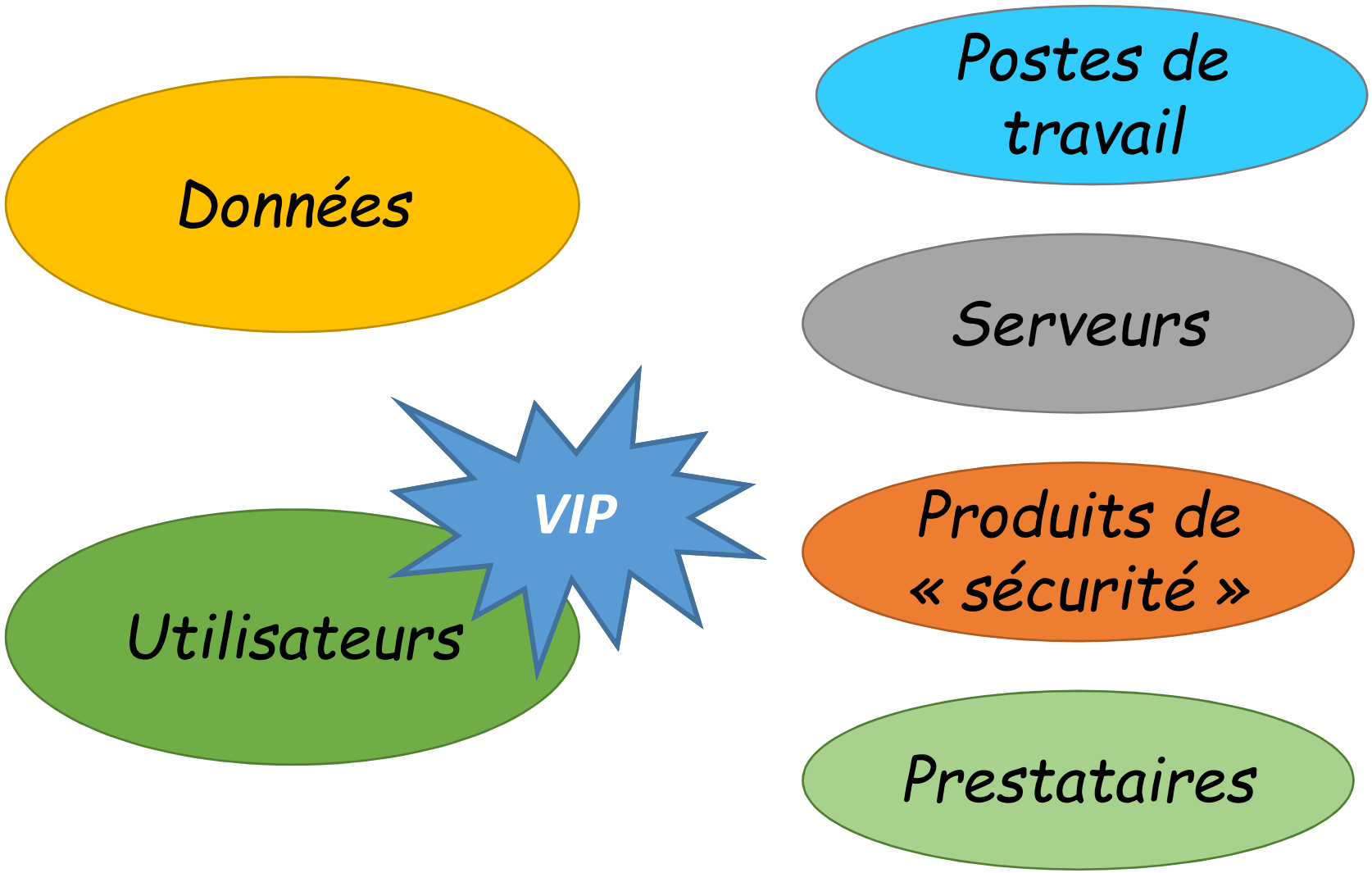
L’administration en silo

Aurélien Bordes

