

# Livre blanc relatif à iCLASS SE et multiCLASS SE OSDP avec SCP

## Livre blanc relatif à OSDP

***OSDP est l'acronyme de « Open Supervised Device Protocol »***

***SCP est l'acronyme de « Secure Channel Protocol »***

Le secteur du contrôle d'accès a enregistré d'énormes avancées au cours des vingt dernières années, mais il reste un aspect qui n'évolue pas beaucoup : la façon dont les lecteurs sont connectés aux systèmes de contrôle d'accès. Les premiers lecteurs RFID ont participé à la popularité de l'interface Wiegand (D0/D1), tandis que les lecteurs à piste magnétique utilisaient une interface avec des signaux Clock and Data. Les schémas de câblage de ces deux interfaces sont devenus des normes SIA pour le secteur du contrôle d'accès.

Les deux interfaces ont beaucoup de points communs. Ce sont toutes les deux des protocoles point-à-point unidirectionnels qui utilisent deux câbles et un câble de retour pour envoyer une série de bits de données depuis le lecteur vers le système. Point-à-point signifie qu'il n'est possible de connecter qu'un seul lecteur à un circuit d'interface. Unidirectionnelle implique que ces interfaces ne fournissent aucun moyen au système d'envoyer des données vers le lecteur, ni de demander des données au lecteur. Si des données doivent être envoyées au lecteur, un câblage discret supplémentaire est en général nécessaire.

Ce système de communication unidirectionnel présente plusieurs inconvénients. Comme le système n'est pas capable de demander un état des lieux au lecteur, il n'existe pas de méthode facile pour déterminer l'état du lecteur autre que l'utilisation d'un circuit supplémentaire ou le fait d'attendre simplement qu'un utilisateur se plaigne. Un autre inconvénient vient du fait que tous les points de connexion des appareils doivent être en permanence prêts à recevoir des données sans les avoir sollicitées, ce qui implique souvent d'avoir des circuits tampons dédiés ou un système de traitement rapide des interruptions en parallèle. Sans capacité de contrôle du flux, les configurations multipoints ne sont pas pratiques en raison du risque élevé de collisions et de l'impossibilité à demander une retransmission en cas de collision.

Il est de plus en plus évident que pour que la technologie et les capacités de lecteur progressent, une connexion bidirectionnelle entre le lecteur et le système de contrôle d'accès est impérative. Certains fabricants de lecteur et de systèmes de contrôle d'accès ont reconnu cette nécessité et ont développé des solutions bidirectionnelles propriétaires. Toutefois, le développement et les investissements en formation pour les solutions propriétaires ralentissent l'évolution des solutions interopérables et réduit le marché disponible. De cette façon, la croissance est mitigée et l'implémentation restreinte.

Les actuels projets OSDP SCP devraient pouvoir être livrés en juin. Le lecteur iCLASS SE constitue la base technologique du produit. Les lecteurs iCLASS SE et pivCLASS ont tous la flexibilité et la sécurité nécessaires pour prendre en charge OSDP et aider à aligner nos stratégies de produits actuelles et améliorer les valeurs pour nos clients.

## **Comprendre OSDP SCP :**

Les spécifications OSDP ont été conçues pour être flexibles et modulables en vue de répondre aux besoins de diverses applications aussi bien aujourd'hui qu'à l'avenir. Les spécifications définissent

les méthodes permettant de créer des commandes spécifiques pour le fabricant qui permettent de tirer pleinement profit des capacités d'un appareil spécifique sans interférer avec l'interopérabilité, la facilité de configuration et l'utilisation prévues pour être le dénominateur commun de tous les appareils OSDP.

Dépassant l'interface Wiegand unidirectionnelle, Open Supervised Device Protocol (OSDP) assure le suivi continu de l'état du lecteur et peut immédiatement indiquer un lecteur défaillant, manquant ou fonctionnant mal. OSDP peut fournir des indications anti-fraude pour les lecteurs dotés de capacités de détection des fraude intégrées. Tous les signaux passent par deux lignes de données plus une ligne de terre, permettant d'utiliser le câble à quatre conducteurs pour alimenter le lecteur ainsi que pour envoyer et recevoir des données, à un faible coût d'installation par rapport aux six conducteurs généralement utilisés pour Wiegand. Certains lecteurs OSDP fournissent également un retour aux utilisateurs via un écran LCD. OSDP est une spécification d'interface non prioritaire susceptible d'être implémentée sans restriction.

