Elektronické dodací listy pro objednávky a dodávky měřících přístrojů a komponent pro měřící systémy

VERZE 1.5

29. ZÁŘÍ 2023

RNDr. Libor Dostálek, Ph.D., Ing. Bc. Martin Mikala, Ing Pavol Rybárik,
Doc. Ing. Petr Mlýnek, Ph.D.

Obsah

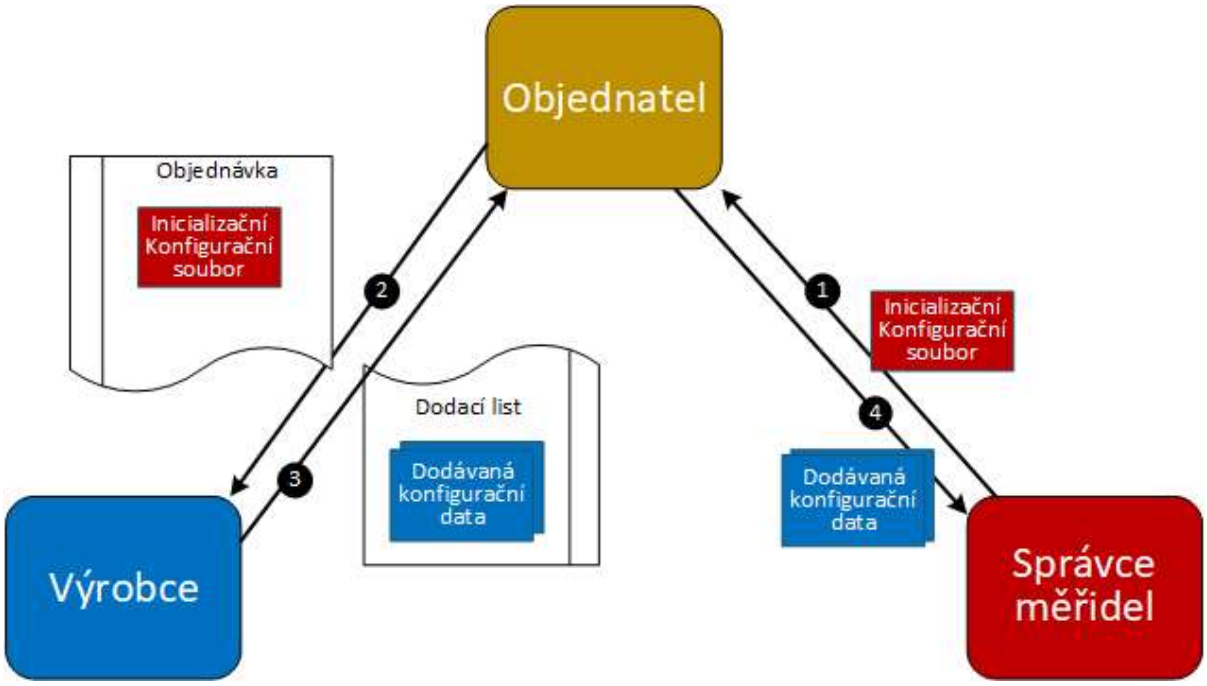
Úvod

Tento dokument popisuje formát jednotné elektronické objednávky a dodacího listu pro zařízení ve všech odvětvích měření energie. Dokument vychází z německého dokumentu *Elektronischer Lieferschein für die Bestellung und Lieferung von Messeinrichtungen und Komponenten für Messsysteme, Version 2.3, 7. Dezember 2021* [1], který rozpracovává pro české prostředí.

Ilustrační příklad elektronického dodacího listu je uveden v kapitole 7.5.

Proces spojený s Objednávkou a Dodacím listem je následující:

1. Správce (provozovatel) měřidel připraví pro každý typ objednávaných měřidel jeden tzv. Inicializační konfigurační soubor (InitialConfigurationFile) obsahující základní společná konfigurační data (např. certifikáty certifikačních autorit).
2. Na základě podkladů od Správce měřidel generuje Objednatel elektronickou objednávku, která obsahuje parametry objednávaných měřidel a mj. obsahuje Inicializační konfigurační soubory (s největší pravděpodobnosti pouze jeden, protože pro každý se bude vytvářet samostatná objednávka, ale nemusí to být pravidlem).
3. Výrobce vyrobí měřidla, která před-personalizuje kryptografickým materiálem. Pro každé měřidlo vytvoří strukturu Dodávaná konfigurační data (DeliveryConfigFile) s před-personalizovaným kryptografickým materiálem. Následně přímo do struktury Objednávky doplní parametry vyrobených měřidel a Dodávaná konfigurační data. Vznikne tak elektronický dodací list. Údaje o objednávce v něm zůstávají zachovány.
4. Objednatel předá buď samotná Dodávaná konfigurační data, nebo celý dodací list Správci měřidel, který tak obdrží kryptografický materiál, kterým jsou měřidla před-personalizována.



Obrázek 1 Role participující na výměně dat (zabezpečení komunikace je popsáno v následujících kapitolách)

Správce měřidel následně na základě pře-personalizovaného kryptografického materiálu personalizuje měřidla „svým“ kryptografickým materiálem. To však nemusí udělat bezprostředně, ale až podle svých provozních možností.

Poznámka: Inicializační konfigurační soubor je nepovinný i v případě objednávky měřidel. Soubor Dodávaná konfigurační data je povinný v případě dodávky měřidel. Je nepovinný zejména v případě dodávky jiného zboží než měřidla.

Elektronická výměna dat se týká nejenom nových objednávek a dodávek, ale i oprav, přejímky zboží a kontroly příchozího zboží a dalších možných využití. Tuto elektronickou výměnu dat lze použít pro objednávku a dodávku jiného zboží, nejenom samotných měřidel (např. datové koncentrátory a SIM karty).

Tento dokument se věnuje zejména elektronické objednávce a elektronickému dodacímu listu.

V této komunikaci vystupují následující role:

- **Výrobce**, který zhotovuje a před-personalizuje měřidla dočasným kryptografickým materiálem.
- **Objednatel**, který objednává měřidla a mj. vede jejich účetní evidenci.
- **Správce měřidel**, který následně personalizuje měřidla svým kryptografickým materiálem. Tj. správce měřidel má k dispozici kryptografický materiál pro komunikaci s měřidly.

Objednatel i Správce měřidel mohou být jedna osoba, avšak i v rámci této osoby budou rozdílné týmy pro:

- Objednávání a účetní evidenci.
- Správu měřidel, tj. tým, který mj. spravuje kryptografický materiál (provozuje *KMS*).

Poznámka: V tomto dokumentu prakticky nevystupuje role: **Spotřebitel**.

České prostředí

České prostí vychází z následujících předpokladů:

- Řešení budou v souladu se standardy DLMS/COSEM s podporou bezpečnostních sad (*Security Suite*) 0, 1 a 2.
- V případě podpory pouze bezpečnostní sady 0 je důsledkem, že měřidla musí být před-personalizována symetrickými klíči – blíže viz **Chyba! Nenalezen zdroj odkazů.** Symetrický klíč (SymmetricKey)
- ID měřidel:
    - Objednatel může zadat interval objednávaných identifikátorů měřidel (*SerialNumber*).
    - Výrobce musí podporovat až osm různých identifikátorů měřidel.
    - V případě DLMS/COSEM měřidla musí výrobce naplnit položku *SystemTitle.* System Title je řetězec dlouhý 8 bajtů s tím, že první 3 bajty identifikují výrobce a zbylých 5 bajtů zjišťuje jedinečnost ID – viz kapitola 5.2. Přitom System Title může, ale nemusí, být uveden mezi identifikátory měřidla (*SerialNumber*).
- V České republice pravděpodobně nevznikne společná národní kořenová certifikační autorita (Root CA). Tj. poskytovatelé budou provozovat vlastní Root-CA. V takovém případě musí být její certifikát bezpečnou cestou (mimo v tomto dokumentu popsanou komunikaci) distribuován výrobci pro před-personalizaci měřidla.

Normativní odkazy a literatura

[1] Elektronischer Lieferschein für die Bestellung und Lieferung von Messeinrichtungen und Komponenten für Messsysteme, VDE FNN Hinweis, 12/2012

[2] Certificate Policy der Smart Metering PKI, BSI, Version 1.1.2, 25.01.2023

[3] ČSN EN 62056-5-3 Výměna dat pro měření elektrické energie — Soubor DLMS/COSEM — Část 5-3: Aplikační vrstva DLMS/COSEM

[4] Směrnice Evropského Parlamentu a rady 2014/32/EU ze dne 26. února 2014 o harmonizaci právních předpisů členských států týkajících se dodávání měřidel na trh

[5] Vyhláška 359/2020 Sb. o měření elektřiny

[6] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES

[7] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES

[8] MINIMÁLNÍ POŽADAVKY NA KRYPTOGRAFICKÉ ALGORITMY, doporučení kryptografické ochrany v oblasti kybernetické, bezpečnosti, NÚKIB, Verze 3.0, platná ke dni 21.07.2023

[9] Cryptographic Message Syntax (CMS), RFC 5652

[10] RFC 5751, Secure/Multipurpose Internet Mail Extensions (S/MIME),Verze 3.2

[11] ETSI EN 319 122-1 V1.2.1 (2021-10), Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures

[12] ETSI EN 319 132-1 V1.2.1 (2022-02), Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures

[13] RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[14] W3C: XML Encryption Syntax and Processing

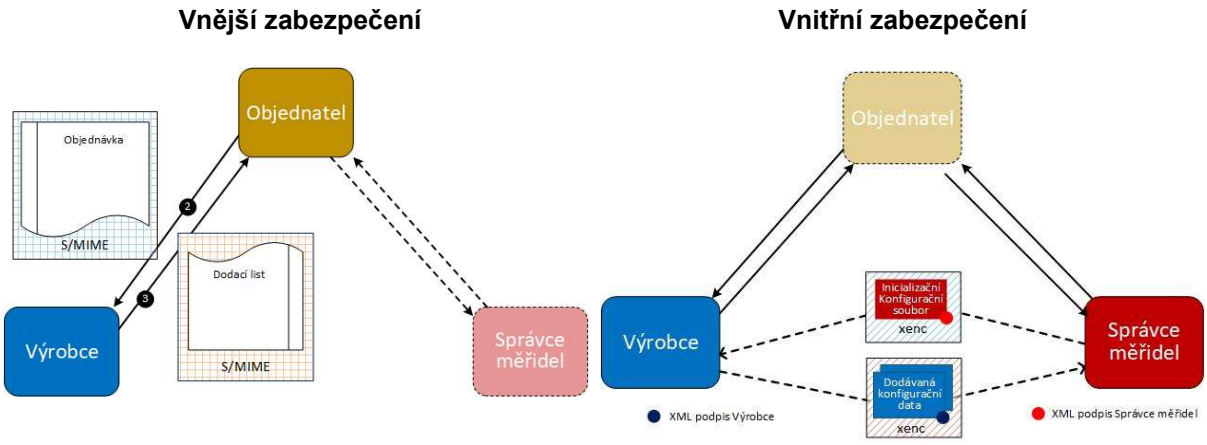
Bezpečnost a ochrana dat

Tato kapitola definuje zabezpečení dat pro objednávání a dodávku měřících zařízení, jejichž vyspělost je na úrovni standardu DLMS/COSEM.

4.1 Vnější a vnitřní zabezpečení

Rozlišujeme vnější a vnitřní zabezpečení:

- Vnější zabezpečení zabezpečuje komunikaci mezi Objednatelem a Výrobcem. Doporučujeme zde využít pro elektronický podpis i šifrování standard S/MIME [11] (*Secure / Multipurpose Internet Mail Extension*) podporovaný např. MS Outlook. Jelikož se jedná o obchodní vztah, tak doporučujeme využít kvalifikovaný elektronický podpis, který je důležitý zejména v případě právních sporů. Zde se jedná o podpis formátu CAdES-B-B označovaný též CAdES-Baseline-B [13].
- Vnitřní zabezpečení je pro komunikaci mezi Výrobcem a Správcem měřidel. Fyzicky tato komunikace probíhá skrze Objednatele, ale ten nemá přístup k před-personalizovanému kryptografickému materiálu. Zde je využito šifrování definované doporučením W3C [15] xenc a podpis XAdES-B-B [14].



Používají se tedy **dva různé** mechanismy zabezpečení:

- S/MIME pro vnější zabezpečení, tj. pro vnější elektronický podpis a vnější šifrování. Elektronický podpis je pak formátu CAdES-B-B.
- Vnitřní zabezpečení využívá XML signature formátu XAdES-B-B a XML encryption (xenc). Pomocí vnitřního zabezpečení se zabezpečuje zejména před-personalizovaný kryptografický materiál.

Poznámka: před archivací elektronicky podepsaných dokumentů se podpisy doplní na podpis XAdES-B-LT a CAdES-B-LT.

4.2 Vnější zabezpečení (S/MIME)

S/MIME [11] je standard zavedený pro šifrování a elektronické podepisování elektronické pošty. Může však být využit i pro zabezpečení libovolných souborů přenášených jinou cestou.

Výhodou využití elektronické pošty je, že pro ni existuje infrastruktura i běžně dostupný software. Stačí, aby si příjemce a odesilatel vyměnili své X.509 certifikáty. Odesilatel pak podepisuje soubor svým soukromým klíčem podepisovacího certifikátu a šifruje veřejným klíčem šifrovacího certifikátu příjemce.

Příjemce dešifruje přijatou zprávu („vybalí z elektronické obálky“) a archivuje ji včetně elektronického podpisu, který před archivací doplní o příslušná časová razítka na podpisy formátů XAdES-B-LT a CAdES-B-LT.

S/MIME umožňuje data zaslat více adresátům. V tomto případě musí mít odesilatel k dispozici certifikáty všech adresátů, kterým je zpráva odesílána.

Příklad zprávy v elektronické obálce („šifrované zprávy“):

```
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

rfvbnj756tbBghyHhHUujhJhjH77n8HHGT9HG4VQpfyF467GhIGfHfYT67n8HHGghyHhHUujhJh4VQpfyF4
67GhIGfHfYGTrfvbnjT6jH7756tbB9Hf8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUuj
pfyF40GhIGfHfQbnj756YT64V
```

Poznámka: Vnější zabezpečení tento materiál dále nespecifikuje.

4.3 Vnitřní zabezpečení

Vnitřní zabezpečení zajišťuje šifrování vybraných prvků XML struktury a podpis celé XML struktury.

Šifrování se týká:

- Inicializačních konfiguračních dat, pokud obsahují symetrické klíče, hesla nebo PINy.
- Dodávaných konfiguračních dat, např. symetrické klíče, hesla nebo PINy.

1.1.1 Vnitřní zabezpečení zajišťuje bezpečnost kryptografického materiálu tak, že k němu má přístup pouze Správce měřidel – přesněji *KMS* provozovaný Správcem měřidel.Způsob zabezpečení

Data v rámci zmíněných struktur jsou šifrovány náhodně generovaným symetrickým klíčem a bezpečným algoritmem (viz kapitola 4.7). Tento náhodně generovaný symetrický klíč je uložen v rámci daného xml souboru ve struktuře EncryptionKey v šifrované formě. K šifrování tohoto klíče je použit jeden ze dvou typů certifikátů:

- certifikát pro šifrování
- certifikát pro dohodu nad klíči (key Agreement)

1.1.1.1 Certifikát pro šifrování

V případě použití certifikátu postaveném pravděpodobně na algoritmu RSA s nastaveným použitím klíče keyUsage = **keyEncipherment** nebo **dataEncipherment** dochází přímo k šifrovaní daného symetrického klíče pomocí šifrovacího certifikátu protistrany.

1.1.1.2 Certifikát pro dohodu nad klíči (key Agreement)

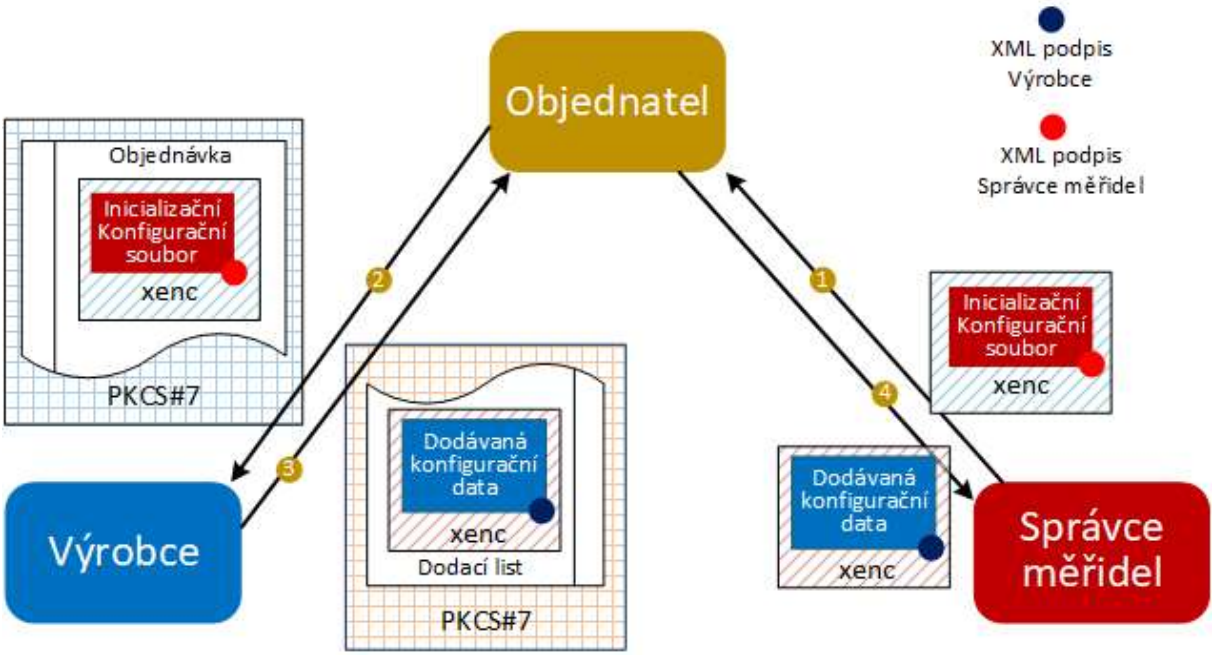
V případě použití certifikátu postaveném pravděpodobně na eliptických křivkách s nastaveným použitím klíče keyUsage = **keyAgreement** dochází k dohodě nad klíčem za použití algoritmu ECDH.

K dohodě nad klíčem je vždy použit certifikát protistrany, zároveň je k ní použit:

- soukromý klíč patřící k certifikátu šifrující strany (varianta static ECDH), nebo
- jednorázový (efemerální) soukromý klíč generovaný specificky pro šifrování dané zprávy (varianta ephemeral ECDH)

4.4 Životní cyklus Objednávky a Dodacího listu

Před zahájením výměny dat je třeba, aby všechny zúčastněné strany vygenerovali příslušný počet párových dat a nechali si vydat certifikáty formátu X.509.



Obrázek 2 Životní cyklus konfiguračních dat

Na zabezpečení komunikace se podílí následující asymetrické klíče (resp. certifikáty, viz kapitola 4.5):

ID klíče	Vlastník	Typ certifikátu	Využití	Poznámka
1	Správce měřidel	podpis	podpis Inicializačního konfiguračního souboru	
2	Správce měřidel	šifrování / key agreement	podpis Dodávaných konfiguračních dat (šifrování) nebo podpis obou stran xml komunikace (key agreement)	konkrétní způsob využití závisí na typu certifikátu, viz kapitola 4.3
3	Objednatel	podpis	podpis celého souboru objednávky pomocí PKCS#7 (CMS) formátu CAdES	vhodný kvalifikovaný certifikát
4	Objednatel	šifrování	vnější zabezpečení celého souboru dodávky od Výrobce Objednateli	
5	Výrobce	šifrování	vnější zabezpečení celého souboru objednávky od Objednatele Výrobci	
6	Výrobce	podpis	podpis celého souboru dodávky pomocí PKCS#7 (CMS) formátu CAdES	vhodný kvalifikovaný certifikát

7	Výrobce	podpis	podpis Dodávaných konfiguračních dat	
8	Výrobce	šifrování / key agreement	podpis Inicializačních konfiguračních dat (šifrování) nebo podpis obou stran xml komunikace (key agreement)	konkrétní způsob využití závisí na typu certifikátu, viz kapitola 4.3

Tabulka 1 Seznam použitých asymetrických klíčů (certifikátů) pro zabezpečení komunikace

Pro přehlednost je zde uvedena přehledová tabulka toho, kdo má k dispozici který certifikát protistrany (soukromý klíč má vždy k dispozici pouze jeho vlastník).

Strana komunikace	**Vlastní klíč**	**Zná certifikát**
Správce měřidel	1,2	7,8
Objednatel	3,4	1,5,6
Výrobce	5,6,7,8	1,2,3,4

Tabulka 2 Vztah stran komunikace a certifikátů

Životní cyklus je pak následující:

1. Správce měřidel vytvoří Inicializační konfigurační soubor, který výrobce využije pro před-personalizaci měřidel. Inicializační konfigurační soubor:
    a. elektronický podepíše podpisem formátu XAdES za použití klíče 1,
    b. vloží do obálky xenc (tj. „šifruje jej“ za pomocí klíče 8 (případně za pomoci klíčů 8 a 2, viz kapitola 4.3) a
    c. předá jej Objednateli.
2. Objednatel:
    a. Vytvoří XML soubor Objednávky, do které jako jednu položku vloží Správcem měřidel zabezpečený Inicializační konfigurační soubor.
    b. Objednávku podepíše podpisem PKCS#7 (CMS) formátu CAdES za pomoci klíče 3
    c. vloží (“šifruje” za pomocí klíče 5) do PKCS#7 (CMS) obálky,
    d. výsledek předá Výrobci.
3. Výrobce:
    a. Dešifruje PKCS#7 (CMS) obálku zprávy
    b. Ověří elektronický podpis CAdES zprávy od Objednatele.
    c. Ověří elektronický podpis XAdES Inicializačního konfiguračního souboru od Správce měřidel.
    d. Výrobce vyrobí a před-personalizuje měřidla dle Objednávky (nemusí se mu podařit vyrobit všechna měřidla).
    e. Pro každé vyrobené měřidlo doplní do původní Objednávky data o vyrobeném měřidle včetně Dodávaných konfiguračních dat. Vznikne tak elektronický dodací list. Každé vyrobené měřidlo má svá Dodávaná konfigurační data. V dodávaných Konfiguračních datech šifruje symetrické klíče, hesla či PINy (xenc) pomocí klíče 2 (případně za pomocí klíčů 2 a 8. viz kapitola 4.3).
    f. Dodávaná konfigurarční data jsou dále podepsána (XAdES) za pomocí klíče 7.
    g. Dodací list podepíše podpisem PKCS#7 (CMS) formátu CAdES za pomocí klíče 6..
    h. Výsledek vloží („šifruje“ za pomocí klíče 5) do PKCS#7 (CMS) zprávy.
    i. Výsledek předá Objednateli.
4. Objednatel:
    a. Dešifruje PKCS#7 (CMS) zprávu.
    b. Ověří podpis CAdES zprávy.

   c. Zpracuje jednotlivé položky elektronického dodacího listu. V rámci tohoto zpracování položky Dodávaná konfigurační data s identifikací měřidla předá Správci měřidel.
5. Správce měřidel pak přijatá před-personalizovaná kryptografická data (Dodávaná konfigurační data) uloží např. do *KMS*. A použije pro počáteční komunikaci
6. Správce měřidel v rámci komunikace s měřidlem vygeneruje nové kryptografické klíče.
7. Správce měřidel i měřidlo přejdou na nové symetrické klíče.

Poznámka: Předmětem tohoto dokumentu je specifikace komunikace mezi Objednatelem a Výrobcem. Komunikace mezi Objednatelem a Správcem měřidel je mimo rozsah tohoto dokumentu.

Poznámka: V rámci je definováno šifrování a elektronický podpis na dvou různých úrovních. Při konkrétním použití je možno zvážit, zda je nutné použit všechny tyto bezpečnostní prvky, či zda je možné některý z těchto prvků vynechat bez dopadu na celkovou bezpečnost výměny informací.

4.5 Certifikáty

Na rozdíl od komunikace DLMS/COSEM je pro výměnu objednávky a dodacího listu doporučené využívat certifikáty ve formátu X.509 vydané veřejnými CA s tím, že použitý kryptografický materiál by měl splňovat aktuální doporučení NÚKIB [9].

Pro elektronické podpisy CAdES i XAdES je doporučeno používat kvalifikované certifikáty pro elektronický podpis (resp. elektronickou pečeť) dle eIDAS [8]. Zejména v případě sporů mezi Objednatelem a Výrobcem je výhodný kvalifikovaný elektronický podpis, neboť má právní relevanci.

V případě výměny zpráv S/MIME elektronickou poštou je třeba zdůraznit, že:

- „Podpisový certifikát“ musí mít v Alternativním jméně předmětu (resp. v Předmětu) certifikátu e-mailovou adresu odesilatele.
- „Šifrovací certifikát“ musí mít v Alternativním jméně předmětu (resp. v Předmětu) certifikátu e-mailovou adresu příjemce.

Poznámka: Výrobce, resp. Objednatel, resp. Správce měřidel mají více certifikátů. Avšak táž osoba může mít stejný předmět svých různých certifikátů.

4.6 Před-personalizace

4.6.1 Před-personalizace *Security Suite* 0

Poznámka: Každá přístupová role má vlastní sadu kryptografického materiálu. Pro které role se mají personalizovat jaké symetrické klíče je specifikováno v Inicializačním konfiguračním souboru.

V případě *Security Suite* 0 musí být během před-personalizace vloženy do měřidla mj. následující symetrické klíče: KEK, GUEK a GAK.

Před-personalizace:

1. Výrobce obdrží v Objednávce Inicializační konfigurační data, ze kterých zjistí, jaké symetrické klíče mají být pro které role vloženy (před-personalizovány) do měřidla.
2. Tyto klíče jsou pro každé měřidlo generovány Výrobcem pomocí generátoru náhodných čísel dostatečné kvality[1], před-personalizovány do měřidla a vloženy do Dat konfigurace dodávky.
3. Objednatel předá měřidla a data konfigurace dodávky Správci měřidel.
4. Správce Měřidel při prvotní komunikaci s měřidlem využije před-personalizované symetrické klíče výrobcem. Během této prvotní komunikace dojde ke generování nových klíčů, které má pod svojí kontrolou pouze Správce měřidel.

[1] Vyhláška 359/2020 Sb. o měření elektřiny uvádí následující generátory náhodných bitů: „HMAC DRBG, Hash DRBG oba pro SHA2 a SHA3“

5. Měřidlo i Správce měřidel přejdou na nové symetrické klíče a začne běžný provoz.

Poznámka: Požadavky na před-pesonalizaci symetrickými klíči se v objednávce vyjadřují položkou SymmetricKey – viz kap. 7.4.23.

4.6.2 Před-personalizace Security Suite 1 a 2

V případě, že měřidlo podporuje Security Suite 1 nebo 2 (česky: bezpečnostní sady 1 a 2), pak není třeba v rámci před-personalizace do měřidla vkládat symetrické klíče – ty mohou být vloženy až jako součást personalizace.

Poznámka: V případě, že správce měřidel bude po nějakou dobu měřidla provozovat s před-personalizovaným kryptografickým materiálem, pak je nutné před-personalizovat měřidlo symetrickými klíči i v případě podpory bezpečnostních sad 1 nebo 2.

