Création d'un démon compatible GlobalPlatform pour un environnement Java Card indépendant

Stage de fin d'école d'ingénieur mené par Vincent Giraud sous la tutelle de Guillaume Bouffard

1er février 2019 – 31 juillet 2019

Le Secrétariat Général de la Défense et de la Sécurité Nationale soutient le gouvernement dans la protection de la nation.

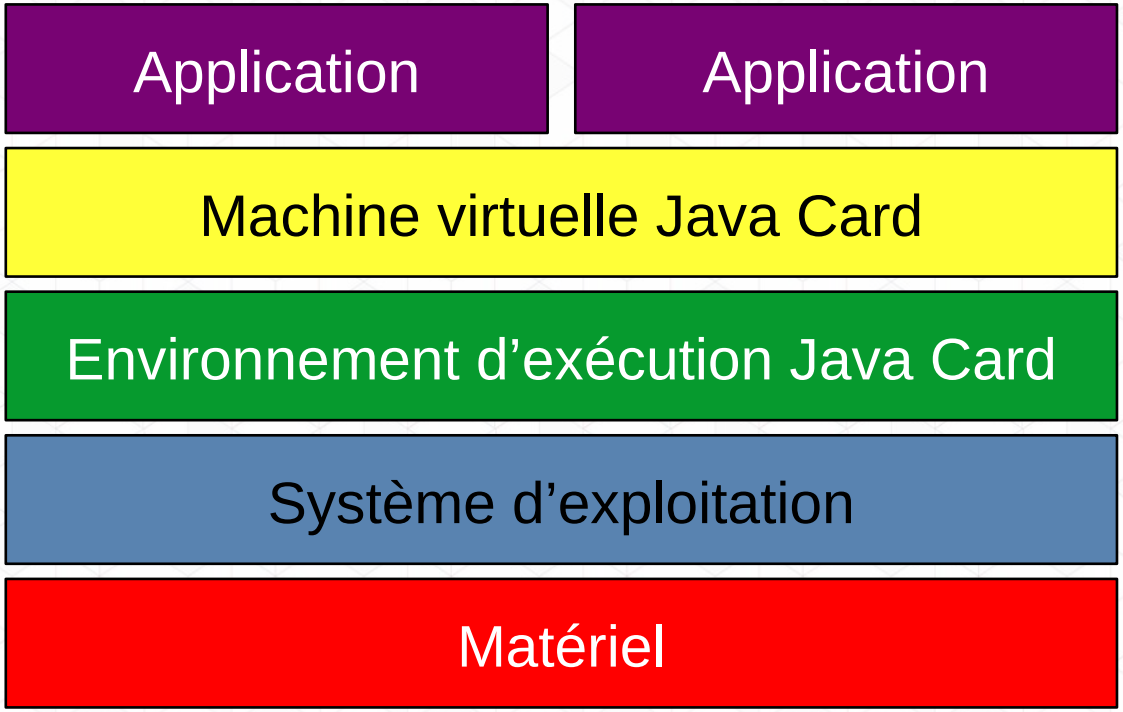
L'Agence Nationale de la Sécurité des Systèmes d'Information se spécialise dans le numérique et réalise un travail d'expertise, de veille, de conseil et d'assistance dans ce domaine.

- Mise en contexte
- Spécification GlobalPlatform
- Gestion des contenus
- Permissions et états de vie
- Isolation et interactions des contenus
- Conclusion

Mise en contexte

Java Card est un environnement d'exécution adapté aux plateformes à faibles ressources exécutant du code sensible.

Il est omniprésent dans beaucoup des périphériques du quotidien.



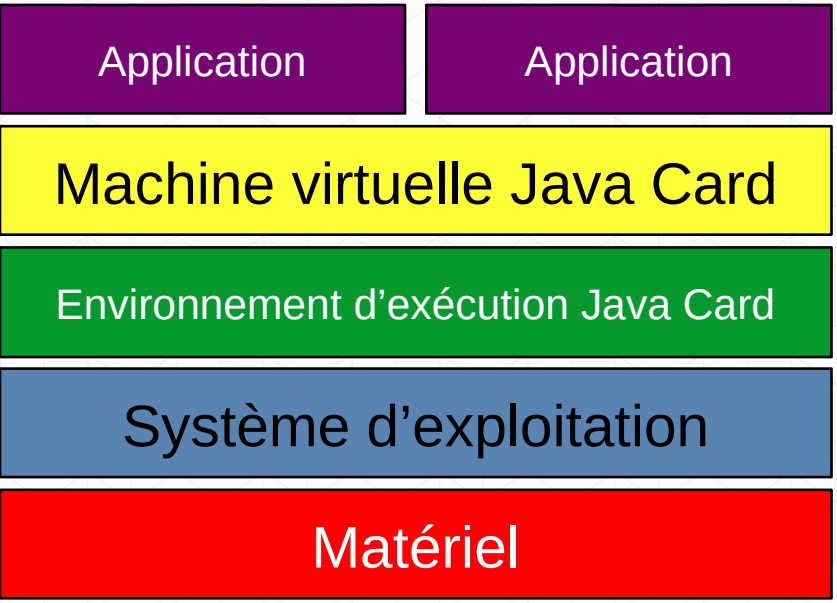
Des systèmes basés sur cet environnement sont très régulièrement validés dans le cadre des Critères Communs.

Stage de Léo Gaspard en 2016 : système d'exploitation

Travail en cours par Guillaume Bouffard : interpréteur Java Card en C++

- Programmation en Rust
- Protection matérielle de la mémoire
- Instanciation d'un environnement propre à chaque application

