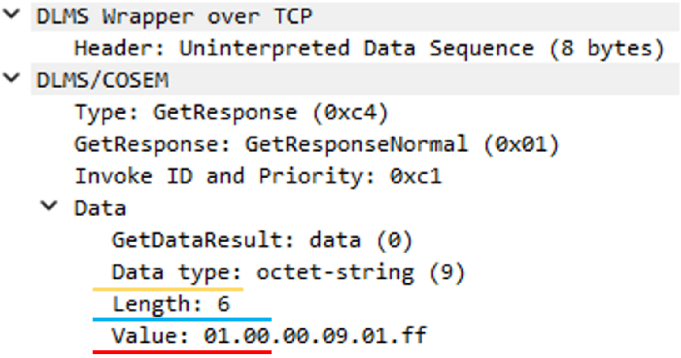
Obr. 6.5: Prijatie a vytvorenie spojenia.

Čítanie dát

K čítaniu dát sa využije okno Manual klient, kde sa z ľavého výberu objektov vyberie jeden. Pre ukážku bol vybratý objekt typu DATA (položku DATA je nutné rozkliknúť a vybrať z kategórie). Kliknutím na tento objekt a následne na tlačítko *Read selected objects* sa tento objekt z elektromeru vyčíta a v konzole sa zobrazí jeho výpis. V okne Wiresharku sa taktiež pridali správy o požiadavku *GetRequestNormal* a vyčítaných *GetResponseNormal* správach. Po vybratí akejkoľvek správy *GetRequestNormal* je v detailnom výpise paketu v časti Cosem-Attribude-Descriptor vidieť tri dôležité parametre. Class-id charakterizuje priamo objekt typu DATA a umožňuje prenášať informácie o konfiguračných dátach alebo parametroch. Tieto dáta sú identifikované atribútom *logical_name*. OBIS code identifikuje položky dát použitých meradlami. Attribute-id naznačuje čítanie prvého atribútu objektu DATA (viz obrázok 6.6). V správe *GetResponseNormal* je vidieť datový typ správy Data type, jeho dĺžku Length a samotnú hodnotu. Každý dátový typ má svoje identifikačné číslo ako napríklad octet-string s číslom 9 alebo boolean s číslom 3. Hodnota správy v položke Value je v tomto prípade V hexadecimálnom tvare, čo značí že komunikácia prebieha v otvorenej podobe bez šifrovania (viz obrázok 6.7).

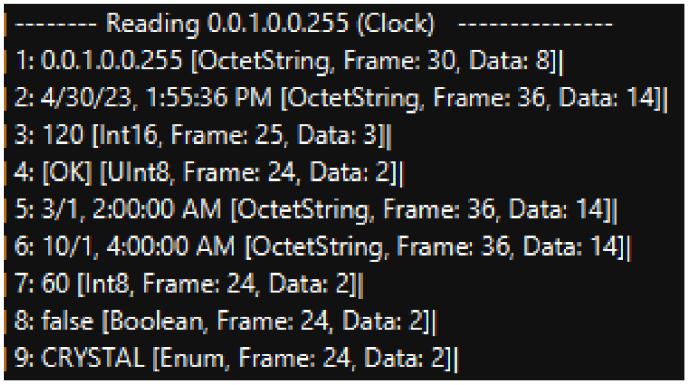


Obr. 6.6: Detail správy GetRequestNormal.