Jelikož v České republice neexistuje jedna centrální důvěryhodná kotva (kořenová CA) pro oblast chytrého měření, ale každý subjekt má vlastní kořenovou CA. Objednatel a Výrobce si před níže popsanou komunikací jinou cestou vymění své důvěryhodné kotvy (kořenové certifikáty) pro DLMS/COSEM komunikaci.

Poznámka: K této výměně se může např. využít výše zmíněná zabezpečená elektronická pošta (S/MIME) opatřená kvalifikovaným elektronickým podpisem dle eIDAS [8]. Avšak kořenový certifikát nelze autenticky přenášet v množině certifikátů CMS [10] zprávy, ale musí se přenést v těle zprávy. Což může zachytit anti-spamový filtr, pokud zpráva není šifrována.

Před-personalizace:

1. Výrobce obdrží v Objednávce Inicializační konfigurační data, ze kterých využije zejména certifikáty HES.
2. Výrobce generuje na své CA (pod svou důvěryhodnou kotvou) certifikáty měřidla:
    - pro elektronický podpis,
    - pro výměnu klíčů,
    - volitelně pro TLS komunikaci.
3. Výrobce vloží důvěryhodnou kotvu (kořenový certifikát) správce měřidel do měřidla. Ta v měřidle již nelze vymazat ani nelze komunikací DLMS/COSEM nahrát. V měřidle může být více důvěryhodných kotev.
4. Výrobce vloží vydané certifikáty a příslušné soukromé klíče do měřidla.
5. Výrobce vloží vydané certifikáty do dat konfigurace dodávky.
6. Výrobce odešle měřidla a elektronický dodací list Objednateli.

Personalizace Správcem měřidel:

1. Správce měřidel pro první komunikaci s měřidlem využije důvěryhodnou kotvu Výrobce. Pro další komunikaci již tuto důvěryhodnou kotvu nikdy nevyužije.
2. V rámci první komunikace:
    a. měřidlo vytvoří žádosti o certifikáty:
        - pro elektronický podpis,
        - pro výměnu klíčů,
        - volitelně pro TLS komunikaci.
    b. Skrze HES je zprostředkováno vydání nových certifikátů pod důvěryhodnou kotvou Správce měřidel.
    c. Za využití nově vydaných certifikátů jsou dohodnuty symetrické klíče.
2. Nyní se přejde na běžnou komunikaci za využití nově vygenerovaného kryptografického materiálu.

Poznámka: Pokud měřidlo podporuje pouze Bezpečnostní sadu 0 a měl by být později proveden upgrade měřidla na bezpečnostní sadu 1 nebo 2, tento upgrade může být z bezpečnostního hlediska problematický.

Poznámka: požadavky na před-personalizaci certifikáty se vyjadřují položkou Certs – viz kapitola 7.4.14.

4.7 Kryptografické algoritmy

Kryptografické algoritmy musí splňovat aktuální doporučení NÚKIB [9], vydané 21. 7. 2023, které mj. uvádí následující algoritmy (**tučně** jsou označeny algoritmy vyhovující též **vyhlášce 359/2020 Sb.** o měření elektřiny):

- V sekci „Schválené blokové a proudové šifry“ mj. uvádí:
  1. **AES** s využitím délky klíčů 128, 192 a **256** bitů
- V sekci „Schválené módy autentizovaného šifrování“ mj. uvádí:
  1. **CCM,**
  2. EAX,
  3. OCB1 a OCB3, doporučujeme preferovat OCB3 před OCB1,
  4. **GCM** s nonce délky 96 bitů a tagem dlouhým 128 bitů, nejpozději po 2^{32} hodnotách nonce musí dojít k výměně klíče.
- V sekci „Schválené algoritmy pro technologii digitálního podpisu“ uvádí:
  1. **DSA** s délkou klíčů **3072** bitů a více, délky parametru cyklické podgrupy 256 bitů a více,
  2. **EC-DSA** s využitím délky klíčů **256** bitů a více,
  3. RSA-PSS s využitím délky klíčů 3072 bitů a více,
     *(vyhláška 359/2020 Sb. zmiňuje pouze **RSA** – nikoliv RSA-PSS).*
  4. EC-Schnorr s využitím délky klíče 256 bitů a více
- V sekci „Schválené algoritmy pro procesy dohod na klíči a šifrování klíčů“ uvádí:
  1. **DH** s délkou klíčů **3072** bitů a více, délky parametru cyklické podgrupy 256 bitů a více,
  2. **ECDH** s využitím délky klíčů **256** bitů a více,
  3. ECIES-KEM s využitím délky klíčů 256 bitů a více,
  4. PSEC-KEM s využitím délky klíčů 256 bitů více,
  5. ACE-KEM s využitím délky klíčů 256 bitů a více,
  6. RSA-OAEP s využitím délky klíčů 3072 a více,
  7. RSA-KEM s využitím délky klíčů 3072 a více.
- V sekcích „Schválené hašovcí funkce“ uvádí:
  - SHA-2:
    1. **SHA-256,**
    2. SHA-384,
    3. SHA-512,
    4. SHA-512/256.
  - SHA-3:
    1. **SHA3-256,**
    2. SHA3-384,
    3. SHA3-512,
    4. SHAKE128,
    5. SHAKE256.

Poznámka: Vyhláška 359/2020 Sb. o měření elektřiny definuje **minimální** kryptografické požadavky. Připouští tedy využití **tučně** uvedených hodnot klíčů a delších.

Kryptografický materiál DLMS/COSEM

Zabezpečení Objednávky a dodacího listu nevyužívá komunikaci DLMS/COSEM [4]. Avšak v konfiguračních datech je přenášen kryptografický materiál určený pro komunikaci DLMS/COSEM. Z tohoto důvodu je níže uveden přehled kryptografického materiálu DLMS/COSEM.

Tato kapitola obsahuje výňatky ze standardu ČSN EN IEC 62056-5-3 [4], které se týkají kryptografického materiálu.

5.1 Klient/server

Klientem je vždy datová centrála a serverem měřidlo.

5.2 Název systému (System title)

Každá DLMS/COSEM entita, ať klient, server anebo třetí strana, je identifikována Názvem systému (*System title*). Název systému:

- je trvale přiřazen (pokud má entita více logických jmen (*Logical Device Name* - LDN), pak sdílejí Název systému),
- je dlouhý 8 bajtů (oktetů),
- je jedinečný.

Vedoucí tři bajty obsahují třípísmennou identifikaci výrobce (obdobně jako Logické jméno zařízení (*Logical Device Name – LDN*). Zbylých pět bajtů zajišťuje jedinečnost názvu systému.

Poznámka: Do předmětů certifikátů se Názvem systému (*System title*) ukládá jako 16 hexadecimálních znaků, které odpovídají 8 bajtům Názvu systému.

5.3 Bezpečnostní sada *(Security suite)*

Bezpečnostní sada určuje sadu kryptografických algoritmů (včetně velikosti klíčů), které budou v AMM implementovány. Rozlišujeme Security Suite 0, 1 a 2.

Poznámka: Měřidlo má zpravidla více přístupových rolí. Každá role má vlastní sadu kryptografického materiálu.

5.4 Security suites DLMS/COSEM

ID bezpečnostní sady	Označení bezpečnostní sady	Autentizace a šifrování	Elektronický podpis	Výměna klíčů	Hash	Přenos klíčů	Komprese
0	AES-GCM-128	AES-GCM-128	-	-	-	AES-128 key wrap	-
1	ECDH-ECDSA-AES-GCM-128-SHA-256	AES-GCM-128	ECDSA with P-256	ECDH with P-256	SHA-256	AES-128 key wrap	V.44
2	ECDH-ECDSA-AES-GCM-256-SHA-384	AES-GCM-256	ECDSA with P-384	ECDH with P-384	SHA-384	AES-256 key wrap	V.44

5.5 Typy symetrických klíčů (platí pro Security Suite 1 i 2)

Symetrické klíče rozlišujeme podle:

a) Způsobu použití:
   1) Klíč pro šifrování klíčů (***Key Encrypting Key*** – KEK, také označován jako Master Key) se používá pro šifrování/dešifrování jiných symetrických klíčů. Šifrování šifrovacích klíčů se též označuje jako ***key wrap***.
   2) Šifrovací klíč (***Encryption Key***) **–** klíč blokové šifry AES-GCM;
   3) Autentizační klíč (**Authentication Key)** se používá pro Přidaná Autentizační data (*Additional Authenticated Data* – AAD), používá se algoritmus AES-GCM.

b) Jejich životního cyklu:
   1) Statické klíče (***Static Keys***), které se používají po relativně delší dobu. V DLMS/COSEM rozlišujeme následující statické klíče:
      - Globální klíč (**Global key**) se používá (je platný) přes několik aplikačních asociací (AA) týchž komunikačních partnerů. Globální klíč může být: **global unicast encryption key (GUEK), global broadcast encryption key (GBEK)** nebo **global authentication key (GAK)**;
      - Dedikovaný klíč (**Dedicated key),** který je platný během jedné asociace (AA). Tzn., jeho životnost je pouze na jednu AA.
   2) Dočasné klíče (**ephemeral keys**) se používají na jednu výměnu v rámci AA.

Typ klíče	Použití	Vytvoření klíče (Key establishment)	Využití
Master key, KEK	• Vytvoření nového Master key • GUEK, GAK • dočasné klíče	Jiným způsobem Šifrování klíčů (Key wrap) Výměna klíčů (Key agreement)	Mohou být identifikovány jako KEK pro šifrování paketů (APDU) mezi klientem a serverem
Global unicast encryption key (GUEK)	Šifrování blokovou šifrou: • xDLMS APDU (pakety) • COSEM Data	Šifrování klíčů (Key wrap) Key agreement	• service-specific global ciphering APDU, client-server global ciphering APDU client-server • general-ciphering APDU client server • "Data protection" object protection parameters
Global broadcast encryption key (GBEK)	Šifrování blokovou šifrou: • xDLMS APDU (pakety) • COSEM Data	Výměna klíčů (Key agreement)	
Global authentication key (GAK)	Součást k procesu šifrování xDLMS APDUs a COSEM data	Šifrování klíčů (Key wrap) Výměna klíčů (Key agreement)	Všechny APDU mezi klientem, serverem a třetí stranou
Dedicated key (unicast)	Šifrování blokovou šifrou xDLMS APDU mezi dvěma entitami v rámci ustanovené AA	Přenos klíče v APDU nesoucí xDLMS Initiate.request	• service-specific dedicated ciphering APDU client-server • general-ded-ciphering APDU client-server • during the lifetime of an AA

Ephemeral encryption key	Šifrování blokovou šifrou: • xDLMS APDUs • COSEM data	Šifrování klíčů (Key wrap)	• šifrování APDU mezi klientem a serverem • Šifrování datových objektů ("Data protection' object protection parameters)
	Šifrování blokovou šifrou: • xDLMS APDUs • COSEM data	Výměnu klíčů (Key agreement)	• šifrování APDU mezi klientem a serverem • Šifrování datových objektů ("Data protection' object protection parameters)

5.6 PKI DLMS/COSEM

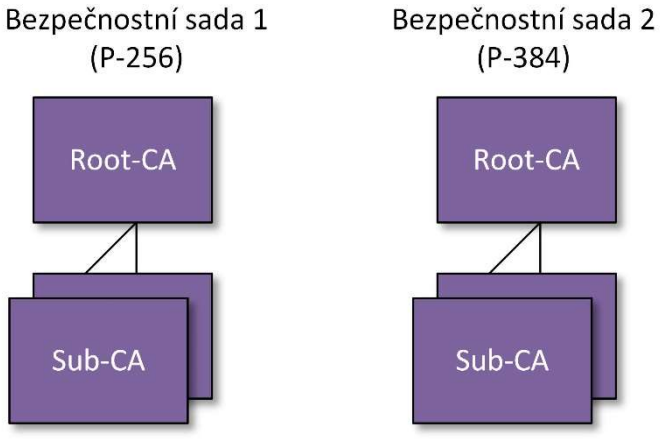
Infrastruktura veřejných klíčů PKI vytváří a spravuje certifikáty veřejného klíče, aby usnadnila použití kryptografie veřejného (asymetrického) klíče. K dosažení tohoto cíle PKI provádí dva základní úkoly:

a) vytváří a distribuuje certifikáty veřejných klíčů, které svazují veřejný klíč s informacemi vedenými v certifikátu,
b) udržuje a spravuje informace o stavu (zneplatnění) certifikátů.

V případě současné podpory Security Suite 1 i 2 je třeba provozovat dvě infrastruktury PKI. Jednu pro bezpečnostní sadu 1 (Security Suite 1) a druhou pro bezpečnostní sadu 2 (Security Suite 2). Obě infrastruktury PKI se skládají z následujících komponent:

- Kořenová certifikační autorita (Root-CA) poskytující bezpečnou kotvu PKI. Root-CA vydává certifikáty podřízeným certifikačním autoritám (Sub-CA). A dále udržuje seznam zneplatněných certifikátů (CRL),
- Podřízené certifikační autority (Sub-CA) vydávají certifikáty koncovým entitám.

DLMS/COSEM využívá pro každou *Security Suite* vlastní PKI [4]:



Obrázek 3 bezpečnostní sady mají své PKI

5.7 Profil certifikátu AMM

X.509 v3 certifikáty mají následující strukturu [RFC 5280]:

Struktura certifikátu X.509

Položka certifikátu	**m/x/o**
`Certificate {`	
`tbsCertificate`	m
`signatureAlgorithm`	m
`signatureValue }`	m

Kde **m/x/o:**

- m (mandatory): povinná položka;
- o (optional): volitelná položka;
- x (do not use): pole nesmí být použito

V DLMS/COSEM používá dva identifikátory objektů (`signatureAlgorithm`):

- ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2) v případě bezpečnostní sady 1 (*security suite 1*),
- ecdsa-with-SHA384 (OID 1.2.840.10045.4.3.3) v případě bezpečnostní sady 2 (*security suite 2*).

Položky struktury tbsCertificate

tbsCertificate	m/x/o	Význam
`tbsCertificate {`		
`Version`	m	'v3' (hodnota musí být 2)
`Serial Number`	m	Sériové číslo certifikátu přidělené CA (nesmí být delší než 20 bajtů)
`Signature`	m	Stejný identifikátor objektu jako v položce certifikátu `signatureAlgorithm`
`Issuer`	m	Jedinečné jméno (Distinguished name – DN) vydavatele certifikátu
`Validity`	m	Platnost certifikátu.
`Subject`	m	Jedinečné jméno (Distinguished name – DN) předmětu certifikátu
`Subject Public Key Info`	m	Veřejný klíč
`Issuer Unique ID`	x	Nesmí se použít
`Subject Unique ID`	o	[EN IEC 62056-5-3]: “Subject unique IDs may be optionally used in end device certificates other than server Certificates. The use of this field is left to project specific companion specifications.” [RFC 5280]: “CAs conforming to this profile MUST NOT generate certificates with unique identifiers.”
`Extensions` `}`	m	Rozšíření

5.7.1 Platnost

Platnost certifikátu je časový interval, během kterého CA zaručuje, že bude udržovat informace o stavu certifikátu. Platnost je sekvencí skládající se ze dvou položek:

- datum a čas od kdy certifikát platí (`notBefore`);
- datum a čas, kdy platnost končí (`notAfter`).

V případě certifikátů certifikačních autorit a koncových entit, které nejsou DLMS/COSEM servery musí být začátek a konec platnosti certifikátu jasně určen.

V případě DLMS/COSEM serverů („elektroměrů“) může být datum konce platnosti neomezeno, tj. může být v položce `notAfter` uveden čas `Generalized Time` s hodnotou `99991231235959Z`.

5.7.2 Sériové číslo

Sériové číslo certifikátu přidělené CA je kladné číslo, které nesmí zaujímat více než 20 bajtů.

5.7.3 Vydavatel a předmět

Vydavatel (`Issuer`) identifikuje entitu, která certifikát podepsala a vydala.

Předmět (`Subject`) identifikuje entitu, která je svázaná s veřejným klíčem uloženým v položce `Subject Public Key Info`. Předmět certifikátu může být uveden v položce předmět certifikátu nebo v rozšíření Alternativní jméno předmětu (`subjectAitName`). Jestliže je položka Předmět prázdná, pak rozšíření Alternativní jméno předmětu musí být označeno jako kritické.

Schéma pojmenovávání jednotlivých entit je uvedeno v následujících tabulkách. Jména se podle potřeby vkládají jako atributy do položek Vydavatel (`Issuer`) nebo Předmět (`Subject`) struktury `tbsCertificate`. Jména uvedená v následujících tabulkách ve špičatých závorkách volí provozovatel PKI.

Jmenné konvence pro Root-CA (informativní)

Atribut	Zkratka	m/x/o	Jméno	Komentář
`Common Name`	`CN`	m	<Root-CA>	Název Root-CA
`Organization`	`O`	o	<PKI-Name>	Název PKI
`Organizational Unit`	`OU`	o		Název organizační jednotky
`Country`	`C`	o		Kód země dle ISO 3166

Jmenné konvence pro Sub-CA (informativní)

Atribut	Zkratka	m/x/o	Jméno	Komentář
`Common Name`	`CN`	m	<XXX-CA>	Název sub-CA CN by mělo končit řetězcem „CA“, aby bylo zjevné, že jde o CA
`Organization`	`O`	o	<PKI-Name>	Název PKI
`Organizational Unit`	`OU`	o		Název organizační jednotky
`Country`	`C`	o		Kód země dle ISO 3166
`Locality`	`L`	o	<Locality>	Místo, kde je Sub-CA umístěna
`State`	`ST or SP`	o	<State>	Vyšší územně správní celek

Jmenné konvence pro koncovou entitu

Attribute	Abbrev.	m/x/o	Name	Comment
`Common Name`	`CN`	m	<System-title>	Název systému DLMS/COSEM (System title): 16 bajtů reprezentováno 32 hexadecinálními číslicemi. Příklad: "4D4D4D0001020304050607000BC614E"
`Organization`	`O`	o	<Organization-Name>	Název PKI
`Organizational Unit`	`OU`	o		Název organizační jednotky
`Country`	`C`	o		Kód země dle ISO 3166
`Locality`	`L`	x		Lokalita
`State`	`ST` nebo `SP`	x	<State>	Vyšší územně správní celek

5.7.4 SubjectPublicKeyInfo

Položka `SubjectPublicKeyInfo` má následující strukturu:

```
SubjectPubuicKeyInfo::= SEQUENCE {
      Algorithm AlgorithmIdentifier,
      subjectPublicKey BIT STRING }
```

položka `AlgorithmIdentifier` má následující strukturu:

```
AlgorithmIdentifier::= SEQUENCE {
      algorithm OBJECT IDENTIFIER,
      parameters ANY DEFINED BY algorithm OPTIONAL }
```

kde `OBJECT IDENTIFIER` v položce `algorithm` může obsahovat následující hodnotu:

- 1.2.840.10045.2.1 pro ECDSA a ECDH Public Key.

Hodnota parametru je:

- 1.2.840.10045.31.7 pro křivku NIST P-256 a
- 1.3.132.0.34 pro křivku NIST P-384.

5.7.5 Rozšíření

Rozšíření X.509 certifikátů poskytují možnost uvádět v certifikátu další atributy spojené s předmětem certifikátu nebo veřejným klíčem v certifikátu uvedeném. Každé rozšíření je opatřeno příznakem, který je buď TRUE, když rozšíření je kritické. Nebo FALSE, v případě, že není kritické.

Následující tabulka obsahuje přehled rozšíření certifikátů užívaných v DLMS/COSEM.

X.509 v3 Rozšíření certifikátu (C je zkratka pro certifikát)

	Rozšíření	CA		Koncové entity		
		C(Root)	C(Sub-CA)	C(TLS)	C(KeyAgree)	C(DataSign)
1	`AuthorityKeyIdentifier`	o	m	m	m	m
2	`Subjectkeyidentifier`	m	m	o	o	o
3	`KeyUsage`	m	m	m	m	m
4	`CertificatePolicies`	o	m	m	o	o
5	`SubjectAltNames`	o	o	o	o	o
6	`IssuerAltNames`	o	o	x	x	x
7	`BasicConstraints`	m	m	x	x	x
8	`ExtendedKeyUsage`	x	x	m	x	x
9	`cRLDistributionPoints`	o	o	x	x	x

5.7.5.1 Identifikátor klíče úřadu (AuthorityKeyIdentifier)

Rozšíření `AuthorityKeyIdentifier` uveřejňuje identifikovat veřejný klíč pro verifikaci certifikátu;

Hodnota: Pole `keyIdentifier` může být spočteno jedním z následujících způsobů:

- 160-bit SHA-1 hash hodnoty `BIT STRING SubjectPublicKey` (nezapočítává se tag, délka a počet nevyužitých bitů), nebo
- Se skládá z hodnoty 0100 následovná posledními významovými 60 bity z SHA-1 hash hodnoty `BIT STRING SubjectPublicKey` (nezapočítává se tag, délka a počet nevyužitých bitů).

5.7.5.2 Identifikátor klíče předmětu (SubjectKeyIdentifier)

Rozšíření `SubjectKeyIdentifier` umožňuje identifikovat certifikát obsahující konkrétní veřejný klíč.

Hodnota: viz pole `keyIdentifier` rozšíření `AuthorityKeyIdentifier`.

5.7.5.3 Použití klíče (KeyUsage)

Definuje způsob použití veřejného klíče z certifikátu.

Hodnota: Bitový řetěz – význam jednotlivých bitů viz následující tabulka.

Rozšíření Použití klíče

	C(Root)	C(Sub-CA)	C(TLS)	C(KeyAgree)	C(DataSign)
Bit nastavený na 1	Podpis certifikátů, Podpis CRL (keyCertSign, cRLSign)	Podpis certifikátů, Podpis CRL (keyCertSign, cRLSign)	Elektronický podpis, Výměna klíčů (digitalSignature keyAgreement)	Výměna klíčů (keyAgreement)	Elektronický podpis (digitalSignature)

5.7.5.4 Certifikační politiky (CertificatePolicies)

Kritické rozšíření: FALSE;

Popis: rozšíření může obsahovat jednu nebo více politik, za které byly certifikát vydán.

Hodnota: OID politiky nebo jen textový řetězec krátkého prohlášení.

5.7.5.5 Alternativní jméno předmětu (SubjectAltNames)

Kritické rozšíření: TRUE v případě, že položka předmět certifikátu je prázdná.

Popis: Toto rozšíření umožňuje navázání dalších identit předmětu s veřejným klíčem.

Rozšíření `SubjectAitName` může obsahovat jedno `GeneralName` typu `OtherName` s pod-typem `Hardware Module Name` (`id-on-HardwareModuleName`) jak je definována v [RFC 4108]. V takovém případě pole `hwSerialNum` bude obsahovat název systému (system title).

Hodnoty v rozšíření SubjectAlternativeName

Certifikát	C(Root)	C(Sub-CA)	C(TLS)	C(KeyAgree)	C(DataSign)
`rfc822Name`	<E-Mail-Address >	<E-Mail-Address>	-	-	-
`URI`	<Web-site >	<Web-site>	-	-	-
`otherName`	-	-	-	<OtherName>	<OtherName>

Poznámka: zajímavé je, že norma neuvažuje `DNSname` byť připouští certifikáty pro TLS.

5.7.5.6 IssuerAltName

Kritické rozšíření: FALSE;

Popisy: toto rozšíření se používá k přidružení identit internetového stylu k vydavateli certifikátu.

Hodnoty Issuer Alternative Name

Certifikát	C(Root)	C(Sub-CA)	C(TLS)	C(KeyAgree)	C(DataSign)
`rfc822Name`	<E-Mail Address>	<E-Mail Address>	-	-	-
`URI`	<Web site>	<Web site>	-	-	-

5.7.5.7 Základní omezeni (Basic constraints)

Kritické rozšíření: TRUE;

Popis: Základní omezení identifikuje, zda je předmětem certifikátu CA a případně maximální hloubku platných certifikačních cest, které tento certifikát obsahují.

Hodnoty rozšíření Basic constraints

Certifikát	C(Root)	C(Sub-CA)	C(TLS)	C(KeyAgree)	C(dataSign)
`cA`	TRUE	TRUE	-	-	-
`pathLenConstraint`	Depends on the structure of the PKI.		-	-	-

5.7.5.8 Rozšířené použití klíče (Extended Key Usage)

Kritické rozšíření: FALSE;

Popis: Indikuje, že se jedná o TLS certifikát serveru nebo klienta:

- TLS server OID: 1.3.6.1.5.5.7.3.1;
- TLS klient OID: 1.3.6.1.5.5.7.3.2.

5.7.5.9 Distribuční místa CRL (CRL Distribution Points)

Kritické rozšíření: FALSE;

Popis: Toto rozšíření definuje přístup, kterým je možné získat CRL;

Toto rozšíření se nepoužije v certifikátech DLMS/COSEM serveru („elektroměrů“)!

5.7.5.10 Další rozšíření

Všechna ostatní rozšíření, která nejsou popsána v tomto profilu, by měla být volitelná; jejich zahrnutí nebo vyloučení a jejich hodnoty budou záviset na konkrétní aplikaci n PKI.

5.8 Management certifikátů

5.8.1 Vybavení serverů důvěryhodnými kotvami

Před provozním nasazením musí být servery vybaveny důvěryhodnými kotvami. Jako důvěryhodné kotvy mohou být certifikáty kořenových certifikačních autorit nebo i certifikáty podřízených certifikačních autorit.

Server může být vybaven jednou nebo více důvěryhodnými kotvami

- Důvěryhodné kotvy mohou být do serverů nahrány jinou cestou (OOB).
- Důvěryhodné kotvy mohou být uloženy společně s ostatními certifikáty.
- Důvěryhodné kotvy mohou být exportovány, ale nikoliv importovány nebo vymazány (myšleno protokolem DLMS/COSEM, tj. musí být importovány jinou cestou.
- Důvěryhodné přímo uložené klíče (bez certifikátu) nesmějí být exportovány.

5.8.2 Vybavení serverů certifikáty dalších CA

Servery mohou být vybaveny dalšími certifikáty.

- Tyto certifikáty nemohou být importovány.

5.8.3 Bezpečná personalizace serverů (tj. měřidel)

Bezpečnou personalizací se míní vybavení serverů páry asymetrických klíčů a příslušných certifikátů. Což se může uskutečnit:

- Ve výrobě, kdy výrobce uloží do serveru párová data a certifikáty. Soukromé klíče pak nikdy nemohou opustit server.
- DLMS/COSEM komunikací (využitím objektu “Security setup” [4]). Tento proces může být využit výrobcem i kdykoliv později, kdy je to třeba.

5.8.4 Certifikáty koncových zařízení (End Entity cert)

Certifikáty koncových zařízení (měřidel, HES, administrátorů měřidel apod.), mj. mají dle DLMS/COSEM následující vlastnosti:

- Doba platnosti certifikátu může být neomezená. Tj. položka *notAfer* (typu *GeneralizedTime*) může být nastavena na hodnotu 99991231235959Z. Což umožní měřidlům komunikaci i po dlouhém vypnutí (viz RFC 5280 [14], odstavec 4.1.2.5.).
- V předmětu certifikátu měřidla se uvádí v položce *Common Name*: tzv. *System title* měřidla, což je 8 bajtů dlouhý řetězec reprezentovaný 16 šestnáctkovými čísly. Např.:“4D4D4D0000BC614E”

Navíc

- [2] uvádí podmínku pro vazbu certifikátu měřidla s certifikátem HES:
  - V certifikátu měřidla se v položce OU předmětu uvede CN z certifikátu HES.
- V případě osob přistupujících k měřidlu lokálními rozhraními (např. při odečtech) za využití Security Suite 1 nebo 2 musí tato osoba být vybavena certifikátem, kde v položce OU bude vyznačena role.

