



WebdynEasy Wireless M-bus
Application Note

HTTP(s) Specifications



Table of contents

1	Spécifications HTTP(s)	3
1.1	Introduction	3
1.2	Configuration	3
1.3	HTTP/HTTPS	4
1.3.1	Demandes	4
1.3.2	Sécurité	6
1.3.3	Gestion des erreurs	6
1.4	Description fonctionnelle	6
1.4.1	Envoyer les données vers le serveur	6
1.4.2	Envoyer l'alerte au serveur	7
1.4.3	Transférer la supervision vers le serveur	8
1.4.4	Envoyer le journal vers le serveur	8
1.4.5	Vérifiez la configuration connue par le serveur	8
1.4.6	Mettre à jour la configuration connue du serveur	9
1.4.7	Vérifier le contenu de la boîte de réception	10
1.4.8	Récupérer le fichier de la boîte de réception	11
1.4.9	Insérer la mention de remerciement	11
1.5	Exemples	11
1.5.1	Mise à jour des commandes et de la configuration	11
1.6	Annexe	14
1.6.1	Version SSL prise en charge	14
1.6.2	Suites de chiffrement SSL prises en charge	15



1 Spécifications HTTP(s)

1.1 Introduction

Ce document présente l'utilisation du protocole HTTP par la passerelle WebdynEasy Wireless M-bus pour le transfert de fichiers.

Afin d'assurer la compatibilité avec les portails utilisant des services cloud sur lesquels le protocole FTP n'est pas disponible, nous introduisons le protocole de transfert HTTP en complément du protocole FTP.

Le protocole HTTP sera utilisé pour télécharger des fichiers sur le serveur (données, supervision, alarmes, etc.) et pour récupérer les fichiers de configuration et de commandes.

La mise en œuvre du client HTTP est assurée par le modem BG95. Le protocole HTTPS est également pris en charge.

Le protocole HTTP/HTTPS s'appuie sur le contenu actuel des fichiers FTP ; seule la couche de transport est mise à jour, la charge utile reste inchangée. Les fonctionnalités et les fichiers associés sont remappés vers des requêtes HTTP/HTTPS.

Warning

Il n'est pas possible de configurer le produit pour qu'il utilise les deux protocoles simultanément ; leur utilisation est exclusive.

1.2 Configuration

Pour des raisons de compatibilité, les paramètres HTTP seront stockés dans l'objet `configuration.remote.ftp` de la configuration de la passerelle.