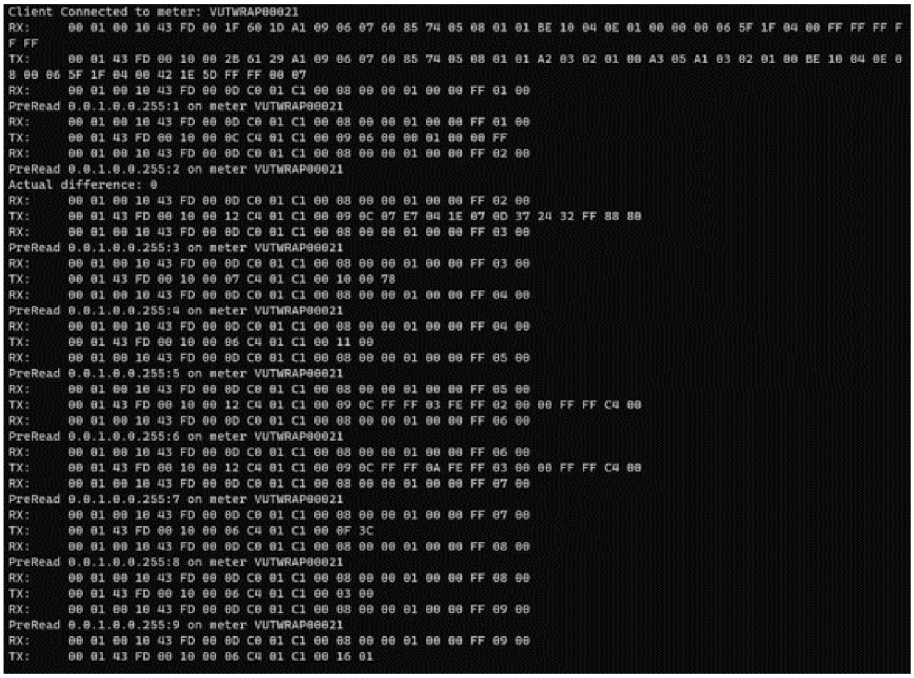


Obr. 6.7: Detail správy GetResponseNormal.

K čítaniu druhého objektu využite objekt typu CLOCK. Objekt sa vyčíta znova kliknutím na atribút CLOCK a následným zvolením *Read selected objects*. V konzole klienta je vidno výpis objektu a v terminálovom okne hexadecimálny výpis správ (viz obrázok 6.8 a 6.9).

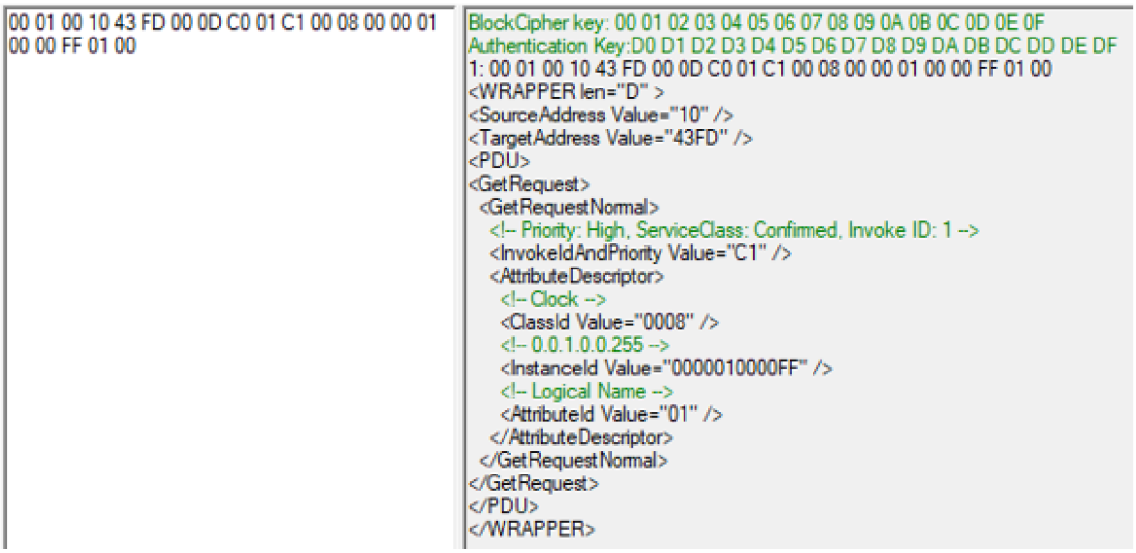


Obr. 6.8: Detail konzole klienta pri čítaní objektu Clock.



Obr. 6.9: Detail terminálového okna serveru pri čítaní objektu Clock.