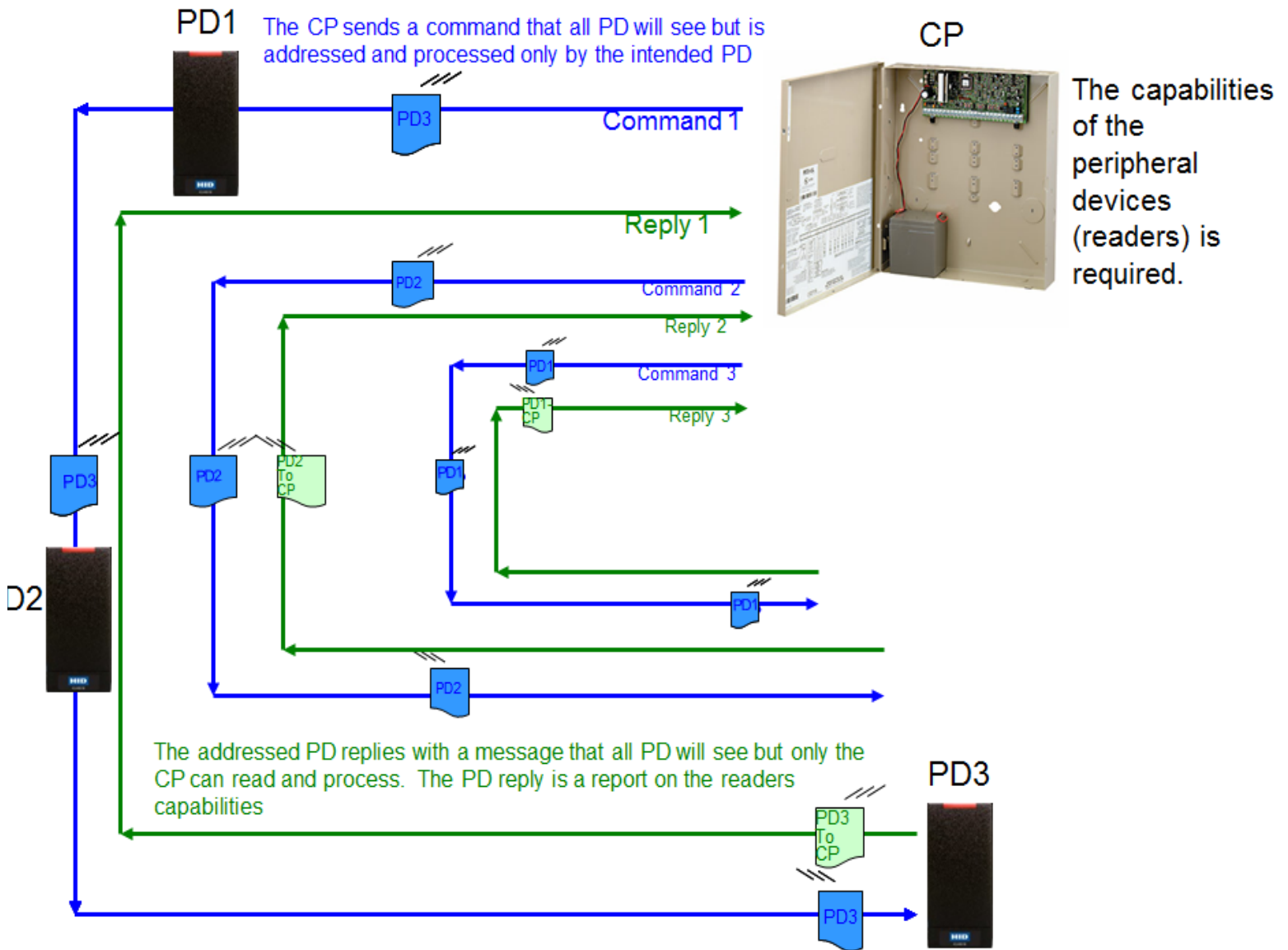
Le besoin de ce type de spécification est impérieux. Actuellement, on pense qu'il n'en existe pas, car le US federal Identity and Access Management space impose des communications sécurisée entre le bord de carte PIV/I et tout lecteur/contrôleur conçu pour s'authentifier en tant que moyen d'identification de ce type. La spécification OSDP est un protocole de communication visant à établir une interface d'un ou plusieurs appareils périphériques (PD, de l'anglais Peripheral Devices) et d'un panneau de commande (CP, de l'anglais Control Panel). OSDP précise l'implémentation du protocole d'un canal de communications série multipoints à deux câbles, comme RS485. OSDP est extensible pour permettre le transport sur un autre média, comme TCP/IP. Dans sa dernière itération, une méthode de chiffrement a été ajoutée. Elle se base sur la plateforme globale, protocole de canal sécurisé 03. L'objectif est de normaliser et de sécuriser les communications entre les appareils périphériques, comme les lecteurs de cartes, et les appareils hôtes comme les panneaux de commande. De nombreux fabricants du secteur disposent de produits OSDP.