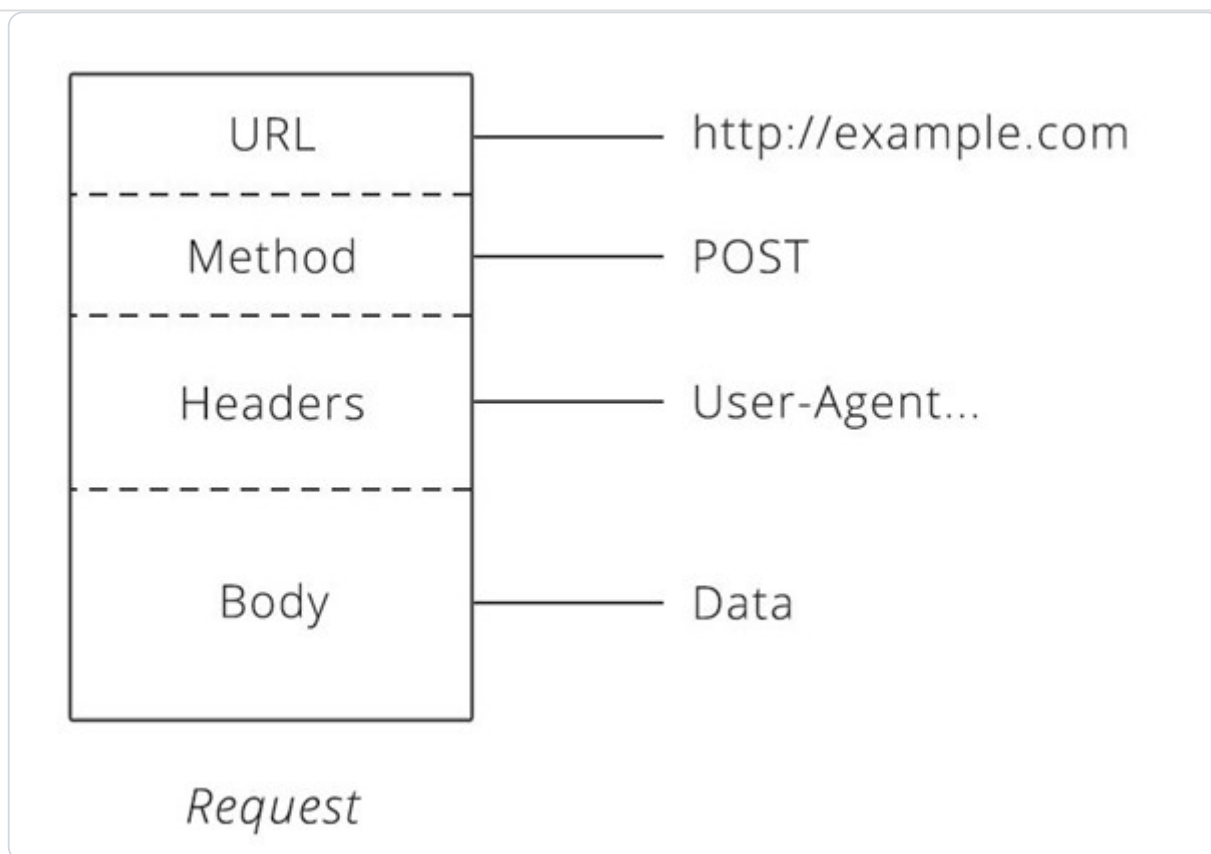


Répertoire	Type	Valeur
/remote/ftp/ mode	Entier	0 : FTP 1 : : FTPS 2 : FTPS + certificats 3 : HTTP 4 : HTTPS 5 : HTTPS + certificats
/remote/ftp/ addr	Chaîne de caractères	Adresse du serveur. Elle peut être numérique ou symbolique. Si le port n'est pas le 80, il doit être ajouté à la fin de l'adresse, après « : ». La longueur maximale est de 128 caractères.
/remote/ftp/ user	Chaîne de caractères	nom d'utilisateur pour l'authentification HTTP
/remote/ftp/ pass	Chaîne de caractères	mot de passe pour l'authentification HTTP
/remote/ftp/ dir	Chaîne de caractères	Chemin d'accès de l'URL La longueur maximale est de 128 caractères.
/remote/ftp/ cacert	Chaîne de caractères	Certification du certificat d'autorité racine
/remote/ftp/ clientcert	Chaîne de caractères	Certificat signé pour le client
/remote/ ftpclientkey	Chaîne de caractères	clé privée pour le client

1.3 HTTP/HTTPS

1.3.1 Demandes

Les requêtes HTTP/HTTPS sont les suivantes :



http request

WebdynEasy W-MBUS respecte les conventions suivantes :

- **URL:** Identifier des objets ou des conteneurs uniques à l'aide d'une adresse unique
- **METHOD:** Les méthodes suivantes sont implémentées :
 - **HTTP/GET** : Récupérer une ressource identifiée par l'URL
 - Corps de la requête : AUCUN
 - Corps de la réponse : BSON pour l'objet demandé ou liste du contenu du conteneur pour les conteneurs
 - **HTTP/PUT** : Modifier ou effacer une ressource
 - Corps de la requête : JSON pour les données modifiées (qui seront fusionnées avec l'objet existant)
 - Corps de la réponse : JSON issu de l'objet modifié
 - **HTTP/POST** : Créer une ressource
 - Corps de la requête : BSON pour l'objet à créer
 - Corps de la réponse :
- **HEADERS** : les en-têtes suivants sont fournis par WebdynEasy W-MBUS
 - Content-Type : application/octet-stream
 - Autorisation : Basic QWxhZGRpbjpvGVuIHNIc2FtZQ== (identifiant et mot de passe conformes à la spécification d'authentification de base)
 - Content-Length : <longueur de la charge utile>