→ Publication à SSTIC 2018

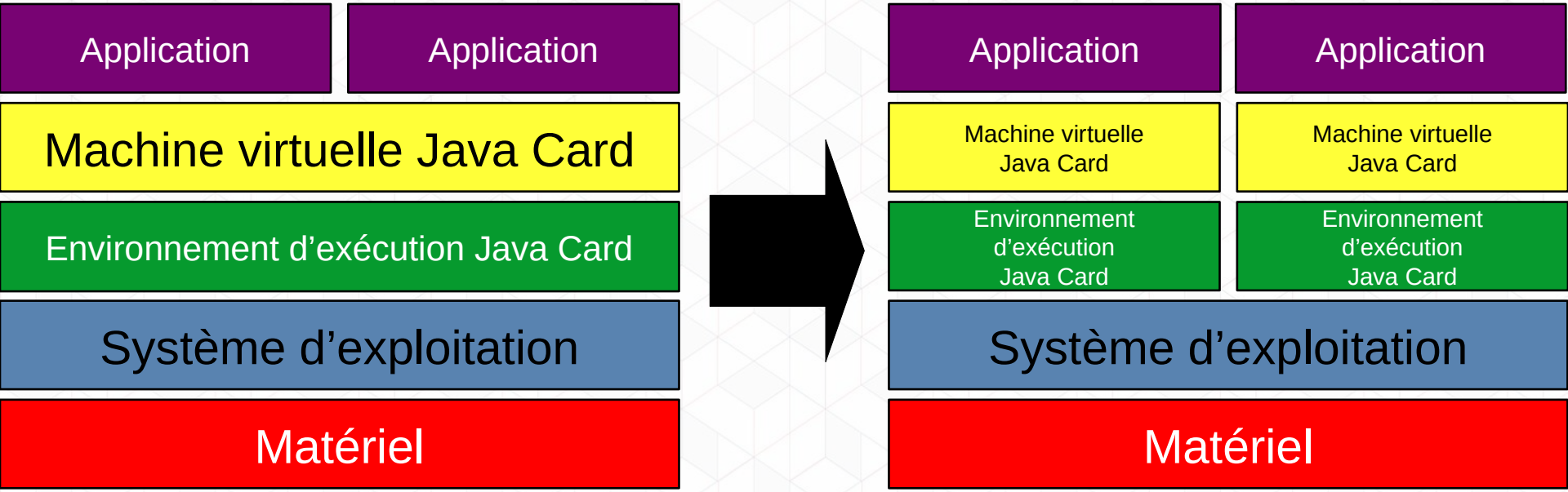


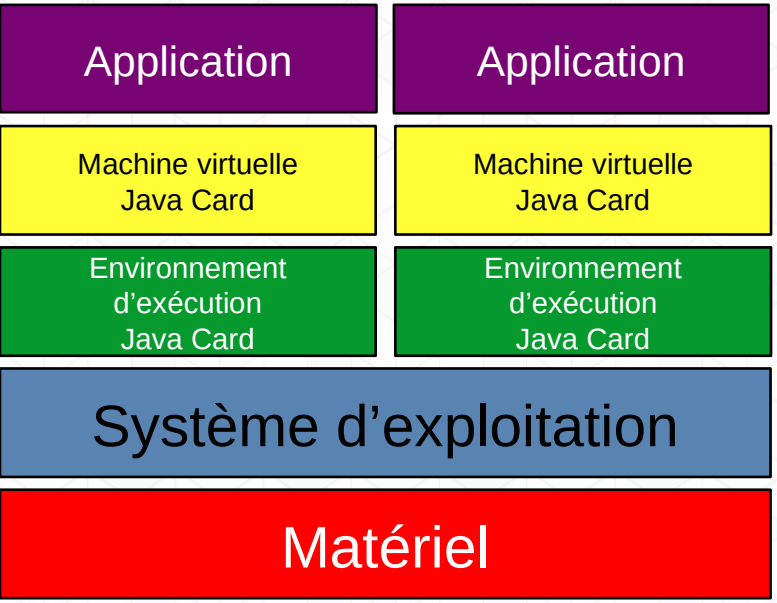
Stage de Léo Gaspard en 2016 : système d'exploitation

Travail en cours par Guillaume Bouffard : interpréteur Java Card en C++

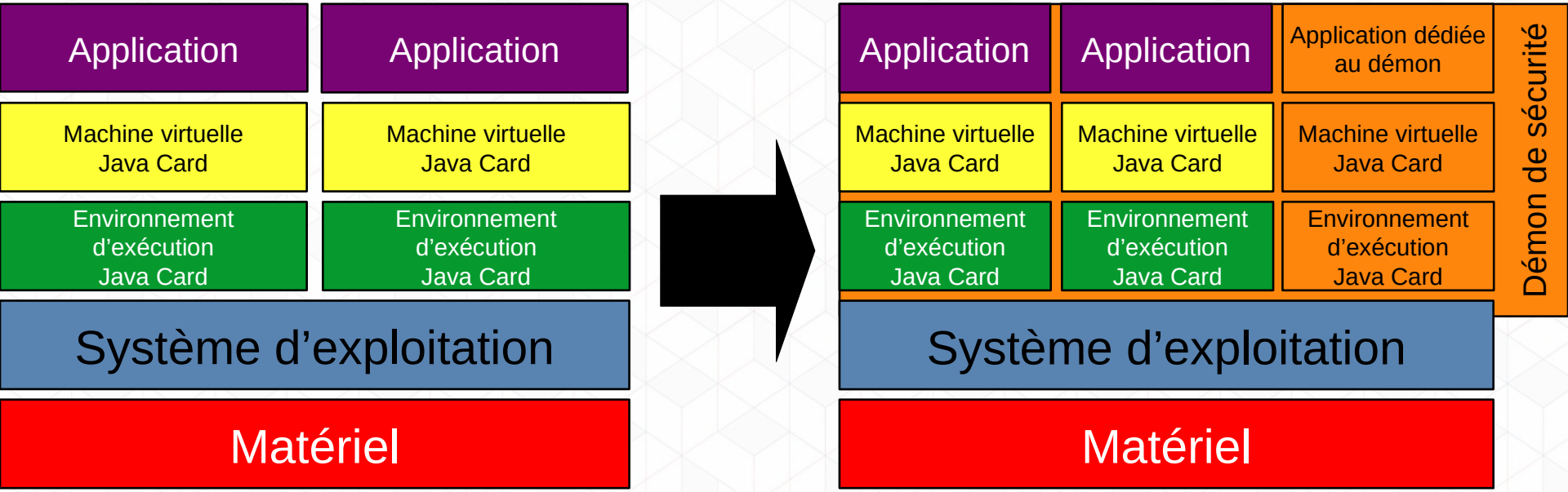
- Programmation en Rust
- Protection matérielle de la mémoire
- Instanciation d'un environnement propre à chaque application