5.9 Doba platnosti certifikátů měřidel

Dle DLMS/COSEM by mělo mít měřidlo certifikát s neomezenou platností (tj. `notAfter= 99991231235959Z`). Avšak nejvhodnějším řešením je, vydávat certifikáty měřidel s hodnotou `notAfter` shodnou s touž hodnotou certifikátu sub-CA, neboť mnohý software bude mít s hodnotou `99991231235959Z` problém.

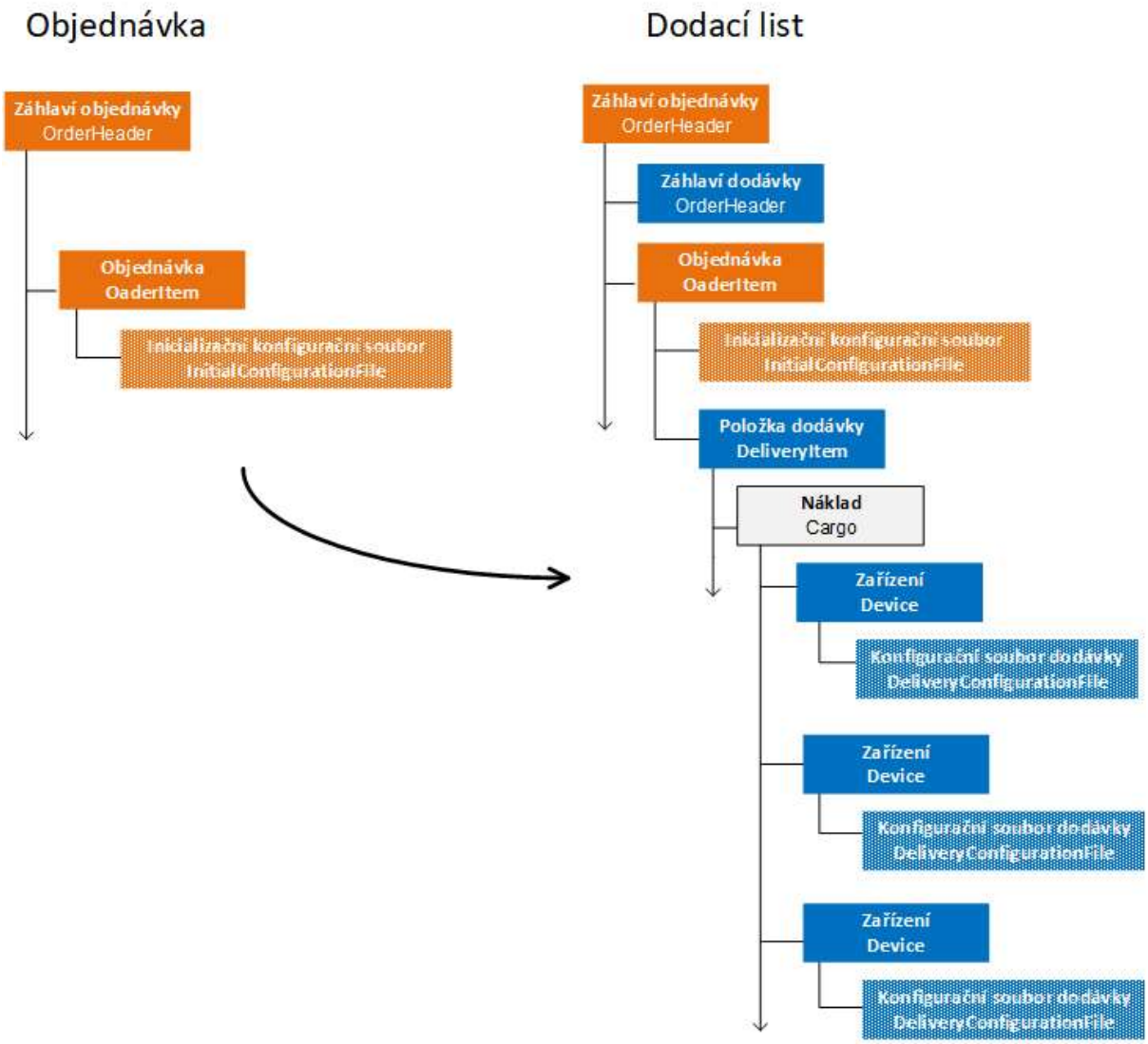
5.10 Příklady certifikátů

Příklady certifikátů pro elektronické objednávání měřidel i certifikátů DLMS/COSEM jsou uvedeny v dodatku A.

Elektronická objednávka a dodací list

Elektronický dodací list slouží pro nové objednávky, opravy i pro přejímku zboží a kontrolu příchozího zboží.

Na následujícím obrázku je znázorněn proces, jak doplněním Objednávky vzniká Dodací list. (Z obrázků je vypuštěn element eOL, což je hlavní element, který je přítomný ve struktuře vždy).



Obrázek 4 Schéma objednávky a dodacího listu

6.1 Pojmenování v případě Objednávky

Pro objednávku je tedy definována následující struktura těchto dvou informací:

```
<Zkratka společnosti kupujícího>_<Číslo objednávky>_<Datum objednávky>
```

- Příklad předmětu e-mailu: DNT_1234567890_20150401
- Příklad názvu souboru: DNT_1234567890_20150401.xml

Poznámka: <Zkratka společnosti objednatele> maximálně 20 znaků

6.2 Pojmenování v případě Dodacího listu

Pro dodávku je tedy definována následující struktura těchto dvou informací:

```
<zkratka výrobce>_<číslo objednávky>_<číslo dodacího listu>_<datum dodání>
```

- Příklad předmětu e-mailu: LUG_1234567890_1234567890_20150430
- Příklad názvu souboru: LUG_1234567890_1234567890_20150430.xml

Poznámka: <zkratka výrobce> maximálně 20 znaků dlouhá

Popis datových formátů v elektronické objednávce a dodacím listu

V následujícím textu jsou názvy XML tagů uvedeny v anglické verzi. Navíc jsou pod nimi kurzivou uvedeny i **originální německé názvy XML tagů**. Umožňuje to tak vytvořit překladový slovník z německé verze do anglické a naopak.

K popisu dat pro objednávání a dodávku měřících zařízení je využit značkovací jazyk XML. s následujícími jmennými prostory (*Namespace*):

- xmlns:eol=http://schemas.smetrid.cz/eOL1_5
  xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
- xmlns:ds=http://www.w3.org/2000/09/xmldsig#

Poznámka: v původním německém dokumentu byl definován jmenný prostor xmlns:els="http://localhost/ELS23“

Poznámka: číslo v namespace eOLx_y odpovídá verzi tohoto dokumentu x.y, který popisuje danou verzi struktury XSD. Současná verze dokumentu, 1.5, tedy odpovídá názvu namespace eOL1_5

Tabulka 3 Popis použitých datových typů

Datový typ ***(dle německého doc.)***	**Definice**	**Komentář**
ds:SignatureType	• http://uri.etsi.org/01903/v1.3.2# • http://uri.etsi.org/01903/v1.4.1# • http://www.w3.org/2000/09/xmldsig#	
ds:X509DataType		Boudou využity pouze typy: X509Data nebo SKIData.
eol:WasteCode	([0-9][0-9])([0-9][0-9])([0-9][0-9](*)?)?	Kód odpadu v souladu s vyhláškou o Evropský katalog odpadů (Vyhláška č. 8/2021 Sb.)
eol:Any	<xs:sequence> <xs:any namespace="##any" minOccurs="0" maxOccurs="unbounded"/> </xs:sequence>	Dává možnost pro nespecifikovanou položku, např. klíče DLMS
eol:IndependentIDNumber	[A-F0-9]{1}[AZ]{3}[A-F0-9]{2}[0-9]{8}	Identifikační číslo měřicích zařízení nezávislé na výrobci
eol:Manufacturer	[AZ]{3}	podle Asociace uživatelů DLMS, https://www.dlms.com/flag-id/flag-id-list
eol:IMEIType	[0-9]{15}	
eol:IPv4Address	((((25[0-5])|(2[0-4][0-9])|(1[0-9]{2})|([1-9][0-9])|([0-9]))\.){3}((25[0-5])|(2[0-4][0-9])|(1[09]{2})|([1-9][0-9])|([0-9]))))(\/([1-9]|([1-2][09])|(3[0 -2]))).	Viz https://medium.com/sroze/regex-ip-v4-et-ipv6-6cc005cabe8c Příklad: 192.1.20.100, /16

eol:IPv6Address	((([0-9A-Fa-f]{1,4}:){7}[0-9A-Fa-f]{1,4})|(([0-9A-Fa-f]{1,4}:){6}:[0-9A-Fa-f]{1,4})|(([0-9AFa-f]{1,4} :){ 5}:([0-9A-Fa-f]{1,4}:)?[0-9A-Faf]{1,4})|(([0-9A-Fa-f]{1,4 }:){4}:([0-9A-Faf]{1,4}:){0,2}[0-9A-Fa-f]{1,4})|(([0-9A-Faf]{1,4}:){3}:([0-9A-Fa-f]{1,4}:){0,3}[0-9A-Faf]{1,4})|(([0-9A-Fa-f]{1,4}:){2}:([0-9A-Faf]{1,4}:){0,4}[0-9A-Fa-f] {1,4})|(([0-9A-Faf]{1,4}:){6}(((25[0-5])|(2[0-4][0-9]) |(1[09]{2})|([1-9][0-9])|([0-9]))\.){3}((25[0-5])|(2 [0-4][0-9])|(1[0-9]{2})|([1-9][0-9])|([0-9])))|(([0-9A-Fa-f]{1,4}:){0,5}:(((25[0-5])|(2[0-4][09])|(1[0-9]{2})|([1-9][0-9])|([0-9]))\.){3}((25[0-5])|(2[0-4][0-9])|(1[0-9]{2})|([1-9][0-9])|([09])) |(::([0-9A-Fa-f]{1,4}:){0,5}(((25[0-5])|(2[0-4][0-9])|(1[0-9]{2})|([1-9][0-9])|([0-9]))\.){3}((25[0-5])|(2[0-4][0-9])|(1[0-9]{2})|([19] [0-9])|([0-9])))|([0-9A-Fa-f]{1,4}::([0-9A-Faf]{1,4}:){0,5}[0-9A-Fa-f]{1,4})|(::([0-9A-Faf]{1,4}:){0,6}[0-9A-Fa- f]{1 ,4})|(([0-9A-Faf]{1,4}:){1,7}:))|(V([1-9]|([1-8] [0-9])|(9[0-6]))).	Příklad: 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 nebo /96
eol:NumberText	1 až 20 znaků	Všechny texty jsou omezeny na délku, aby byly požadavky na systémy zpracování předvídatelné. Vysvětlení v kapitole 7.2.2
eol:ShortText	2 až 100 znaků	
eol:LongText	4 až 1000 znaků	
eol:ParameterVersionLength	1 až 64 znaků	
eol:MACType	([A-F0-9][A-F0-9]:){5}([A-F0-9][A-F0-9])	Hardwarová adresa rozhraní.
eol:IMSIType	[0-9]{14,15}	
eol:OBIS	(((25[0-5])|(2[0-4][0-9])|(1[0-9][0-9])|([1-9][0-9])|([0-9]))-((25[0-5])|(2[0-4][0-9])|(1[0-9][0-9])|([1-9][0-9])|([0-9])):(((25[0-5])|(2[0-4][0-9])|(1[0-9][0-9])|([1-9][0-9])|([0-9]))\.){2})((25[0-5])|(2[0-4][0-9])|(1[0-9][09])|([1 -9][0-9])|([0-9]))	x-x:x.x.x, kde x je mezi 0 a 255. Viz [19] V případě potřeby by měl příjemce sám přidat posledních 255
eol:Port	positiveInteger, maxInclusive=65535	TCP nebo UDP port
eol:PINType	4-20 číslic	
eol:Password	2–20 znaků	
eol:Arity	((1[0-9],[0-9])|[0-9],[0-9])	Formát: vv,n [v: počet číslic před desetinnou čárkou; n: počet číslic za čárkou]
eol:PhoneNumber	[0\+][1-9][0-9]{4,14}(-[0-9]{1,4})?	
eol:EMailAddress	[^@]+@[^\.]+\..+	
eol:SystemTitle	[0-9a-fA-F]{16}	16 hexadecimálních číslic. Nezáleží na to, jsou-li použity malá nebo velká písmena.
eol:LogicalDeviceName	[0-9a-fA-F]{32}	32 hexadecimálních číslic. Nezáleží na to, jsou-li použity malá nebo velká písmena.
xs:decimal	Výchozí datový typ, reference https://www.w3.org/TR/xmlschema112/#decimal	Podle zadané definice se jako symbol desetinné čárky používá desetinná čárka.

xenc:EncryptedDataType	Výchozí datový typ, reference https://www.w3.org/TR/xmlenc-core1/	
xenc:EncryptedKeyType		
xs:anyURI	Standardní datový typ, odkaz: https://www.w3.org/TR/xmlschema11-2/	
xs:base64Binary		
xs:Boolean		True nebo False
xs:date		YYYY-MM-DD
xs:dateTime		
xs:float		
xs:gYear		yyyy
xs:hexBinary		
xs:ID		
xs:nonNegativeInteger		
xs:positiveInteger		
xs:schema		
xs:unsigned		
xs:unsignedByte		

Vysvětlení vzorů v definici: [] definuje rozsah, např. [0-5], libovolné číslo mezi 0 a 5. () Seskupuje výraz, např. Např. ([A-F0-9][A-F0-9]:), dvoumístné hexadecimální číslo následované dvojtečkou. {2,4}, +, ? definuje, jak často se výraz může objevit: 2 až 4krát, alespoň jednou (+) a maximálně jednou (?). \ znamená, že následující znak je brán doslovně, i když má zvláštní význam, např. ? nebo +.

7.1 Deklarace přípustných hodnot

Tabulka 4 Popis datových typů XML se sadou hodnot

XML datový typ	Hodnoty
DisplayType	Typ displeje: Roll; Display; Without_Display
ItemDefect	Způsob poškození: Transport_Damage; Metrological; Formally; Mechanically; Functional
QuantitativeUnit	Množstevní jednotka: Sheet; Block; Case; Cardboard; Crate; Package; Palette; Role; Set; Piece; Pair; Meter; Kilo; Liter
InstallationPosition	Vertical; Horizontal; Universal
MeasuringUnit	Wh; kWh; MWh; GWh; var; kvar; mvar; kvarh; kW; MW; V; A; MJ; GJ; m³; Nm³; K; VA; °C; m; kg; l; W; Hz
FirmwareType	Metrological_FW; Application_FW; Operating_System_FW; Display_FW; GSM_Module_FW; Security_Module_FW; Other_FW1; Other_FW2; Other_FW3; Other_FW4; Other_FW5
CargoType	Typ nákladu: Lattice_Box; Cardboard; Workpiece_Carrier; Palette; Plastic_Box; Other_Load_Carrier; Transport_Case; Euro_Pallet; Container_20_Ft; Container_40_Ft; Safe_Bag; Safety_Box; Sky_Box/

DeliveryCondition	Stav dodávky: Expanded; Ready_For_Installation; Built-in; To_Edit; Claim; New; Scrap; Repaired; Malfunction
DeliveryConditionSMGW	Stav dodání SMGW: Empty; Integrated; Pre-personalized_1; Pre-personalized_2; Personalized; Terminated
Class	Třída udávající v závislosti na utilitě metrologickou třídu nebo třídu přesnosti přístroje. Údaj odpovídá měřicímu rozsahu podle:: A; B; C; R10; R12,5; R16; R20; R25; R31,5; R40; R50; R63; R80; R100; R125; R160; R200; R250; R315; R400; R500; R630; R800; R1000; R1250; R1600; R2000; R2500; R3150; R4000; R5000; R6300; R8000; 0,2; 0,5; 1; 2; 0,2S; 0,5S; 1,5; 3
Relationship	1:1; 1:8; 1:10; 1:25; 1:50; 1:100; 1:250; 1:400
IPAddressType	Fixed; DHCP_Client; DHCP_Server; Hostname; Zero_Conf; SIM; NDP; Fixed_Incremented
TestTypeCode	MID_Compliant; MessEV_Compliant; MID_MessEV_Compliant; Calibration; Individually_Tested; Randomly_Tested; WE_Piece_Checked
OutputSwitchingType	Opener; Closer; Changer
InterfaceType	Typ rozhraní: LAN; WANA; WAN; WAN1; WAN2; HAN; LMN; CLS; CLS1; CLS2; WakeUp; GWAManagement; GWAService; GWANTP; SMGWHKS3; EMTNTP; EMTDATA
SIMSize	Fullsize_SIM; Mini_SIM; Micro_SIM; Nano_SIM; Embedded_SIM; Fullsize_SIM_Robust; Mini_SIM_Robust; Micro_SIM_Robust; Nano_SIM_Robust; Embedded_SIM_Robust
ActivityType	Důvod opravy: Disassembly; Internal_Parameterization; Calibration_Testing; Quality_Check; Modification; Assembly; Overhaul
Technology	2G; 3G; GPRS; LTE; PLC; G3-PLC; Prime; Ethernet; WLAN; RS-485; Bluetooth; M-Bus; Wireless-M-Bus; LWL; BPL; CDMA; LoRaWAN; Other
CertificateType	(použít v datovém typu ds:X509Datatyp jako dílčí prvek v prvku libovolného jmenného prostoru): TLS; AUT; ENC; SIG; Root; CA; Transport; AGR; Other
AccessRoleList	Přístupová role: Admin_Access; Service_Access; Read_Access; Customer_Access; Public
Authentication	CHAP; PAP; NONE; ANY
ContactType	Typ kontaktu: Logistics; Technology; Commercial; Logistics_SMGW
ActivationType	Typ aktivace: OTAA; ABP
DeviceClass	A; B; C
ProviderName	T-Mobile; O2; Vodafone; Other
KeyType	Typ symetrického klíče: KEK; GUEK; GAK; GBEK
CertificateEntity	Server; Client; Certification_Authority; Other

7.2 Popis datových struktur

Níže je uveden popis datové struktury používané v eOL.

Pořadí prvků/atributů popsaných v následujících tabulkách odpovídá pořadí v XSD. Pro automatickou verifikaci eOL musí být kód vygenerován ze schémat. Vytvořený eOL musí být úspěšně verifikován podle schémat.

Název	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ

Obrázek 19: Záhlaví tabulky složených (komplexních) datových prvků

Název:

- Tento sloupec mapuje hlavní strukturu formátu.
- Jména označená * obsahují šifrovaná data.

Prvek / atribut:

- V tomto sloupci je pojmenován název proměnné příslušného atributu, případně další prvky. V datovém modelu jsou vlastnosti, které se v databázi používají spíše jako primární klíče, reprezentovány jako atributy XML.
- Vlastnost atributu [A] nebo prvku (elementu) [E] je označena odpovídajícím způsobem. V případě, že atribut patří k předchozímu elementu, je označen [AX].

Popis:

Zde je zevrubnější popis parametru, který se zde vkládá.

Počet:

V každém případě je specifikováno, zda prvek:

- musí se vyskytnout přesně t-krát (x=t), například x=2 znamená, že se prvek musí vyskytnout přesně dvakrát,
- je naprosto nezbytný a může se vyskytnout bez omezení (x=1-n),
- je naprosto nezbytný a může se vyskytnout minimálně s-krát a maximálně t-krát (x=s-t), například x=2-4 znamená, že se prvek může vyskytnout dvakrát, třikrát nebo čtyřikrát,
- není nezbytně nutný, může se vyskytnout bez omezení (x=0-n),
- není nezbytně nutný, a může se vyskytnout maximálně t-krát (x=0-t), například x=0-3 znamená, že se prvek může vyskytnout jednou, dvakrát nebo třikrát, ale také se nemusí vyskytnout vůbec,
- pokud je přítomen, může se vyskytnout pouze jednou (x=0-1).

XML datový typ

Použitý datový typ podle kapitoly 7.2 Použité datové typy

Záznamy v tabulkách se světle modrým pozadím označují složené (komplexní) prvky (prvky mající vnitřní strukturu). Sloupec "Popis" pak odkazuje na odpovídající kapitolu.

1.1.2 Datová struktura pro více možností

Některé datové struktury jsou připraveny tak, aby mohly obsahovat více možností vnořených elementů. Tyto prvky jsou označeny termínem „Jeden z“ v druhém sloupci. Jednotlivé možnosti volby jsou pak označeny různými odstíny žluté. Prvky označené různým odstínem (kromě bílé barvy) se navzájem vylučují, prvky označené stejným odstínem musí být ve struktuře obsaženy společně (omezení definované Počtem stále platí, nepovinné položky jsou tedy i v rámci volby stále nepovinné.

Pro přehlednost jsou vždy v rámci dané kapitoly jednotlivé možnosti, které může daný prvek obsahovat, konkrétně popsány.

Tabulka 5 Příklad fungování datové struktury pro více možností

Název	Prvek [E] a atribut [A]			Popis	Počet	XML datový typ
příklad_struktury		A	E		0-1	-
	Jeden z	B	E		1	-
		C	E		0-1	-
		D	E		1	-

V příkladu výše obsahuje prvek vždy nepovinně prvek A (protože počet je 0-1), a k tomu:

- BUĎ povinně prvek B a nepovinně prvek C (protože počet je 0-1),
- NEBO povinně prvek D

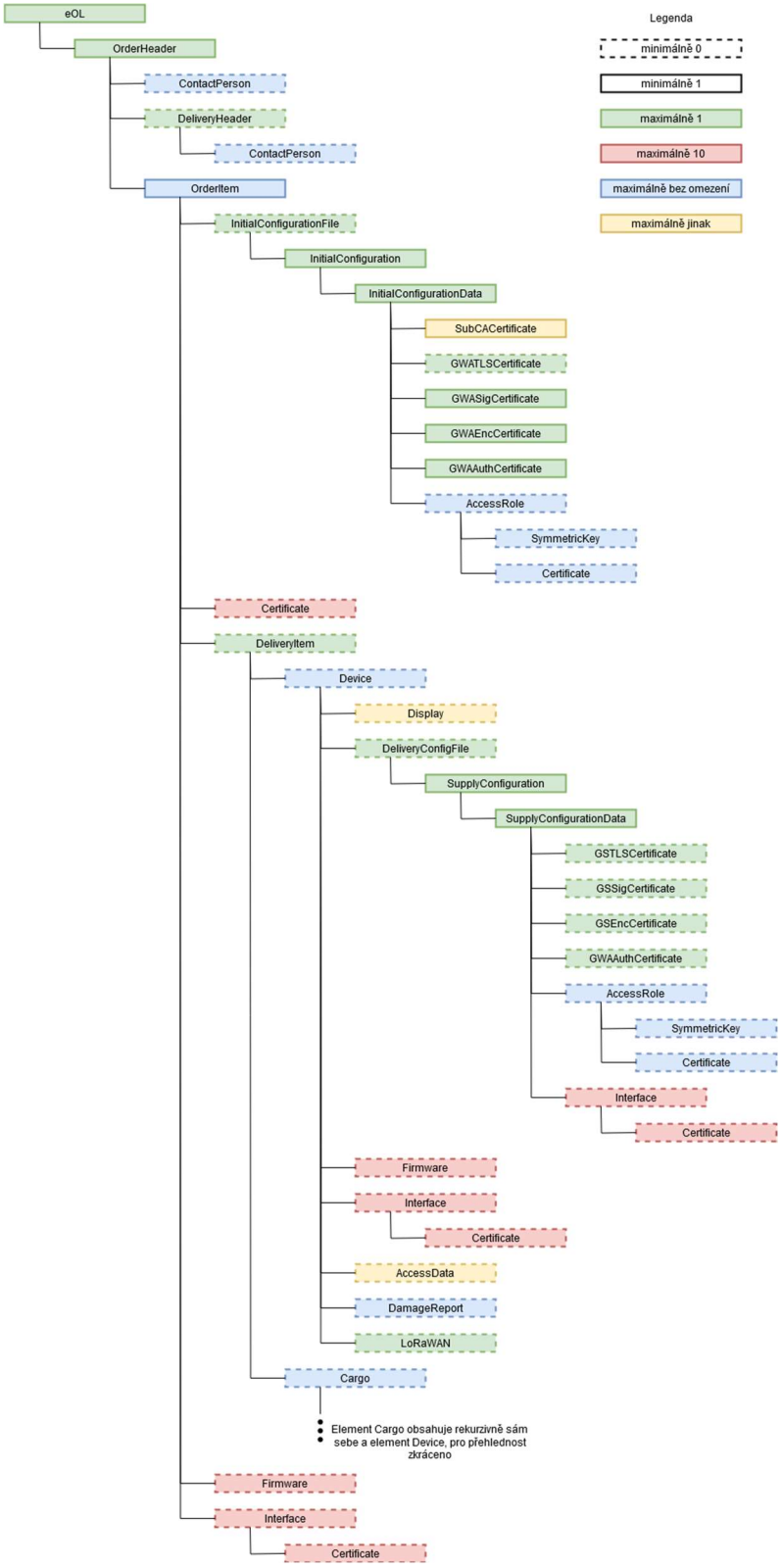
Mezi povolené možnosti tedy patří (výčet není úplný):

- A a B a C
- samotné D
- samotné B
- A a B

Mezi nepovolené možnosti pak patří (výčet není úplný):

- samotné A (není obsažen žádný prvek z volby)
- B a D (B a D jsou prvky z různých voleb a nemohou být použity zároveň)

7.3 Struktura složených prvků



Obrázek 5 Struktura Dodacího listu (pouze složené prvky)

Obrázek shrnuje celou eOL strukturu, pro přehlednost obsahuje pouze složené prvky. Ohraničení a barva prvku značí jeho minimální a maximální počet výskytů (viz legenda).

Popsaná je kompletní struktura, která je využitá pro elektronickou objednávku / dodací list. Ostatní specifické použití různých částí struktury (viz volba v kapitole 7.4.1) nejsou v obrázku shrnuty.

7.4 Popis složených prvků

7.4.1 Záhlaví Objednávky/Dodacího listu

Tento blok obsahuje údaje důležité pro vytvoření následného dodacího listu, jako jsou specifikace a verze dodacího listu.

Blok podporuje 4 možnosti struktury:

- Struktura obsahuje položky EncryptedKey, OrderHeader a Signature – slouží k předání celé objednávky / dodacího listu
- Struktura obsahuje jen položku InitialConfiguration – slouží k ověření validity konfiguračních dat před jejich šifrováním
- Struktura obsahuje jen položky EncryptedKey a InitialConfigurationFile – data, která předává Správce měřidel Objednateli (viz kapitola 4.4)
- Struktura obsahuje jen položky EncryptedKey a Device – slouží k předání šifrovaných exportovaných kryptografických dat z měřidla

Tabulka 6 Kořen eOL

Název	Prvek [E] a atribut [A]			Popis	Počet	XML datový typ
eOL		EncryptedKey	E	Symetrický klíč pro šifrování citlivých položek eOL	0-1	xenc:EncryptedKeyType
	Jeden z	OrderHeader	E	Viz 7.4.2	1	eol:OrderHeader
		InitialConfiguration	E	K ověření validity xml struktury InitialConfiguration	1	eol:InitialConfiguration
		InitialConfigurationFile	E	K ověření validity xml struktury InitialConfigurationFile	1	eol:InitialConfigurationFile
		Device	E	K exportu dat o jednom zařízení	1	eol:Device
		Signature	E	Podpis XAdES-Baseline-B položky OrderHeader	0-1	ds:SignatureType
		eOLVersionNumber	A	verze eOL (datové struktury)	1	eol:NumberText

7.4.2 Záhlaví objednávky (OrderHeader)

Hlavička objednávky obsahuje údaje o objednávce a také technické, obchodní a logistické kontakty objednatele.