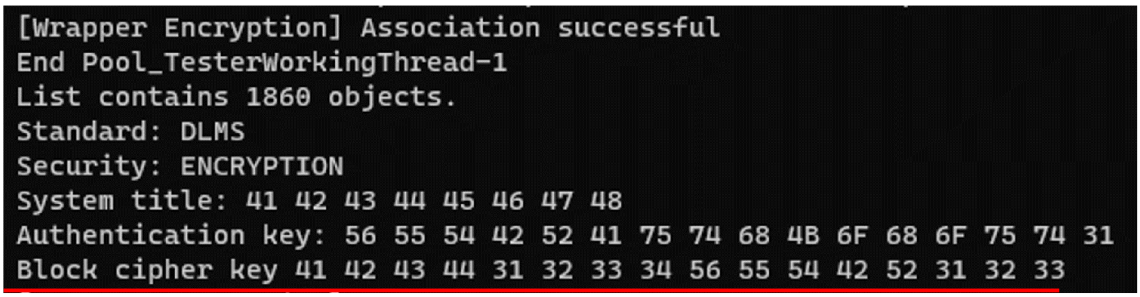
K zobrazeniu prenesených správ v čitateľnej podobe sa využije program GXDLMS-Director. Po spustení programu sa vyberie položka DLMS Translator z ponuky Tools na hornej lište programu. Do ľavého okna zložky Messages sa skopíruje akákoľvek hexidecimálna správa z terminálového okna a preklad sa spustí kliknutím na Translate v položke File. Na obrázku 6.10 je zobrazený preklad správy.



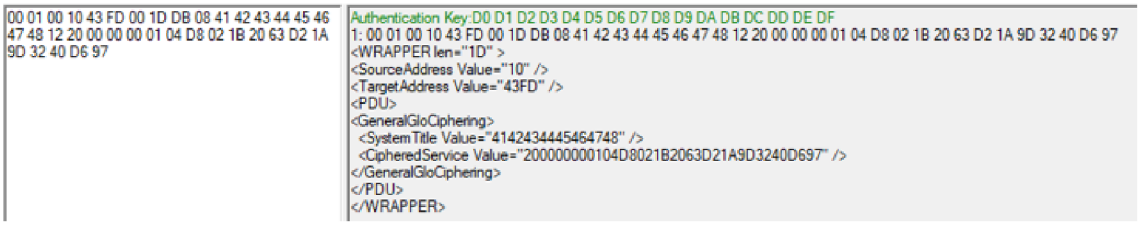
Obr. 6.10: Preklad objektu objektu Clock.

6.2.2 Komunikácia so šifrovaním správ

K simulácii tohto typu spojenia sa využije elektromer *Wrapper Encryption*. Po pripojení elektromera je v konzole vidieť šifrovací kľúč Block cypher key (viz obrázok 6.11). Z objektov elektromeru sa vyberie jeden a spustí sa čítanie objektu. Z terminálového okna sa do okna DLMS Translator skopíruje akákoľvek správa z vyčítaných objektov elektromeru Wrapper Encryption. Po spustení prekladača sa v okne vedľa nezobrazí celá preložená správa (viz obrázok 6.12). Na zobrazenie celej správy je nutné do zložky Ciphering vložiť šifrovací kľúč. V časti Security sa vyberie typ šifrovania a do políčka Block Cipher key sa vloží šifrovací kľúč. Po vložení kľúča sa v prekladači zobrazí celý preklad správy (viz obrázok 6.13).



Obr. 6.11: Šifrovací kľúč v terminálovom okne.



Obr. 6.12: Snaha o preklad správy bez pridania šifrovacieho kľúča.

Obr. 6.13: Preklad správy s pridaním šifrovacieho kľúča.

6.3 Samostatná úloha – Komunikácia so šifrovaním a autentizáciou

1. Ku spojeniu so šifrovaním aj autentizáciou sa využije elektromer *Wrapper AE*. Výslednú rozšifrovanú správu objektu **GPRS_SETUP** je nutné prezentovať v programe Gurux.
2. Pomocou programu Wireshark prezentujte rozdiel v DLMS správach pri šifrovanej a nešifrovanej komunikácii.
3. Cieľom druhej úlohy je nájsť kľúč k elektromeru a vyčítajte hodnotu objektu 0.0.128.2.0.255. Nápoveda: odpoveď začína v 1.1.1.8.0.101.
4. Pomocou aplikácie DATEL overte, či sa pri komunikácii využívajú normy a štandardy odpovedajúce minimálne Vyhláške č. 359/2020 Sb. a normám NÚKIB.