Les en-têtes suivants doivent être fournis par le serveur

- Content-Length : <longueur de la charge utile>
- Content-Type : application/octet-stream

Dans le protocole HTTPS, le protocole TLS et la suite de chiffrement sont décrits en détail en annexe. Le modem BG95 prend en charge le protocole SSL/TLS pour assurer la sécurité des communications. Il est possible d'utiliser une authentification simple par identifiant et mot de passe ou de recourir à des certificats.



Note

Si l'on utilise des certificats et des clés, il faut d'abord charger les fichiers dans la mémoire du modem à l'aide de la commande « certificate ».

Note

Veuillez noter que les protocoles HTTP/HTTPS sont gérés par la couche Quectel ; aucune modification ne peut être apportée au niveau de cette couche.

1.3.2 Sécurité

Le modem BG95 prend en charge le protocole SSL/TLS pour assurer la sécurité des communications. Il est possible d'utiliser une authentification simple par identifiant et mot de passe ou de recourir à des certificats.

Note

Si l'on utilise des certificats et des clés, il faut d'abord charger les fichiers dans la mémoire du modem à l'aide de la commande « certificate ».

1.3.3 Gestion des erreurs

Les commandes HTTP ont un délai d'expiration de 300 secondes. Si une commande a échoué, une nouvelle tentative est effectuée.

1.4 Description fonctionnelle

1.4.1 Envoyer les données vers le serveur

Demande

```
POST /DATA/<UID>-<TimeStamp>-data.bson
POST /DATA/<UID>-<TimeStamp>-data.bson.aes (if AES encryption is used)
```

Parameters

- **UID** : Identifiant unique de la passerelle
- **TimeStamp** : horodatage des données

Example

```
POST /DATA/499198-1690876878-data.bson
```

Données utiles de la requête

```
<Bson file contents>
```



Données utiles de réponse

```
<empty>  
content-length=0
```

Exemple de transfert de fichier (capture TCP)

Request

```
POST /DATA/499198-1690876878-data.bson HTTP/1.1  
Host: 172.20.30.1:8000  
Accept: */*  
User-Agent: QUECTEL_MODULE  
Connection: Keep-Alive  
Content-Type: application/octet-stream  
Content-Length: 6832
```

Reply

```
HTTP/1.0 200 OK  
Server: minimal_dav Python/3.8.10  
Date: Thu, 11 Jan 2024 14:49:25 GMT  
Last-modified: Thu, 11 Jan 2024 13:22:31 GMT  
Content-length: 0
```

1.4.2 Envoyer l'alerte au serveur

Demande

```
POST /ALARM/<UID>-<TimeStamp>-alarm.bson  
POST /ALARM/<UID>-<TimeStamp>-alarm.bson.aes (if AES encryption is used)
```

Parameters

- **UID** : Identifiant unique de la passerelle
- **TimeStamp** : horodatage des données

Données utiles de la requête

```
<Bson file contents>
```

Données utiles de réponse

```
<empty>  
content-length=0
```



1.4.3 Transférer la supervision vers le serveur

Demande

```
POST /SUPERVISION/<UID>-<TimeStamp>-supervision.bson
POST /SUPERVISION/<UID>-<TimeStamp>-supervision.bson.aes (if AES encryption is used)
```

Parameters

- **UID** : Identifiant unique de la passerelle
- **TimeStamp** : horodatage des données

Données utiles de la requête

<Bson file contents>

Données utiles de réponse

<empty>
content-length=0

1.4.4 Envoyer le journal vers le serveur

Demande

```
POST /SUPERVISION/<UID>-<TimeStamp>-log.bson
POST /SUPERVISION/<UID>-<TimeStamp>-log.bson.aes (if AES encryption is used)
```

Parameters

- **UID** : Identifiant unique de la passerelle
- **TimeStamp** : horodatage des données