→ Publication à SSTIC 2018





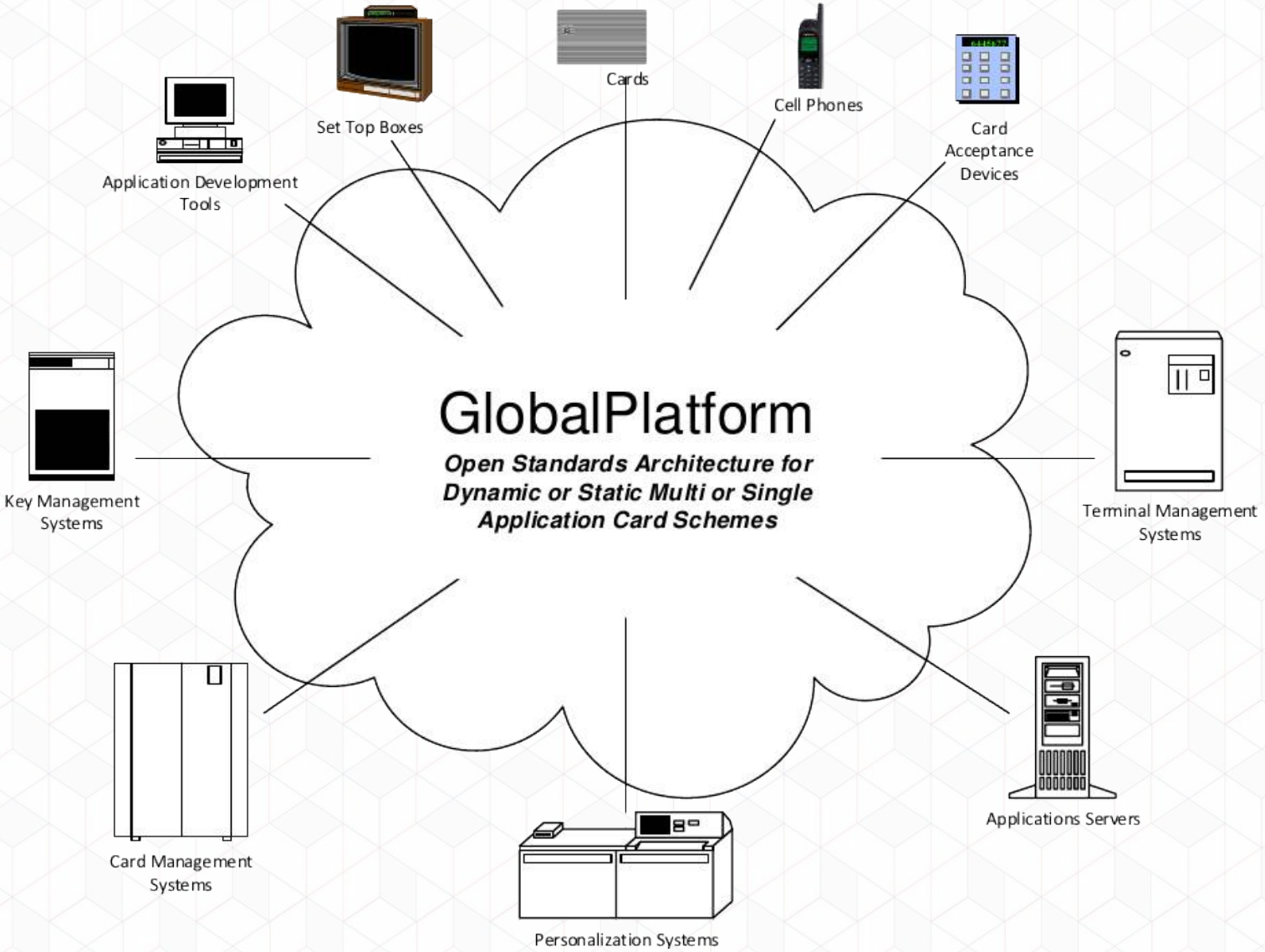
L'objectif du stage est d'implémenter un démon de sécurité dans l'environnement logiciel maison.



L'objectif du stage est d'implémenter un démon de sécurité dans l'environnement logiciel maison.

Spécification GlobalPlatform

GlobalPlatform permet d'améliorer l'interopérabilité dans la gestion des applications et de la sécurité.