6.4 Otázky

1. Ktoré z algoritmov použitých DLMS/COSEM zaisťujú integritu, ktoré dostupnosť a ktoré dôvernosť?
2. Čo vieme vyčítať z paketov prenosu správ šifrovaného odpočtu DLMS komunikácie pomocou programu Wireshark?
3. Aký dlhý je autentizačný tag?
4. Akú verziu Security Suite využívajú elektromery Wrapper, a v ktorom objekte sa táto informácia nachádza?
5. Akú rolu má System title na začiatku spojenia medzi klientom a serverom?

6.5 Literatúra

- COSEM Interface Classes and OBIS Object Identification System (Blue Book). Dostupné z: `https://www.dlms.com/files/Blue-Book-Ed-122-Excerpt.pdf`
- Bezpečnost chytrých elektroměrů. Dostupné z `https://dspace.vutbr.cz/xmlui/handle/11012/197914`
- Implementace zabezpečení do DLMS protokolu. Dostupné z `https://dspace.vutbr.cz/xmlui/handle/11012/196917`.

Záver

Cieľom diplomovej práce bolo v teoretickej časti spracovať komunikačné technológie, ktoré sa bežne využívajú v oblasti komunikácie inteligentných meracích systémov. Medzi tieto technológie patria hlavne technológie PLC, PRIME a LTE-M. Tieto teoretické poznatky boli následne použité pri spracovaní fyzických a softvérových testov, ktoré sú pri vývoji elektromera nevyhnutné. Tieto testy sú v súlade s európskymi normami a vyhláškami upravujúcimi inteligentné meracie systémy. Rovnako sú v tejto kapitole zhrnuté rôzne nástroje na vykonanie týchto testov, z ktorých bol jeden využitý aj na prípravu laboratórnej úlohy.

Dôležitým hľadiskom v tejto oblasti je životný cyklus inteligentného elektromera. Hlavne v oblastiach aktualizácií softvéru (bezpečnej aktualizácie), digitálnych certifikátov a životnosti kľúčov vo vzťahu ku Key Management Systému. Životný cyklus sa týka aj samotného Key Management Systému, a to vo fázach generovania a ukladania kľúčov, distribúcii a použitiu týchto kľúčov. Systém taktiež využíva služieb certifikačnej autority v prospech systému distribučnej spoločnosti na certifikáciu a zabezpečenie komunikácie.

V ďalších častiach je popísaná metodika bezpečnosti ENCS, ktorá definuje požiadavky na inteligentný elektromer, dátový koncentrátor, kryptografiu, integritu a dôvernosť dát alebo riadenie prístupu.

V závere práce je využitá aplikácia DATEL ako softvérový nástroj testovania komunikácie medzi dátovou centrálou a inteligentným zariadením. V laboratórnej úlohe si študenti budú môcť detailne prezrieť spôsob a priebeh tejto komunikácie ako aj túto komunikáciu odchytiť a zanalyzovať. Samostatná úloha naväzuje na teoretickú časť, kde študenti využijú získané poznatky.

Literatúra

[1] THOBEKILE, J. N.; FARZAD, G. *An overview of DLMS/COSEM and g3-plc for smart metering applications* [online]. Júl 2022, [cit. 2022-24-9].
Dostupné z: https://sciendo.com/article/10.2478/ijssis-2022-0011

[2] G3 PLC Alliance *Setting up and maintaining G3 PLC networks* [online]. Október 2020, [cit. 2022-27-9].
Dostupné z: https://www.youtube.com/watch?v=9YpM_7GJBFw&ab_channel=G3-PLCAlliance

[3] G3 PLC Alliance *Overview* [online]. [cit. 2022-27-9].
Dostupné z: https://g3-plc.com/g3-plc/overview-benefits/

[4] Computerphile *Reed Solomon Encoding* [online]. Február 2019, [cit. 2022-12-10].
Dostupné z: https://www.youtube.com/watch?v=fBRMaEAFLE0&ab_channel=Computerphile

