Préconisations sur l'adressage des lecteurs PC/SC

DSPS

1 INTRODUCTION

Cette note a pour objectif de fournir aux éditeurs de logiciels des préconisations pour contourner les problèmes liés aux déconnexions des lecteurs PC/SC.

Ces déconnexions peuvent avoir pour origine :

- Le débranchement et le rebranchement des lecteurs PC/SC par les utilisateurs. C'est le cas par exemple du TLA en mode PC/SC qui génère une déconnexion des applications au niveau du Resource Manager PC/SC, lors de son départ en visite et nécessite, lors de son retour de visite, une reconnexion à la carte.
- Des coupures, ou microcoupures, de l'alimentation électrique des lecteurs, qui ont pour effet au niveau du Resource Manager de déconnecter les applications clientes et qui nécessitent, suite au rétablissement de l'alimentation, une reconnexion à la carte.
- La mise en veille du poste de travail par l'OS avec coupure de l'alimentation des ports USB est un exemple de cas générant une déconnexion des lecteurs PC/SC.

Après avoir rappelé dans le paragraphe 2 les principes d'adressage des ressources PC/SC dans les FSV, le paragraphe 3 décrit les problèmes liés à cette déconnexion des lecteurs PC/SC. Le paragraphe 4 fournit une préconisation permettant de contourner ces problèmes.

Les préconisations décrites dans la présente version de ce document sont applicables aux FSV à partir de la version 1.40.14.12

2 RAPPEL SUR L'ADRESSAGE DES RESSOURCES PC/SC

Dans les FSV et MICA, l'accès aux lecteurs et aux cartes peut se faire suivant 2 modes :

- **La détection automatique des lecteurs/cartes** pour des configurations simples, le nom des lecteurs PC/SC n'est pas renseigné en entrée des fonctions SSV et MICA :

  Un mode de détection des cartes.

  - Les SSV détectent automatiquement les lecteurs dans lesquels sont insérées les cartes CPS et Vitale. Ce mode ne peut être utilisé que pour les configurations simples avec une seule CPS et une seule carte Vitale.

  Un mode de détection des lecteurs.

  - Les SSV recherchent automatiquement le nom des lecteurs PC/SC exposés par le TLA. Ce mode fonctionne uniquement pour des configurations simples, c'est à dire avec un seul lecteur homologué TLA connecté au poste de travail.
    Ce mode permet, pour les fonctions n'utilisant pas les cartes, de ne pas renseigner le nom des lecteurs PC/SC en paramètre. Il s'agit des fonctions de gestion du TLA n'utilisant pas la CPS (IdentifierTLA, ChargerDonneesTLA, ChargerFacturesPdT), ainsi que des fonctions de gestion de la configuration des lecteurs (LireDateLecteur, MajDateLecteur, ChargerAppli).

- **L'adressage direct** des lecteurs de cartes pour des configurations multi cartes ou multi lecteurs : dans ce mode, le nom des lecteurs PC/SC doit être renseigné en entrée des fonctions SSV et MICA. Ce mode est obligatoire pour les configurations nécessitant la présence simultanée de plusieurs CPS ou plusieurs cartes Vitale.

3 PROBLEMES LIES A LA DECONNEXION DES LECTEURS PC/SC

Le nom des lecteurs PC/SC natifs (non homologués par le GIE SESAM-Vitale) de même marque est susceptible de changer en fonction de l'ordre de branchement et/ou de détection des lecteurs. En effet, dans ce cas, l'index du lecteur de cartes Vitale ou CPS renseigné dans le nom du lecteur est incrémenté au fur et à mesure du branchement et/ou détection des lecteurs.

Exemple : cas de deux lecteurs PC/SC natifs

- *Nom du premier lecteur branché : GEMPLUS USB SmartCard Reader **0***
- *Nom du deuxième lecteur branché : GEMPLUS USB SmartCard Reader **1***

Si l'adressage des lecteurs dans les FSV se fait via le mode d'adressage direct, un changement d'ordre du branchement des lecteurs, nécessite alors de reconfigurer l'association entre le nom des lecteurs PC/SC et les cartes à adresser.