SSTIC – 7 juin 2017

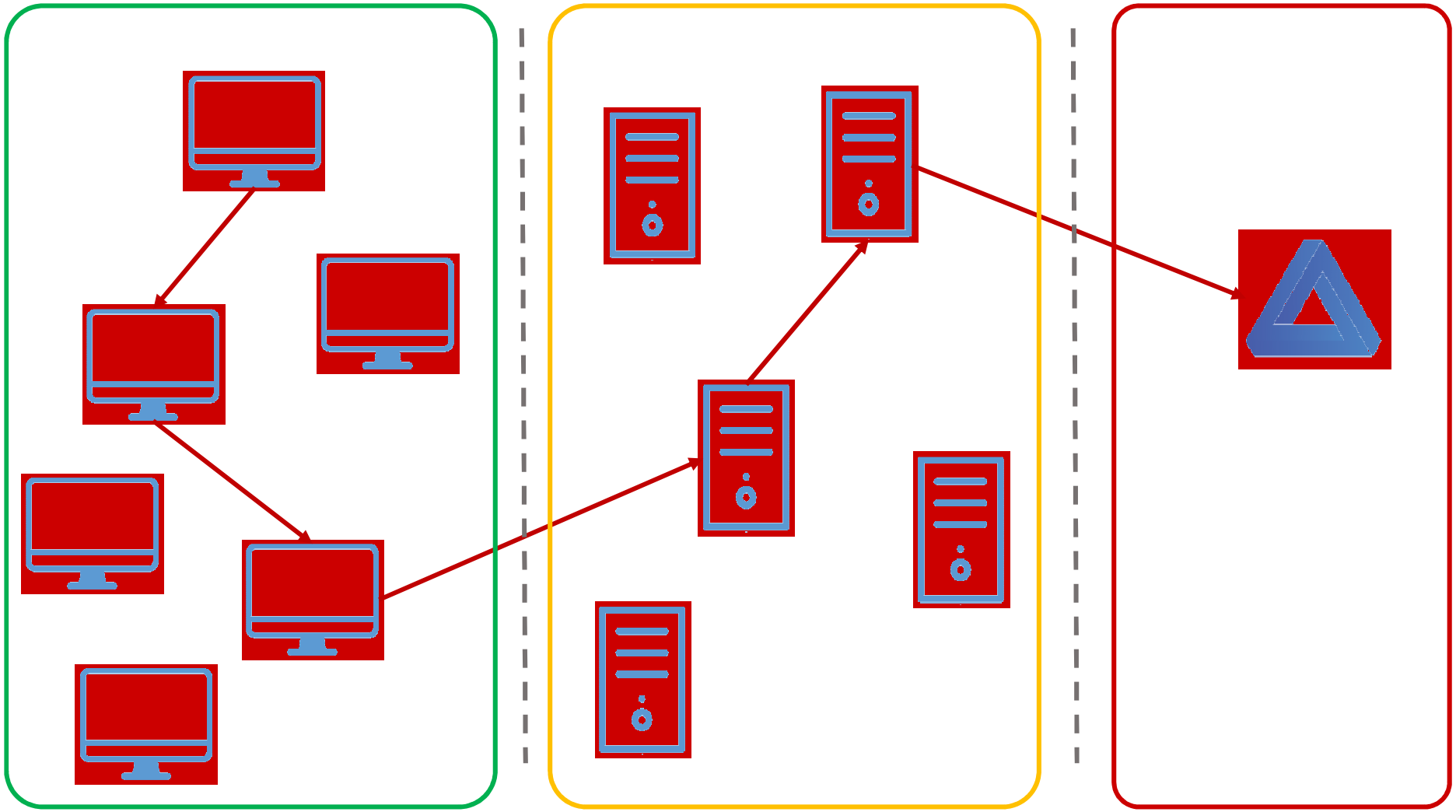
« Dessine-moi ton SI »