[5] RILEY, M.; RICHARDSON, I. *Reed-Solomon Codes* [online]. 1998, [cit. 2022-12-10].
Dostupné z: https://www.cs.cmu.edu/~guyb/realworld/reedsolomon/reed_solomon_codes.html

[6] SKRÁŠEK, T. *ÚZKOPÁSMOVÁ PLC KOMUNIKACE SE STANDARDY G3-PLC, PRIME A IEEE-1901.2* [online]. 2015, [cit. 2022-12-10].
Dostupné z: https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=100768

[7] BUAYAIRAKSA, S.; THEPPHAENG, S.; PIRAK, C. *On the performance of G3 power line communication network with smart energy meter* [online]. Máj 2013, [cit. 2022-11-10].
Dostupné z: https://ieeexplore.ieee.org/document/6559532

[8] PRIME Alliance Technical Working Group *Draft Specification for Powerline Intelligent Metering Evolution* [online]. [cit. 2022-20-10].
Dostupné z: https://www.prime-alliance.org/wp-content/uploads/2020/04/PRIME-Spec_v1.3.6.pdf

[9] NORDIC Semiconductor *ECB — AES electronic codebook mode encryption* [online]. November 2021, [cit. 2022-23-10].
Dostupné z: https://infocenter.nordicsemi.com/index.jsp?topic=%2Fcom.nordic.infocenter.nrf52832.ps.v1.1%2Fecb.html

[10] WM Systems *SMART ELECTRICITY METERING ON CELLULAR* [online]. [cit. 2022-24-10].
Dostupné z: https://m2mserver.com/en/smart-electricity-metering-on-cellular/

[11] BALASUBRAMANYA, C. *Testing challenges in smart energy meters and ensuring product assurance in mass roll out.* [online]. September 2020, [cit. 2022-29-10].
Dostupné z: https://www.linkedin.com/pulse/testing-challenges-smart-energy-meters-ensuring-product-c/

[12] LAOREN *Life Cycle of CLOU Energy Meters* [online]. January 2022, [cit. 2022-17-11].
Dostupné z: https://clouglobal.com/life-cycle-of-clou-energy-meters/

[13] KEDIA, M. *Enhancing Privacy and Security in the Smart-Meter Life Cycle* [online]. September 2019, [cit. 2022-17-11].
Dostupné z: https://www.eetimes.eu/enhancing-privacy-and-security-in-the-smart-meter-life-cycle/

[14] HAAS, J. *LTE CAT NB1 and M1: What are the benefits for smart metering?* [online]. Júl 2020, [cit. 2022-17-11].
Dostupné z: https://eu.landisgyr.com/blog/the-right-communication-concept-for-smart-metering-what-are-the-benefits-of-lte-cat-nb1-and-lte-cat-m1

[15] TONYALI, S.; AKKAYA, K.; SAPUTRO, N. *An attribute-based reliable multicast-over-broadcast protocol for firmware updates in smart meter networks* [online]. Máj 2017, [cit. 2022-18-11].
Dostupné z: https://ieeexplore.ieee.org/document/8116359

[16] NES *Smart meters: Which next-gen cellular and why* [online]. Február 2022, [cit. 2022-18-11].
Dostupné z: https://www.smart-energy.com/digitalisation/smart-meters-which-next-gen-cellular-and-why/

[17] Digi-Key's European Editors *Cellular Connectivity for Smart Metering* [online]. November 2017, [cit. 2022-18-11].
Dostupné z: https://www.digikey.com/en/articles/cellular-connectivity-for-smart-metering

[18] PAUZET, O. *Cellular Communications and the Future of Smart Metering* [online]. September 2010, [cit. 2022-18-11].
Dostupné z: https://www.gsma.com/iot/wp-content/uploads/2012/03/energy20cellular20communications20and20the20future20of20smart20metering.pdf

[19] PAUZET, O. *COSEM Conformance Test Process* [online]. 2002, [cit. 2022-27-11].
Dostupné z: http://www.fusdom.com/upload/file/xx/DLMS_Yellow_Book_Conformance_Test.pdf