Point d'attention, dans certains cas, cette renumérotation des noms de lecteurs **de même marque** est susceptible de changer suite à une déconnexion et reconnexion des lecteurs, sans que l'utilisateur n'ait débranché les lecteurs (suite à une coupure ou microcoupure).

Exemple : sur macOS, il a été constaté une renumérotation arbitraire des noms de lecteur après une sortie veille de la machine.

Le renommage intempestif des lecteurs n'apparait pas lorsqu'on utilise des lecteurs de marques ou de modèles différents.

Exemple : cas de deux lecteurs PC/SC natifs

- *Nom du premier lecteur branché : GEMPLUS USB SmartCard Reader **0***
- *Nom du deuxième lecteur branché : LITEO USB SmartCard Reader **0***

A moins d'être certain d'utiliser uniquement des lecteurs natifs de marques différentes sur le poste de travail du PS, nous recommandons :

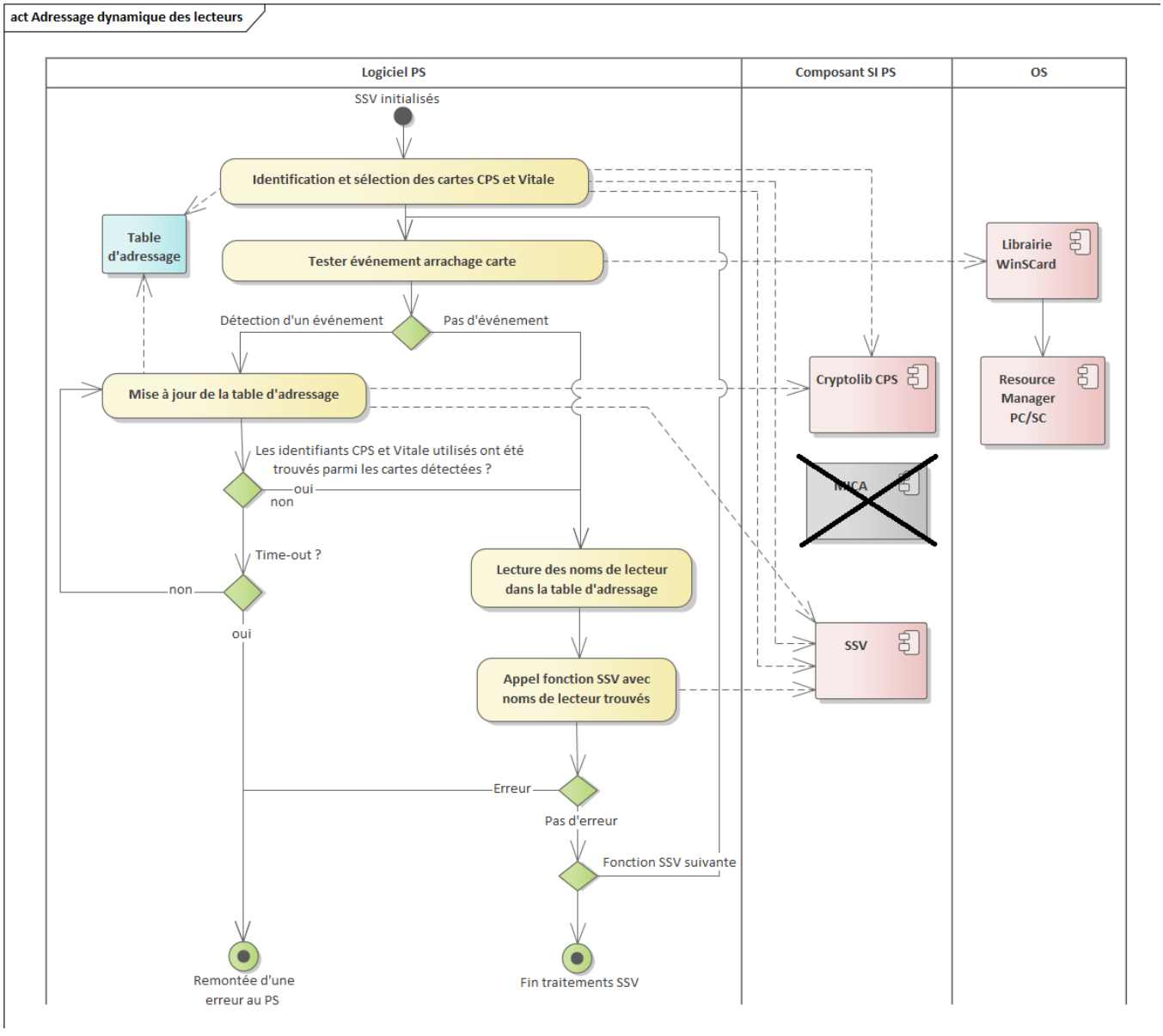
- Pour les configurations dont on est certain que le Resource Manager PC/SC détectera au plus une seule carte CPS et/ou au plus une seule carte Vitale, d'utiliser la détection automatique des cartes
- Pour les configurations dont le Resource Manager PC/SC est susceptible de détecter plusieurs cartes CPS ou plusieurs cartes Vitale, d'implémenter un mécanisme d'adressage dynamique des lecteurs basé sur l'identification des cartes utilisées (voir le paragraphe §4 pour un exemple de solution de ce type).