Tabulka 7 Záhlaví objednávky

Název	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
OrderHeader	ContactPerson	E	Kontaktní osoba u klienta Viz 7.4.20	0-n	eol:ContactPerson
	SupplierNumber	E	Identifikační číslo dodavatele (určené objednavatelem)	0-1	eol:NumberText
	PurchaserNumber	E	Identifikační číslo objednatele	0-1	eol:NumberText
	DeliveryHeader	E	Viz 7.4.3	0-1	eol:DeliveryHeader
	OrderItem	E	Viz 7.4.4	1-n	eol:OrderItem
	OrderDate	A	Datum objednávky nebo odvolání ze strany objednavatele	1	xs:date
	OrderNumber	A	Číslo objednávky nebo číslo odvolávky objednavatele	1	eol:ShortText
	ContractNumber	A	Číslo smlouvy mezi objednatelem a výrobcem, ze které je zakázka	0-1	eol:ShortText

7.4.3 Záhlaví dodávky (DeliveryHeader)

Záhlaví dodávky obsahuje údaje o dodávce a také technické, obchodní a logistické kontakty výrobce.

Tabulka 8 Záhlaví dodávky (Delivery Header)

Název	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
DeliveryHeader	CargoCount	E	Počet nákladů (v první úrovni hlavní náklad)	1	xs:positiveInteger
	ContactPerson	E	Kontaktní osoba u výrobce Viz 7.4.20	0-n	eol:ContactPerson
	DeliveryDate	A	Datum dodání	1	xs:date
	DeliveryNoteNumber	A	Číslo dodacího listu	1	eol:NumberText

7.4.4 Objednávka (OrderItem)

Podrobné specifikace zboží k dodání jsou na úrovni položky objednávky.

Tabulka 9 Objednávka (OrderItem)

Název	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
OrderItem	ProductIdentification	E	Reference zboží (produktu) v objednávkovém systému objednatele	0-1	eol:NumberText
	ArticleType	E	Typ produktu	0-1	eol:NumberText

ShortText	E	Obecný obchodní popis	0-1	eol:ShortText
DeviceIDInterval	E	Interval identifikátorů zařízení zadaných objednatelem (1234-4321)	0-n	eol:ShortText
LongText	E	Dlouhý text definovaného popisu	0-1	eol:LongText
ManufacturerTypeDesignation	E	Schválené typové označení	0-1	eol:ShortText
ManufacturerArticleNumber	E	Číslo výrobku u výrobce	0-1	eol:ShortText
FeaturesListOrderer	E	Označení / název (např. název souboru) seznamu s detailním popisem funkcí výrobku. Lze zadat i označení výrobce.	0-1	eol:ShortText
SubCAName	E	Předmět (Common Name) vydávající CA	0-1	eol:ShortText
InitialConfigurationFile	E	Viz 7.4.14	0-1	eol:InitialConfigurationFile
Owner	E	Identifikátor vlastníka	0-1	eol:ShortText
PropertyNumberStart	E	Počáteční číslo čísla nemovitosti objednavatele. Předpokládá se, že se vždy použijí po sobě jdoucí čísla a že rozsah čísel vyplývá automaticky z množství objednávky.	0-1	eol:NumberText
OrderAmount	E	Objednané množství na jednotku	1	xs:positiveInteger
MeasureUnit	E	Měrná jednotka. Viz tabulka 4	1	eol:QuantitativeUnit
Certificate	E	Šifrovací certifikát Správce měřidel	0-10	eol:Certificate
DeliveryItem	E	Položka dodávky. Viz 7.4.5	0-1	eol:DeliveryItem

	DeliveryConditionSMGW	E	Je zde soubor hodnot. Viz tabulka 4	0-1	eol: DeliveryCondition
	InitialConfigurationPIN	E	Toto je počáteční inicializační PIN přidělený montérovi se zvýšenými oprávněními (Počáteční konfigurace)	0-1	eol:PINType
	HardwareVersion	E	Hardwarová verze zařízení, specifikuje hardwarovou verzi dodaného zařízení, aby ji mohl výrobce dohledat.	0-1	eol:NumberText
	Firmware	E	Viz 7.4.11	0-10	eol:Firmware
	ParameterVersion	E	Verze konfigurace zařízení	0-1	eol:NumberText
	Interface	E	Viz 7.4.16	0-10	eol:Interface
	CmNTPServerIP	E	IP adresa NTP serveru	0-3	eol:IPAddress
	NMSHeartbeatEnabled	E	Aktivujte/deaktivujte Heartbeat pro NMS1 a NMS2	0-1	xs:boolean
	NMSIP1	E	IP adresa primárního serveru NMS.	0-1	eol:IPAddress
	NMS1HeartbeatInterval	E	Interval pro odesílání SNMP trapů v sekundách pro NMS1	0-1	xs:positiveInteger
	NMSIP2	E	IP adresa sekundárního serveru NMS.	0-1	eol:IPAddress
	NMS2HeartbeatInterval	E	Interval pro odesílání SNMP trapů v sekundách pro NMS2	0-1	xs:positiveInteger
	OrderItemNumber	A	Číslo objednávky	1	eol:NumberText
	ContractItem	A	Číslo položky smlouvy	0-1	eol:NumberText
	SystemTitleStart	E	(pro Výrobce) První SystemTitle, od kterého se budou sekvenčně tvořit další SystemTitle v	0-1	eol:SystemTitle

			počtu stanoveném v OrderAmount		

7.4.5 Položka dodávky (DeliveryItem)

Tato úroveň popisuje podrobnou specifikaci dodaného zboží. Dva datové prvky "OrderItem" a "DeliveryItem" jsou vždy přítomny **v poměru 1:1**. Jedna Dodávka může obsahovat více zařízení (Device).

Tabulka 10 Dodávka (DeliveryItem)

Název	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
DeliveryItem	Manufacturer	E	Identifikátor výrobce	1	eol:Manufacturer
	ManufacturerNumber	E	Číslo produktu (zboží) u výrobce	0-1	eol:ShortText
	ManufacturerType	E	Název produktu výrobce	0-1	eol:ShortText
	DeliveryAmount	E	Aktuálně dodávané množství této položky dodávky	1	xs:positiveInteger
	QuantitativeUnit	E	Množstevní jednotka. Viz tabulka 4	1	eol:QuantitativeUnit
	FeaturesListOrderer	E	Označení / název (např. název souboru) seznamu s detailním popisem funkcí výrobku	0-1	eol:ShortText
	DeliveryCondition	E	Typ dodávky. Viz tabulka 4	1	eol:DeliveryCondition
	ActivityType	E	Důvod opravy. Viz tabulka 4	0-1	eol:ActivityType
	WasteCode	E	Kód odpadu v souladu s vyhláškou o Evropský katalog odpadů (Vyhláška č. 8/2021 Sb.)	0-1	eol:WasteCode
	QCertificateMID	E	Číslo certifikátu zajišťování jakosti podle MID (modul D)	0-1	eol:ShortText
	ManufacturingNotifiedBody	E	Oznámená osoba Výrobce	0-1	eol:ShortText
	MeasuringNotifiedBody	E	Tato oznámená osoba podle MessEV vyhodnocovala proces výroby produktu u výrobce (modul D); příklad pro PTB: 0102	0-1	eol:ShortText
	QCertificateMeasureEV	E	Číslo certifikátu zajišťování jakosti podle MessEV (modul D)	0-1	eol:ShortText
	TestType	E	Typ testu. Viz tabulka 4	0-1	eol:TestTypeCode

Class	E	Třída udává v závislosti na utilitě metrologickou třídu nebo třídu přesnosti přístroje. Údaj odpovídá měřicímu rozsahu podle MID a udává se v souvislosti s prvkem „prostředí instalace. Viz tabulka 4	0-6	eol:Class
MIDTypeTestCertificate	E	Osvědčení o typové zkoušce nebo osvědčení o zkoušce návrhu podle MID vydané oznámenou osobou.	0-1	eol:ShortText
Revision	AX	Číslo revize osvědčení o typové zkoušce nebo číslo revize osvědčení o zkoušce návrhu podle MID)	1	xs:nonNegativeInteger
MIDTypeCertIssueDate	E	Datum vystavení osvědčení o typové zkoušce nebo osvědčení o zkoušce návrhu podle MID vydaného oznámenou osobou	0-1	xs:date
MIDTypeCertificate	E	Osvědčení o typové zkoušce nebo osvědčení o zkoušce návrhu podle MID vydané oznámenou osobou.	0-1	eol:ShortText
Revision	AX	Číslo revize osvědčení o typové zkoušce nebo číslo revize osvědčení o zkoušce návrhu podle MID	1	xs:nonNegativeInteger
MIDTypeNotifiedBody	E	Oznámená osoba, která vystavila osvědčení o typové zkoušce nebo osvědčení o zkoušce návrhu	0-1	eol:ShortText
CountryConformityAssessment	E	Národní hodnocení konformity podle MessEV (datum vystavení od 2015)	0-1	eol:ShortText
Revision	AX	Číslo revize národního hodnocení konformity	1	xs:nonNegativeInteger
CountryNotifiedBody	E	Oznámená osoba, která vystavila národní hodnocení konformity	0-1	eol:ShortText
CountryAssessmentDate	E	Datum vystavení národního hodnocení konformity	0-1	xs:date
ESTestNumber	E	Číslo zkoušení ES podle starých směrnic EHS	0-1	eol:ShortText

ESAssesNumberDate	E	Datum udělení čísla zkoušení ES podle starých směrnic EHS	0-1	xs:date
ESLaboratory	E	Pracoviště, které udělilo číslo zkoušení ES	0-1	eol:ShortText
DVGWApproval	E	Schválení DVGW (relevantní pouze pro plyn a vodu)	0-1	eol:ShortText
DVGWApprovalDate	E	Datum vystavení schválení DVGW	0-1	xs:date
DVGWLaboratory	E	Pracoviště, které vystavilo schválení DVGW	0-1	eol:ShortText
BSICertificateNumber	E	Číslo certifikátu BSI	0-1	xs:anyURI
BSICertificateNotAfrer	E	Datum vypršení certifikátu BSI	0-1	xs:date
OMSCertificateNumber	E	Číslo certifikátu OMS	0-1	eol:ShortText
OMSCertificateIssuingDate	E	Datum vystavení certifikátu OMS	0-1	xs:date
OMSLaboratory	E	Pracoviště, které vystavilo certifikát OMS	0-1	eol:ShortText
FNNCertificateNumber	E	Číslo certifikátu FNN	0-1	eol:ShortText
FNNCertificateIssuingDate	E	Datum vystavení certifikátu FNN	0-1	xs:date
FNNLaboratory	E	Pracoviště, které vystavilo certifikát FNN	0-1	eol:ShortText
InstallationPosition	E	Montážní poloha zařízení	0-1	eol:InstallationPosition
TransportKey	E	Veřejným klíč, příjemce, šifrovaný klíč pro šifrování všech polí obsahující prvky xenc.	0-10	xenc:EncryptedKeyType
Device	E	Viz 7.4.7	0-n	eol:Device
Cargo	E	Viz 7.4.6	0-n	eol:Cargo
AccessoriesWithoutIdNumber	E	Viz 7.4.8	0-n	eol: AccessoriesWithoutIdNumber
DeliveryItemNumber	A	Číslo položky dodávky	1	eol:NumberText
RatioMeasurementRange	E	Poměr měřicího rozsahu měřiče (např. poměr průtoku qi/qp) nebo převodníku	0-1	eol:Relationship

7.4.6 Náklad (Cargo)

- Náklad specifikuje podrobnosti o tom, jak bude zboží doručeno.
- Náklady mohou být vnořené, náklady se mohou vyskytovat v rámci jiného nákladu. Například krabice se zařízeními jsou obsaženy v kontejneru.
- Každá struktura Cargo může obsahovat také element CargoDescription, který obsahuje přesnější popis daného elementu

- Pomocí elementu Cargo je tedy možné popsat i komplexní strukturu uložení
- Do každého element Cargo je možné vložit element Device, který obsahuje popis daného zařízení (viz 7.4.7). V případě zatřizování popisu zařízení do struktury Cargo je třeba mít na paměti, že každý konkrétní výrobek má být ve struktuře uveden právě jednou

Tabulka 11 Náklad

Jméno	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
Cargo	CargoType	E	Typ nákladu. Viz tabulka 4	1	eol:CargoType
	CargoDescription	E	Bližší popis nákladu	0-1	eol:ShortText
	ManufacturerArticleNumber	E	Číslo nákladu	0-1	eol:NumberText
	TrackingNumber	E	Sledovací číslo dopravce	0-1	eol:ShortText
	WebTrackingNumber	E	URL na které je možné sledovat dodávku	0-1	xs:anyURI
	Weight	E	Tara nakladu v kg	0-1	xs:decimal
	Cargo	E	Viz 7.4.6	0-n	eol:Cargo
	Device	E	Viz 7.4.7	0-n	eol:Device
	AccessoriesWithoutIdNumber	E	Viz 7.4.8	0-n	eol: AccessoriesWithoutIdNumber
	CargoLoadNumber	A	Počet naložených kusů nákladu	0-1	eol:NumberText
	RFIDIdentification	A	Pokud je nosič nákladu vybaven čipem RFID, musí zde být toto ID uvedeno	0-1	eol:ShortText

Tabulka 10: Nosič nákladu

7.4.7 Zařízení (Device)

Položka zařízení obsahuje všechny relevantní údaje o konkrétním dodávaném zařízení. Doporučuje se zadávat údaje, tak, jak jsou uvedeny na originálních dokumentech od vydávajících orgánů (např. bez dalších úvodních nul nebo mezer navíc).

Položka zařízení mohou být uvedeny buď přímo ve struktuře DeliveryItem, nebo zařazené ve stromu elementů Cargo (viz 7.4.6).

Tabulka 12 Zařízení (Device)

Jméno	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
Device	RFIDIdentification	E	Pokud jsou zařízení vybavena čipem RFID, musí zde být uvedeno příslušné ID	0-1	eol:NumberText
	SecurityModuleNumber	E	ICCID bezpečnostního modulu v SMGW	0-1	eol:NumberText

	SerialNumber	E	Výrobní číslo zařízení	0-8	eol:NumberText
	LogicalDeviceName	E	LDN systému	0-1	eol:LogicalDeviceName
	SystemTitle	E	Název systému – viz odstavec 5.2	1	eol:SystemTitle
	ProductionBatch	E	Označení výrobní šarže zařízení	0-1	eol:NumberText
	ProductionDate	E	Datum výroby zařízení	0-1	xs:date
	BrandNumber	E	Číslo značky (MID)	0-1	eol:NumberText
	BrandNumberMessEV	E	Číslo značky podle MessEV	0-1	eol:NumberText
	CalibrationMarkNumber	E	Číslo kalibrační značky pro rekalibrace a servis	0-1	eol:NumberText
	OperatingVoltage	E	Základní provozní napětí	0-1	eol:NumberText
	OperatingCurrent	E	Základní provozní proud	0-1	eol:NumberText
	OperatingPressure	E	Max. provozní tlak v bar, relevantní pouze pro plyn.	0-1	xs:decimal
	TestDate	E	Datum testu nebo kalibrace zařízení	0-1	xs:date
	VerifiedUntil	E	Rok, ve kterém vyprší platnost kalibrace zařízení	0-1	xs:gYear
	Display	E	Viz 7.4.10	0-255	eol:Display
	KeyM	E	Inicializační klíč M v otevřeném textovém tvaru k prvotnímu spárování se SGMW (dodá výrobce)	0-1	xs:hexBinary
	PublicKey	E	veřejný klíč	0-1	xs:hexBinary
	AnyKey	E	Další kryptografický materiál (např. DLMS), např. kryptografické klíče. Povoleno pouze bez OMS	0-n	eol:Any
	DeliveryConfigurationFile	E	Viz 7.4.12	0-1	eol:DeliveryConfigurationFile
	DeliveryConditionSMGW	E	Stav dodání SGMW. Viz tabulka 4	0-1	eol:DeliveryCondition
	InitialConfigurationPIN	E	Počáteční instalační PIN ke změně nastavení komunikace SMGW pro techniky vybavené rozšířenými právy (počáteční konfigurace).	0-1	eol:PINType

RootCertificateExpiryDate	E	Datum vypršení platnosti kořenového certifikátu (Počáteční konfigurační data)	0-1	xs:date
GWACertificateExpiryDate	E	Datum vypršení platnosti certifikátu HES (Počáteční konfigurační data)	0-1	xs:date
GSCertificateExpiryDate	E	Datum vypršení platnosti certifikátu GS (Počáteční konfigurační data)	0-1	xs:date
SwitchingCommand	E	spínací příkaz, Viz 7.4.17	0-10	eol: SwitchingCommand
HardwareVersion	E	Verze hardwaru zařízení, tak, aby byla dohledatelná výrobcem.	0-1	eol:NumberText
Firmware	E	Viz 7.4.11	0-10	eol:Firmware
ParameterVersion	E	Verze konfigurace zařízení	0-1	eol:NumberText
Interface	E	Viz 7.4.16	0-10	eol:Interface
SIMCardNumber	E	Číslo SIM karty (ICCID)	0-1	eol:ShortText
SIMCardPhoneNumber	E	telefonní číslo SIM karty	0-1	eol:PhoneNumber
SIMCardIPAddressType	E	Typ IP adresy nastavené výrobcem	0-1	eol:IPAddressType
SIMCardIPAdress	E	IP adresa SIM karty	0-1	eol:IPAddress
SIMSize	E	Velikost SIM karty. Je zde soubor hodnot. Viz tabulka 4	0-1	eol:SIMSize
SIMCardPIN	E	PIN pro odemknutí SIM karty	0-1	eol:PINType
SIMCardPUK1	E	PUK1 pro odemknutí SIM karty	0-1	eol:PINType
SIMCardPUK2	E	PUK2 pro odemknutí SIM karty	0-1	eol:PINType
SIMCardDataNumber	E	datové telefonní číslo SIM karty	0-1	eol:PhoneNumber
SIMCardFaxNumber	E	číslo faxu (faxové číslo) SIM karty	0-1	eol:PhoneNumber
SIMCardIMSI	E	IMSI: Mezinárodní identita mobilního účastníka	0-1	eol:IMSIType
SIMCardIMEI	E	IMEI: Mezinárodní identita mobilního zařízení	0-1	eol:IMEIType
SIMCardPinless	E	Označuje, zda se jedná o kartu bez kódu PIN.	0-1	xs:boolean
ServerID	E	ID serveru zařízení	0-1	xs:hexBinary
DevicePIN	E	4 místný PIN pro odemknutí měřiče	0-1	eol:PINType

AccessData	E	Viz 7.4.19	0-6	eol:AccessData
AssemblyCarrier	E	identifikační číslo nadřazeného zařízení ze sestavy zarážení (pokud se jedná o prvek obsahující vnitřní zařízení)	0-1	eol:NumberText
DamageReport	E	Viz 7.4.9	0-n	eol:DamageReport
LoRaWAN	E	Viz 7.4.22	0-1	eol:LoRaWAN
PropertyNumber	A	Identifikátor vlastnictví zařízení, pokud pro zařízení neexistuje 14místný identifikátor nezávislý na výrobci podle normy DIN (např. oprava starého zařízení).	0-1	eol:NumberText
Cross-manufacturerIdentificationNumber	A	Identifikační číslo mezi výrobci	0-1	xs:ID
InAssembly	A	Zařízení se instaluje společně a alespoň jedním dalším zařízením, např. Modem se SIM kartou	0-1	xs:boolean

7.4.8 Příslušenství (AccessoriesWithoutIdNumber)

Tento prvek elektronického dodacího listu popisuje zboží/položky, které nemají sériová čísla. Lze uvést i zboží, které je dodatečně dodáváno, ale není objednáno samostatně (např. příslušenství, návody atd.).

Týká se pouze příslušenství bez identifikačního čísla, jinak musí být uvedeno jako Zařízení (Device).

Tabulka 13 Příslušenství (AccessoriesWithoutIdNumber)

Jméno	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
AccessoriesWithoutIdNumber	ManufacturerNumber	E	Číslo výrobku (poskytne jej výrobce nebo dodavatel)	0-1	eol:ShortText
	ManufacturerTypeDesignation	E	Název produktu výrobce	1	eol:ShortText
	ArticleTypeID	E	Výrobní číslo příslušenství	0-1	eol:ShortText
	IsInAssembly	E	Příslušenství se instaluje	0-1	xs:boolean
	BelongsToParentArticle	E	Příslušenství je součástí dodávky a musí být instalováno do zařízení vyšší úrovně	0-1	eol:NumberText

7.4.9 Hlášení o poškození (DamageReport)

Tento prvek popisuje protokol o škodě v elektronickém dodacím listu, ke kterému dojde při příchozí kontrole zboží a/nebo při přejímce zboží.

V případě reklamace nebo zpětného doručení zde může být důvod patřičně doložen.

Tabulka 14 Hlášení o poškození (DamageReport)

Jméno	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
DamageReport	ItemDefect	E	Způsob poškození. Viz tabulka 4	1	eol:ItemDefect
	DefectDescription	E	Popis chyby/poškození	1-10	eol:LongText

7.4.10 Displej (Display)

Tento prvek se vkládá pro každý kód OBIS zařízení. V případě elektronických měřičů (včetně měřičů RLM) se nepřenášejí žádné předchozí hodnoty a profily zatížení.

Pokud jsou z výrobních zařízení k dispozici další číslice, měly by být zkráceny a nikoli zaokrouhleny. Pokud má měřidlo několik možností zobrazení (např. displej, elektrické rozhraní), musí být zvoleno zobrazení viditelné pro objednavatele.

Tabulka 15 Displej (Display)

Jméno	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
Display	DisplayType	E	Je zde soubor hodnot. Viz tabulka 4	0-1	eol:DisplayType
	DisplayArity	E	Libovolné počítadlo zobrazené podle kódu OBIS na zařízení	0-1	eol:Arity
	DisplayReadingValue	E	Hodnota odečtu měřiče. Relevantní je údaj měřiče viditelný pro spotřebitele.	0-1	xs:decimal
	DisplayMeasuringUnit	E	Jednotka čtení počítadla	0-1	eol:MeasuringUnit
	OBISCodeForDisplay	A	OBIS kód příslušného registru	1	eol:OBIS

7.4.11 Firmware

Tato položka je k dispozici pro každý firmware přítomný v zařízení.

Tabulka 16 Firmware

Jméno	Prvek [E] a atribut [A]	Popis	Počet	XML datový typ

Firmware	FirmwareVersion	E	Verze firmwaru zařízení	1	eol:NumberText
	FirmwareType	E	Je zde soubor hodnot. Viz tabulka 4	1	eol:FirmwareType

Tabulka 17 Doporučení typu firmwaru

typ firmwaru	Doporučení k použití
Metrological_FW	Musí být použit pro firmware, pokud obsahuje metrologickou část.
Application_FW	Je hlavním firmwarem zařízení, pokud zařízení neobsahuje Metrological_FW.
Operating_System_FW	Používá se pro firmware, pokud tento firmware plní hlavně funkci, která pokud možno odpovídá operačnímu systému, např. Linux.
Display_FW	Používá se pro firmware, pokud tento firmware ovlivňuje hlavně displej zařízení.
GSM_Module_FW	Používá se pro firmware, pokud tento firmware ovlivňuje především komunikační modul zařízení.
Security_module_FW	Používá se pro firmware, pokud tento firmware ovlivňuje hlavně bezpečnostní modul zařízení.
Other_FW[1-5].	Použití "Other_FW" musí být koordinováno s příjemcem eOL.

7.4.12 Konfigurační soubor dodávky (DeliveryConfigurationFile)

Máme dvě varianty konfiguračního souboru dodávky, ten může obsahovat pouze jeden z následujících prvků:

- DeliveryConfigurationFile obsahuje prvek DeliveryConfigurationEncrypted, který je datového typu XML xenc:EncryptedDataType, a obsahuje DeliveryConfiguration zašifrovaný pomocí specifikace xenc. Blíže viz kapitola 7.4.13), nebo
- DeliveryConfigurationFile obsahuje prvek DeliveryConfiguration, který je datového typu XML eol: DeliveryConfiguration, který obsahuje data v otevřené podobě, některé elementy samostatně nicméně mohou být šifrovány (viz dále).

Tabulka 18 DeliveryConfigurationFile

Jméno	Prvek [E] a atribut [A]			Popis	Počet	XML datový typ
DeliveryConfigFile	Jeden z	DeliveryConfigurationEncrypted	E	Prvek DeliveryConfiguration zašifrovaný podle specifikace xenc	1	xenc:EncryptedDataType
		DeliveryConfiguration	E	Prvek DeliveryConfigurationData v nešifrované formě	1	eol:DeliveryConfiguration
		Id	A	Identifikační číslo	0-1	xs:ID

7.4.13 Konfigurace dodávky (DeliveryConfiguration)

Tento prvek inicializační konfigurační data, případně elektronický podpis těchto dat ve formátu XAdES.

Tabulka 19 Konfigurace dodávky

Jméno	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
DeliveryConfiguration	DeliveryConfigurationData	E	Struktura DeliveryConfigurationData	1	eol:DeliveryConfigurationData
	DeliveryConfigurationSignature	E	elektronický podpis struktury DeliveryConfigurationData	0-1	ds:SignatureType

7.4.14 Data konfigurace dodávky (DeliveryConfigurationData)

Tento prvek obsahuje „vnitřek“ položky CipherData Konfiguračního souboru dodávky. Obsahuje volitelnou položku Signature – viz odstavec 7.4.24.

Tabulka 20 Data konfigurace dodávky (DeliveryConfigurationData)

Jméno	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
DeliveryConfigurationData	RootCertificateExpiryDate	E	Datum vypršení platnosti kořenového certifikátu	0-1	xs:dateTime
	GSTLSCertificate	E	TLS certifikát zařízení	0-1	eol:Certificate
	GSSigCertificate	E	podpisový certifikát zařízení	0-1	eol:Certificate
	GSEncCertificate	E	šifrovací certifikát SMG zařízení	0-1	eol:Certificate
	GWAAuthCertificate	E	Autentizační certifikát HES	0-1	eol:Certificate
	GWAName	E	Předmět (Common Name) autentizačního certifikátu HES. Může být nakonfigurován jako organizační jednotka (OU) v žádosti o certifikát (CSR) pro certifikáty měřidel.	0-1	eol:ShortText
	AccessRole	E	Před-personalizované symetrické klíče	0-n	eol:AccessRole

	Id	A	Identifikační číslo	0-1	xs:ID
	Interface	E	Viz 7.4.16	0-10	eol:Interface

7.4.15 Inicializační konfigurační soubor (InitialConfigurationFile)

Máme dvě varianty inicializačního konfiguračního souboru, ten může obsahovat pouze jeden z následujících prvků:

- InitialConfigurationFile obsahuje prvek InitialConfigurationEncrypted, který je datového typu XML xenc:EncryptedDataType, a obsahuje IntialConfiguration zašifrovaný pomocí specifikace xenc. Blíže viz kapitola 7.4.16), nebo
- InitialConfigurationFile obsahuje prvek InitialConfiguration, který je datového typu XML eol:InitialConfiguration, který obsahuje data v otevřené podobě

Tabulka InitialConfigurationFile

Jméno	Prvek [E] a atribut [A]			Popis	Počet	XML datový typ
InitialConfigurationFile	Jeden z	InitialConfigurationEncrypted	E	Zašifrovaná InitialConfiguration	1	xenc:EncryptedDataType
		InitialConfiguration	E	InitalConfiguration v otevřené podobě	1	eol:InitialConfiguration
		Id	A	Identifikátor varianty Inicializačního konfiguračního souboru, který lze jednoznačně přiřadit k příslušné variantě konfigurace DSU.	0-1	xs:ID

7.4.16 Inicializační konfigurace (InitialConfiguration)

Tento prvek inicializační konfigurační data, případně elektronický podpis těchto dat ve formátu XAdES.