[20] Netbeheer Nederland – WG DSMR *P1 Companion Standard* [online]. 2014, [cit. 2022-2-12].
Dostupné z: https://www.netbeheernederland.nl/_upload/Files/Slimme_meter_15_32ffe3cc38.pdf

[21] SHENGZONG, H.; HUIWEI, W.; YOULIANG, W. *Reliability assessment test for smart electrical energy meters based on failure mechanism* [online]. August 2014, [cit. 2022-20-11].
Dostupné z: https://ieeexplore.ieee.org/document/7107307

[22] Wang, A.; Luo, R.; Zhou, H.; Su, J.; Zhu, X. *Research on Reliability Enhancement Testing for Single-phase Smart Meter* [online]. 2011, [cit. 2022-20-11].
Dostupné z: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6057806

[23] Smart Energy International *IEC standards for electricity metering* [online]. December 2018, [cit. 2022-2-12].
Dostupné z: https://www.smart-energy.com/policy-regulation/iec-standards-for-electricity-metering/#:~:text=IEC%2062052%2D11%20specifies%20general,the%20application%2C%20robust%20and%20safe.

[24] HBM Prenscia Inc. *IEC standards for electricity metering* [online]. [cit. 2022-2-12].
Dostupné z: https://www.weibull.com/hotwire/issue14/relbasics14.htm

[25] QI, B.; SUN, Y.; HU, W.; DING, X. *A Multi-Stress Accelerated Life Tests Method for Smart Electricity Meter Based Upon the Life Stress Model* [online]. Jún 2011, [cit. 2022-2-12].
Dostupné z: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5979441

[26] ENCS *Security requirements for procuring smart meters and data concentrators* [online]. Júl 2022, [cit. 2023-2-4].
Dostupné z: https://encs.eu/wp-content/uploads/2021/09/ENCS-Security-requirements-for-procuring-Smart-Meters-and-DCs-v2_3_28uJCyG.pdf

[27] ADALIER M.; TEKNIK A. *Efficient and Secure Elliptic Curve Cryptography Implementation of Curve P-256* [online]. [cit. 2023-2-4].
Dostupné z: https://csrc.nist.gov/csrc/media/events/workshop-on-elliptic-curve-cryptography-standards/documents/papers/session6-adalier-mehmet.pdf

[28] COOK, J. D. *Elliptic curve P-384* [online]. Máj 2019, [cit. 2023-2-4].
Dostupné z: https://www.johndcook.com/blog/2019/05/11/elliptic-curve-p-384/

[29] BERNSTEIN, D. J.; LANGE, T. *SafeCurves: choosing safe curves for elliptic-curve cryptography* [online]. Január 2017, [cit. 2023-2-4].
Dostupné z: https://safecurves.cr.yp.to/

[30] NÚKIB *MINIMÁLNÍ POŽADAVKY NA KRYPTOGRAFICKÉ ALGORITMY* [online]. Jún 2022, [cit. 2023-15-4].
Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/Kryptograficke_prostredky_doporuceni_v2.0.pdf

[31] DLMS User Association *DLMS/COSEM Architecture and Protocols* [online]. 2019, [cit. 2023-15-4].
Dostupné z: https://www.dlms.com/files/Green_Book_Edition_9-Excerpt.pdf

[32] *AES-GCM* [online]. November 2019, [cit. 2023-15-4].
Dostupné z: https://www.aes-gcm.com/

[33] DWORKIN, M. *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC* [online]. November 2007, [cit. 2023-18-4].
Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

[34] KOZOLE, M.; KEMETHY, G. *Security in DLMS A White Paper by the DLMS User Association* [online]. November 2019, [cit. 2023-18-4].
Dostupné z: https://www.dlms.com/files/DLMS-White-Paper-Security_November_2019.pdf

[35] BENNETT, C. J.; PETTY D. M.; MILLER, K. P.; MEDVINSKY, A. *System and method for authenticating data* [online]. Jún 2014, [cit. 2023-2-12]. Dostupné z: https://patents.google.com/patent/US20130132722