Note importante : Après un certain nombre de tentatives de déconnexions-reconnexions sur des lecteurs homologués 04.xx en mode PC/SC, le GIE SESAM-Vitale n'a pas réussi à reproduire ce problème de renommage intempestif des noms de lecteurs.

4 EXEMPLE DE SOLUTION POUR RESOUDRE LES PROBLEMES DE DECONNEXION ET DE STABILITE D'ADRESSAGE DES LECTEURS PC/SC

L'adressage dynamique des lecteurs permet de résoudre d'une manière générique, les problèmes de renommage des lecteurs PC/SC, décrits au paragraphe 3, dans le cadre de l'utilisation des FSV.

4.1.1 Algorithme



4.1.2 Principe

Une « table d'adressage des lecteurs » permet de faire l'association entre l'identifiant de la carte sélectionnée et le nom du lecteur PC/SC correspondant. Cette table contient deux entrées : une pour la carte CPS, une autre pour la carte Vitale. Avant appel d'une fonction SSV, le nom des lecteurs PC/SC à transmettre à la fonction est lu dans cette table.

La table d'adressage des lecteurs est créée lors d'une phase initiale d'identification et de sélection des cartes CPS et Vitale. Elle est ensuite mise à jour dynamiquement par le progiciel, suite à la détection par ce dernier d'un événement PC/SC, dû à un arrachage carte ou une déconnexion lecteur, sur un des deux slots CPS ou Vitale.

Cette mise à jour consiste à énumérer les slots CPS et Vitale et à récupérer pour chacun d'eux les identifiants cartes et le nom des lecteurs associés. Les identifiants des cartes CPS et Vitale, mémorisés lors de la phase initiale de sélection des cartes, sont alors recherchés dans la liste des identifiants cartes obtenus afin de récupérer les noms de lecteurs correspondants, suite à quoi la table d'adressage est mise à jour avec ces noms de lecteurs.

> Le principe décrit ci-dessus permet de répondre aux problématiques de renommage des lecteurs (cf. §3).

L'algorithme proposé s'appuie sur les composants suivants :

- Les SSV, pour les traitements liés à la facturation,
- La Cryptolib CPS, pour l'identification des CPS,
- ~~La librairie MICA pour l'identification des cartes Vitale,~~
- La librairie cliente PC/SC de l'OS (exemple WinScard), pour la détection des événements PC/SC.

4.1.3 Identification et sélection des cartes CPS et Vitale

Ce traitement comprend :

- La détection des cartes CPS et Vitale insérées dans les lecteurs PC/SC,
- La lecture des informations d'identification des CPS et des Vitale,
- Si plusieurs CPS, ou si plusieurs Vitale sont détectées :
  - La lecture des informations sur le porteur de la carte,
  - La demande de sélection de la carte par l'utilisateur,
- La récupération et la mémorisation dans la table d'adressage des noms de lecteur PC/SC correspondants aux cartes sélectionnées.