Tabulka 21 Inicializační konfigurace

Jméno	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
InitialConfiguration	InitialConfigurationData	E	Struktura InitialConfigurationData	1	eol:InitialConfigurationData
	InitialConfigurationSignature	E	elektronický podpis struktury InitialConfigurationData	0-1	ds:SignatureType

7.4.17 Data (vnitřek) inicializačního konfiguračního souboru (InitialConfigurationData)

Inicializační konfigurační data popisují parametry, které jsou nezbytné k tomu, aby bylo možné měřidlo před-personalizovat pro komunikaci s konkrétním HES. Objednatel si musí nejprve vyžádat aktuální

informace/data (počáteční konfigurační data) od Správce měřidel. Tato zašifrovaná data se používají pouze při objednávce zařízení komunikujícího s HES. Nevztahuje se to na jiné produkty, a proto tato položka není pro ostatní produkty vyžadována.

Tabulka 22 Počáteční data konfigurace SMGW

Jméno	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
InitialConfigurationData	SubCACertificate	E	Sub-CA certifikát	1-2	eol:Certificate
	RootCertificateExpiryDate	E	Datum vypršení platnosti kořenového certifikátu	0-1	xs:dateTime
	GWATLSCertificate	E	TLS certifikát DSU	0-1	eol:Certificate
	GWASigCertificate	E	Podpisový certifikát DSU	0-1	eol:Certificate
	GWAEncCertificate	E	Šifrovací certifikát DSU	0-1	eol:Certificate
	GWAAuthCertificate	E	Autentizační certifikát DSU	0-1	eol:Certificate
	GWACertificateExpiryDate	E	Datum vypršení platnosti DSU certifikátů	0-1	xs:date
	GWAName	E	Obecný název DSU (CN). Může být nakonfigurován jako organizační jednotka (OU) v žádosti o podpis certifikace (CSR) pro aktivní certifikáty.	0-1	eol:ShortText
	Id	A	Identifikátor varianty Inicializačního konfiguračního souboru, který lze jednoznačně přiřadit k příslušné variantě konfigurace DSU.	1	xs:ID
	Certs	A	V případě bezpečnostních sad 1 a 2 se zde specifikuje, jaké certifikáty mají být měřidlu před-personalizovány. Mohou být: TLS, ENC nebo SIGN. V případě více certifikátů se oddělí požadavky pomlčkou. Např. ENC-SIGN.	0-1	eol:ShortText
	SecuritySuite	A	Bezpečnostní sada, která specifikuje použitou křivku při tvorbě certifikátů (viz Certs)	0-1	eol:NumberText
	AccessRole	E	Požadavek na před-personalizaci symetrickými klíči	0-n	eol:AccessRole
	QoSMaxLoopCount	E	Parametry QoS dle standardu DIN 43863-8: max_loop_count: Maximální počet opakování	0-1	xs:unsignedByte
	QoSLogLoopFailures	E	Parametry QoS dle standardu DIN 43863-8: log_loop_failures: Pokud je „Pravda“, provede se záznam v Deníku při zahájení druhého nebo dalšího kola.	0-1	xs:boolean

	QoSLoopTimes	E	Parametry QoS dle standardu DIN 43863-8: loop_times: Každá položka seznamu vkládá jednu Zaokrouhlená čekací doba v sekundách. První položka seznamu nastaví první čekací doba opravena. Pokud existuje druhý záznam seznamu, druhý záznam seznamu určuje dobu čekání druhého kola. Podle toho je třeba použít další položky seznamu. Viz 7.4.21	0-1	eol:UintArray
	QoSMaxRetryCount	E	Parametry QoS dle standardu DIN 43863-8: max_retry_count Maximální počet opakování (pokusy) v rámci kola.	0-1	xs:unsignedByte
	QoSLog	E	Parametry QoS dle standardu DIN 43863-8: log_retry_failures Je-li „true“, provede se záznam v deníku, když je restartováno druhé nebo jedno další opakování.	0-1	xs:boolean
	QoSRetryTimes	E	Parametry QoS dle standardu DIN 43863-8: opakování_krát Každá položka seznamu vkládá jednu Opakujte dobu čekání v sekundách. První položka seznamu definuje první čekací dobu. Pokud existuje druhý záznam seznamu, druhý záznam seznamu určuje druhou latenci opakování. Podle toho je třeba použít další položky seznamu. Viz 7.4.21	0-1	eol:UintArray
	Interface	E	Viz 7.4.16	0-n	eol:InterfaceType

7.4.18 Rozhraní (Interface)

Tento prvek popisuje rozhraní v elektronickém dodacím listu. Pokud existuje několik rozhraní, tento prvek se vyskytuje několikrát.

Pro snazší přiřazení rozhraní k v budoucnu používané technologii bude v popisu rozhraní uveden atribut „technologie“.

Prvek rozhraní lze použít jak v objednávce, tak v dodávce. Prvky, které v popisu obsahují poznámku „Dodávka pouze“, lze použít pouze jako součást dodacího listu.

Tabulka 23 Rozhraní (Interface)

Jméno	Prvek [E] a atribut [A]	Popis	Počet	XML datový typ

Interace Schnittstelle	Certificate	E	Certifikáty serveru, např. Pečeť osvědčení o schválení	0-10	eol:Certificate
	Hostname	E	Používá se, když je IP adresa získána přes DNS.	0-1	eol:ShortText
	IPAddress	E	pevná adresa rozhraní	0-1	eol:IPAddress
	Netmask	E	maska podsítě	0-1	eol:IPAddress
	DefaultGateway	E	Pevná IP adresa výchozí brány	0-1	eol:IPAddress
	DNSServer	E	Pevná IP adresa DNS serveru	0-10	eol:IPAddress
	Port	E	číslo portu	0-1	eol:Port
	MACAddress	E	MAC adresa	0-1	eol:MACType
	IMEI	E	IMEI: Mezinárodní identita mobilního zařízení	0-1	eol:IMEIType
	IPTGatename	E	přihlašovací jméno	0-1	eol:NumberText
	IPTPassword	E	přihlašovací heslo	0-1	eol:Password
	IPTNumber	E	Pořadové číslo IPT mastera	0-1	eol:ShortText
	SIMCardAuthNet	E	autentizační protokol	0-1	eol:Authentication
	APNName	E	Název použitého přístupového bodu	0-1	eol:ShortText
	APNUser	E	Jméno uživatele, který se používá	0-1	eol:ShortText
	APNPassword	E	Heslo, které se používá	0-1	eol:Password

	SIMCardPinless	E	Označuje, zda se jedná o kartu bez kódu PIN.	0-1	xs:boolean
	SIMCardSupported	E	Označuje, že do zařízení by měly být vloženy SIM karty.	0-1	xs:boolean
	SIMProvider	E	Přidělení SIM karty poskytovatelem	0-1	eol:ProviderName
	SIMCustomerNumber	E	Zákaznické číslo zákazníka s přiděleným poskytovatelem	0-1	eol:NumberText
	SIMCustomerAccount	E	Číslo zákaznického účtu zákazníka u přiděleného poskytovatele	0-1	eol:NumberText
	CDMA_PPP_Dom	E	PPP doména v síti CDMA	0-1	eol:NumberText
	CDMA_PPP_AuthType	E	Typ autentizace pro připojení PPP	0-1	eol:NumberText
	CDMA_EVDO_Domain_Operator	E	Provozovatel domény EVDO	0-1	eol:NumberText
	CDMA_PPP_Domain_Operator	E	Provozovatel PPP domény	0-1	eol:NumberText
	CDMA_ EVDO-HW-ID-Type	E	Typ identifikace pro hardwarové adresování	0-1	eol:ShortText
	CDMA_PPP-User	E	Uživatelské jméno pro připojení PPP	0-1	eol:ShortText
	CDMA_PPP-PW	E	Heslo pro připojení PPP	0-1	eol:Password
	CDMA_MEID	E	Dodávka pouze HW. Identifikátor Rádiového modulu CDMA bez kontrolního součtu	0-1	eol:NumberText

	CDMA_ESN	E	Dodávka pouze.HW. Identifikátor radiového modulu CDMA	0-1	eol:NumberText
	CDMA_HDR NAI	E	Uživatelské jméno pro připojení EVDO	0-1	eol:ShortText
	CDMA_HDR_PW	E	Heslo pro připojení EVDO	0-1	eol:Password
	CDMA_IMSI	E	Dodávka pouze HW. IMSI rádiového modulu CDMA	0-1	eol:IMSIType
	InterfaceType	A	Typ rozhraní. Viz tabulka 4	1	eol:InterfaceType
	IPAddressType	A	Typ IP adresy. Viz tabulka 4	0-1	eol:IPAddressType
	Technology	A	Technologie sítě. Viz tabulka 4	0-1	eol:Technology
	Id	A	Generováno tvůrcem eOL. (Již se nepoužívá, ale je zachováno pro zpětnou kompatibilitu)	0-1	xs:ID

Tabulka 24 Doporučení pro typ rozhraní

typ rozhraní	Doporučení k použití
WAN	Lze jej použít k dokumentaci interních rozhraní WAN zařízení.
WANA	Lze použít po zvláštní dohodě mezi objednatelem a výrobcem.
WAN1	Popisuje uživatelsky přístupné externí rozhraní WAN zařízení. Pokud má zařízení rozhraní WAN, musí být rozhraní popsáno s tímto typem rozhraní. Pokud je k dispozici druhé externí rozhraní WAN, je popsáno také rozhraní s rozhraním typu WAN2.
WAN2	Pokud jsou na zařízení dvě externí rozhraní WAN, jsou tato dvě rozhraní popsána s rozhraním typu WAN1 a WAN2.
CLS	Popisuje rozhraní CLS zařízení, pokud zařízení CLS provozuje obě rozhraní přemostěná.
CLS1; CLS2	Pokud jsou dvě rozhraní CLS konfigurována samostatně, musí být použity typy rozhraní "CLS1" a "CLS2".
SMGWHKS3	Definuje ve scénáři komunikace HAN 3, jak může zařízení CLS dosáhnout SMGW.

EMTNTP	Definováno ve scénáři komunikace HAN 3, jako je systém řízení CLS je dosažitelný. Pro časovou synchronizaci CLS se používá rozhraní typu EMTNTP
EMTDATA	Definuje ve scénáři komunikace HAN 3, jak lze dosáhnout systému řízení CLS. Pro datové připojení CLS se používá rozhraní typu EMTDATA přístroj

7.4.19 Spínací příkaz (SwitchingCommand)

Tabulka 25 7. Spínací příkaz (SwitchingCommand)

Jméno	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
SwitchingCommand	Command	E		1	eol:NumberText
	SwitchingOutput	E	Viz 7.4.18	0-1	eol:SwitchingOutput

Tabulka 23: Spínací příkaz

7.4.20 Spínací výstup (SwitchingOutput)

Tabulka 26 Spínací výstup (SwitchingOutput)

Jméno	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
SwitchingOutput	ElectricCurrent	E	Jmenovitý proud v [A]	0-1	xs:positiveInteger
	Voltage	E	Jmenovité napětí ve [V]	0-1	xs:positiveInteger
	SwitchingCapacity	E	Jmenovitý výkon v [VA]	0-1	xs:positiveInteger
	SwitchingOutputType	A	Je zde soubor hodnot. Viz tabulka 4	0-1	eol:OutputSwitchingType

7.4.21 Přístup (AccessData)

Tento prvek obsahuje informace, které umožňují přístup k zařízení, např. Hesla, uživatelská jména.

Tabulka 27 Přístupová data

Jméno	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
AccessData	User	E	Uživatelské jméno	1	eol:NumberText
	Password	E	Heslo	1	eol:Password
	AccessRole	A	Přístupová role. Viz tabulka 4	1	eol:AccessRoleList

7.4.22 Kontaktní osoba (ContactPerson)

Tento prvek obsahuje informace o kontaktní osobě.

Tabulka 28 Kontaktní osoba (ContactPerson)

Jméno	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
ContactPerson *Ansprechpartner*	Title	E		0-1	eol:ShortText
	LastName	E		1	eol:ShortText
	FirstName	E		1	eol:ShortText
	Phone	E		0-10	eol:PhoneNumber
	EMailAddress	E		0-1	eol:EMailAddress
	ContactType	A	Typ kontaktu. Viz tabulka 4	1	eol:ContactType

7.4.23 UintArray

Tento prvek umožňuje zadat pole hodnot

Tabulka 29 UintArray

Jméno	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
UintArray	Value	E	Tento prvek umožňuje zadat pole hodnot.	0-n	xs:unsignedInt
	ID	AX	Aby bylo možné řazení, má každý prvek hodnoty svůj vlastní Atribut s názvem "id"	1	xs:unsignedInt

Příklad:

```
<QoSRetryTimes>
<Value id=1>1</Value>
<Value id=2>10</Value>
<Value id=3>100</Value>
</QoSRetryTimes>
```

7.4.24 LoRaWAN®

Tento prvek obsahuje informace o LoRaWAN®.

Tabulka 30 LoRaWAN®

Jméno	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
LoRaWAN	SpecificationVersion	A	číslo verze Specifikace LoRaWAN Např. 1.1 nebo 1.1.1	1	eol:NumberText
	ActivationType	E	Je zde soubor hodnot. Viz tabulka 4.	0-1	eol:ActivationType

	DeviceClass	E	Typ aktivace. Viz tabulka 4.	0-1	eol:DeviceClass
	JoinEUI	E	Globální ID aplikace v adresním prostoru IEEE EUI64, které jednoznačně identifikuje připojovací server	1	xs:hexBinary
	AppKey	E	Kořenový klíč AES-128 přiřazený během výroby.	0-1	xs:hexBinary
	NwkKey	E	Kořenový klíč AES-128 přiřazený během výroby.	0-1	xs:hexBinary
	AppSKey	E	ApplicationSessionKey	0-1	xs:hexBinary
	NwkSKey	E	NetworkSessionKey	0-1	xs:hexBinary
	DevAddr	E	Adresa zařízení v síti	0-1	xs:hexBinary

7.4.25 IP adresa (IPAddress)

Tento prvek obsahuje informace o IP adrese. Může být v jednom z následujících formátů:

- IPAddress obsahuje element IPv4Address, který je ve formátu eol:IPv4Address a obsahuje IPv4 adresu, nebo
- IPAddress obsahuje element IPv6Address, který je ve formátu eol:IPv6Address a obsahuje IPv6 adresu, nebo
- IPAddress obsahuje element URIAddress, který je ve formátu xs:anyURI a obsahuje jinou URI adresu

Tabulka 31 IP adresa

Jméno	Prvek [E] a atribut [A]			Popis	Počet	XML datový typ
IPAddress	Jeden z	IPv4Address	E		1	eol:IPv4Address
		IPv6Address	E		1	eol:IPv6Address
		URIAddress	E		1	xs:anyURI

7.4.26 Přístupová role (AccessRole)

Tento prvek obsahuje informace týkající se konkrétní role v rámci zařízení, včetně symetrických klíčů a certifikátů svázaných s touto rolí.

Tabulka 32 Přístupová data

Jméno	Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
AccessData	Name	A		0-1	eol:AccessRoleList

	SAPAddress	E		1	xs:unsignedShort
	ApplicationContext	E		0-1	xs:unsignedShort
	UserAuthentication	E		0-1	xs:unsignedShort
	LLSPassword	E		0-1	xenc:EncryptedDataType
	SecuritySuite	E		0-1	xs:byte
	ClientSystemTitle	E		0-1	xs:string
	UseDedicatedKey	E		0-1	xs:boolean
	AuthenticatedRequest	E		0-1	xs:boolean
	EncryptedRequest	E		0-1	xs:boolean
	AuthenticatedResponse	E		0-1	xs:boolean
	EncryptedResponse	E		0-1	xs:boolean
	PrivateSigningKey	E		0-1	xenc:EncryptedDataType
	MeterSigningCertificate	E		0-1	xenc:EncryptedDataType
	SymmetricKey	E		0-n	eol:SymmetricKey
	Certificate	E	Další certifikáty	0-n	eol:Certificate

7.4.27 Symetrický klíč (SymmetricKey)

V případě, že měřidlo podporuje výhradně Bezpečnostní sadu 0, pak výrobce musí předpersonalizovat měřidla symetrickými klíči. Jedná se zpravidla o klíče: KEK, GUEK, GAK a případně GBEK (blíže viz odstavec 5.5 Typy symetrických klíčů.

Na místě symetrických klíčů mohou být přenášena i hesla a PINy, budou typu: Password a PIN.

Každá přístupová role má vlastní sady symetrických klíčů.

Symetrické klíče mohou mít následující vlastnosti:

- Typ klíče <KeyType>
- Algoritmus <KeyAlgorithm>
- Hodnota klíče <KeyValue> nebo <KeyValuePlaintext>
- Kontrolní hodnotu klíče (KCV) <KeyKCV>
- Případné parametry klíče <KeyParameters>

Pozor!: Struktura umožňuje zadat pomocí elementu KeyValuePlaintext hodnotu klíče nešifrovaně (nebo šifrovaně externím způsobem mimo xenc). Použití této struktury nemusí být bezpečné! Je důrazně doporučeno používat strukturu KeyValue, která obsahuje hodnotu klíče šifrovanou.

Jméno		Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
SymmetricKey		KeyType	E	Typ symetrického klíče	1	eol:KeyType
		KeyAlgorithm	E	Název algoritmu, např.: AES128, AES192 a AES256	0-1	eol:ShortText
	Jeden z	KeyValuePlaintext	E	Nešifrovaná hodnota klíče (nebo šifrovaná externě)	0-1	xs:string
		KeyValue	E	Šifrovaná hodnota klíče v textovém tvaru	0-1	xenc:EncryptedDataType
		KeyKCV	E	KCV klíče	0-1	eol:ShortText
		KeyParameters	E	Případné parametry klíče	0-1	eol:Any

V případě Inicializačního konfiguračního souboru se neuvedou KeyValue a KeyParametrs, protože symetrické klíče generuje výrobce. Výrobci se tak sděluje, jakými klíči má měřidlo před-formátovat.

V případě, že data konfigurace dodávky nejsou šifrována jako celek, pak SymmetricKey musí být šifrovány samostatně. A to minimálně položky keyValue a KeyParameters.

7.4.28 Certifikát (Certificate)

Tento prvek obsahuje X509 certifikát, nepovinně pak vybrané informace o daném certifikátu a zašifrovaný soukromý klíč patřící k certifikátu (typu xenc:EncryptedDataType).

Pozor!: Struktura umožňuje zadat pomocí elementu PrivateKeyPlaintext hodnotu privátního klíče nešifrovaně (nebo šifrovaně externím způsobem mimo xenc). Použití této struktury nemusí být bezpečné! Je důrazně doporučeno používat strukturu PrivateKey, která obsahuje hodnotu klíče šifrovanou.

Tabulka 33 Přístupová data

Jméno		Prvek [E] a atribut [A]		Popis	Počet	XML datový typ
Certificate		CertificateEntity	E		0-1	eol:CertificateEntity
		CertificateType	E		0-1	eol:CertificateType
		SerialNumber	E		0-1	eol:ShortText
		Issuer	E		0-1	eol:ShortText

		Subject	E		0-1	eol:ShortText
		SubjectAltName	E		0-1	eol:ShortText
		Certificate	E		1	ds:X509DataType
	Jeden z	PrivateKeyPlaintext	E	Nešifrovaná hodnota privátního klíče (nebo šifrovaná externě)	0-1	xs:string
		PrivateKey	E		0-1	xenc:EncryptedDataType
		KeyKCV	E		0-1	eol:ShortText

7.4.29 Podpis (Signature)

Specifikace elektronického podpisu je mimo rozsah tohoto dokumentu (je uvedena v [13]).

Níže je uveden příklad kvalifikovaného elektronického podpisu formátu XAdES-Baseline-B vytvořený aplikací DSS Demonstration WebApp. Byl využit algoritmus RSA z důvodu, že nebyl k dispozici kvalifikovaný certifikát ECDSA. Delší hodnoty jsou zkráceny.

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="id-263fad5a62a0580a1c44a0de0d22fc40">
    <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
        <ds:Reference Id="r-id-263fad5a62a0580a1c44a0de0d22fc40-1" URI="">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                    <dsig-filter2:XPath xmlns:dsig-filter2=http://www.w3.org/2002/06/xmldsig-filter2
                                Filter="subtract">/descendant::ds:Signature</dsig-filter2:XPath>
                </ds:Transform>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
            <ds:DigestValue>d+cymznDmac5g+p8vFvUnG/yQravA0J11PdSsh0x7x0=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#xades-id-263fad5a62a0580a1c44a0de0d22fc40">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
            <ds:DigestValue>kogrbql6un7cpvHksXkWMTvRByJGW/Cwk4DCyT4QfvY=</ds:DigestValue>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue Id="value-id-263fad5a62a0580a1c44a0de0d22fc40">gNDRFFTrabLeoYiKw…</ds:SignatureValue>
    <ds:KeyInfo>
        <ds:X509Data>
            <ds:X509Certificate>MIIIoTCCBomgAw…ds:X509Certificate>
        </ds:X509Data>
    </ds:KeyInfo>
    <ds:Object>
        <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" Target="#id-263fad5a62a0580a1c44a0de0d22fc40">
            <xades:SignedProperties Id="xades-id-263fad5a62a0580a1c44a0de0d22fc40">
```

```
            <xades:SignedSignatureProperties>
                <xades:SigningTime>2023-07-08T12:04:43Z</xades:SigningTime>
                <xades:SigningCertificateV2>
                    <xades:Cert>
                        <xades:CertDigest>
                            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
                            <ds:DigestValue>XREsyKj66WMyQapIL6qcxR7FACpDx5…ds:DigestValue>
                        </xades:CertDigest>
                        <xades:IssuerSerialV2>MIGNMIGEpIGBMH8xCzAJBgN…</xades:IssuerSerialV2>
                    </xades:Cert>
                </xades:SigningCertificateV2>
            </xades:SignedSignatureProperties>
            <xades:SignedDataObjectProperties>
                <xades:DataObjectFormat ObjectReference="#r-id-263fad5a62a0580a1c44a0de0d22fc40-1">
                    <xades:MimeType>text/plain</xades:MimeType>
                </xades:DataObjectFormat>
            </xades:SignedDataObjectProperties>
        </xades:SignedProperties>
    </xades:QualifyingProperties>
</ds:Object>
</ds:Signature>
```

7.4.30 EncryptedKey

Specifikace šifrování je mimo rozsah tohoto dokumentu (je uvedena v [15]). Cílem je připravit symetrický klíč, kterým budou šifrovány vybrané prvky XML struktury eOL.

Níže je uveden jednoduchý příklad využívající zabezpečení symetrického klíče algoritmem RSA. Příklad využití algoritmu ECDH je možné nalézt v [15].

```
<xenc:EncryptedKey Id="SymetricKey" Type="http://www.w3.org/2001/04/xmlenc# EncryptedKey">
    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#aes256-gcm" />
    <ds:KeyInfo>
        <xenc:EncryptedKey>
            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5">
            </xenc:EncryptionMethod>
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate>MIIDJzC...8mYfX8/jw==</ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
            <xenc:CipherData>
                <xenc:CipherValue>bSYaL0cXyC...UjDBQ==</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedKey>
    </ds:KeyInfo>
</xenc:EncryptedKey>
```

Id symetrického klíče je v uvedeném případě "SymetricKey". Pomocí tohoto Id se pak budou na tento klíč odkazovat jednotlivé šifrované části XML souboru. Např.:

```
…
      <xenc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Content">
          <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
          <ds:KeyInfo>
              <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey" URI="#SymetricKey"/>
          </ds:KeyInfo>
          <xenc:CipherData>
              <xenc:CipherValue>A2gFdsVB3n…</xenc:CipherValue>
          </xenc:CipherData>
      </xenc:EncryptedData>
…
```

7.5 Ilustrační příklad XML souboru

Následující příklad je ilustrační. Dleší hodnoty a opakující se položky byly zkráceny. Podbarvení zvýrazňuje šifrování a podepisování

```
<eOL xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" eOLVersionNumber="1.0"
xmlns="http://localhost/EOL10">
    <eOLVersion>1.0</eOLVersion>
    <xenc:EncryptedKey Id="SymetricKey" Type="http://www.w3.org/2001/04/xmlenc# EncryptedKey">
        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#aes256-gcm" />
        <ds:KeyInfo>
            <xenc:EncryptedKey>
                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"></xenc:EncryptionMethod>
                <ds:KeyInfo>
                    <ds:X509Data>
                        <ds:X509Certificate>MIIDJzC...8mYfX8/jw==</ds:X509Certificate>
                    </ds:X509Data>
                </ds:KeyInfo>
                <xenc:CipherData>
                    <xenc:CipherValue>bSYaL0cXyC...UjDBQ==</xenc:CipherValue>
                </xenc:CipherData>
            </xenc:EncryptedKey>
        </ds:KeyInfo>
    </xenc:EncryptedKey>
    <OrderHeader OrderDate="2023-03-27" OrderNumber="PF 2023034" ContractNumber="2021_S_188_490147">
        <ContactPerson ContactPersonType="Salesman">
            <Title>Mr.</Title>
            <LastName>Jan</LastName>
            <FirstName>Novak</FirstName>
            <Phone>+420603500600</Phone>
            <eMailAdress>Jan.Novák@test.de</eMailAdress>
        </ContactPerson>
        <SupplierNumber>45303</SupplierNumber>
        <PurchaserNumber>1200965</PurchaserNumber>
        <DeliveryHeader DeliveryDate="2023-03-27" DeliveryNoteNumber="PF 2023034">
            <CargoCount>1</CargoCount>
            <ContactPerson ContactPersonType="Logistic">
                <Title>Ms.</Title>
                <LastName>Božeena</LastName>
```

```
        <FirstName>Nováková</FirstName>
        <Phone>+420700800900</Phone>
        <eMailAdress>bozena.novakova@testik.cz</eMailAdress>
    </ContactPerson>
</DeliveryHeader>
<OrderItem OrderItemnummer="1" ContractItem="01">
    <ProduktIdentifikacion>V1 31180001</ProduktIdentifikacion>
    <ArticleType>4U110017007</ArticleType>
    <ShortText>mME, 3-Punkt-Bauform</ShortText>
    <LongText>mME, 3-Punkt-Bauform, GS303.D-S2-55.22-21</LongText>
    <ManufacturerTypeDesignation>GS303.D-S2-55.22-21</ManufacturerTypeDesignation>
    <FeaturesListOrderer>4U110017007_1-Konfig-1.0-DIGImeto</FeaturesListOrderer>
    <Owner>DIGImeto GmbH Co KG</Owner>
    <OrderAmount>2</OrderAmount>
    <QuantitativeUnit>Stueck</QuantitativeUnit>
    <DeliveryItem DeliveryItemsnummer="1">
        <Manufacturer>ZPA</Manufacturer>
        <Manufacturernummer>V1 31180001</Manufacturernummer>
        <ManufacturerTypeDesignation>GS303.D-S2-55.22-21</ManufacturerTypeDesignation>
        <DeliveryAmount>2</DeliveryAmount>
        <QuantitativeUnit>Stueck</QuantitativeUnit>
        <DeliveryCondition>Neu</DeliveryCondition>
        <ManufacturingNotifiedBody>1383</ManufacturingNotifiedBody>
        <TestTypeCode>MID_konform</TestTypeCode>
        <Class>A</Class>
        <MIDtypeTestCertificate Revision="0">TCM 221/18-5613_REV.03</MIDtypeTestCertificate>
        <MIDtypeCertIssuieDate>2020-02-24</MIDtypeCertIssuieDate>
        <MIDtypeNotifiedBody>1383</MIDtypeNotifiedBody>
        <CountryConformityAssessment Revision="0">EU17600DE</CountryConformityAssessment>
        <CountryNotifiedBody>ZPA Smart Energy a.s.</CountryNotifiedBody>
        <CountryAssessmentDate>2019-04-05</CountryAssessmentDate>
        <InstallationPosition>Vertikal</InstallationPosition>
        <Cargo Cargonummer="ZPA2023-0055">
            <CargoType>Karton</CargoType>
            <Device CrossmanufacturerIdentificationNumber="1ZPA0020184024">
                <SerialNumber>20184025</SerialNumber>
                <SystemTitle>0123456789ABCDEF</SystemTitle>
                <ProductionBatch>2023-3</ProductionBatch>
```

