



25.10.2012

---

## Bulletin à l'intention des caisses de compensation AVS et des organes d'exécution des PC No 317

---

### Adaptation technique des accès KSSL-SSL

**Ce bulletin s'adresse en particulier aux responsables techniques des organes d'exécution. Il concerne l'accès au réseau AVS/AI.**

Tous les organes d'exécution qui communiquent par le réseau AVS/AI, qui utilisent le gateway SSL de l'OFIT pour accéder à des applications (p.ex. Telezas3) et qui utilisent l'accès „xxx.kssl.admin.ch“ pour cela, sont priés d'adapter leurs paramétrages avec le nouvel accès „xxx.ssl.admin.ch“ et d'ouvrir sur leurs firewall l'adresse IP 162.23.92.26 avec le port 443.

**L'ancienne adresse du gateway sera hors service dès le 31.12.2012; c'est pourquoi la modification doit être effectuée auparavant.**

Les accès aux services qui se font par „Internet“ sont déjà effectués par „xxx.ssl.admin.ch“ (gateway «Rossini», 162.23.37.24).

Les accès aux services qui se font par „AHV-IV-NETZ“ (le réseau AVS/AI) sont encore effectués avec „xxx.kssl.admin.ch“ (gateway «Verdi», 131.102.106.10).

L'OFIT a mis en place une CAZ (Central Access Zone) qui permet d'utiliser le même gateway depuis „Internet“, „KOMBV-KTV“ et „AHV-IV-NETZ“..

Depuis 2011, l'OFIT migre les accès des gateways «Rossini» et «Verdi» sur le nouveau gateway (ACC5). La migration est aussi nécessaire car les gateways actuels sont anciens et ne répondent plus à la nouvelle génération.

Avec la CAZ, un nouveau gateway-SSL accessible depuis „Internet“, „KOMBV-KTV“ et „AHV-IV-NETZ“ est mis à disposition avec un seul accès: „xxx.ssl.admin.ch“.

### Qu'est-ce qui doit être modifié d'ici fin 2012 ?

1. Modifier tous les accès „xxx.kssl.admin.ch“ en „xxx.ssl.admin.ch“.
2. La nouvelle adresse du gateway SSL (ACC5) est: adresse IP = 162.23.92.26 avec le port = 443

Les organes d'exécution doivent ouvrir l'adresse IP 162.23.92.26 avec le port 443 jusqu'au 31.12.2012 et désactiver l'accès par les gateways «Rossini» et «Verdi».

La résolution de la zone DNS „admin.ch“ demeure par KNS1 et KNS2.

L' URL ci-après permet de tester si les accès fonctionnent avec le nouveau paramétrage  
<https://service.ssl.admin.ch>

## Résultat

### Test effectué avec succès



#### SSL-Access Service

##### SSL-Access Testseite

Diese Seite zeigt Informationen aus dem Benutzerzertifikat.

##### Page test SSL-Access

Cette page montre des informations du certificat client.

DATE_LOCAL:	17 Oct 2012 11:21:44 GMT
CLIENT_IP:	178.197.232.95
SERVER_IP:	162.23.92.26
SERVER_NAME:	service.ssl.admin.ch

**SSL\_RESULT:** ok

SSL_ISSUER:	CN=AdminCA-CD-T01,OU=Certification Authorities,OU=Services,O=admin,C=CH
SSL_START	Feb 7 09:09:04 2012 GMT
SSL_END	Feb 7 09:09:04 2014 GMT
SSL_ALGORITHM	sha1WithRSAEncryption
SSL_SUBJECT	CN=Hayoz Xavier YJIEWC,OU=Anwendungen,OU=Weisse Seiten,O=admin,C=CH
SSL_RSA_BITS	1024
SSL_KEY_TYPE	RSA
SSL_CIPHER_NAME	AES256-SHA
SSL_CIPHER_VERSION	TLSv1
SSL_CIPHER_BITS	256

### Echec du test



#### SSL-Access Service

##### SSL-Access Testseite

Diese Seite zeigt Informationen aus dem Benutzerzertifikat.

##### Page test SSL-Access

Cette page montre des informations du certificat client.

DATE_LOCAL:	17 Oct 2012 11:22:16 GMT
CLIENT_IP:	178.197.232.95
SERVER_IP:	162.23.92.26
SERVER_NAME:	service.ssl.admin.ch

**SSL\_RESULT:** No Cert

SSL_ISSUER:	N/A
SSL_START	N/A
SSL_END	N/A
SSL_ALGORITHM	N/A
SSL_SUBJECT	N/A
SSL_RSA_BITS	N/A
SSL_KEY_TYPE	N/A
SSL_CIPHER_NAME	AES256-SHA
SSL_CIPHER_VERSION	SSLv3
SSL_CIPHER_BITS	256

**Bulletin à l'intention des caisses de compensation AVS et des organes d'exécution des PC No 317**

Pour toute question relative à sedex ou à l'échange de données, l'adresse email suivante est à votre disposition [ahv-ivnetz@bsv.admin.ch](mailto:ahv-ivnetz@bsv.admin.ch).