Données utiles de la requête

<Bson file contents>

Données utiles de réponse

<empty>
content-length=0

1.4.5 Vérifiez la configuration connue par le serveur

Note

La synchronisation de la configuration s'effectue en deux étapes :

- vérifier la configuration connue du serveur



- mettez à jour la configuration si nécessaire

Demande

```
GET /CONFIG/<UID>
```

Parameters

- **UID** : Identifiant unique de la passerelle

Données utiles de réponse

Vide si le serveur ne dispose d'aucune configuration connue

```
<empty>  
content-length=0
```

Ou une configuration connue du serveur, respectant la même convention de nommage que le protocole FTP

```
<UID>-<TimeStamp>-config.bson  
<UID>-<TimeStamp>-config.bson.aes (if AES encryption is used)
```

Info

Si la réponse est vide (content-length=0) ou si le nom de fichier fourni ne correspond pas à la configuration locale, ALORS la configuration est envoyée au serveur

Exemple

```
499198-1690876878-config.bson
```

1.4.6 Mettre à jour la configuration connue du serveur

Note

La synchronisation de la configuration s'effectue en deux étapes :

- vérifier la configuration connue du serveur
- mettez à jour la configuration si nécessaire

Demande

```
POST /CONFIG/<UID>-<TimeStamp>-log.bson  
POST /CONFIG/<UID>-<TimeStamp>-log.bson.aes (if AES encryption is used)
```

Parameters

- **UID** : Identifiant unique de la passerelle
- **TimeStamp** : horodatage des données



Données utiles de la requête

```
<Bson file contents>
```

Données utiles de réponse

```
<empty>  
content-length=0
```

1.4.7 Vérifier le contenu de la boîte de réception

La gestion du contenu de la boîte de réception s'effectue en suivant les étapes suivantes :

- vérifier le contenu de la boîte de réception (noms des fichiers) Ensuite, pour chaque fichier
- Récupérer le fichier de la boîte de réception
- Traitez le fichier conformément à la documentation de WebdynEasy
- INSÉRER la mention de reconnaissance.

Une fois l'accusé de réception envoyé, le serveur doit considérer que la commande a été traitée et doit supprimer le fichier de commande du contenu de la boîte de réception.

Demande

```
GET /INBOX/<UID>
```

Parameters

- **UID** : Identifiant unique de la passerelle

Données utiles de réponse

Vide s'il n'y a aucun fichier en attente dans la boîte de réception

```
<empty>  
content-length=0
```

Ou une liste de fichiers en attente dans la boîte de réception, séparés par un point-virgule. Les noms de fichiers respectent la convention de nommage FTP.

```
<UID>-<TimeStamp>-cfg.bson  
<UID>-<TimeStamp>-cmd.bson  
<UID>-<TimeStamp>-xxx.bson  
  
<UID>-<TimeStamp>-cfg.bson.aes (if AES encryption is used)  
<UID>-<TimeStamp>-cmd.bson.aes (if AES encryption is used)  
<UID>-<TimeStamp>-xxx.bson.aes (if AES encryption is used)
```

Info

Si la réponse est vide (content-length=0) ou si le nom de fichier fourni ne correspond pas à la configuration locale, ALORS la configuration est envoyée au serveur



Example

```
499198-1690876878-cfg.bson
```

1.4.8 Récupérer le fichier de la boîte de réception

Demande

```
GET /INBOX/<filename>
```

Parameters

- **filename** : récupéré par la requête précédente. Comme indiqué, il respecte la règle de nommage FTP

Données utiles de réponse

```
<Bson file contents>
```

Contenu de la réponse

```
<empty>  
content-length=0
```

1.4.9 Insérer la mention de remerciement

Demande

```
PUT /INBOX/<filename>
```

Parameters

- **filename** : récupéré par la requête précédente. Comme indiqué, il respecte la règle de nommage FTP

Données utiles de réponse

```
<Bson file contents>
```

Contenu de la réponse

```
<empty>  
content-length=0
```

1.5 Exemples

1.5.1 Mise à jour des commandes et de la configuration

Dans cet exemple, le sous-répertoire « inbox » de la passerelle contient 2 fichiers.