```
        <ProductionDate>2023-03-23</ProductionDate>
        <BrandNumber>CEM231383;DE-M230102</BrandNumber>
        <TestDate>2023-03-24</TestDate>
        <VerifiedUntil>2031</VerifiedUntil>
        <Display OBIScodeForDisplay="1-0:1.8.0">
            <DisplayType>Display</DisplayType>
            <Displayarity>6,0</Displayarity>
            <DisplayStandWert>0</DisplayStandWert>
            <DisplayMeasuringUnit>kWh</DisplayMeasuringUnit>
        </Display>
        <DeliveryConfigFile>
            <SupplyConfigurationData>
                <SymmetricKeys>
                    <AccessRole>ADMIN_access</AccessRole>
                    <KeyType>KEK</KeyType>
                    <KeyAlgorithm>AES256</KeyAlgorithm>
                    <xenc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Content">
                        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
                        <ds:KeyInfo>
                            <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey" URI="#SymetricKey"/>
                        </ds:KeyInfo>
                        <xenc:CipherData>
                            <xenc:CipherValue>A2gFdsVB3n…</xenc:CipherValue>
                        </xenc:CipherData>
                    </xenc:EncryptedData>
                </SymmetricKeys>
            </SupplyConfigurationData>
        </DeliveryConfigFile>
        <HardwareVersion>11</HardwareVersion>
        <Firmware>
            <FirmwareVersion>05r00</FirmwareVersion>
            <FirmwareType>Metrologische_FW</FirmwareType>
        </Firmware>
        <ParameterVersion>00750090</ParameterVersion>
        <ServerID>0A015A5041000133FBD8</ServerID>
        <CounterPIN>5365</CounterPIN>
    </Device>
    <Device CrossmanufacturerIdentificationNumber="1ZPA0020184025">
```

```
<SerialNumber>20184026</SerialNumber>
<SystemTitle>0123456789ABCDE0</SystemTitle>
<ProductionBatch>2023-3</ProductionBatch>
<ProductionDate>2023-03-23</ProductionDate>
<BrandNumber>CEM231383;DE-M230102</BrandNumber>
<TestDate>2023-03-24</TestDate>
<VerifiedUntil>2031</VerifiedUntil>
<Display OBIScodeForDisplay="1-0:1.8.1">
    <DisplayType>Display</DisplayType>
    <Displayarity>6,0</Displayarity>
    <DisplayStandWert>0</DisplayStandWert>
    <DisplayMeasuringUnit>kWh</DisplayMeasuringUnit>
</Display>
<DeliveryConfigFile>
    <SupplyConfigurationData>
        <SymmetricKeys>
            <AccessRole>ADMIN_access</AccessRole>
            <KeyType>KEK</KeyType>
            <KeyAlgorithm>AES256</KeyAlgorithm>
            <xenc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Content">
                <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
                <ds:KeyInfo>
                    <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey" URI="#SymetricKey"/>
                </ds:KeyInfo>
                <xenc:CipherData>
                    <xenc:CipherValue>AXXXYUVB3n…</xenc:CipherValue>
                </xenc:CipherData>
            </xenc:EncryptedData>
        </SymmetricKeys>
    </SupplyConfigurationData>
</DeliveryConfigFile>
<HardwareVersion>11</HardwareVersion>
<Firmware>
    <FirmwareVersion>05r00</FirmwareVersion>
    <FirmwareType>Metrologische_FW</FirmwareType>
</Firmware>
<ParameterVersion>00750090</ParameterVersion>
<ServerID>0A015A5041000133FBD9</ServerID>
```

```
                    <CounterPIN>2793</CounterPIN>
                </Device>
            </Cargo>
        </DeliveryItem>
    </OrderItem>
</OrderHeader>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="id-263fad5a62a0580a1c44a0de0d22fc40">
    <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
        <ds:Reference Id="r-id-263fad5a62a0580a1c44a0de0d22fc40-1" URI="">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
                    <dsig-filter2:XPath xmlns:dsig-filter2=http://www.w3.org/2002/06/xmldsig-filter2 …
                    </dsig-filter2:XPath>
                </ds:Transform>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
            <ds:DigestValue>d+cymznDmac5g+p8vFvUnG/yQravA0J11PdSsh0x7x0=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#xades-id-263fad5a62a0580a1c44a0de0d22fc40">
            <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
            <ds:DigestValue>kogrbql6un7cpvHksXkWMTvRByJGW/Cwk4DCyT4QfvY=</ds:DigestValue>
        </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue Id="value-id-263fad5a62a0580a1c44a0de0d22fc40">gNDRFFTrabLeoYiKw…</ds:SignatureValue>
    <ds:KeyInfo>
        <ds:X509Data>
            <ds:X509Certificate>MIIIoTCCBomgAw…ds:X509Certificate></ds:X509Data>
        </ds:KeyInfo>
        <ds:Object>
            <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" Target="#id-263fad5a62a0580a1c44a0de0d22fc40">
                <xades:SignedProperties Id="xades-id-263fad5a62a0580a1c44a0de0d22fc40">
                    <xades:SignedSignatureProperties>
```

```
                    <xades:SigningTime>2023-07-08T12:04:43Z</xades:SigningTime>
                    <xades:SigningCertificateV2>
                        <xades:Cert>
                            <xades:CertDigest>
                                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
                                <ds:DigestValue>XREsyKj66WMyQapIL6qcxR7FACpDx5…ds:DigestValue></xades:CertDigest>
                                <xades:IssuerSerialV2>MIGNMIGEpIGBMH8xCzAJBgN…</xades:IssuerSerialV2>
                            </xades:Cert>
                        </xades:SigningCertificateV2>
                    </xades:SignedSignatureProperties>
                    <xades:SignedDataObjectProperties>
                        <xades:DataObjectFormat ObjectReference="#r-id-263fad5a62a0580a1c44a0de0d22fc40-1">
                            <xades:MimeType>text/plain</xades:MimeType>
                        </xades:DataObjectFormat>
                    </xades:SignedDataObjectProperties>
                </xades:SignedProperties>
            </xades:QualifyingProperties>
        </ds:Object>
    </ds:Signature>
</eOL>
```

Zkratky

Zkratka	Význam
AES	Advanced Encryption Standard
Atribut	Další informace týkající se prvku XML
CP	Certificate Policy
CR	Change Request
CSR	Certificate Signing Request
DLMS	Device Language Message Specification
DNS	Domain Name System
ECDH	Elliptic Curve Diffie Hellman
ENC	Encryption
HAN	Home Area Network
HES	Head End System
ICC-ID	Integrated Circuit Card Identification Number
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IPT	Internet Protocol Telemetry
ISO-IEC	International Organization for Standardization International Electro technical Commission
KEK	Key Encryption Key
KMS	Key Management System
LDAP	Lightweight Directory Access Protocol
LMN	Local Metrological Network
LoRaWAN®	Long Range Wide Area Network
M-Bus	Meter-Bus
MAC	Media-Access-Control-Addresses
MID	Measuring Instruments Directive
OBIS	Object Identification System
OMS	Open Metering System
OU	Organization Unit
PUK	Personal Unblocking Key
RFID	Radio Frequency Identification
Root-CA	Root Certificate Authority
RSA	RSA Security Inc., (Rivest-Shamir-Adleman)
S/MIME	Secure / Multipurpose Internet Mail Extensions
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SLA	Service-Level-Agreement
SMGW	Smart-Meter-Gateway (BSI TR-03109)
SMPKI	Smart Metering Public Key Infrastructure
SMTP	Simple Mail Transfer Protocol
TLS	Transport Layer Security
WAN	Wide Area Network
XML	Extensible Markup Language
XSD	XML Schema Definition

Příloha A

Tato příloha obsahuje příklady certifikátů DLMS/COSEM

9.1 NIST křivky v OpenSSL pro DLMS/COSEM

Název křivky		**OID**	**Název**
FIPS PUB 186-3	**openssl** ecparam -listcurves		
P-256	prime256v1	1.2.840.10045.3.1.7	X9.62/SECG curve over a 256 bit prime field
P-384	secp384r1	1.3.132.0.34	NIST/SECG curve over a 384 bit prime field

V následujících odstavcích jsou uvedeny příklady certifikátů pro křivku P256. Pro křivku P-384 platí obdobné příkazy s následujícími změnami:

- Příkaz:
  `openenssl ecparam -out ecparam.pem -name prime256v1`
  se nahradí příkazem:
  `openenssl ecparam -out ecparam.pem -name secp384r1`
- Jelikož se v podpisovém schématu dle DLMS/COSEM má použít SHA384, tak příkazy
  `openssl x509 -req …`
  musí být doplněny o přepínač `-sha384` (v případě kořenového certifikátu se to týká příkazu `openssl req -x509 …`)

V následujících odstavcích jsou uvedeny příklady certifikátů a příklady příkazů OpenSSL, kterými byly tyto certifikáty vytvořeny. Každý certifikát byl generován v samostatném adresáři. Pro tyto účely byla vytvořena následující adresářová struktura:

```
-RootCA
-sub-CA
  -měřidlo1
     -digitalSignature
     -keyAgreement
  -datová centrála
     -digitalSignature
     -keyAgreement
  -Objednatel
     -podpis
     -šifrování
  -Správce
     -podpis XadES
     -Šifrování XAdES
  -Výrobce
     -keyAgreement CAdES
     -Podpis CAdES
     -Podpis XAdES
```

Poznámka: Textový editor může pomlčky změnit na jiné typy pomlček, než akceptuje program OpenSSL. V případě kopírování následujících příkazů je třeba na to brát ohled.

9.2 Root CA

9.2.1 Párová data P-256

```
$ openssl ecparam -out ecparam.pem -name prime256v1
$ openssl genpkey -paramfile ecparam.pem -out ecdhkey.pem

Vygenerovaná párová data je možné vypasat příkazem:
$ openssl pkey -in ecdhkey.pem -text -noout
```

9.2.2 Root Certifikát

Samopodepsaný certifikát je možné generovat již jako žádost o certifikát:

```
$ openssl req -x509 -new -key ecdhkey.pem -out root.cer  -config root-256.cnf
-days 3650
```

Obsah souboru root-256.cnf:

```
[ req ]
default_keyfile           = root-key.pem
distinguished_name  = req_distinguished_name
x509_extensions           = v3_ca# The extensions to add to the self signed cert
prompt                   = no


[ req_distinguished_name ]
C  = CZ
O  = SMetrID
CN = SM-Suite1-Test-RootCA

[ v3_ca ]
basicConstraints = CA:TRUE
keyUsage = cRLSign, keyCertSign
subjectKeyIdentifier=hash
```

```
$ openssl x509 -in root.cer -text

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            50:69:01:cf:9d:f5:b8:71:c4:7c:96:b7:28:5e:cc:7f:76:1c:b7:fd
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = CZ, O = SMetrID, CN = SM-Test-RootCA
        Validity
            Not Before: May 13 10:00:08 2023 GMT
            Not After : May 10 10:00:08 2033 GMT
        Subject: C = CZ, O = SMetrID, CN = SM-Test-RootCA
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:0d:f1:b4:b7:86:f3:59:bc:13:69:2f:e3:71:68:
                    c5:62:19:94:29:28:9a:42:f5:0c:fc:ef:af:ca:76:
                    af:9e:35:7a:8d:36:ce:30:22:7a:f6:74:07:f9:6a:
                    f2:7b:71:aa:b2:af:cd:a2:5e:68:06:73:c6:0c:d7:
                    28:06:58:a3:58
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE
```

```
            X509v3 Key Usage:
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                53:DE:20:EA:8D:A6:9A:63:55:3C:31:42:AC:B7:38:0E:EA:79:DC:67
    Signature Algorithm: ecdsa-with-SHA256
    Signature Value:
        30:44:02:20:79:b0:94:b1:95:d9:8d:28:04:7d:d7:fa:b2:d9:
        3e:01:7f:7d:69:ee:0e:89:8e:a6:0b:22:eb:be:3f:7c:b0:75:
        02:20:58:8e:f9:5f:0c:0e:db:b4:8c:1b:d2:b2:d6:ec:16:ca:
        fd:4f:1d:de:e8:bc:98:85:61:45:8a:56:ad:ae:ed:17
-----BEGIN CERTIFICATE-----
MIIBrTCCAVSgAwIBAgIUUGkBz531uHHEfJa3KF7Mf3Yct/0wCgYIKoZIzj0EAwIw
ODELMAkGA1UEBhMCQ1oxEDAOBgNVBAoMB1NNZXRySUQxFzAVBgNVBAMMDlNNLVRl
c3QtUm9vdENBMB4XDTIzMDUxMzEwMDAwOFoXDTMzMDUxMDEwMDAwOFowODELMAkG
A1UEBhMCQ1oxEDAOBgNVBAoMB1NNZXRySUQxFzAVBgNVBAMMDlNNLVRlc3QtUm9v
dENBMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEDfG0t4bzWbwTaS/jcWjFYhmU
KSiaQvUM/O+vynavnjV6jTbOMCJ69nQH+Wrye3Gqsq/Nol5oBnPGDNcoBlijWKM8
MDowDAYDVR0TBAUwAwEB/zALBgNVHQ8EBAMCAQYwHQYDVR0OBBYEFFPeIOqNpppj
VTwxQqy3OA7qedxnMAoGCCqGSM49BAMCA0cAMEQCIHmwlLGV2Y0oBH3X+rLZPgF/
fWnuDomOpgsi674/fLB1AiBYjvlfDA7btIwb0rLW7BbK/U8d3ui8mIVhRYpWra7t
Fw==
-----END CERTIFICATE-----
```

9.3 Sub-CA 256 certifikát

```
$ openssl ecparam -out ecparam.pem -name prime256v1
$ openssl genpkey -paramfile ecparam.pem -out ecdhkey.pem
```

```
$ openssl req -new -config Sub-CA-256.cnf -key ecdhkey.pem -out Sub-CA-256.req
```

Obsah souboru Sub-CA-256.cnf:

```
[ req ]
default_keyfile           = ecdhkey.pem
distinguished_name  = req_distinguished_name
prompt                    = no

[ req_distinguished_name ]
C  = CZ
O  = SMetrID
CN = SM-Suite1-Test-Sub-CA
```

```
$ openssl x509 -req -in Sub-CA-256.req -extfile Ext-file-256.cnf     -extensions v3_usr -CA ..\RootCA\root.cer    -CAkey ..\RootCA\root-key.pem -out Sub-CA-256-certificate.cer -days 1750
```

Obsah souboru Ext-file-256.cnf:

```
[ v3_usr ]
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer
basicConstraints = critical,CA:true,pathlen:0
keyUsage = critical, cRLSign, keyCertSign
certificatePolicies =  1.2.3.4
```

```
openssl x509 -in Sub-CA-256-certificate.cer -text
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            45:e1:57:84:8d:65:55:40:dc:a0:77:f6:2a:5f:70:cd:a1:86:68:7b
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = CZ, O = SMetrID, CN = SM-Test-RootCA
```

```
        Validity
            Not Before: May 15 10:02:30 2023 GMT
            Not After : Feb 28 10:02:30 2028 GMT
        Subject: C = CZ, O = SMetrID, CN = SM-Suite1-Test-Sub-CA
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:b1:32:b7:86:b3:63:ad:b0:ca:c0:5a:d2:7e:dc:
                    fd:04:c2:cc:e7:b1:de:ef:90:86:33:e9:49:49:ff:
                    fe:2a:22:3a:50:91:61:b3:68:9f:0a:f6:e5:fe:11:
                    7b:10:f6:6e:99:ae:ba:fe:29:18:ce:48:c5:8c:95:
                    33:cd:66:97:d7
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                76:1B:F9:1A:75:E7:95:D9:53:DE:6F:0C:69:F2:43:8D:DE:1A:93:7A
            X509v3 Authority Key Identifier:
                53:DE:20:EA:8D:A6:9A:63:55:3C:31:42:AC:B7:38:0E:EA:79:DC:67
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Certificate Policies:
                Policy: 1.2.3.4
    Signature Algorithm: ecdsa-with-SHA256
    Signature Value:
        30:45:02:20:55:39:96:30:ad:ff:f6:91:d4:f0:a7:aa:07:d9:
        c1:50:c8:1b:b7:fd:ef:cb:6f:27:80:78:c9:2d:03:f6:cf:8a:
        02:21:00:c3:c3:ad:5f:01:e7:71:85:01:d5:89:eb:76:b0:6a:
        86:a4:c7:91:6b:02:b2:aa:05:39:37:ee:07:b9:60:0e:ba
-----BEGIN CERTIFICATE-----
MIIB8TCCAZegAwIBAgIUReFXhI1lVUDcoHf2Kl9wzaGGaHswCgYIKoZIzj0EAwIw
ODELMAkGA1UEBhMCQ1oxEDAOBgNVBAoMB1NNZXRySUQxFzAVBgNVBAMMDlNNLVRl
c3QtUm9vdENBMB4XDTIzMDUxNTEwMDIzMFoXDTI4MDIyODEwMDIzMFowPzELMAkG
A1UEBhMCQ1oxEDAOBgNVBAoMB1NNZXRySUQxHjAcBgNVBAMMFVNNLVN1aXRlMS1U
ZXN0LVN1Yi1DQTBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABLEyt4azY62wysBa
0n7c/QTCzOex3u+QhjPpSUn//ioiOlCRYbNonwr25f4RexD2bpmuuv4pGM5IxYyV
M81ml9ejeDB2MB0GA1UdDgQWBBR2G/kadeeV2VPebwxp8kON3hqTejAfBgNVHSME
GDAWgBRT3iDqjaaaY1U8MUKstzgO6nncZzASBgNVHRMBAf8ECDAGAQH/AgEAMA4G
A1UdDwEB/wQEAwIBBjAQBgNVHSAECTAHMAUGAyoDBDAKBggqhkjOPQQDAgNIADBF
AiBVOZYwrf/2kdTwp6oH2cFQyBu3/e/LbyeAeMktA/bPigIhAMPDrV8B53GFAdWJ
63awaoakx5FrArKqBTk37ge5YA66
-----END CERTIFICATE-----
```

9.4 Certifikát měřidla P-256

System Title měřidla: 0123456789ABCDEF

Dle DLMS/COSEM by mělo mít měřidlo ceritá s neomezenou platností (tj. `notAfter= 99991231235959Z`). V následujících příkladech je platnost certifikátů 100 let. Avšak nejvhodnějším řešením je, vydávat certifikáty měřidel s hodnotou `notAfter` shodnou s touž hodnotou certifikátu sub-CA.

9.4.1 KeyAgreement DLMS/COSEM

```
$ openssl ecparam -out ecparam.pem -name prime256v1
$ openssl genpkey -paramfile ecparam.pem -out ecdhkey.pem
```

```
$ openssl req -new -config meridlo1.cnf -key ecdhkey.pem -out meridlo1.req
```

```
$ openssl x509 -req -in meridlo1.req -extfile meridlo1.cnf -extensions
v3_usr -CA ..\..\Sub-CA-256-certificate.cer -CAkey ..\..\ecdhkey.pem -out
meridlo1-256-certificate.cer -days 36524
```

meridlo1.cnf:

```
[ req ]
default_keyfile           = ecdhkey.pem
distinguished_name  = req_distinguished_name
prompt                    = no

[ req_distinguished_name ]
C  = CZ
O  = SMetrID
OU = "Datova centrala 1"
CN = 123456789ABCDEF

[ v3_usr ]
authorityKeyIdentifier=keyid,issuer
keyUsage = keyAgreement
```

```
$ openssl x509 -in meridlo1-256-certificate.cer -text
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            40:93:ea:73:3d:57:89:20:d0:3c:ed:30:b5:3e:81:9e:a0:fa:93:40
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = CZ, O = SMetrID, CN = SM-Suite1-Test-Sub-CA
        Validity
            Not Before: May 15 10:37:33 2023 GMT
            Not After : May 15 10:37:33 2123 GMT
        Subject: C = CZ, O = SMetrID, OU = Datova centrala 1, CN = 123456789ABCDEF
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:8b:d9:4c:c7:eb:06:b0:04:d2:ad:45:80:6d:4c:
                    0f:db:20:c3:5c:82:da:72:8f:9c:f1:f4:78:c9:41:
                    47:b7:a7:1d:06:81:ab:fe:49:05:d9:07:25:4f:23:
                    1c:c0:90:7f:64:e1:8e:c6:51:ce:7a:94:d7:de:e4:
                    1a:a1:22:ea:b2
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                76:1B:F9:1A:75:E7:95:D9:53:DE:6F:0C:69:F2:43:8D:DE:1A:93:7A
            X509v3 Key Usage:
                Key Agreement
            X509v3 Subject Key Identifier:
                D7:DC:37:BC:18:6D:E2:B7:51:F7:37:73:2A:6D:A1:83:80:8F:8D:C1
    Signature Algorithm: ecdsa-with-SHA256
    Signature Value:
        30:45:02:21:00:9e:a4:c4:b7:c8:bc:cd:47:05:84:d9:95:0b:
        09:c5:3f:9f:be:a3:0e:2b:0c:4e:cd:94:e4:09:50:69:18:d9:
        b1:02:20:69:f9:11:62:9a:34:19:56:15:71:92:db:e2:79:ae:
        f6:91:4c:1f:c0:7c:a7:49:75:a9:73:e6:89:2c:4e:35:4e
-----BEGIN CERTIFICATE-----
MIIB5zCCAY2gAwIBAgIUQJPqcz1XiSDQPO0wtT6BnqD6k0AwCgYIKoZIzj0EAwIw
PzELMAkGA1UEBhMCQ1oxEDAOBgNVBAoMB1NNZXRySUQxHjAcBgNVBAMMFVNNLVN1
aXRlMS1UZXN0LVN1Yi1DQTAgFw0yMzA1MTUxMDM3MzNaGA8yMTIzMDUxNTEwMzcz
M1owVTELMAkGA1UEBhMCQ1oxEDAOBgNVBAoMB1NNZXRySUQxGjAYBgNVBAsMEURh
dG92YSBjZW50cmFsYSAxMRgwFgYDVQQDDA8xMjM0NTY3ODlBQkNERUYwWTATBgcq
hkjOPQIBBggqhkjOPQMBBwNCAASL2UzH6wawBNKtRYBtTA/bIMNcgtpyj5zx9HjJ
QUe3px0Ggav+SQXZByVPIxzAkH9k4Y7GUc56lNfe5BqhIuqyo08wTTAfBgNVHSME
GDAWgBR2G/kadeeV2VPebwxp8kON3hqTejALBgNVHQ8EBAMCAwgwHQYDVR0OBBYE
FNfcN7wYbeK3Ufc3cyptoYOAj43BMAoGCCqGSM49BAMCA0gAMEUCIQCepMS3yLzN
RwWE2ZULCcU/n76jDisMTs2U5AlQaRjZsQIgafkRYpo0GVYVcZLb4nmu9pFMH8B8
p0l1qXPmiSxONU4=
-----END CERTIFICATE-----
```

9.4.2 DigitalSignature DLMS/COSEM

```
$ openssl ecparam -out ecparam.pem -name prime256v1
$ openssl genpkey -paramfile ecparam.pem -out ecdhkey.pem
```

```
$ openssl req -new -config meridlo1.cnf -key ecdhkey.pem -out meridlo1.req
```

```
$ openssl x509 -req -in meridlo1.req -extfile meridlo1.cnf -extensions
v3_usr -CA ..\..\Sub-CA-256-certificate.cer -CAkey ..\..\ecdhkey.pem -out
meridlo1-256-certificate.cer -days 36524
```

meridlo1.cnf:

```
[ req ]
default_keyfile           = ecdhkey.pem
distinguished_name  = req_distinguished_name
prompt                    = no

[ req_distinguished_name ]
C  = CZ
O  = SMetrID
OU = "Datova centrala 1"
CN = 123456789ABCDEF

[ v3_usr ]
authorityKeyIdentifier=keyid,issuer
keyUsage = digitalSignature  = SMetrID
CN = SM-Suite1-Test-Sub-CA
```

```
$ openssl x509 -in meridlo1-256-certificate.cer -text
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            36:f5:7e:34:be:42:dc:e3:99:62:9b:14:5d:89:55:f6:28:08:e7:c0
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = CZ, O = SMetrID, CN = SM-Suite1-Test-Sub-CA
        Validity
            Not Before: May 15 10:42:59 2023 GMT
            Not After : May 15 10:42:59 2123 GMT
        Subject: C = CZ, O = SMetrID, OU = Datova centrala 1, CN = 123456789ABCDEF
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:6e:98:9d:b1:5e:bf:9a:37:d5:aa:7a:36:47:60:
                    cf:6d:f9:9b:b1:a4:52:ad:6c:fa:f3:6f:42:f8:09:
                    9e:64:d6:c8:0c:82:a8:50:90:65:83:20:44:ac:d4:
                    0f:05:96:5c:90:af:59:99:19:c0:3a:a2:28:52:37:
                    38:1f:00:bc:39
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                76:1B:F9:1A:75:E7:95:D9:53:DE:6F:0C:69:F2:43:8D:DE:1A:93:7A
            X509v3 Key Usage:
                Digital Signature
            X509v3 Subject Key Identifier:
                11:AC:23:B4:64:71:F5:D2:65:AF:C4:1D:33:E1:F9:9B:CC:DE:2C:9C
    Signature Algorithm: ecdsa-with-SHA256
    Signature Value:
        30:45:02:21:00:e4:96:39:dc:03:1f:e9:e4:18:b9:e7:64:a6:
        59:f8:1c:ab:51:51:f0:c2:59:bd:56:e7:c3:4f:fb:fc:22:05:
        94:02:20:4e:9d:e8:4c:42:2a:73:83:9e:24:bd:ef:9c:52:db:
        9f:36:8c:be:6e:38:5b:cb:09:d7:2b:9c:32:31:8a:60:79
-----BEGIN CERTIFICATE-----
```

```
MIIB5zCCAY2gAwIBAgIUNvV+NL5C3OOZYpsUXYlV9igI58AwCgYIKoZIzj0EAwIw
PzELMAkGA1UEBhMCQ1oxEDAOBgNVBAoMB1NNZXRySUQxHjAcBgNVBAMMFVNNLVN1
aXRlMS1UZXN0LVN1Yi1DQTAgFw0yMzA1MTUxMDQyNTlaGA8yMTIzMDUxNTEwNDI1
OVowVTELMAkGA1UEBhMCQ1oxEDAOBgNVBAoMB1NNZXRySUQxGjAYBgNVBAsMEURh
dG92YSBjZW50cmFsYSAxMRgwFgYDVQQDDA8xMjM0NTY3ODlBQkNERUYwWTATBgcq
hkjOPQIBBggqhkjOPQMBBwNCAARumJ2xXr+aN9WqejZHYM9t+ZuxpFKtbPrzb0L4
CZ5k1sgMgqhQkGWDIESs1A8FllyQr1mZGcA6oihSNzgfALw5o08wTTAfBgNVHSME
GDAWgBR2G/kadeeV2VPebwxp8kON3hqTejALBgNVHQ8EBAMCB4AwHQYDVR0OBBYE
FBGsI7RkcfXSZa/EHTPh+ZvM3iycMAoGCCqGSM49BAMCA0gAMEUCIQDkljncAx/p
5Bi552SmWfgcq1FR8MJZvVbnw0/7/CIFlAIgTp3oTEIqc4OeJL3vnFLbnzaMvm44
W8sJ1yucMjGKYHk=
-----END CERTIFICATE-----
```

9.5 HES

Common Name v certifikátu HES se rovná OU v certifikátech měřidel.

9.5.1 KeyAgreement DLMS/COSEM