[36] *Vyhláška č. 359/2020 o měření elektřiny* [online]. 2020, [cit. 2023-18-4]. Dostupné z: https://www.zakonyprolidi.cz/cs/2020-359

[37] LEPING, Z. *Research on Key Test Methods of the Smart Meter Software Based on Failure Modes* [online]. 2019, [cit. 2023-23-4]. Dostupné z: https://iopscience.iop.org/article/10.1088/1742-6596/1325/1/012172/pdf

[38] DLMS User Association *COSEM Interface Classes and OBIS Object Identification System* [online]. Január 2017, [cit. 2023-23-4]. Dostupné z: https://www.dlms.com/files/Blue-Book-Ed-122-Excerpt.pdf

[39] FITERE, I. Bezpečnost chytrých elektroměrů [online]. Brno, 2021 [cit. 2023-5-10]. Dostupné z: https://dspace.vutbr.cz/xmlui/handle/11012/197914. Bakalářská práce. Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií. Ústav telekomunikací. Vedoucí práce Petr Mlýnek.

[40] KOHOUT, D.; LIESKOVAN, T.; MLYNEK, P. *Smart Metering Cybersecurity—Requirements, Methodology, and Testing* [online]. Apríl 2023, [cit. 2023-5-7]. Dostupné z: https://www.mdpi.com/1424-8220/23/8/4043

Zoznam symbolov a skratiek

IMS	Inteligentný merací systém
AMI	Advanced Metering Infrastructure
PLC	Power-line communication)
SM	Smart Meter
GSM	Global System for Mobile Communications
SNR	Signal to noise ratio
ITU	International Telecommunication Union
IEEE	Institute of Electrical and Electronics Engineers
UNB-PLC	Ultra-Narrowband Powerline Communication
NB-PLC	Narrowband Powerline Communication
BPL	Broadband over power lines
LDR	Low data rate
HDR	High data rate
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
IPv6	Internet Protocol version 6
MAC	Medium access control
FCC	Federal Communications Commission
ARIB	Association of Radio Industries and Businesses
FCH	Frame check sequence
DBPSK	Differential Binary Phase Shift Keying
DQPSK	Differential Quadrature Phase Shift Keying
D8PSK	Differential 8-Phase Shift Keying
CL	Convergence layer

MPDU	Moderately Priced Dwelling Unit
PPDU	Physical Layer Protocol Data Unit
CRC	Cyclic redundancy check
OFDM	Orthogonal frequency-division multiplexing
IFFT	Inverse Fast Fourier Transform
ECB	Electronic codebook mode encryption
AES	Advanced Encryption Standard
DSK	Device Secret Key
KDIV	Key Diversifier
USK	Unique Secret Key
MK	Master Keys
LTE	Long Term Evolution
IoT	Internet of things
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
ENCS	European Network for Cyber Security
DSMR	Dutch Smart Meter Requirements
IEC	International Electrotechnical Commission
ANSI	American National Standards Institute
IEC	International Electrotechnical Commission
TC	Technical Committee
DLMS	Device Language Message Specification
COSEM	Companion Specification for Energy Metering
CTT	Conformance test tool
KMS	Key Management Systém
HSM	Hardware Security Module

HES	Head End System
PKI	Public key infrastructure
CSR	Certificate signing request
PSK	Pre-shared keys
PKI	Pulic key infrastructure
LAN	Local Area Network
WAN	Wide Area Network
FIPS	Federal Information Processing Standards
ECDSA	Elliptic Curve Digital Signature Algorithm
NSA	National security agency
CA	Certification Authority
DH	Diffie Hellman
ECC	Elliptic Curve Key Generation
GCM	Galois/Counter Mode
GCM	Galois/Counter Mode
GUEK	Global Unicast Encryption Key
GAK	Global Authentication Key
KEK	Key Encryption Key
RAM	Random Access Memory
TRNG	True Random Number Generator
FLASH	Flash Memory
NIST	The National Institute of Standards and Technology
EK	Encryption Key
IV	Initialization Vector
ADD	Additional Authenticated Data

OBIS	Object Identification System
AA	Aplication Association
HDLC	High-level Data Link Control
TPM	Trusted Platform Module