4.1.3.1 Cas de la carte CPS

La Cryptolib CPS peut être utilisée pour effectuer les traitements décrits ci-dessus liés à la CPS.

La liste des slots PC/SC contenant une CPS peut être obtenue à l'aide de la fonction C_GetSlotList.

L'identification des CPS peut être faite à l'aide de l'identifiant logique de la CPS. Cette information peut être obtenue à l'aide de la fonction C_TokenInfo. L'information en question est renseignée dans le champ *label* de la structure *CK_TOKEN_INFO*.

Le nom du lecteur PC/SC peut être obtenu avec la fonction C_GetSlotInfo. Le nom du lecteur est renseigné dans le champ *slot_description* de la structure *CK_SLOT_INFO.*

Les informations sur le PS comprennent le nom et le prénom du PS. Elles peuvent être obtenues de la façon suivante :

- Les attributs à définir dans le template de recherche sont CKA_CLASS, CKA_TOKEN, CKA_PRIVATE et CKA_LABEL.
- CKA_CLASS vaut CKO_DATA
- CKA_TOKEN est positionné à vrai (CK_TRUE) pour indiquer que l'on recherche un objet de la carte

- CKA_PRIVATE est positionné à faux (CK_FALSE) pour indiquer que l'on recherche un objet public
- CKA_LABEL : la valeur de cet attribut vaut « CPS_NAME_PS ».
- Par la suite, la recherche effective de l'objet est réalisée par les appels C_OpenSession, C_FindObjectsInit, C_FindObjects, C_FindObjetsFinal, C_CloseSession, dans cet ordre.

4.1.3.2 Cas de la carte Vitale

La liste des slots PC/SC contenant une carte Vitale peut être obtenue à l'aide de la fonction SSV_LireConfig. Cette fonction retourne autant de groupes 67 que de lecteurs PC/SC détectés. Le champ 67-1 contient le nom du lecteur PC/SC et le champ 67-2 contient le type de carte (valorisé à 1 dans le cas d'une carte Vitale).

L'identification des cartes Vitale peut être faite à l'aide du numéro de série des cartes Vitale. Cette information peut être obtenue à l'aide de la fonction SSV_LireNumSerieCarteVitale, présente dans les FSV à partir de la version 1.40.14.12 ~~du composant MICA en appelant la fonction MICA_ControlePresenceCarteVitale~~. Cette fonction prend en entrée le nom du lecteur PC/SC contenant la carte Vitale et donne en retour le numéro de série de la carte.

Les informations sur le porteur de la carte comprennent :

- Le nom et le prénom du titulaire de la carte,
- Le NIR de l'assuré.

Ces informations peuvent être obtenues en appelant la fonction SSV_LireDroitsVitale.

Si plusieurs CPS sont présentes, l'appel de la fonction SSV_LireDroitsVitale nécessite de renseigner en entrée le nom du lecteur PC/SC contenant une des CPS. Il est nécessaire dans ce cas d'avoir fait une sélection au préalable de la CPS.

Si une seule CPS est présente, il est possible de demander à la fonction de faire une détection automatique de la CPS, en ne renseignant pas le nom du lecteur en entrée.

Si aucune CPS n'est présente, il est possible d'appeler la fonction en ne renseignant pas le nom du lecteur CPS. Dans ce cas, la fonction retourne un warning F001 (CPS absente) et renseigne les données en sortie (contenant les informations sur le porteur carte), sans les données d'exonération.