OSDP est un protocole connu et fiable pour les lecteurs et autres périphériques. OSDP est actuellement envisagé par la Security Industry Association (SIA) pour une éventuelle adoption et codification en tant que norme, ce qui conduirait à davantage d'efficacité et un temps de commercialisation plus rapide. L'un des points faibles d'OSDP réside dans la sécurité de messagerie forte et basée sur des normes. L'ajout de SCP apporte une authentification robuste, permettant des communications\connexions sécurisées et fiables. En tant que norme, OSDP continuera de progresser et les changements seront implémentés au fur et à mesure de leur normalisation et de leur application dans le processus de développement des produits.

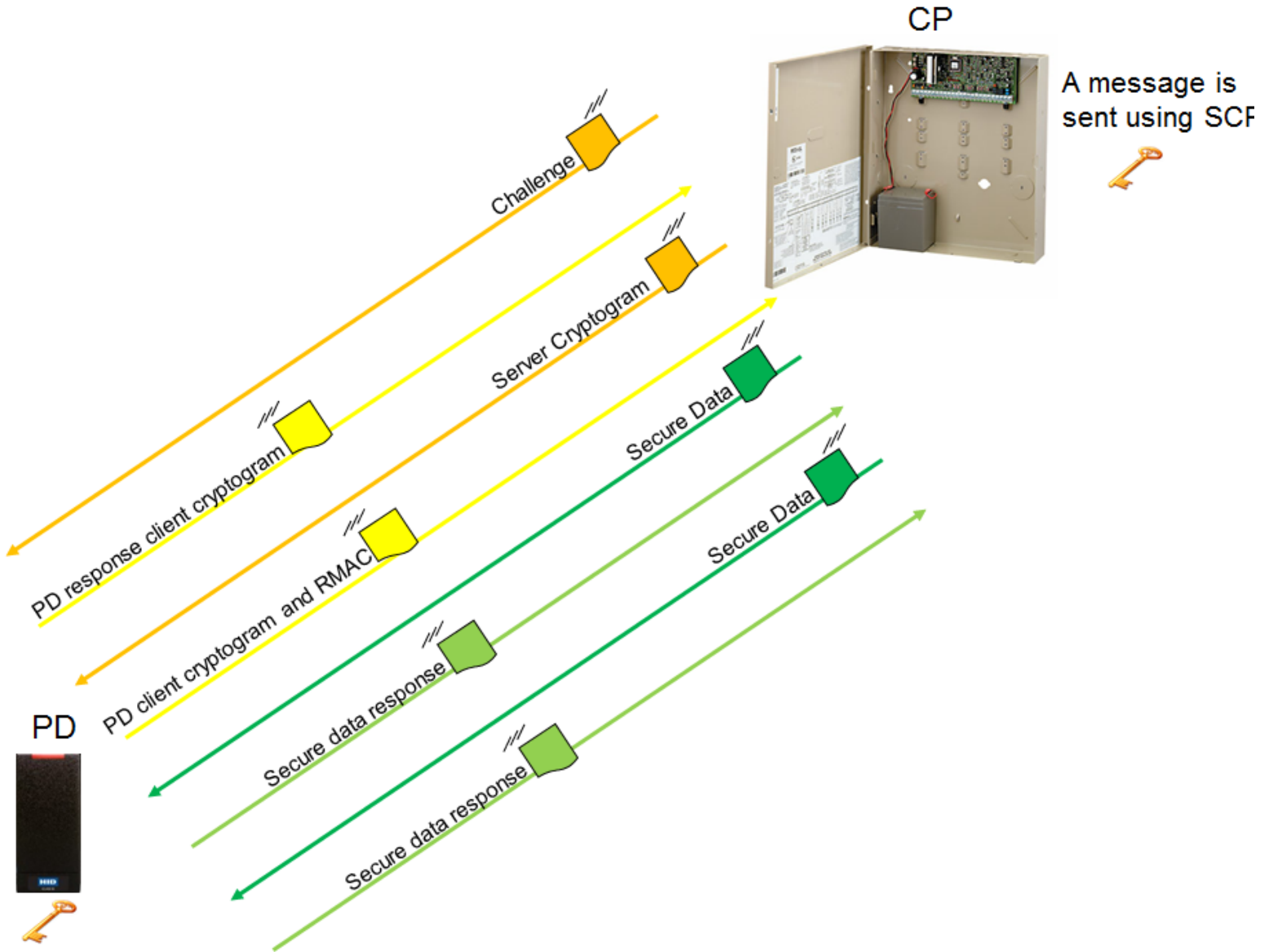
SCP (secure channel protocol) a été développé par Global Platform, organisme de normalisation de l'industrie. Au départ, Global Platform avait établi des normes pour cartes à puce autour de la sécurité et de l'interopérabilité entre des systèmes, des organisations et des appareils. OSDP est établi avec des designs matures, mais SCP est très récent et de nombreuses personnes développent leur propre norme. Devant un intérêt renouvelé envers les meilleures pratiques pour la sécurité, SCP comble un manque dans la sécurité des communications en utilisant une autre norme de l'industrie. En dépit de sa nouveauté pour OSDP et les appareils périphériques, SCP est une méthode de sécurité connue qui s'appuie sur plusieurs années d'utilisation.