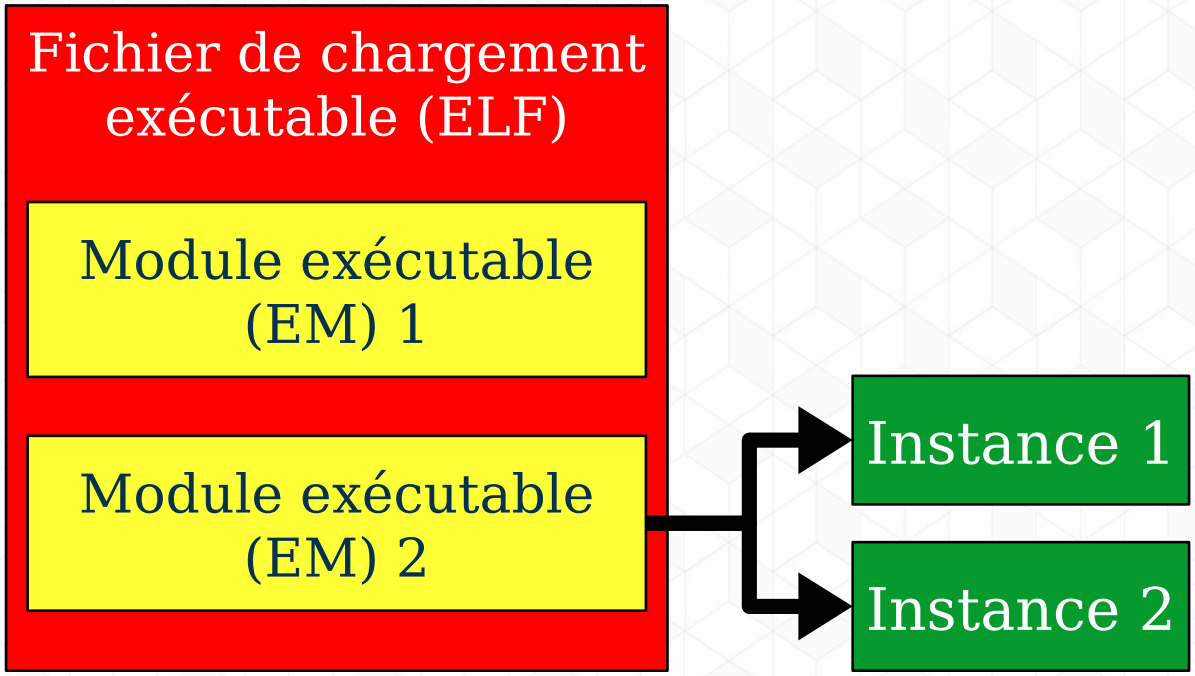
GlobalPlatform®

The Standard for Managing Applications on Secure Chip Technology

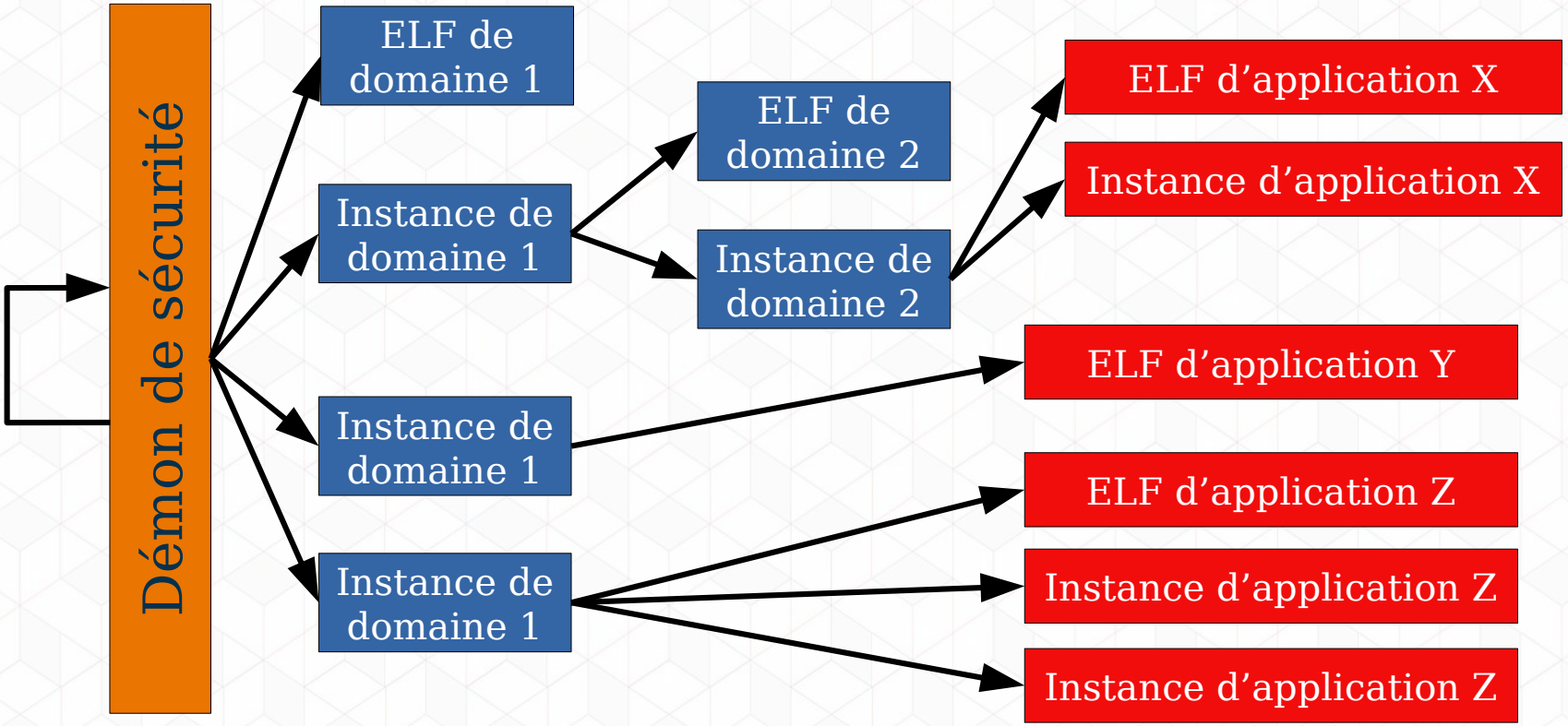
- Superviser les contenus et applications sur la carte
- Contrôler les droits et le partage de privilèges
- Sécuriser les communications (intra et extra-carte)
- Gérer les états de vie de la carte et des contenus
- ...

Gestion des contenus

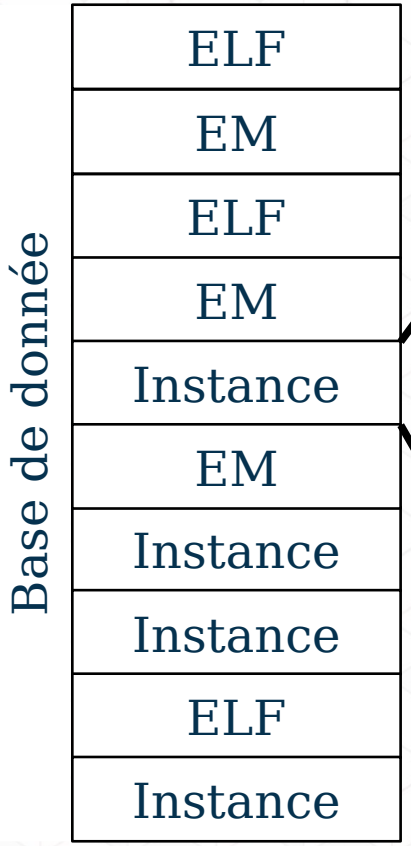
Structure des contenus



Le démon applique également des politiques de sécurité sur des applications pas encore instanciées.



