ZPA Smart Energy
Going the Smarter Way

SW ReadEn

a AMM elektroměry

Pavol Rybárik
ZPA SE
Projektová skupina

ReadEn odečtová centrála

- Moderní aplikace pro **sběr a rozbor odečtů** měřidel energií s podporou zabezpečení komunikace dle platné legislativy.
- Výkonná SW **služba pro energetický management**, VEE, fakt. podklady, reporting na OTE a EDC.
- **Obousměrná komunikace** s chytrými měřidly, včetně příjmu PUSH zpráv z AMM měřidel.
- Napojení na **KMS systém ProID** – “trezor” pro uložení krypto materiálu AMM měřidel.

ReadEn Edice

- **ReadEn Lite** pro PC
  Neobsahuje KMS, krypto materiál uložen v DB ReadEn.
  Určeno pro desítky měřidel.
- **ReadEn Professional** serverové řešení pro provoz přímo v LDS (On premise)
  Kompletní řešení včetně KMS ProID.
  Určeno pro neomezený počet měřidel.
- **ReadEn IMU** cloudové řešení dostupné jako služba (SaaS)
  Kompletní řešení poskytované jako SW služba.
  Přístup přes webový portál.

ReadEn rozhraní na IT okolí

Rozhraní ReadEn vůči ostatním IT systémům - podle složitosti formátu a obsahu dat lze použít různé přístupy:

- **Import / Export úlohy**

Cílem exportních úloh mohou být soubory (TXT, XML, …) nebo sdílené databázové tabulky včetně tabulek v jiné databázi.

- **Service / Webservice**

Pro složitější a více sofistikovaná rozhraní poskytuje systém samostatné aplikace typu service (služba).

- **Rozhraní pro GIS, CRIS, OTE, EDC, ČHMÚ…**

Jedná se o služby operačního systému s plánovačem, které dokáží načítat data z externích zdrojů a publikují SOAP metody pro případné volání z externích systémů.

ZPA Smart Energy a.s. nabízí

- Přípravu projektu a poradenství
- Dodávku / výměnu měřidel
- Hardware
  Vybudování (doplnění) komunikační infrastruktury
- Software
- Provozní podporu
- Školení

Příloha č. 4 k vyhlášce č. 359/2020 Sb.

Minimální kryptografické požadavky
Zajištění důvěrnosti
Použití blokové šifry **AES-256**
Zajištění důvěrnosti a integrity
Použití módu blokové šifry **GCM**, CCM
Zajištění integrity
Digitální podpis DSA 3072, **EC-DSA-256**, RSA 3072
Hashe SHA2-256, **SHA3-256**
Mód pro ochranu integrity **HMAC**, CMAC
Zajištění klíčového managementu
DH-3072, **ECDH-256**
Generátor náhodných bitů
HMAC_DRBG, Hash _DRBG oba pro SHA2 a SHA3

Příloha č. 4 k vyhlášce č. 359/2020 Sb.

Technické požadavky na měření typu C kategorií C1, C2 - kráceno

7	Bezpečnostní události musí být zaznamenány a reportovány, log musí být chráněn proti modifikaci a smazání, velikost min. pro 1000 bezpečnostních záznamů
9	Data ve zprávách musí být šifrována
12	Přístup do prvků zpracovávajících citlivé údaje vyžaduje proniknutí bezpečnostním perimetrem s plombou
13	Kryptografická pověření musí být pro elektroměr unikátní a bezpečně uložena, nesmí po zcizení způsobit snížení bezpečnosti jiného elektroměru
14	Oddělení funkcionalit měření a komunikace
15	Vzdálená aktualizace bezpečnostních funkcionalit a kryptografických primitiv
16	Vzdálená aktualizace kryptografických pověření

AMM ELM s DLMS SS2
příklad krypto materiálu

jT#rw?Xej$gh0;D

TrSzX/m4SBD4m/NOvspQcfbb37lSouGd6lyHS4sFtk2cJm831FCj7bKSRi8SebOm
5tisS9pAYpEQFagOzvTKh0Sc1HY0PDmouzyXqMwkR6baEP7tNVozXhKkZW4T59mk
4CwmFxhPYwH0g1+eesKmMXcA8PusObhxMxBF6MXXWfaI0TSHQEWw3t2oqAIjJjne

6l16keUv8hLcxhXnNKE8VOd1Qw1l6tnTJxwnFC4Uf8Iz1vHKKIBvjjN+4ebceyuX
k/23J3FbUifIF78W7sBA2m4o4KC0p/9E0k/8skZusJ3ujPLcqslRe09Jo7OdUy9O
zptVUZxGJeUiD9eaMfv0MaDLQYyoPn61AUm8SfM1xTd8CZ/UTbVYP0cN1X3/PZwS

9TOwaLcIs0a1+dlv4kD9BvbxHM6XMp3Z8Mf58S17X07Q+3EyEqPVB0zG1znIEI4p
2i0io+EYo5E0O5XHDpvTCvkwRjZ/GmNeHqvIqjqNFd6JnD/N4ij0IMrU0CubI120
X3sZBjjvxQKjpG3B1W6v4OmBAXZw8v97ry2E9v+ESDX0U3LRY46+7Fj0nE7Z0OH8
il2EnLfhedk+jc5HMQuqweGx8tlaEt06FaM/pZS61EoI4CJqmMb67+4O7l1uXyiM

3K4b0CJ3J5xTir+FK7QFTwoVqGvGXEFNiW5DQ1CoBvhYiyKelRxWUF0pxL16lJTz
daG4M652Y/2m7ZrU9Amup8vLd8KBSJhS43AFSUzEoHMuBQGaP1ggn8roE/k838xB
GBHJcCJMdlG05cUbAto6B1yKwZsar7BkvHaXGRwXLdmU0J85Pcv0Y0WX2MiUQZor
r57GO0sl/w0+/T7RUn6gO7ysiNiw3I1oa5VMDnVssYyiXqpAqiChfO4gY2vtSQ/x

Y9uc475Tf5o5Xgx2Ao/nzoScg7VAqZ4AP1MubS6Zn2ub1/MN6MhuceR7rnDsW75F
89LCJYPzd/j2tFXShmR+61bCQkW1yDhOYqCv04czzAOvcitDpXY45MISQLDtJsTo
P9qqgt5G9Ttgm/Nd4kPGrgewOy3CozXMlfNP679jBB4CGKdL2LYf9MtbVbqMZguf
5m9v/NpVEbaub3Uq/BeZgY8x6UUjmRMJa6Z5hYEdnzj/cZj0sxQwXgYJ7DsSnz4r

f0ca8970539f62322a260916aea587a4b8b8b8e8