Pour établir une session en se servant du protocole SCP (secure channel protocol), le Client et le Serveur doivent s'authentifier mutuellement l'un auprès de l'autre et, dans le même processus, un jeu de clés est établi pour cette session. La session à canal sécurisé est résiliée et les clés de session sont détruites chaque fois qu'une erreur est détectée dans le protocole SCP (secure

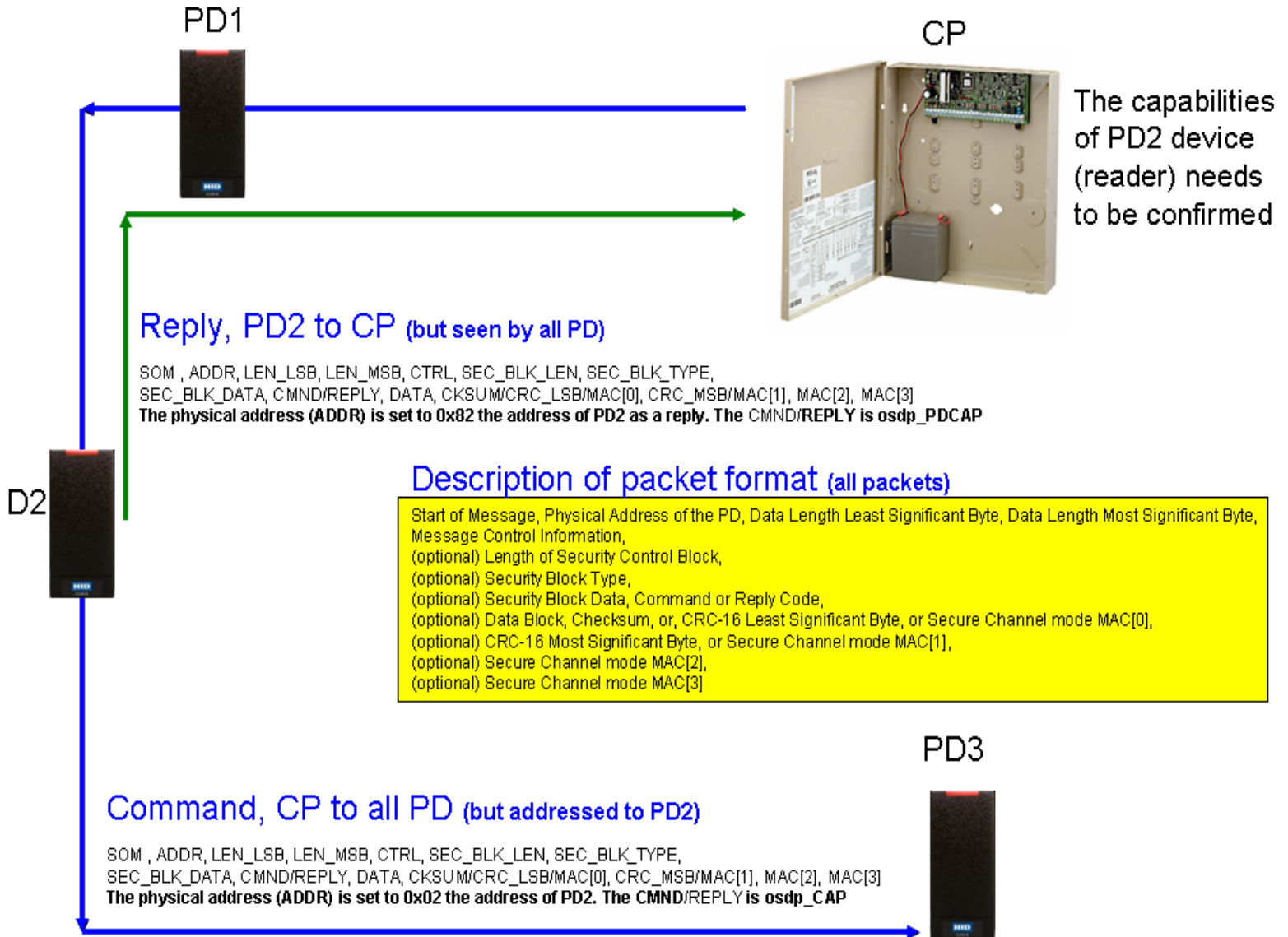
channel protocol). Par exemple, la session peut être résiliée par l'une ou l'autre partie en forçant un délai, ou simplement en envoyant un MAC non valide.