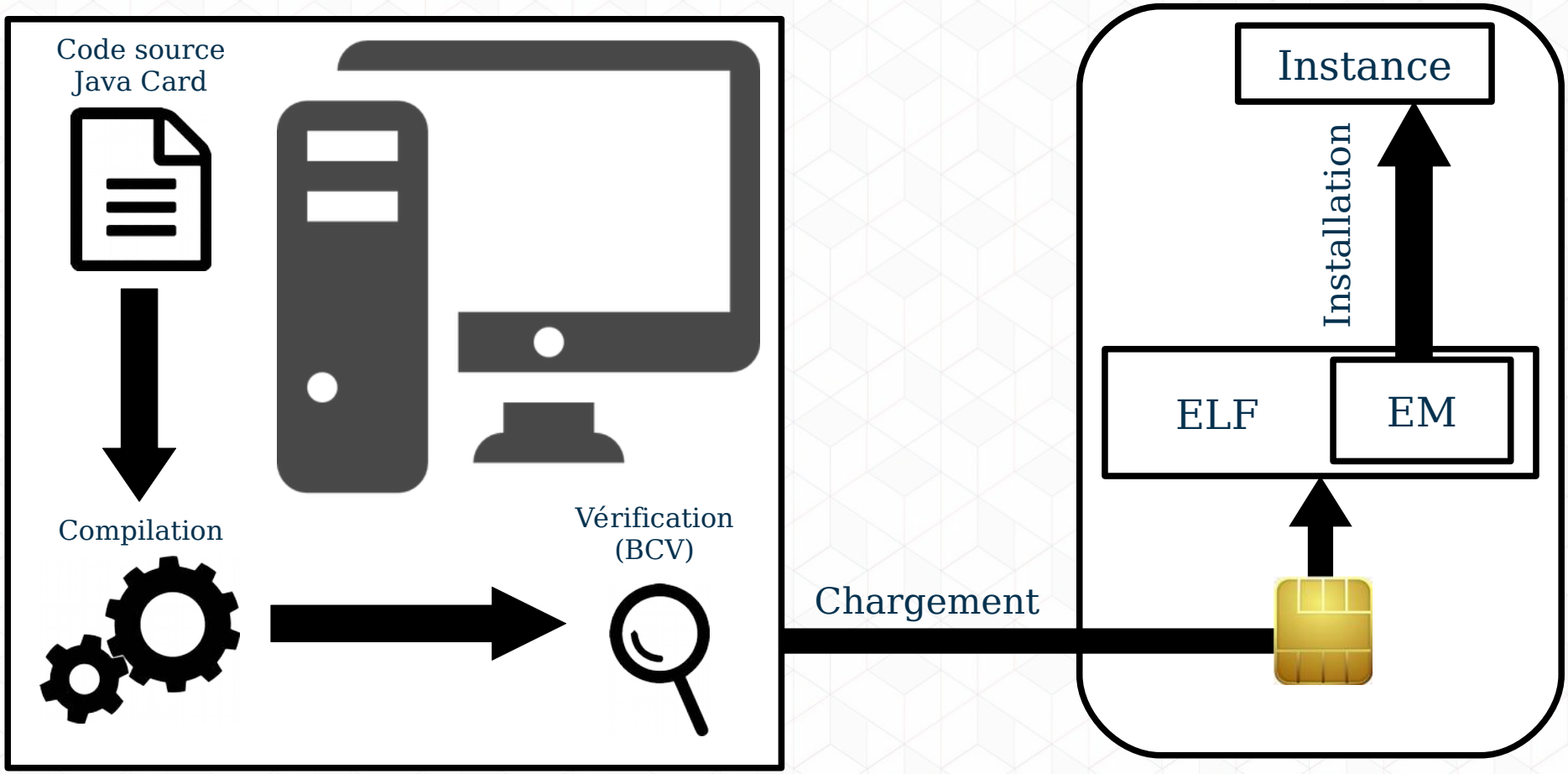
GlobalPlatform impose une certaine classification et ségrégation des applications.



- Indicateur pour différencier entre ELF, EM, ou instance
- Identifiant
- État de cycle de vie
- Entité parente
- Permissions
- Services globaux
- Éventuellement les identifiants des EM ou instances liés

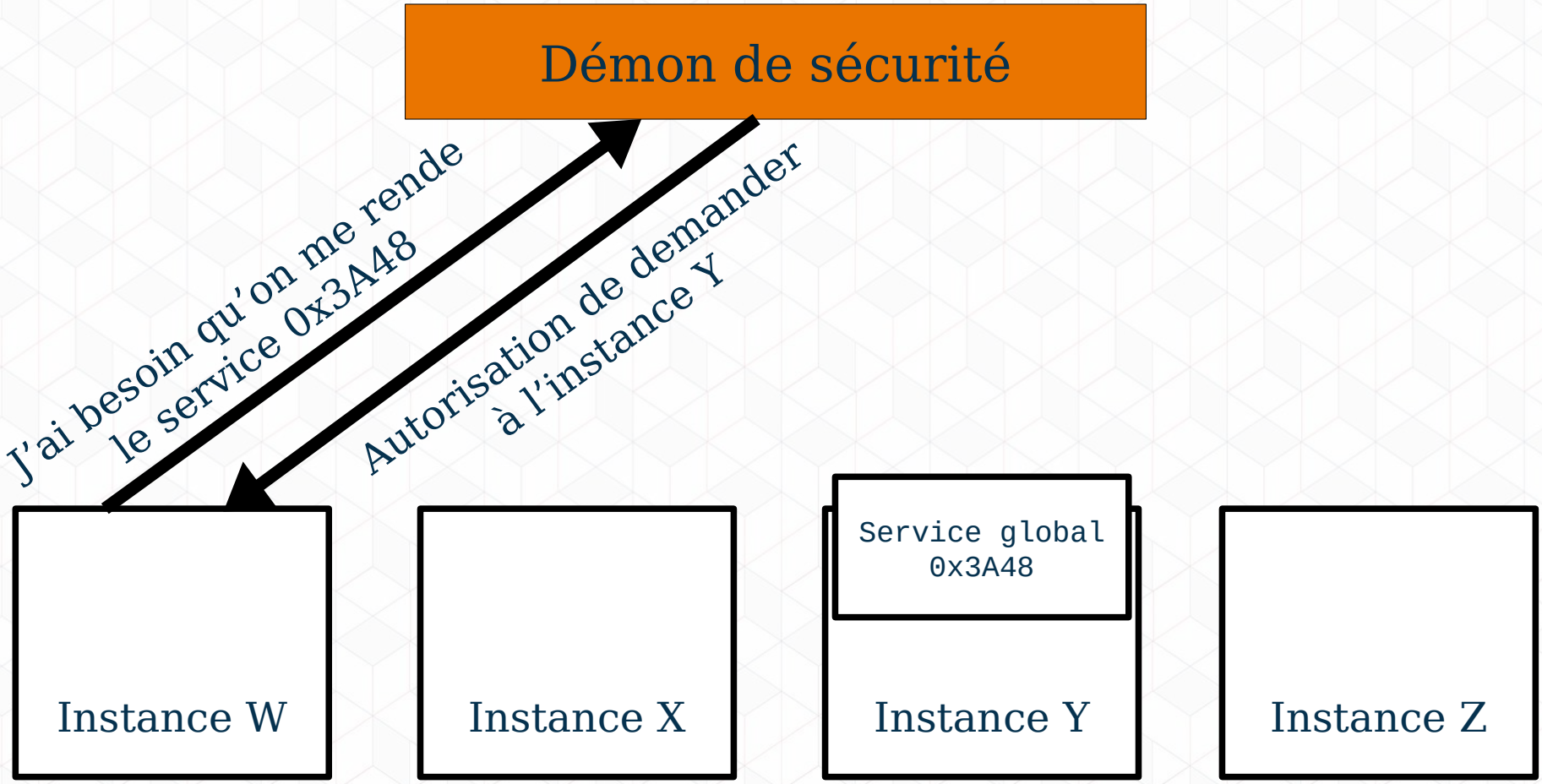
On choisit de modéliser notre base de données comme un long vecteur dont chaque élément est une structure commune à tout type d’entité.