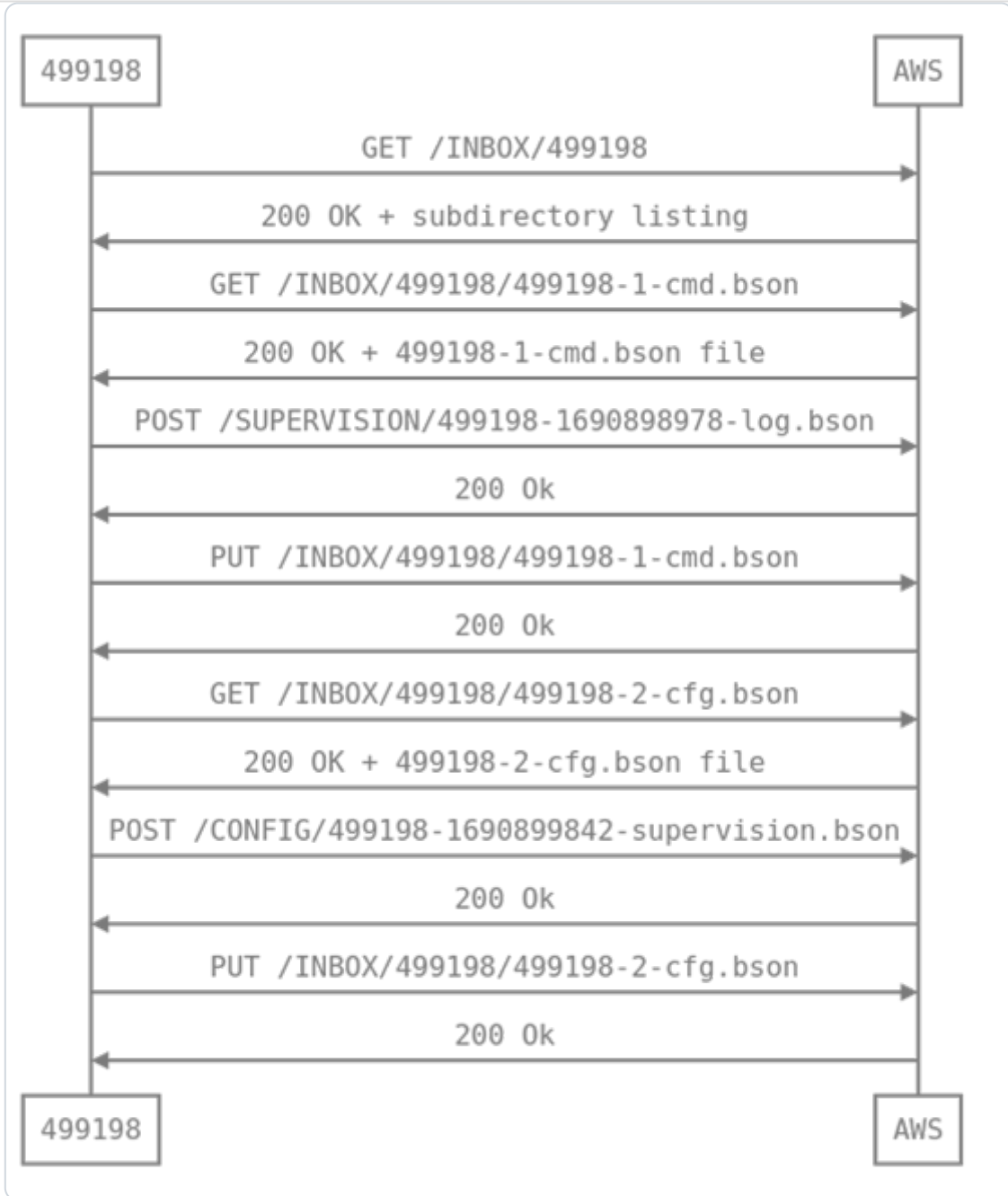
499198-1-cmd.bson

```
{
  "cmd": [
    {
      "type": "logGet",
      "cid": "1"
    }
  ],
  "crc": 2040707386
}
```