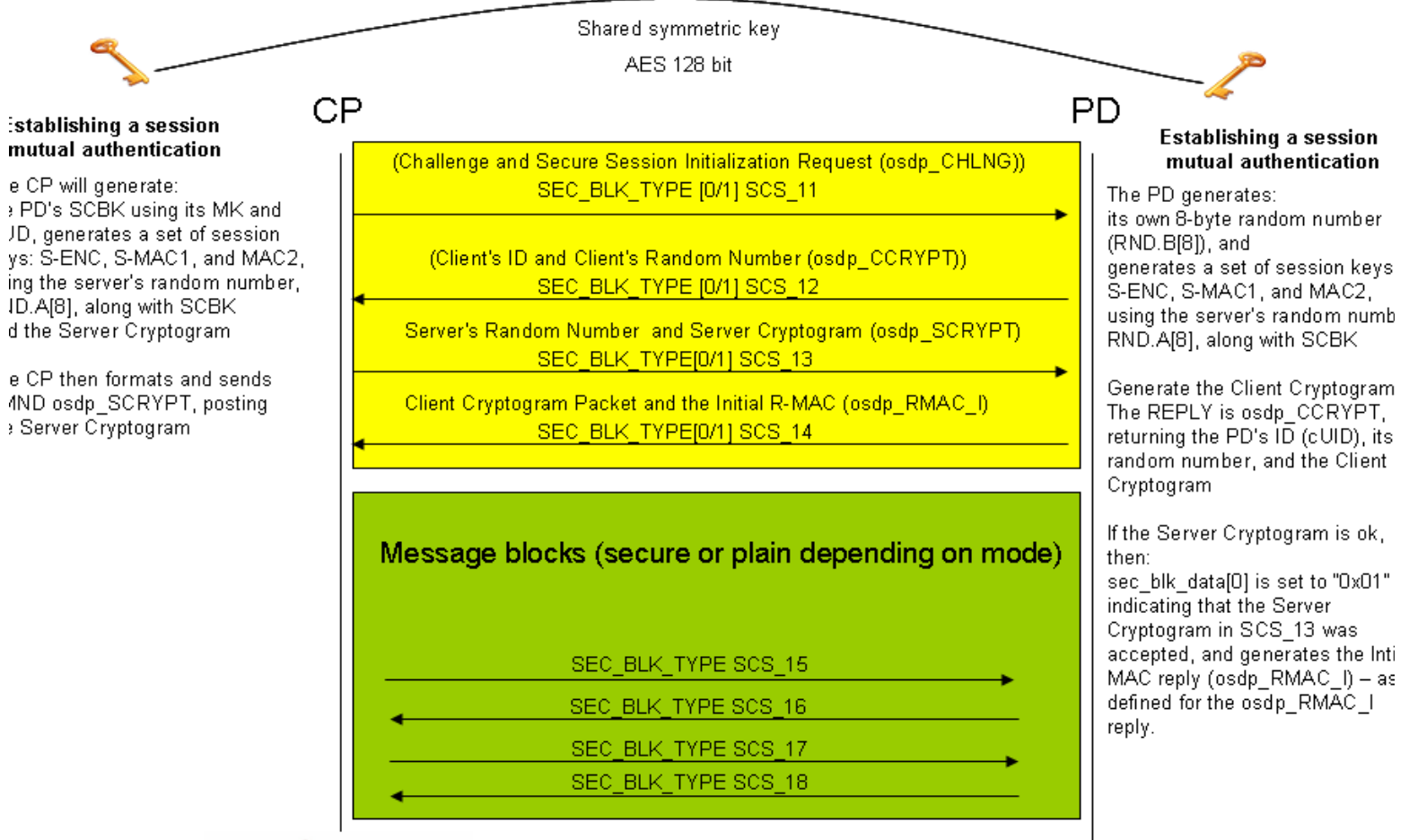
Flux de messages de base pour SCP :