```
$ openssl ecparam -out ecparam.pem -name prime256v1
$ openssl genpkey -paramfile ecparam.pem -out ecdhkey.pem
```

```
$ openssl req -new -config dc.cnf -key ecdhkey.pem -out dc.req
```

```
$ openssl x509 -req -in dc.req -extfile dc.cnf -extensions v3_usr -CA
..\..\Sub-CA-256-certificate.cer -CAkey ..\..\ecdhkey.pem -out dc-256-
certificate.cer -days 365
```

```
[ req ]
default_keyfile           = ecdhkey.pem
distinguished_name  = req_distinguished_name
prompt                    = no

[ req_distinguished_name ]
C  = CZ
O  = SMetrID
CN = "Datova centrala 1"

[ v3_usr ]
authorityKeyIdentifier=keyid,issuer
keyUsage = keyAgreement
```

```
$ openssl x509 -in dc-256-certificate.cer -text
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            28:e1:ad:2e:c9:54:f8:e5:e3:a1:a8:02:42:10:93:d7:94:59:9d:5e
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = CZ, O = SMetrID, CN = SM-Suite1-Test-Sub-CA
        Validity
            Not Before: May 16 16:03:37 2023 GMT
            Not After : May 15 16:03:37 2024 GMT
        Subject: C = CZ, O = SMetrID, CN = Datova centrala 1
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:cb:62:4b:67:01:6c:31:51:3e:f0:ba:60:9e:e6:
                    60:89:79:aa:b3:0e:1b:af:9a:0b:69:bc:a9:2c:f3:
                    a6:e6:61:c6:1d:c5:56:7b:b4:2f:a6:98:cd:37:a4:
                    cf:26:51:0b:1f:2e:03:25:6b:cd:c5:78:4d:e7:86:
                    39:1d:fe:0d:2e
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
```

```
            X509v3 Authority Key Identifier:
                76:1B:F9:1A:75:E7:95:D9:53:DE:6F:0C:69:F2:43:8D:DE:1A:93:7A
            X509v3 Key Usage:
                Key Agreement
            X509v3 Subject Key Identifier:
                54:04:DE:52:D9:87:34:57:65:4A:F6:DE:5E:1D:B1:EC:A7:5F:18:61
    Signature Algorithm: ecdsa-with-SHA256
    Signature Value:
        30:46:02:21:00:85:97:62:32:ce:06:a1:09:cb:e4:bc:08:9e:
        67:84:b5:ef:b9:72:98:09:78:9b:88:f9:94:eb:a1:83:f9:63:
        6d:02:21:00:f8:0a:67:ec:c6:ac:77:ce:ba:3b:d1:07:44:1c:
        43:8e:73:49:8c:9c:69:4c:c0:98:3e:49:eb:6a:3d:41:6f:3c
-----BEGIN CERTIFICATE-----
MIIBzDCCAXGgAwIBAgIUKOGtLslU+OXjoagCQhCT15RZnV4wCgYIKoZIzj0EAwIw
PzELMAkGA1UEBhMCQ1oxEDAOBgNVBAoMB1NNZXRySUQxHjAcBgNVBAMMFVNNLVN1
aXRlMS1UZXN0LVN1Yi1DQTAeFw0yMzA1MTYxNjAzMzdaFw0yNDA1MTUxNjAzMzda
MDsxCzAJBgNVBAYTAkNaMRAwDgYDVQQKDAdTTWV0cklEMRowGAYDVQQDDBFEYXRv
dmEgY2VudHJhbGEgMTBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABMtiS2cBbDFR
PvC6YJ7mYIl5qrMOG6+aC2m8qSzzpuZhxh3FVnu0L6aYzTekzyZRCx8uAyVrzcV4
TeeGOR3+DS6jTzBNMB8GA1UdIwQYMBaAFHYb+Rp155XZU95vDGnyQ43eGpN6MAsG
A1UdDwQEAwIDCDAdBgNVHQ4EFgQUVATeUtmHNFdlSvbeXh2x7KdfGGEwCgYIKoZI
zj0EAwIDSQAwRgIhAIWXYjLOBqEJy+S8CJ5nhLXvuXKYCXibiPmU66GD+WNtAiEA
+Apn7Masd866O9EHRBxDjnNJjJxpTMCYPknraj1Bbzw=
-----END CERTIFICATE-----
```

9.5.2 DigitalSignature DLMS/COSEM

```
$ openssl ecparam -out ecparam.pem -name prime256v1
$ openssl genpkey -paramfile ecparam.pem -out ecdhkey.pem
```

```
$ openssl req -new -config dc.cnf -key ecdhkey.pem -out dc.req
```

```
$ openssl x509 -req -in dc.req -extfile dc.cnf -extensions v3_usr -CA ..\..\Sub-CA-256-certificate.cer -CAkey ..\..\ecdhkey.pem -out dc-256-certificate.cer -days 365
```

```
[ req ]
default_keyfile           = ecdhkey.pem
distinguished_name  = req_distinguished_name
prompt                    = no

[ req_distinguished_name ]
C  = CZ
O  = SMetrID
CN = "Datova centrala 1"

[ v3_usr ]
authorityKeyIdentifier=keyid,issuer
keyUsage = digitalSignature
```

```
$ openssl x509 -in dc-256-certificate.cer -text
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            71:33:b5:72:18:81:39:ed:6f:1d:6a:2e:f7:56:f5:c3:18:91:bb:0b
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = CZ, O = SMetrID, CN = SM-Suite1-Test-Sub-CA
        Validity
            Not Before: May 16 16:11:26 2023 GMT
            Not After : May 15 16:11:26 2024 GMT
        Subject: C = CZ, O = SMetrID, CN = Datova centrala 1
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
```

```
                pub:
                    04:6f:e9:c6:29:84:de:82:2a:fd:eb:e8:47:61:40:
                    92:e4:67:3f:08:0c:35:7e:67:46:b3:36:ca:65:ea:
                    c7:97:60:1b:4c:f1:c5:48:06:ca:44:c8:75:d9:dd:
                    f9:9f:ba:ac:7b:f3:ed:c2:96:22:53:85:c8:a1:dc:
                    97:7c:cc:a8:e1
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                76:1B:F9:1A:75:E7:95:D9:53:DE:6F:0C:69:F2:43:8D:DE:1A:93:7A
            X509v3 Key Usage:
                Digital Signature
            X509v3 Subject Key Identifier:
                2F:AA:AD:C9:75:68:72:4C:B9:22:1C:F8:EE:66:13:7D:EF:B4:7A:A7
    Signature Algorithm: ecdsa-with-SHA256
    Signature Value:
        30:46:02:21:00:cf:a0:32:88:9d:9a:93:90:10:fe:76:67:5d:
        9b:a4:ee:7c:e7:dc:dc:e1:30:87:43:47:e6:bd:84:46:7a:72:
        8a:02:21:00:ea:da:19:4a:b5:89:dc:dd:a2:f5:9c:d0:bb:a0:
        b4:1e:be:03:93:58:e4:91:cd:2c:24:20:91:53:9f:e0:6e:ff
-----BEGIN CERTIFICATE-----
MIIBzDCCAXGgAwIBAgIUcTO1chiBOe1vHWou91b1wxiRuwswCgYIKoZIzj0EAwIw
PzELMAkGA1UEBhMCQ1oxEDAOBgNVBAoMB1NNZXRySUQxHjAcBgNVBAMMFVNNLVN1
aXRlMS1UZXN0LVN1Yi1DQTAeFw0yMzA1MTYxNjExMjZaFw0yNDA1MTUxNjExMjZa
MDsxCzAJBgNVBAYTAkNaMRAwDgYDVQQKDAdTTWV0cklEMRowGAYDVQQDDBFEYXRv
dmEgY2VudHJhbGEgMTBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABG/pximE3oIq
/evoR2FAkuRnPwgMNX5nRrM2ymXqx5dgG0zxxUgGykTIddnd+Z+6rHvz7cKWIlOF
yKHcl3zMqOGjTzBNMB8GA1UdIwQYMBaAFHYb+Rp155XZU95vDGnyQ43eGpN6MAsG
A1UdDwQEAwIHgDAdBgNVHQ4EFgQUL6qtyXVocky5Ihz47mYTfe+0eqcwCgYIKoZI
zj0EAwIDSQAwRgIhAM+gMoidmpOQEP52Z12bpO5859zc4TCHQ0fmvYRGenKKAiEA
6toZSrWJ3N2i9ZzQu6C0Hr4Dk1jkkc0sJCCRU5/gbv8=
-----END CERTIFICATE-----
```

9.6 Výrobce

9.6.1 Digital Signature CAdES

```
$ openssl ecparam -out ecparam.pem -name prime256v1
$ openssl genpkey -paramfile ecparam.pem -out ecdhkey.pem
```

```
$ openssl req -new -config openssl.cnf -key ecdhkey.pem -out request.req
```

```
$ openssl x509 -req -in request.req -extfile openssl.cnf -extensions v3_usr
-CA ..\..\Sub-CA-256-certificate.cer    -CAkey ..\..\ecdhkey.pem   -out
vyrobceSign.cer -days 730
```

```
[ req ]
default_keyfile           = ecdhkey.pem
distinguished_name  = req_distinguished_name
prompt                    = no

[ req_distinguished_name ]
C  = CZ
O  = Výrobce
CN = Výroba

[ v3_usr ]
authorityKeyIdentifier=keyid,issuer
keyUsage = digitalSignature
subjectAltName = email:vyroba@vyrobce.cz
```

```
$ openssl x509 -in vyrobceSign.cer -text
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            60:10:60:5d:b1:20:8b:cd:ab:db:ae:9c:52:64:9c:16:fe:a7:15:24
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = CZ, O = SMetrID, CN = SM-Suite1-Test-Sub-CA
        Validity
            Not Before: May 15 11:52:38 2023 GMT
            Not After : May 14 11:52:38 2025 GMT
        Subject: C = CZ, O = V\C3\83\C2\BDrobce, CN = V\C3\83\C2\BDroba
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:26:c7:41:f5:8e:0f:3a:9d:a6:14:29:c0:ef:17:
                    3a:93:01:9a:75:73:53:6e:ca:d2:4d:14:87:dc:cf:
                    2a:b8:e2:7f:26:07:d4:93:7c:95:1e:38:5d:70:33:
                    73:95:02:b2:91:07:cf:95:a0:47:6e:f3:e5:94:34:
                    f4:97:ca:90:d9
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                76:1B:F9:1A:75:E7:95:D9:53:DE:6F:0C:69:F2:43:8D:DE:1A:93:7A
            X509v3 Key Usage:
                Digital Signature
            X509v3 Subject Alternative Name:
                email:vyroba@vyrobce.cz
            X509v3 Subject Key Identifier:
                EF:D1:F9:53:32:50:34:A4:51:A4:DD:2C:81:11:1C:7E:FD:B2:4C:C0
    Signature Algorithm: ecdsa-with-SHA256
    Signature Value:
        30:45:02:20:1d:45:f6:44:f5:79:ec:9c:87:a8:57:83:56:a1:
        1b:2a:30:05:08:15:3c:d9:63:27:cd:19:2a:65:fc:32:63:52:
        02:21:00:d9:77:15:40:4a:aa:9e:00:b2:c9:af:0d:f1:82:3a:
        5a:69:c4:0c:3e:3c:b7:53:d3:8c:17:0a:6c:29:2b:cb:80
-----BEGIN CERTIFICATE-----
MIIB5DCCAYqgAwIBAgIUYBBgXbEgi82r266cUmScFv6nFSQwCgYIKoZIzj0EAwIw
PzELMAkGA1UEBhMCQ1oxEDAOBgNVBAoMB1NNZXRySUQxHjAcBgNVBAMMFVNNLVN1
aXRlMS1UZXN0LVN1Yi1DQTAeFw0yMzA1MTUxMTUyMzhaFw0yNTA1MTQxMTUyMzha
MDYxCzAJBgNVBAYTAkNaMRMwEQYDVQQKDApWw4PCvXJvYmNlMRIwEAYDVQQDDAlW
w4PCvXJvYmEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQmx0H1jg86naYUKcDv
FzqTAZp1c1NuytJNFIfczyq44n8mB9STfJUeOF1wM3OVArKRB8+VoEdu8+WUNPSX
ypDZo20wazAfBgNVHSMEGDAWgBR2G/kadeeV2VPebwxp8kON3hqTejALBgNVHQ8E
BAMCB4AwHAYDVR0RBBUwE4ERdnlyb2JhQHZ5cm9iY2UuY3owHQYDVR0OBBYEFO/R
+VMyUDSkUaTdLIERHH79skzAMAoGCCqGSM49BAMCA0gAMEUCIB1F9kT1eeych6hX
g1ahGyowBQgVPNljJ80ZKmX8MmNSAiEA2XcVQEqqngCyya8N8YI6WmnEDD48t1PT
jBcKbCkry4A=
-----END CERTIFICATE-----
```

9.6.2 Digital Signature XAdES

Identické s předchozím – pouze jiná párová data.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0b:a1:19:6d:a6:a5:76:58:90:4d:a7:8b:85:c4:df:56:77:a0:82:95
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = CZ, O = SMetrID, CN = SM-Suite1-Test-Sub-CA
        Validity
            Not Before: May 15 12:04:46 2023 GMT
            Not After : May 14 12:04:46 2025 GMT
        Subject: C = CZ, O = V\C3\83\C2\BDrobce, CN = V\C3\83\C2\BDroba
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
```

```
                Public-Key: (256 bit)
                pub:
                    04:2e:79:6c:39:72:02:a1:8a:9a:01:e8:51:26:9e:
                    80:5d:7a:72:e6:7d:fb:f6:84:77:3b:e7:77:67:bd:
                    68:18:05:07:de:ff:06:e8:12:9b:c5:06:a3:5d:13:
                    8f:ae:9a:c1:74:2d:67:6e:9e:94:33:14:53:81:c8:
                    61:d5:f2:e3:2b
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                76:1B:F9:1A:75:E7:95:D9:53:DE:6F:0C:69:F2:43:8D:DE:1A:93:7A
            X509v3 Key Usage:
                Digital Signature
            X509v3 Subject Alternative Name:
                email:vyroba@vyrobce.cz
            X509v3 Subject Key Identifier:
                D8:8E:D2:44:CC:8B:B5:11:9F:C5:E5:8F:06:6A:30:F2:FF:FD:93:7A
    Signature Algorithm: ecdsa-with-SHA256
    Signature Value:
        30:46:02:21:00:c8:18:f1:1f:ba:d6:bc:fd:66:5a:b5:a9:79:
        da:70:e2:66:30:12:50:b7:0f:f5:02:c5:e8:f8:be:18:5d:fe:
        d7:02:21:00:d9:d8:0a:8c:6e:d5:8d:27:37:5f:19:f2:3f:e6:
        dd:b0:28:16:0b:37:b2:3b:d1:33:49:34:17:4b:af:3b:15:f4
-----BEGIN CERTIFICATE-----
MIIB5TCCAYqgAwIBAgIUC6EZbaaldliQTaeLhcTfVneggpUwCgYIKoZIzj0EAwIw
PzELMAkGA1UEBhMCQ1oxEDAOBgNVBAoMB1NNZXRySUQxHjAcBgNVBAMMFVNNLVN1
aXRlMS1UZXN0LVN1Yi1DQTAeFw0yMzA1MTUxMjA0NDZaFw0yNTA1MTQxMjA0NDZa
MDYxCzAJBgNVBAYTAkNaMRMwEQYDVQQKDApWw4PCvXJvYmNlMRIwEAYDVQQDDAlW
w4PCvXJvYmEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQueWw5cgKhipoB6FEm
noBdenLmffv2hHc753dnvWgYBQfe/wboEpvFBqNdE4+umsF0LWdunpQzFFOByGHV
8uMro20wazAfBgNVHSMEGDAWgBR2G/kadeeV2VPebwxp8kON3hqTejALBgNVHQ8E
BAMCB4AwHAYDVR0RBBUwE4ERdnlyb2JhQHZ5cm9iY2UuY3owHQYDVR0OBBYEFNiO
0kTMi7URn8XljwZqMPL//ZN6MAoGCCqGSM49BAMCA0kAMEYCIQDIGPEfuta8/WZa
tal52nDiZjASULcP9QLF6Pi+GF3+1wIhANnYCoxu1Y0nN18Z8j/m3bAoFgs3sjvR
M0k0F0uvOxX0
-----END CERTIFICATE-----
```

9.6.3 KeyAgreement CAdES

```
$ openssl ecparam -out ecparam.pem -name prime256v1
$ openssl genpkey -paramfile ecparam.pem -out ecdhkey.pem
```

```
$ openssl req -new -config openssl.cnf -key ecdhkey.pem -out request.req
```

```
$ openssl x509 -req -in request.req -extfile openssl.cnf -extensions v3_usr
-CA  ..\..\Sub-CA-256-certificate.cer      -CAkey  ..\..\ecdhkey.pem     -out
vyrobce.cer -days 730
```

```
[ req ]
default_keyfile           = ecdhkey.pem
distinguished_name  = req_distinguished_name
prompt                    = no

[ req_distinguished_name ]
C  = CZ
O  = Výrobce
CN = Výroba

[ v3_usr ]
authorityKeyIdentifier=keyid,issuer
keyUsage = digitalSignature
subjectAltName = email:vyroba@vyrobce.cz
```

```
$ openssl x509 -in vyrobce.cer -text
```

```
Certificate:
```

```
    Data:
        Version: 3 (0x2)
        Serial Number:
            4f:73:5c:56:3b:9d:3f:fa:1d:d4:f7:ea:d6:24:37:38:b0:62:50:90
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = CZ, O = SMetrID, CN = SM-Suite1-Test-Sub-CA
        Validity
            Not Before: May 15 11:59:47 2023 GMT
            Not After : May 14 11:59:47 2025 GMT
        Subject: C = CZ, O = V\C3\83\C2\BDrobce, CN = V\C3\83\C2\BDroba
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:39:50:f9:81:31:3d:07:a0:e1:cd:ef:38:f2:5c:
                    b7:a4:18:b5:36:ed:d8:83:b8:d9:89:aa:2f:bd:20:
                    d1:cd:7e:14:d2:ab:ff:0b:85:b0:13:08:92:bc:5e:
                    bb:14:9f:1c:08:fa:ca:c8:77:06:1c:ff:ea:f1:70:
                    cf:ac:e2:1f:13
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                76:1B:F9:1A:75:E7:95:D9:53:DE:6F:0C:69:F2:43:8D:DE:1A:93:7A
            X509v3 Key Usage:
                Key Agreement
            X509v3 Subject Alternative Name:
                email:vyroba@vyrobce.cz
            X509v3 Subject Key Identifier:
                95:99:69:4E:69:22:66:56:99:79:B3:3E:C3:50:35:4B:A3:DC:D6:E1
    Signature Algorithm: ecdsa-with-SHA256
    Signature Value:
        30:44:02:20:76:f8:3e:b6:fd:95:4c:16:54:c6:55:ea:da:5d:
        6c:fe:ef:67:be:ba:fb:25:33:8b:95:01:e6:01:9c:76:2c:1b:
        02:20:38:e3:b1:2b:19:d2:6a:16:b5:df:36:b4:a3:36:91:3f:
        88:65:ec:cb:db:b7:5b:f5:8b:2a:64:27:da:3d:13:bd
-----BEGIN CERTIFICATE-----
MIIB4zCCAYqgAwIBAgIUT3NcVjudP/od1Pfq1iQ3OLBiUJAwCgYIKoZIzj0EAwIw
PzELMAkGA1UEBhMCQ1oxEDAOBgNVBAoMB1NNZXRySUQxHjAcBgNVBAMMFVNNLVN1
aXRlMS1UZXN0LVN1Yi1DQTAeFw0yMzA1MTUxMTU5NDdaFw0yNTA1MTQxMTU5NDda
MDYxCzAJBgNVBAYTAkNaMRMwEQYDVQQKDApWw4PCvXJvYmNlMRIwEAYDVQQDDAlW
w4PCvXJvYmEwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQ5UPmBMT0HoOHN7zjy
XLekGLU27diDuNmJqi+9INHNfhTSq/8LhbATCJK8XrsUnxwI+srIdwYc/+rxcM+s
4h8To20wazAfBgNVHSMEGDAWgBR2G/kadeeV2VPebwxp8kON3hqTejALBgNVHQ8E
BAMCAwgwHAYDVR0RBBUwE4ERdnlyb2JhQHZ5cm9iY2UuY3owHQYDVR0OBBYEFJWZ
aU5pImZWmXmzPsNQNUuj3NbhMAoGCCqGSM49BAMCA0cAMEQCIHb4Prb9lUwWVMZV
6tpdbP7vZ766+yUzi5UB5gGcdiwbAiA447ErGdJqFrXfNrSjNpE/iGXsy9u3W/WL
KmQn2j0TvQ==
-----END CERTIFICATE-----
```

9.7 Objednatel

9.7.1 Digital Signature CAdES

```
$ openssl ecparam -out ecparam.pem -name prime256v1
$ openssl genpkey -paramfile ecparam.pem -out ecdhkey.pem

$ openssl req -new -config openssl.cnf -key ecdhkey.pem -out request.req

$ openssl x509 -req -in request.req -extfile openssl.cnf -extensions v3_usr
-CA  ..\..\Sub-CA-256-certificate.cer      -CAkey  ..\..\ecdhkey.pem     -out
objednatelSign.cer -days 730
```

```
[ req ]
default_keyfile           = ecdhkey.pem
distinguished_name  = req_distinguished_name
prompt                    = no
```

```
[ req_distinguished_name ]
C  = CZ
O  = Objednatel
CN = Objednávky

[ v3_usr ]
authorityKeyIdentifier=keyid,issuer
keyUsage = digitalSignature
subjectAltName = email:objednavky@objednatel.cz
```

```
$ openssl x509 -in objednatelSign.cer -text
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            10:0b:e8:e4:7a:cf:4a:86:f3:fa:d1:cf:a9:22:19:93:5c:1b:6e:a1
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = CZ, O = SMetrID, CN = SM-Suite1-Test-Sub-CA
        Validity
            Not Before: May 15 12:12:40 2023 GMT
            Not After : May 14 12:12:40 2025 GMT
        Subject: C = CZ, O = Objednatel, CN = Objedn\C3\83\C2\A1vky
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:2c:0f:8b:2c:0f:41:7b:5a:1b:2e:93:75:8c:ce:
                    cb:7b:64:96:15:0e:51:c9:d1:0e:f0:90:59:dd:4f:
                    9c:5e:af:78:b0:f7:fa:24:09:33:7b:98:e7:c7:dd:
                    b4:5c:9e:7e:be:b9:4c:7d:c8:a6:d2:ed:99:d4:40:
                    cf:41:7a:4b:71
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                76:1B:F9:1A:75:E7:95:D9:53:DE:6F:0C:69:F2:43:8D:DE:1A:93:7A
            X509v3 Key Usage:
                Digital Signature
            X509v3 Subject Alternative Name:
                email:objednavky@objednatel.cz
            X509v3 Subject Key Identifier:
                A2:18:0B:85:2E:9B:65:1E:54:D4:8B:13:FF:04:EC:D5:9A:1B:BB:6B
    Signature Algorithm: ecdsa-with-SHA256
    Signature Value:
        30:45:02:21:00:8d:1b:61:e0:60:9f:8c:e5:7c:32:1e:cd:ec:
        1d:37:38:ab:1b:a6:88:b3:8a:92:8f:c6:3a:96:fd:2a:f0:27:
        04:02:20:27:83:ca:48:ac:31:95:56:c2:06:9e:3b:ba:b2:5d:
        25:13:a7:76:e7:77:07:e5:bc:4f:30:81:0a:d6:20:df:7a
-----BEGIN CERTIFICATE-----
MIIB7zCCAZWgAwIBAgIUEAvo5HrPSobz+tHPqSIZk1wbbqEwCgYIKoZIzj0EAwIw
PzELMAkGA1UEBhMCQ1oxEDAOBgNVBAoMB1NNZXRySUQxHjAcBgNVBAMMFVNNLVN1
aXRlMS1UZXN0LVN1Yi1DQTAeFw0yMzA1MTUxMjEyNDBaFw0yNTA1MTQxMjEyNDBa
MDoxCzAJBgNVBAYTAkNaMRMwEQYDVQQKDApPYmplZG5hdGVsMRYwFAYDVQQDDA1P
YmplZG7Dg8Khdmt5MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAELA+LLA9Be1ob
LpN1jM7Le2SWFQ5RydEO8JBZ3U+cXq94sPf6JAkze5jnx920XJ5+vrlMfcim0u2Z
1EDPQXpLcaN0MHIwHwYDVR0jBBgwFoAUdhv5GnXnldlT3m8MafJDjd4ak3owCwYD
VR0PBAQDAgeAMCMGA1UdEQQcMBqBGG9iamVkbmF2a3lAb2JqZWRuYXRlbC5jejAd
BgNVHQ4EFgQUohgLhS6bZR5U1IsT/wTs1Zobu2swCgYIKoZIzj0EAwIDSAAwRQIh
AI0bYeBgn4zlfDIezewdNzirG6aIs4qSj8Y6lv0q8CcEAiAng8pIrDGVVsIGnju6
sl0lE6d253cH5bxPMIEK1iDfeg==
-----END CERTIFICATE-----
```

