webdyn
Flexitron group

WebdynEasy W M-Bus

Application Note

AES128 CBC Encryption

Table of contents

1 Chiffrement AES128 des fichiers BSON 3
1.1 Objet 3
1.2 Principe 3
1.3 Paramètres 3
1.4 Firmware V4.0 et supérieur 4
1.5 Format du fichier chiffré 4
1.6 Procédure de déchiffrement 4
1.6.1 Pour les firmwares V4.0 et supérieurs : 4
1.6.2 Pour les firmwares antérieurs à la V4.0 : 4
1.7 Exemple de configuration 4

1 Chiffrement AES128 des fichiers BSON

1.1 Objet

Cette note d'application décrit le mécanisme de chiffrement des fichiers BSON utilisés par la WebdynEasy Wireless M-Bus.

Elle s'adresse aux intégrateurs souhaitant générer ou déchiffrer des fichiers de configuration compatibles avec le concentrateur.

1.2 Principe

Le concentrateur peut protéger les fichiers BSON par chiffrement AES afin d'assurer leur confidentialité.

> **Warning**
>
> Depuis le Firmware V4.02, toutes les passerelles ont le chiffrement activé avec une clé unique par produit.

Lorsque le chiffrement est activé :

- tous les fichiers BSON sont chiffrés en AES-128 mode CBC ;
- le fichier chiffré reçoit l'extension `.aes`.

Par exemple :

Fichier BSON	Fichier chiffré
`123456-config.bson`	`123456-config.bson.aes`

1.3 Paramètres

Paramètre	Valeur
Algorithme	AES-128
Mode	CBC
Taille de clé	128 bits (16 octets)
Taille du vecteur d'initialisation (IV)	16 octets
Padding	PKCS#7 (PKCS5Padding dans certaines bibliothèques)
Encodage de la clé dans le fichier JSON	Base64

La clé AES est renseignée dans le champ :

`config.security.key`

au format Base64.

Exemple :

```
Hex :
44:00:AA:F7:83:78:04:9C:AB:13:EE:4E:35:0E:28:1B

Base64 :
RACq94N4BJyrE+5ONQ4oGw==
```

1.4 Firmware V4.0 et supérieur

À partir de la version V4.0 :

- un IV aléatoire est généré à chaque chiffrement ;
- l'IV est ajouté à la fin du fichier chiffré ;
- l'IV doit être différent à chaque génération afin de respecter les bonnes pratiques cryptographiques.

Le paramètre :

`config.security.aesLegacy`

permet de conserver le comportement historique (IV fixe) lorsque cela est nécessaire pour assurer la compatibilité avec les anciens firmwares.

1.5 Format du fichier chiffré

Pour les firmwares V4.0 et supérieurs, le fichier est constitué de :

```
+----------------------+------------------+
| Ciphertext           | IV (16 octets)   |
+----------------------+------------------+
```

où :

le ciphertext est le résultat du chiffrement AES-128-CBC ; l'IV correspond aux 16 derniers octets du fichier ; l'IV est stocké sous forme de données binaires.

1.6 Procédure de déchiffrement

1.6.1 Pour les firmwares V4.0 et supérieurs :

- Lire les 16 derniers octets du fichier.
- Utiliser ces 16 octets comme IV.
- Considérer le reste du fichier comme le ciphertext.
- Déchiffrer en AES-128-CBC.
- Retirer le padding PKCS#7.
- Le résultat obtenu correspond au fichier BSON d'origine.

1.6.2 Pour les firmwares antérieurs à la V4.0 :

- utiliser l'IV fixe défini au §4 ;
- considérer l'intégralité du fichier comme le ciphertext.

1.7 Exemple de configuration

```
{
  "config": {
    "security": {
      "crcMode": 1,
```

```
        "encryption": true,
        "key": {
          "$type": "00",
          "$binary": "RACq94N4BJyrE+5ONQ4oGw=="
        }
      }
    },
    "crc": 0
}
```