Ajout d'un contenu



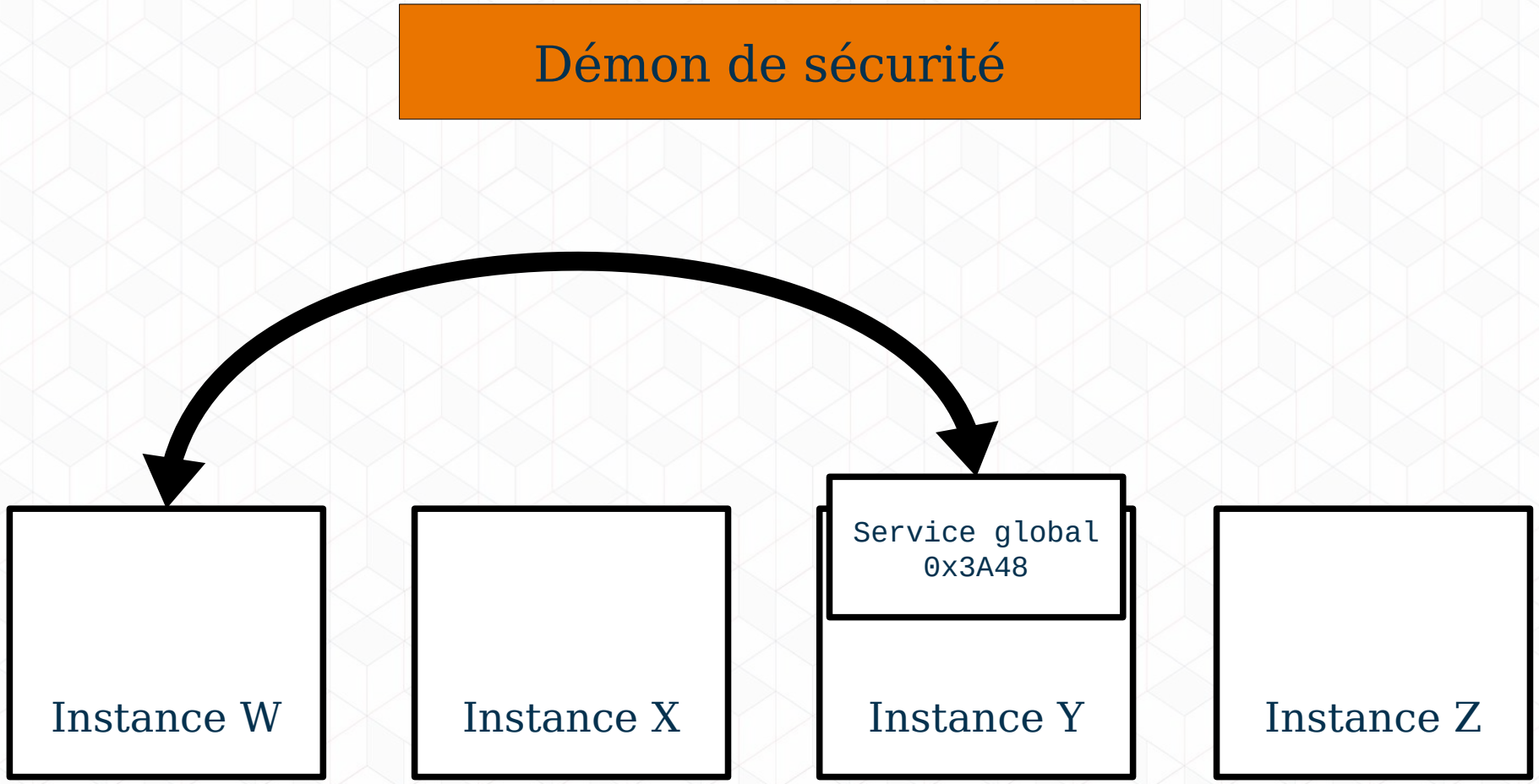
Les contraintes de sécurité complexifient la mise en place d'une application.

Gestion des services globaux



Le partage de services est strictement réglementé.

Gestion des services globaux



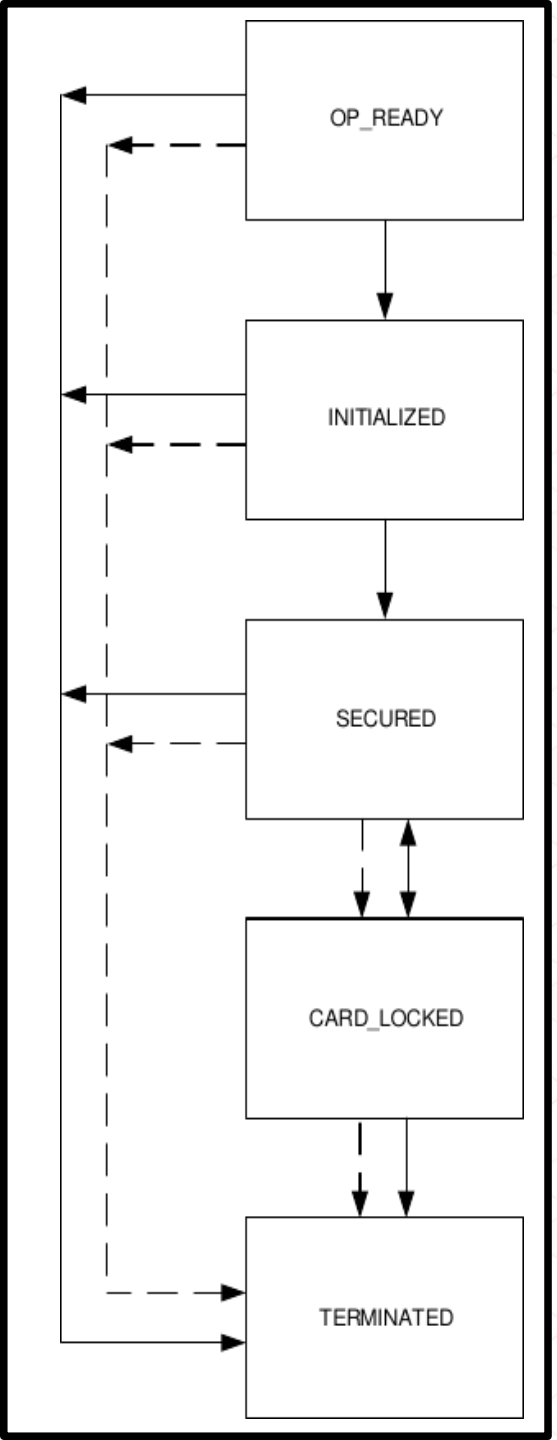
Le partage de services est strictement réglementé.