4.1.4 Contrôle sur les événements d'arrachage carte

Ce traitement peut être réalisé en utilisant la librairie cliente PC/SC, disponible nativement sur les OS Windows et macOS et fournie sur Linux par l'implémentation libre « PCSC Lite ». Cette librairie peut être chargée dynamiquement via la fonction LoadLibrary sous Windows, ou dlopen sous macOS et Linux, en lui passant en paramètre le chemin suivant :

- Windows : "winscard.dll"
- macOS : "/System/Library/Frameworks/PCSC.framework/PCSC"
- Linux : "libpcsclite.so"

La documentation de l'API de cette librairie est disponible aux adresses suivantes :

- Windows : https://docs.microsoft.com/en-us/windows/win32/secauthn/smart-card-resource-manager-api
- macOS et Linux : https://pcsclite.apdu.fr/api/group__API.html

Le contrôle consiste à vérifier si un événement d'arrachage carte a eu lieu sur un des deux slots CPS et Vitale. Pour ce faire, il est possible d'appeler la fonction SCardGetStatusChange de la librairie cliente PC/SC. Cette fonction prend en entrée un tableau de structures *SCARD_READERSTATE*, chaque élément du tableau correspondant à un slot sur lequel on souhaite détecter les événements.

Les champs de la structure *SCARD_READERSTATE* sont à renseigner comme suit :

- szReader : nom du lecteur PC/SC
- pvUserData = NULL

- dwCurrentState = SCARD_STATE_PRESENT | SCARD_STATE_INUSE (état courant de la carte)

La fonction prend également en paramètre un time-out, à valoriser en millisecondes.

La fonction rend la main suite à la survenue d'un événement par rapport à l'état dwCurrentState fourni en entrée, ou suite au time-out si aucun événement ne s'est produit.

Si un événement est survenu, le champ dwEventState de la structure *SCARD_READERSTATE* est renseigné avec le nouvel état de la carte (SCARD_STATE_EMPTY en cas d'arrachage carte). Si aucun événement ne s'est produit (time-out de la fonction), le champ dwEventState est alors égal à dwCurrentState.

> A noter qu'une déconnexion d'un lecteur provoque la remontée d'un événement d'arrachage carte.

4.1.5 Mise à jour de la table d'adressage des lecteurs

Cette opération consiste, suite à la détection d'un événement d'arrachage carte sur un des slots CPS ou Vitale, à mettre à jour la table d'adressage contenant l'association entre les identifiants de cartes et les noms des lecteurs.

Les traitements à effectuer sont :

- Lister les slots CPS et Vitale,
- Pour chaque slot, récupérer les informations d'identification de la carte et le nom du lecteur PC/SC correspondant,
- Rechercher dans la liste établie ci-dessus l'identifiant des cartes CPS et Vitale en cours d'utilisation (cartes sélectionnées lors de l'étape d'identification et de sélection des cartes) et récupérer les noms des lecteurs correspondants,
- Mettre à jour les noms des lecteurs dans la table d'adressage des lecteurs.

La récupération des slots CPS et des informations d'identification de la CPS (identifiant logique de la CPS) peut être effectuée à l'aide de la Cryptolib CPS (cf. §4.1.3.1).

La récupération des slots Vitale peut être effectuée à l'aide de la fonction SSV_LireConfig et la récupération des informations d'identification de la Vitale (numéro de série de la carte) peut être faite à l'aide de la fonction SSV_LireNumSerieCarteVitale ~~MICA~~ (cf. §4.1.3.2).

Les traitements décrits ci-dessus peuvent nécessiter d'être réitérés plusieurs fois pour laisser le temps au Resource Manager PC/SC de détecter les lecteurs suite à leur reconnexion.

5 CONCLUSION

1 - En cas d'utilisation de lecteurs PC/SC natifs, il est préconisé d'utiliser des lecteurs de marques ou de modèles différents.

2 - Si cela n'est pas possible, nous préconisons :

- Pour les configurations dont on est certain que le Resource Manager PC/SC détectera au plus une seule carte CPS et/ou au plus une seule carte Vitale, d'utiliser la détection automatique des cartes
- Pour les configurations dont le Resource Manager PC/SC est susceptible de détecter plusieurs cartes CPS ou plusieurs cartes Vitale, d'utiliser un mécanisme d'adressage dynamique du type de la solution décrite dans le chapitre 4.