9.7.2 KeyAgreement CAdES

```
$ openssl ecparam -out ecparam.pem -name prime256v1
```

```
$ openssl genpkey -paramfile ecparam.pem -out ecdhkey.pem

$ openssl req -new -config openssl.cnf -key ecdhkey.pem -out request.req

$ openssl x509 -req -in request.req -extfile openssl.cnf -extensions v3_usr
-CA  ..\..\Sub-CA-256-certificate.cer      -CAkey  ..\..\ecdhkey.pem     -out
objednatel.cer -days 730
```

```
[ req ]
default_keyfile           = ecdhkey.pem
distinguished_name  = req_distinguished_name
prompt                    = no

[ req_distinguished_name ]
C   = CZ
O   = Objednatel
CN = Objednávky

[ v3_usr ]
authorityKeyIdentifier=keyid,issuer
keyUsage = keyAgreement
subjectAltName = email:objednavky@objednatel.cz
```

```
$ openssl x509 -in objednatel.cer -text
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            09:63:d7:b3:fd:35:69:04:12:5e:17:0e:93:eb:1f:a4:12:3a:22:fb
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = CZ, O = SMetrID, CN = SM-Suite1-Test-Sub-CA
        Validity
            Not Before: May 15 12:18:41 2023 GMT
            Not After : May 14 12:18:41 2025 GMT
        Subject: C = CZ, O = Objednatel, CN = Objedn\C3\83\C2\A1vky
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:b1:99:dc:58:ae:65:02:72:c6:ef:52:03:0c:7d:
                    51:59:00:35:28:e2:0c:84:3d:c5:33:1b:7a:4c:df:
                    82:3d:8c:de:0a:dd:cf:65:ff:1b:e5:ac:e2:fb:10:
                    f6:f8:27:df:a0:bb:4c:47:d9:a9:16:68:30:12:c5:
                    2d:fe:e3:c4:ff
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                76:1B:F9:1A:75:E7:95:D9:53:DE:6F:0C:69:F2:43:8D:DE:1A:93:7A
            X509v3 Key Usage:
                Key Agreement
            X509v3 Subject Alternative Name:
                email:objednavky@objednatel.cz
            X509v3 Subject Key Identifier:
                18:E8:1C:F5:7A:2E:4D:68:68:2E:6E:97:60:77:9C:93:DC:D5:8E:63
    Signature Algorithm: ecdsa-with-SHA256
    Signature Value:
        30:45:02:20:74:28:97:06:80:90:ef:35:54:76:df:f6:00:09:
        99:a0:37:77:c5:2b:68:ec:84:40:8e:ea:04:21:f3:a3:52:80:
        02:21:00:e2:a1:23:fc:6e:77:b0:2e:79:4c:0b:32:6e:fc:87:
        e5:90:ab:a5:31:03:34:3e:a8:2c:a0:a3:60:72:5b:39:57
-----BEGIN CERTIFICATE-----
MIIB7zCCAZWgAwIBAgIUCWPXs/01aQQSXhcOk+sfpBI6IvswCgYIKoZIzj0EAwIw
PzELMAkGA1UEBhMCQ1oxEDAOBgNVBAoMB1NNZXRySUQxHjAcBgNVBAMMFVNNLVN1
aXRlMS1UZXN0LVN1Yi1DQTAeFw0yMzA1MTUxMjE4NDFaFw0yNTA1MTQxMjE4NDFa
MDoxCzAJBgNVBAYTAkNaMRMwEQYDVQQKDApPYmplZG5hdGVsMRYwFAYDVQQDDA1P
```

```
YmplZG7Dg8Khdmt5MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEsZncWK5lAnLG
7lIDDH1RWQA1KOIMhD3FMxt6TN+CPYzeCt3PZf8b5azi+xD2+CffoLtMR9mpFmgw
EsUt/uPE/6N0MHIwHwYDVR0jBBgwFoAUdhv5GnXnldlT3m8MafJDjd4ak3owCwYD
VR0PBAQDAgMIMCMGA1UdEQQcMBqBGG9iamVkbmF2a3lAb2JqZWRuYXRlbC5jejAd
BgNVHQ4EFgQUGOgc9XouTWhoLm6XYHeck9zVjmMwCgYIKoZIzj0EAwIDSAAwRQIg
dCiXBoCQ7zVUdt/2AAmZoDd3xSto7IRAjuoEIfOjUoACIQDioSP8bnewLnlMCzJu
/IflkKulMQM0PqgsoKNgcls5Vw==
-----END CERTIFICATE-----
```

9.8 Správce

9.8.1 DigitalSignature XAdES

```
$ openssl ecparam -out ecparam.pem -name prime256v1
$ openssl genpkey -paramfile ecparam.pem -out ecdhkey.pem

$ openssl req -new -config openssl.cnf -key ecdhkey.pem -out request.req

$ openssl x509 -req -in request.req -extfile openssl.cnf -extensions v3_usr
-CA  ..\..\Sub-CA-256-certificate.cer      -CAkey  ..\..\ecdhkey.pem     -out
spravceSign.cer -days 730
```

```
[ req ]
default_keyfile           = ecdhkey.pem
distinguished_name  = req_distinguished_name
prompt                    = no

[ req_distinguished_name ]
C   = CZ
O   = Správce
CN = administrátor

[ v3_usr ]
authorityKeyIdentifier=keyid,issuer
keyUsage = digitalSignature
subjectAltName = email:admin@spravce.cz
```

```
$ openssl x509 -in spravceSign.cer -text

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            37:1a:b4:69:47:26:78:b7:d7:68:82:3a:70:ce:65:44:fd:24:49:4b
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = CZ, O = SMetrID, CN = SM-Suite1-Test-Sub-CA
        Validity
            Not Before: May 15 12:28:23 2023 GMT
            Not After : May 14 12:28:23 2025 GMT
        Subject: C = CZ, O = Spr\C3\83\C2\A1vce, CN = administr\C3\83\C2\A1tor
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:59:8f:af:06:53:1a:4d:b8:c4:57:bb:68:55:52:
                    ae:5e:3b:41:36:b6:d3:f7:58:74:7e:8f:e9:f5:a5:
                    49:c6:b0:12:bf:cf:72:2e:a4:3e:73:fb:08:df:37:
                    68:66:7e:ab:da:b2:a5:6e:06:e2:1d:c7:d1:aa:f9:
                    e1:1f:70:11:6e
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                76:1B:F9:1A:75:E7:95:D9:53:DE:6F:0C:69:F2:43:8D:DE:1A:93:7A
            X509v3 Key Usage:
                Digital Signature
```

```
            X509v3 Subject Alternative Name:
                email:admin@spravce.cz
            X509v3 Subject Key Identifier:
                75:C8:66:8B:B1:DE:EA:1B:42:22:88:31:17:C4:AF:D0:3E:BC:19:C6
    Signature Algorithm: ecdsa-with-SHA256
    Signature Value:
        30:46:02:21:00:b5:fb:21:bd:00:6a:fe:72:75:83:35:f7:8d:
        c5:d8:01:25:0d:e8:f0:d3:a6:87:b8:fa:4d:18:36:a3:1b:34:
        51:02:21:00:e4:8b:98:99:dd:05:e1:0b:69:6f:b3:a9:4d:da:
        31:25:0d:69:98:be:35:4b:8f:63:06:65:c7:11:5b:39:7e:c3
-----BEGIN CERTIFICATE-----
MIIB6zCCAZCgAwIBAgIUNxq0aUcmeLfXaII6cM5lRP0kSUswCgYIKoZIzj0EAwIw
PzELMAkGA1UEBhMCQ1oxEDAOBgNVBAoMB1NNZXRySUQxHjAcBgNVBAMMFVNNLVN1
aXRlMS1UZXN0LVN1Yi1DQTAeFw0yMzA1MTUxMjI4MjNaFw0yNTA1MTQxMjI4MjNa
MD0xCzAJBgNVBAYTAkNaMRMwEQYDVQQKDApTcHLDg8KhdmNlMRkwFwYDVQQDDBBh
ZG1pbmlzdHLDg8KhdG9yMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEWY+vBlMa
TbjEV7toVVKuXjtBNrbT91h0fo/p9aVJxrASv89yLqQ+c/sI3zdoZn6r2rKlbgbi
HcfRqvnhH3ARbqNsMGowHwYDVR0jBBgwFoAUdhv5GnXnldlT3m8MafJDjd4ak3ow
CwYDVR0PBAQDAgeAMBsGA1UdEQQUMBKBEGFkbWluQHNwcmF2Y2UuY3owHQYDVR0O
BBYEFHXIZoux3uobQiKIMRfEr9A+vBnGMAoGCCqGSM49BAMCA0kAMEYCIQC1+yG9
AGr+cnWDNfeNxdgBJQ3o8NOmh7j6TRg2oxs0UQIhAOSLmJndBeELaW+zqU3aMSUN
aZi+NUuPYwZlxxFbOX7D
-----END CERTIFICATE-----
```

9.8.2 KeyAgreement XAdES

```
$ openssl ecparam -out ecparam.pem -name prime256v1
$ openssl genpkey -paramfile ecparam.pem -out ecdhkey.pem

$ openssl req -new -config openssl.cnf -key ecdhkey.pem -out request.req

$ openssl x509 -req -in request.req -extfile openssl.cnf -extensions v3_usr
-CA  ..\..\Sub-CA-256-certificate.cer      -CAkey  ..\..\ecdhkey.pem     -out
spravce.cer -days 730
```

```
[ req ]
default_keyfile           = ecdhkey.pem
distinguished_name  = req_distinguished_name
prompt                    = no

[ req_distinguished_name ]
C   = CZ
O   = Správce
CN = administrátor

[ v3_usr ]
authorityKeyIdentifier=keyid,issuer
keyUsage = keyAgreement
subjectAltName = email:admin@spravce.cz
```

```
$ openssl x509 -in spravce.cer -text

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            4e:33:07:dd:85:6e:1a:e0:16:46:6c:25:52:f7:ac:28:a7:b2:b8:40
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = CZ, O = SMetrID, CN = SM-Suite1-Test-Sub-CA
        Validity
            Not Before: May 15 12:33:56 2023 GMT
            Not After : May 14 12:33:56 2025 GMT
        Subject: C = CZ, O = Spr\C3\83\C2\A1vce, CN = administr\C3\83\C2\A1tor
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
```

```
                    04:b1:f5:7b:a3:ab:76:6f:3b:a3:38:5c:9a:ec:6c:
                    11:27:5f:f1:7c:07:2c:66:63:43:4f:94:5f:e6:75:
                    6f:c4:60:a6:ca:a1:2c:95:23:e7:b6:55:cf:1c:fc:
                    a9:92:c1:60:9a:b8:94:67:56:cd:5e:56:bc:f7:28:
                    cf:fc:f4:99:9a
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                76:1B:F9:1A:75:E7:95:D9:53:DE:6F:0C:69:F2:43:8D:DE:1A:93:7A
            X509v3 Key Usage:
                Key Agreement
            X509v3 Subject Alternative Name:
                email:admin@spravce.cz
            X509v3 Subject Key Identifier:
                EA:65:F5:42:CB:21:7B:6C:00:EC:01:16:5E:EB:43:71:5A:40:A8:2A
    Signature Algorithm: ecdsa-with-SHA256
    Signature Value:
        30:45:02:20:33:a7:4d:fd:95:39:b1:cf:f4:2d:d6:72:14:5a:
        c5:5f:18:c9:59:48:c2:a6:e7:eb:5e:28:96:a3:98:4f:be:5b:
        02:21:00:ba:bd:62:dc:e7:68:02:db:0d:20:6d:ed:d2:ea:20:
        4e:89:ec:c1:01:83:a7:85:79:c4:d0:c6:76:0b:9f:e8:f7
-----BEGIN CERTIFICATE-----
MIIB6jCCAZCgAwIBAgIUTjMH3YVuGuAWRmwlUvesKKeyuEAwCgYIKoZIzj0EAwIw
PzELMAkGA1UEBhMCQ1oxEDAOBgNVBAoMB1NNZXRySUQxHjAcBgNVBAMMFVNNLVN1
aXRlMS1UZXN0LVN1Yi1DQTAeFw0yMzA1MTUxMjMzNTZaFw0yNTA1MTQxMjMzNTZa
MD0xCzAJBgNVBAYTAkNaMRMwEQYDVQQKDApTcHLDg8KhdmNlMRkwFwYDVQQDDBBh
ZG1pbmlzdHLDg8KhdG9yMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEsfV7o6t2
bzujOFya7GwRJ1/xfAcsZmNDT5Rf5nVvxGCmyqEslSPntlXPHPypksFgmriUZ1bN
Xla89yjP/PSZmqNsMGowHwYDVR0jBBgwFoAUdhv5GnXnldlT3m8MafJDjd4ak3ow
CwYDVR0PBAQDAgMIMBsGA1UdEQQUMBKBEGFkbWluQHNwcmF2Y2UuY3owHQYDVR0O
BBYEFOpl9ULLIXtsAOwBFl7rQ3FaQKgqMAoGCCqGSM49BAMCA0gAMEUCIDOnTf2V
ObHP9C3WchRaxV8YyVlIwqbn614olqOYT75bAiEAur1i3OdoAtsNIG3t0uogTons
wQGDp4V5xNDGdguf6Pc=
-----END CERTIFICATE-----
```

```
<SymetricKey>
<AccessRole>ADMIN_access</AccessRole>
<KeyValue>0102030705060708091011121314151 6</KeyValue>
<KeyType>KEK</KeyType>
<KeyType>KEK</KeyType>
<KeyType>KEK</KeyType>
<KeyType>KEK</KeyType>
<KeyAlgorithm>AES256</KeyAlgorithm>
<A>
<KeyValue>01020307050607080910 11</KeyValue>
</A>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="id-
263fad5a62a0580a1c44a0de0d22fc40">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
<ds:Reference Id="r-id-263fad5a62a0580a1c44a0de0d22fc40-1" URI="">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
<dsig-filter2:XPath xmlns:dsig-filter2="http://www.w3.org/2002/06/xmldsig-
filter2" Filter="subtract">/descendant::ds:Signature</dsig-filter2:XPath>
</ds:Transform>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
```

```
<ds:DigestValue>d+cymznDmac5g+p8vFvUnG/yQravA0J11PdSsh0x7x0=</ds:DigestValu
e>
</ds:Reference>
<ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#xades
-id-263fad5a62a0580a1c44a0de0d22fc40">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>kogrbql6un7cpvHksXkWMTvRByJGW/Cwk4DCyT4QfvY=</ds:DigestValu
e>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue Id="value-id-
263fad5a62a0580a1c44a0de0d22fc40">QrBzSFaH8YBK0eWK08CAJMQaBSnQVJRyOjiPzV/on
9NTN0A7ls1aMVRh2afwTMhfk58joPocWqOkpiU+dLyOSi500mr7nlAPvit7lTY5cAIsgypg07E/
HCgaXvm/dDuDs68kP3JrWBNJ2a5hnm7B1v8bhaOurPs1jOfoHzCw1HDv3+93HHqDRVcCrk+M+Tc
YiSfH4eQ00mULGxJFucvTdKl0X+KONXKkf8G/om9cKwHNvUVVSSqOUA2+GNNVkl+FzjyEXaynCv
DEmeGKaUYigYC1gNARh2rXg2IohGUS1Wj0Bi8SFe51lgOM/tY7+D0SJZyj6gNDRFFTrabLeoYiK
w==</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MIIIoTCCBomgAwIBAgIEALiK5TANBgkqhkiG9w0BAQsFADB/MQswCQY
DVQQGEwJDWjEoMCYGA1UEAwwfSS5DQSBRdWFsaWZpZWQgMiBDQS9SU0EgMDIvMjAxNjEtMCsGA1
UECgwkUHJ2bsOtIGNlcnRpZmlrYcSNbsOtIGF1dG9yaXRhLCBhLnMuMRcwFQYDVQQFEw5OVFJDW
i0yNjQzOTM5NTAeFw0yMjEyMTYwOTA3NTlaFw0yMzEyMTYwOTA3NTlaMIG4MR4wHAYDVQQDDBVS
TkRyLiBMSUJPUiBET1NUw4FMRUsxDjAMBgNVBCoMBUxJQk9SMRIwEAYDVQQEDAlET1NUw4FMRUs
xCzAJBgNVBAYTAkNaMREwDwYDVQQHDAhCb3JvdmFueTETMBEGA1UECQwKVSBEdWJ1IDU2NjEOMA
wGA1UEEQwFMzczMTIxFDASBgNVBAgMC0ppaG/EjWVza8O9MRcwFQYDVQQFEw5JQ0EgLSAxMDU2O
DA1NTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK7Wdf6CwvNrTHFEr8/rAW/XYFoQ
a/oyfDWmBtledDnJqBpAhTLwQttAvI+/cLV3BAxhDFyvUmHM2rOOjBFFPRKmeUUFsLPG/hGdjkF
c5LKRuUpeUeo+KVdSGnmDP5SqN7JZ6AMQvrfDinUgrDWcxXkq5KhI2o8NGcCK6siY8f8Rq23mFy
PQdtx1jTJ6ls8d2M0TcHezbk5oAeEMgJjgDUxKYCLkKwxj1SHGHeB5RZR5h8VAw4o+HSQnM7mm2
rZ97SvTVkTZqjTVSxTfKsXK8s1SdWobRaBIAl+TQf4A+hCorrEOV3+BAdZRb0b24vUBpWXhX47j
u9UEcG2mKn0O0FkCAwEAAaOCA+kwggPlMCUGCisGAQQBgbhIBAcEFzAVDA01NzA4NjEwOTgyMTM
zAgECAQH/MB0GCisGAQQBgbhIBAMEDxoNNTcwODYxMDk4MjEzMzBSBgNVHREESzBJgRJsaWJvcm
Rvc0BnbWFpbC5jb22gGAYKKwYBBAGBuEgEBqAKDAgxMDU2ODA1NaAZBgkrBgEEAdwZAgGgDAwKM
TIwMDIxNDEzNjAfBglghkgBhvhCAQ0EEhYQOTIwMzE1MDEwMDAyMzQ3ODAOBgNVHQ8BAf8EBAMC
BsAwCQYDVR0TBAIwADCCASgGA1UdIASCAR8wggEbMIIBDAYNKwYBBAGBuEgKAR4BATCB+jAdBgg
rBgEFBQcCARYRaHR0cDovL3d3dy5pY2EuY3owgdgGCCsGAQUFBwICMIHLDIHIVGVudG8ga3ZhbG
lmaWtvdmFueSBjZXJ0aWZpa2F0IHBybyBlbGVrdHJvbmlja3kgcG9kcGlzIGJ5bCB2eWRhbiB2I
HNvdWxhZHUgcyBuYXJpemVuaW0gRVUgYy4gOTEwLzIwMTQuVGhpcyBpcyBhIHF1YWxpZmllZCBj
ZXJ0aWZpY2F0ZSBmb3IgZWxlY3Ryb25pYyBzaWduYXR1cmUgYWNjb3JkaW5nIHRvIFJlZ3VsYXR
pb24gKEVVKSBObyA5MTAvMjAxNC4wCQYHBACL7EABAjCBjwYDVR0fBIGHMIGEMCqgKKAmhiRodH
RwOi8vcWNybGRwMS5pY2EuY3ovMnFjYTE2X3JzYS5jcmwwKqAooCaGJGh0dHA6Ly9xY3JsZHAyL
mljYS5jei8ycWNhMTZfcnNhLmNybDAqoCigJoYkaHR0cDovL3FjcmxkcDMuaWNhLmN6LzJxY2Ex
Nl9yc2EuY3JsMIGSBggrBgEFBQcBAwSBhTCBgjAIBgYEAI5GAQEwCAYGBACORgEEMFcGBgQAjkY
BBTBNMC0WJ2h0dHBzOi8vd3d3LmljYS5jei9acHJhdnktcHJvLXV6aXZhdGVsZRMCY3MwHBYWaH
R0cHM6Ly93d3cuaWNhLmN6L1BEUxMCZW4wEwYGBACORgEGMAkGBwQAjkYBBgEwZQYIKwYBBQUHA
QEEWTBXMCoGCCsGAQUFBzAChh5odHRwOi8vcS5pY2EuY3ovMnFjYTE2X3JzYS5jZXIwKQYIKwYB
BQUHMAGGHWh0dHA6Ly9vY3NwLmljYS5jei8ycWNhMTZfcnNhMB8GA1UdIwQYMBaAFHSCCJHj2WR
ocYXW6zHkct+LJrFtMB0GA1UdDgQWBBQtCamsLSbciFZehkcDnMI6yxahsDATBgNVHSUEDDAKBg
grBgEFBQcDBDANBgkqhkiG9w0BAQsFAAOCAgEAPgJ4EV0fmrAPYXw1wIqaCJn9M2hOqlP+3EcQY
kGGju/x8Gq2YSsLbPp/tBpd0oUzi7TLRQkHQWNfRbrTri10yp3sljGzBBc/LwEeCQSeiDaynEFL
wlMvP0xhnUudAmbUUJpqPK4OJ88jjQAi1tecrNvCXwaWsFJxuTr0fbExoPWeCn9QlUqDTXCNvjW
qncyF5YIElxOP2y6LMhnfGmlXE62e/7GhsbobCsJ1wQ5KHzpnejW2MxR3Ndo0wn2EaUV4V6u1X5
K3KsO2h+HSnyZjd4gjISLQfDSxRNZ3HepWjzOP50wFfZ+oX2LVF/T2xl3AFnxXLAiNDoZa6HNPG
KZuFhYT18uJCd/wVecXV5LGHt+IvIZlbhpJTo/0+reZRjqXpCDfgkKxOkcFXRY/htiGNWMHs1z/
b1w57xPbd+faYi2eVTy2WMD3CxYqhDdpegArkt9UPuZQCBpu6Dg4fAfRzr1X6le+Lvs3/UIc/ZE
Ced15IB+x188TPED1d+tGpDWAwQtl00L8wppd5K7THfpK1m+li15ake+a/mqDW12SZoO8FvlWrB
```

```
PYL6AMMpTTSydAaRsGyFZctl2isxGW1GFdnydfhONJqDXR8xRxZosOWdDUcwtBt9llgWYyMVoGp
QO6JBX9hgMsYuZPKj8Ted8YxzaHMoHD9hsZ4juFnEaaPpE=</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
<ds:Object>
<xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#"
 Target="#id-263fad5a62a0580a1c44a0de0d22fc40">
<xades:SignedProperties Id="xades-id-263fad5a62a0580a1c44a0de0d22fc40">
<xades:SignedSignatureProperties>
<xades:SigningTime>2023-07-08T12:04:43Z</xades:SigningTime>
<xades:SigningCertificateV2>
<xades:Cert>
<xades:CertDigest>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha512"/>
<ds:DigestValue>XREsyKj66WMyQapIL6qcxR7FACpDx5bui8on3EccOzZold1TW8ZF4xj4S90
zQ8yB5gimW6DdpeK/M5nrum8mRQ==</ds:DigestValue>
</xades:CertDigest>
<xades:IssuerSerialV2>MIGNMIGEpIGBMH8xCzAJBgNVBAYTAkNaMSgwJgYDVQQDDB9JLkNBI
FF1YWxpZmllZCAyIENBL1JTQSAwMi8yMDE2MS0wKwYDVQQKDCRQcnZuw60gY2VydGlmaWthxI1u
w60gYXV0b3JpdGEsIGEucy4xFzAVBgNVBAUTDk5UUkNaLTI2NDM5Mzk1AgQAuIrl</xades:Iss
uerSerialV2>
</xades:Cert>
</xades:SigningCertificateV2>
</xades:SignedSignatureProperties>
<xades:SignedDataObjectProperties>
<xades:DataObjectFormat ObjectReference="#r-id-
263fad5a62a0580a1c44a0de0d22fc40-1">
<xades:MimeType>text/plain</xades:MimeType>
</xades:DataObjectFormat>
</xades:SignedDataObjectProperties>
</xades:SignedProperties>
</xades:QualifyingProperties>
</ds:Object>
</ds:Signature>
</SymetricKey>
```

```
<xenc:EncryptedData
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:dsig11="http://www.w3.org/2009/xmldsig11#"
    xmlns:xenc11="http://www.w3.org/2009/xmlenc11#"
    Type="http://www.w3.org/2001/04/xmlenc#">

  <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
  <!-- describes the encrypted AES content encryption key -->
  <ds:KeyInfo>
    <xenc:EncryptedKey>
      <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes128"/>
      <!-- describes the key encryption key -->
      <ds:KeyInfo>
        <xenc:AgreementMethod
Algorithm="http://www.w3.org/2009/xmlenc11#ECDH-ES">
          <xenc11:KeyDerivationMethod
Algorithm="http://www.w3.org/2009/xmlenc11#ConcatKDF">
            <xenc11:ConcatKDFParams AlgorithmID="00" PartyUInfo=""
PartyVInfo="">
```

```
                <ds:DigestMethod
    Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
              </xenc11:ConcatKDFParams>
            </xenc11:KeyDerivationMethod>
            <xenc:OriginatorKeyInfo>
              <ds:KeyValue>
                <dsig11:ECKeyValue>
                  <!-- ephemeral ECC public key of the originator -->
                </dsig11:ECKeyValue>
              </ds:KeyValue>
            </xenc:OriginatorKeyInfo>
            <xenc:RecipientKeyInfo>
              <ds:X509Data>
                <ds:X509SKI></ds:X509SKI>
                <!-- hint for the recipient's private key -->
              </ds:X509Data>
            </xenc:RecipientKeyInfo>
          </xenc:AgreementMethod>
        </ds:KeyInfo>
        <xenc:CipherData>
          <xenc:CipherValue><!-- encrypted AES content encryption key --
    ></xenc:CipherValue>
        </xenc:CipherData>
      </xenc:EncryptedKey>
    </ds:KeyInfo>

    <xenc:CipherData>
      <xenc:CipherValue>
        <!-- encrypted data -->
      </xenc:CipherValue>
    </xenc:CipherData>

  </xenc:EncryptedData>
```

<SymetricKey>

<AccessRole>ADMIN_access</AccessRole>

<KeyType>KEK</KeyType>

<KeyType>KEK</KeyType>

<KeyType>KEK</KeyType>

<KeyType>KEK</KeyType>

<KeyAlgorithm>AES256</KeyAlgorithm>

<A>

<KeyValueEncrypted><xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Type="http://www.w3.org/2001/04/xmlenc#Element"><xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/><dsig:KeyInfo xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"><xenc:EncryptedKey><xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/><xenc:CipherData><xenc:CipherValue>JfEkiG2aatWTy+Rdk/mCPu1UNENhFEawbZarmmDZJ2bmiD7y+ATm6nqfhLLDE7Yw4/GJvj6ZfDwaSwWQkI7nxD7B8Hyca15jbg2hI74SYB1564pASthY6cTOBWeDhj/im0Jf5E/EsTmxiR8E0F5Pz8+c9v4DtfrVVUPCKpXYmeZT5bufrEKem7uPvW7qXuzCV/hVTZ1zPbGSW2grBWj63be3/QuB7FSQg++YdyDY4if12hTGB1x0RcnBpqMAtoPScaE8S78PQa+8TKz2xzIl5

1O+TR+624wKYyWTInCshM/qXhUI8Bypfns2JZEwYGQtCeVV1W/jxYatFWjbP84xkg==</xenc:CipherValue></xenc:CipherData></xenc:EncryptedKey></dsig:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>eTKU+lo/jnaxK5VrCgAO0pPruxgI7VtMG0ZAI3L1kv+RENNlssmHW7CH4NS21+Y6CAqEn0CSmBv67RwDnkFfWQ==</xenc:CipherValue>

</xenc:CipherData>

</xenc:EncryptedData></KeyValueEncrypted></A>

<KeyValueEncrypted><xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Type="http://www.w3.org/2001/04/xmlenc#Element"><xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/><dsig:KeyInfo xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"><xenc:EncryptedKey><xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/><xenc:CipherData><xenc:CipherValue>T93L++n62H8W/Qnjk2jfwNfNkfeUTDz7WyxoSsk77o0IRABKgYp45VuLlPVru67a7M6VZZ/jq4rzy+Yg7Hd4nVubWUnrxFZvcJvd6frgj5aCmSrDxl22bxV7OK3ssMo6Z27rZVeUzKDubzR3gqS72T+Cx0lJsLDCl6Kbc692s8qYBaqKBzDZ6JByqt2QBv0B02478Z2w+2dfXKJIbYrV6y5anGVsFkWyNf2tNj6TyejVBRts3yAnaVwxZ4YafanDa72fXNK5iQb7YOuT+CTjLDnst4XBr/JMaY7GdIwl4buwE4Yt0zAg0dmbuCfvDq5jzPEkhAiNZUWN7teWuBDlKw==</xenc:CipherValue></xenc:CipherData></xenc:EncryptedKey></dsig:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue>2COJfm3VQoR1/H4xcsyUforve4rxVqMEf7WK9D1yrgZjyKgn6cLHf+zYJ0RAT5kp5EaT3Nvv2H0Fs8B799nIDXXLZ8/NiZwkNk/WCCLrwY8=</xenc:CipherValue>

</xenc:CipherData>

</xenc:EncryptedData></KeyValueEncrypted></SymetricKey>