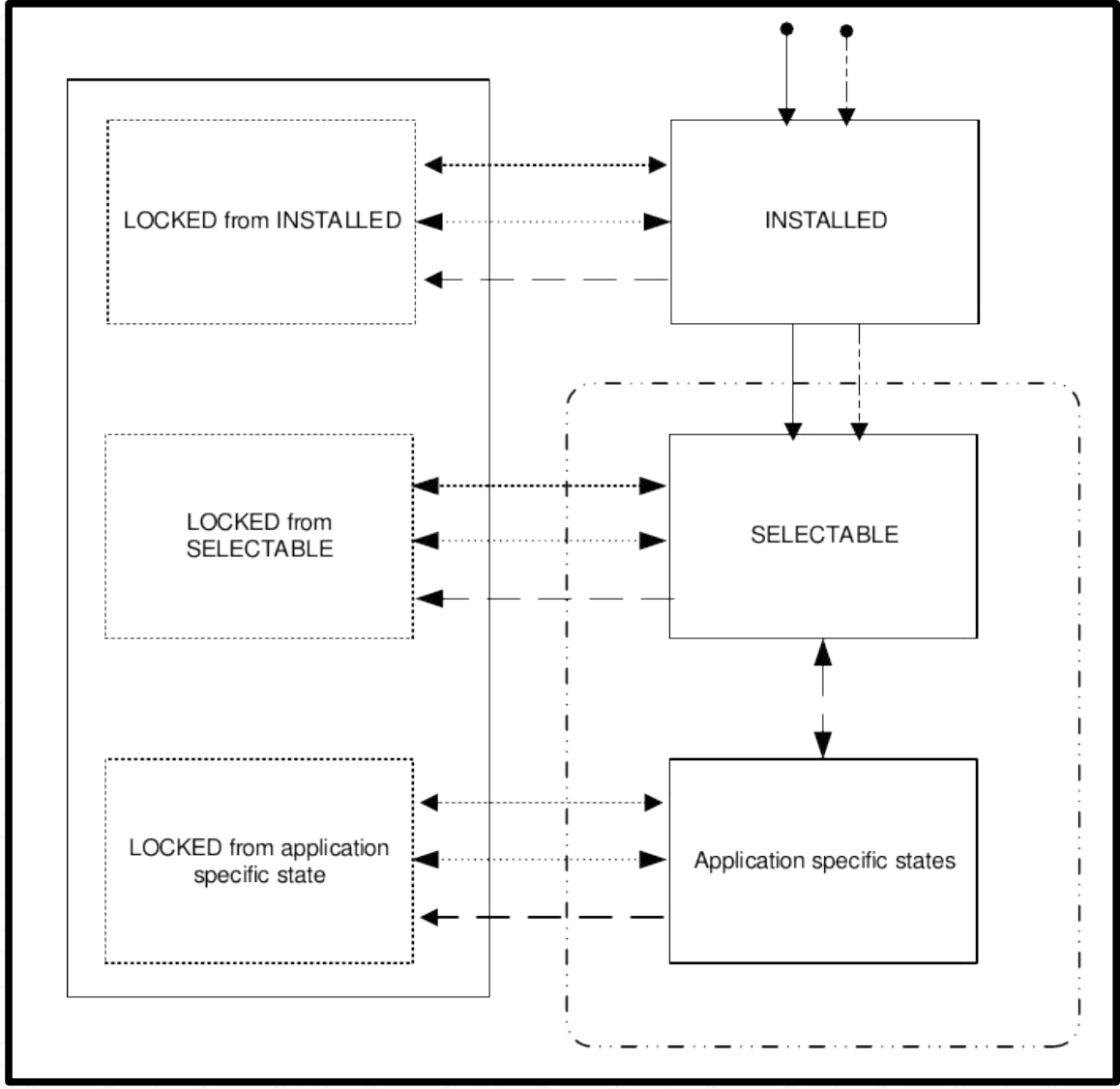
Permissions et états de vie

Le système de permissions mis en place est différent de ceux habituellement trouvés dans des systèmes classiques.

À l’heure actuelle, 20 privilèges sont définis dans l’environnement.

Si on peut les stocker comme bon nous semble, leur transmission entre applications est standardisée par GlobalPlatform.