Cette commande demande à la passerelle de télécharger le fichier journal. 499198-2-cfg.bson

```
{
  "config": {
    "radio": {
      "manufFilter": {
        "$binary": "j\lw=",
        "$type": "00"
      }
    }
  },
  "crc": -1156637560
}
```

Il s'agit d'une simple mise à jour d'un paramètre dans la configuration. Diagramme de séquence :



http request2

Inbox Listing Request:

```
GET /INBOX/499198 HTTP/1.1
Host: 172.20.30.1:8000
Accept: */*
User-Agent: QUECTEL_MODULE
Connection: Keep-Alive
```

Subdirectory listing answer:

```
HTTP/1.0 200 OK
Server: minimal_dav Python/3.8.10
Date: Thu, 11 Jan 2024 14:49:25 GMT
Last-modified: Thu, 11 Jan 2024 13:22:31 GMT
Content-length: 38
```



499198-1-cmd.bson;499198-2-cfg.bson

Command file download request:

```
GET /INBOX/499198/499198-1-cmd.bson HTTP/1.1
Host: 172.20.30.1:8000
Accept: */*
User-Agent: QUECTEL_MODULE
Connection: Keep-Alive
```

Answer:

```
HTTP/1.0 200 OK
Server: minimal_dav Python/3.8.10
Date: Thu, 11 Jan 2024 14:49:25 GMT
Last-modified: Thu, 11 Jan 2024 13:22:31 GMT
Content-length: 60

<499198-1-cmd.bson file>
```

1.6 Annexe

1.6.1 Version SSL prise en charge

- TLS 1.2



1.6.2 Suites de chiffrement SSL prises en charge



Code des suites de chiffrement	Nom des suites de chiffrement
0x0035	TLS_RSA_WITH_AES_256_CBC_SHA
0x002F	TLS_RSA_WITH_AES_128_CBC_SHA
0x0005	TLS_RSA_WITH_RC4_128_SHA
0x0004	TLS_RSA_WITH_RC4_128_MD5
0x000A	TLS_RSA_WITH_3DES_EDE_CBC_SHA
0x003D	TLS_RSA_WITH_AES_256_CBC_SHA256
0xC002	TLS_ECDH_ECDSA_WITH_RC4_128_SHA
0xC003	TLS_ECDH_ECDSA_AVEC_3DES_EDE_CBC_SHA
0xC004	TLS_ECDH_ECDSA_AVEC_AES_128_CBC_SHA
0xC005	TLS_ECDH_ECDSA_AVEC_AES_256_CBC_SHA
0xC007	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
0xC008	TLS_ECDHE_ECDSA_AVEC_3DES_EDE_CBC_SHA
0xC009	TLS_ECDHE_ECDSA_AVEC_AES_128_CBC_SHA
0xC00A	TLS_ECDHE_ECDSA_AVEC_AES_256_CBC_SHA
0xC011	TLS_ECDHE_RSA_WITH_RC4_128_SHA
0xC012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
0xC013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
0xC014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
0xC00C	TLS_ECDH_RSA_WITH_RC4_128_SHA
0xC00D	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
0xC00E	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
0xC00F	TLS_ECDH_RSA_AVEC_AES_256_CBC_SHA
0xC023	TLS_ECDHE_ECDSA_AVEC_AES_128_CBC_SHA256
0xC024	TLS_ECDHE_ECDSA_AVEC_AES_256_CBC_SHA384
0xC025	TLS_ECDH_ECDSA_AVEC_AES_128_CBC_SHA256
0xC026	TLS_ECDH_ECDSA_AVEC_AES_256_CBC_SHA384
0xC027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
0xC028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384



Code des suites de chiffrement	Nom des suites de chiffrement
0xC029	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
0xC02A	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
0xC02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
0xFFFF	Prise en charge de toutes les suites de chiffrement ci-dessus