Vue détaillée de SCP :



### Secure Channel Protocol :



**Stratégie :**

L'impact d'une norme de communications ouverte dans le secteur PACS (et les secteurs associés) est énorme et a le potentiel de réduire les coûts, permettre l'interopérabilité et améliorer la sécurité. En tant que leader technologique, HID Global a entrepris de travailler dans le secteur des normes pour guider et contribuer à leur mise en place. HID Global est un leader technologique et permet l'utilisation de normes via ; des produits conformes, des formations, des kits d'outils de développement, du marketing et des débats sur les questions et normes importantes pour nos clients et le secteur. HID est l'un des premiers à publier un produit OSDP compatible SCP.

**Comparaison :**

Wiegand	OSDP SCP
Données en clair (ou faible sécurité)	Données sécurisées
Câblage à coût plus élevé	Câblage à coût moins élevé
Données unidirectionnelles	Données bidirectionnelles
Aucune fonction d'administration prise en charge	Configuration et administration à distance (voir point 6 des caractéristiques)
	Statut et identité du lecteur retour
	Mode transparent pour carte à puce

**Considérations :**

Les systèmes devront prendre en charge les avancées concernant OSDP SCP et le développement devra avoir lieu avant toute implémentation planifiée d'un système OSDP.

Pour aider à réduire les coûts et à accélérer la commercialisation pour nos clients, HID Global a développé des kits d'outils pour développeur adaptés à leurs programmes de développement.

**FAQ :**

- Q** Quels lecteurs sont disponibles avec OSDP SCP ?
- A** Le design d'OSDP SCP nécessite un appareil très sécurisé. Les lecteurs compatibles SE. Les lecteurs iCLASS SE et multiCLASS SE prennent en charge OSDP SCP. La même ingénierie centrale est utilisée pour pivCLASS et OSDP est également pris en charge dans pivCLASS. Au fur et à mesure que les technologies se déplaceront vers les nouveaux lecteurs SE, elles seront à même de prendre en charge OSDP SCP.

**Q** J'ai un ancien lecteur (pas un modèle SE). Peut-il être mis à niveau vers OSDP SCP ?

**R** Non, le design n'est pas compatible avec les critères nécessaires pour satisfaire OSDP SCP

**Q** Mon lecteur OSDP actuel (pas un modèle SE) peut-il utiliser SCP ?

**R** Non, le design n'est pas compatible avec les critères nécessaires pour satisfaire OSDP SCP

**Q** Comment savoir si mon système PACS peut prendre en charge OSDP ?

**A** Vérifiez auprès de votre fournisseur de solution logiciel et de panneau PACS et dites-lui que vous envisagez d'effectuer une mise à niveau vers les nouveaux lecteurs SE compatibles OSDP de HID.

[hidglobal.fr](http://hidglobal.fr)

© 2013 HID Global Corporation/ASSA ABLOY AB. Tous droits réservés. HID, HID Global, le logo en brique bleue HID, la conception de chaîne, multiCLASS SE, pivCLASS et iCLASS SE sont des marques commerciales ou des marques déposées de HID Global et/ou des détenteurs des licences aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales, marques de service, et noms de produits ou de services sont des marques commerciales appartenant à leur propriétaire respectif.

2013-06-11-hid-OSDP-wp-fr

PLT-02399