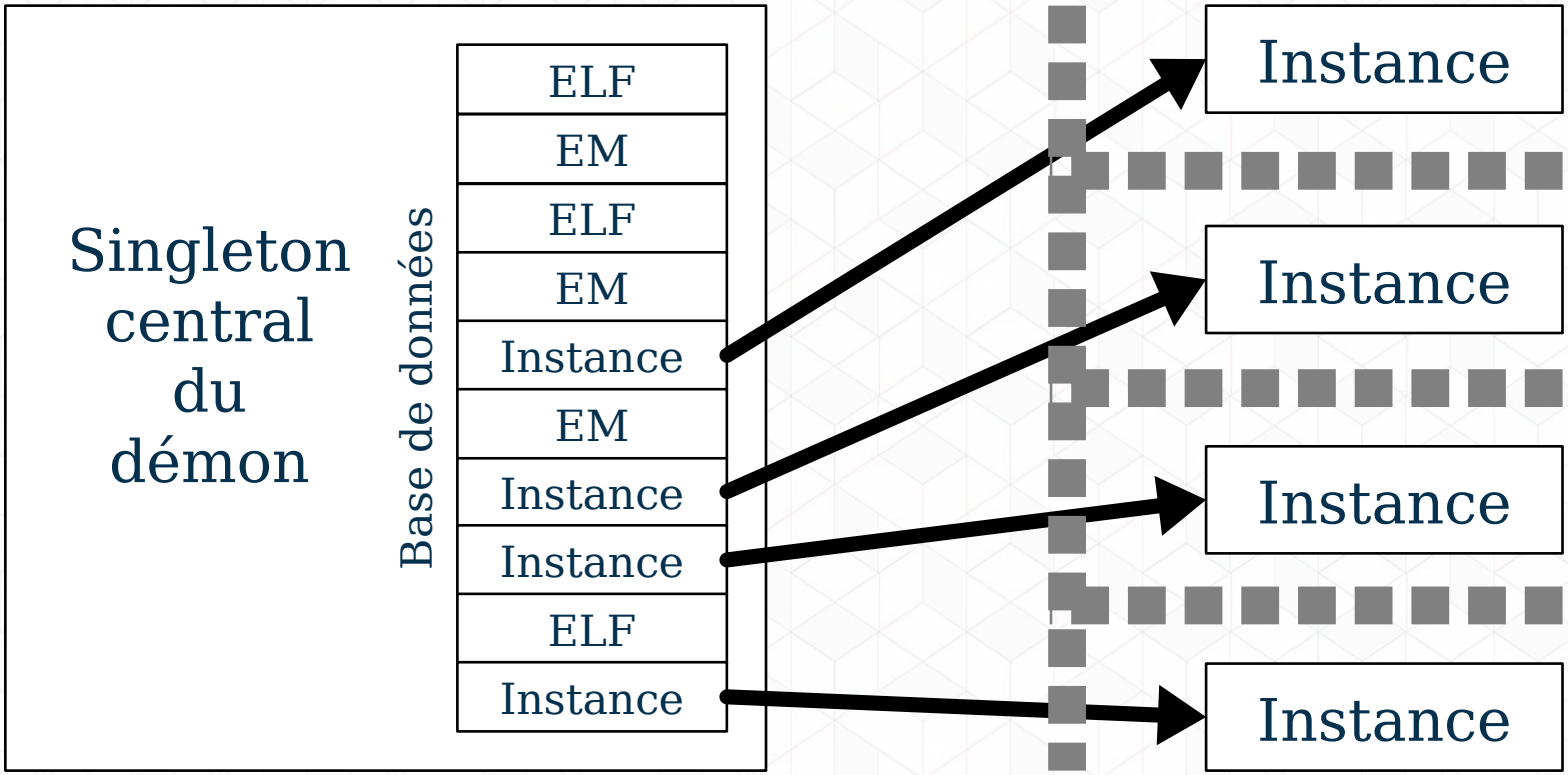


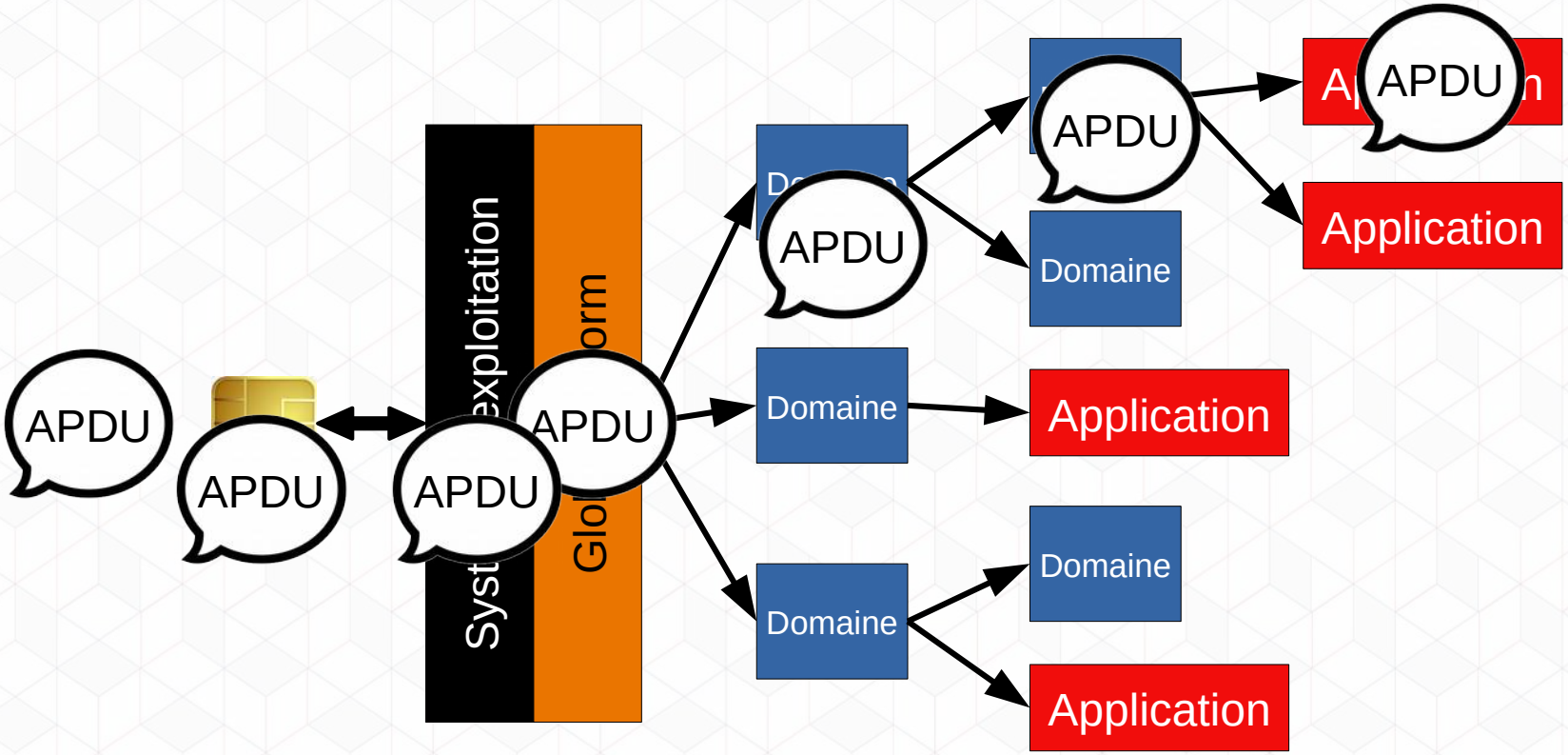


Un système d’états de vie est mis en place pour chaque application et pour la carte en elle-même.

Isolation et interactions des contenus

Ségréguer correctement les entités est crucial. Les appels ou partages de données doivent être strictement encadrés.





Lors du transit d'un message, de nombreux acteurs peuvent avoir leur mot à dire. Il faut s'assurer de respecter l'intervention de chacun.

Commande :	CLA	INS	P1	P2	Lc	Données	Le

Réponse :	Données	SW1	SW2

Conclusion

- Si l’essentiel du travail a été réalisé, certaines fonctionnalités ne l’ont pas été :
  - ✔ Gestion des contenus,
  - ✔ Cycles de vie,
  - ✔ Permissions,
  - ✔ Services globaux,
  - ✔ Gestion des partages,
  - ✔ Gestion des APDU,
  - ✗ Cryptographie,
  - ✗ Canaux logiques.
- Des mesures facilitant la réutilisation ont été prises.
- Le démon peut travailler avec n’importe quelle application développée en accord avec la spécification GlobalPlatform.
- À terme, le système complet devrait ouvrir de nombreuses possibilités de recherche ou d’exploitation.