Acteurs d'un SI

- Les ressources
- Les utilisateurs
- Les administrateurs

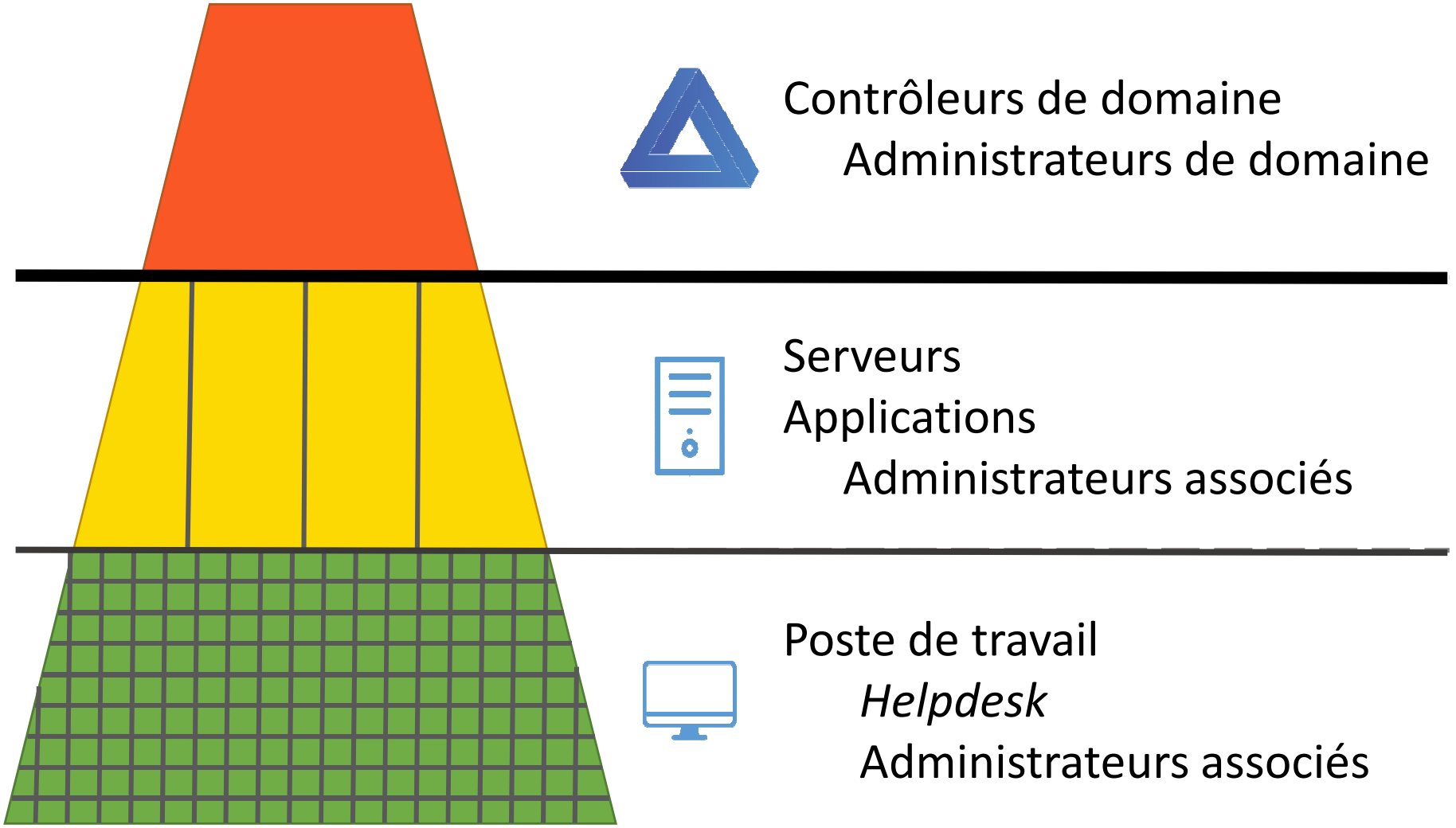
Synopsis d'une intrusion en environnement Active Directory



Mise en place des niveaux d'administration

- **ROUGE** :
  - Ressources et serveurs hébergeant des mécanismes d'administration auxquels toutes les ressources des autres niveaux sont adhérentes
- **JAUNE** :
  - Données métier et serveurs associés (messagerie, fichiers, bases de données, etc.)
  - Serveurs d'infrastructure
- **VERT** :
  - Postes de travail et le reste

Pyramide d'administration en environnement Active Directory

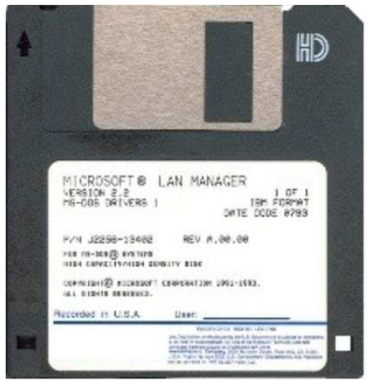


Méthodes d'élévation

- Récupération de secrets d'authentification en mémoire
- Réutilisation de mots de passe
- Tests de mots de passe prédictibles ou faibles
- Attaque sur les secrets des comptes avec des SPN
- Attaque sur les secrets des comptes sans pré-authentification Kerberos
- Attaque via les délégations d'authentification
- Récupération de MS-CACHE
- Récupération de fichiers de sauvegarde de l'AD
- Scripts dans les GPO
- Mot de passe de type *cpassword* dans les GPO de préférences
- Chemins de contrôle (droits sur objets de l'AD)
- *Pass-the-Hash*, *Pass-the-Key*
- Génération de TGT ou de ticket de service
- Prise de contrôle des hyperviseurs
- WSUS ☺

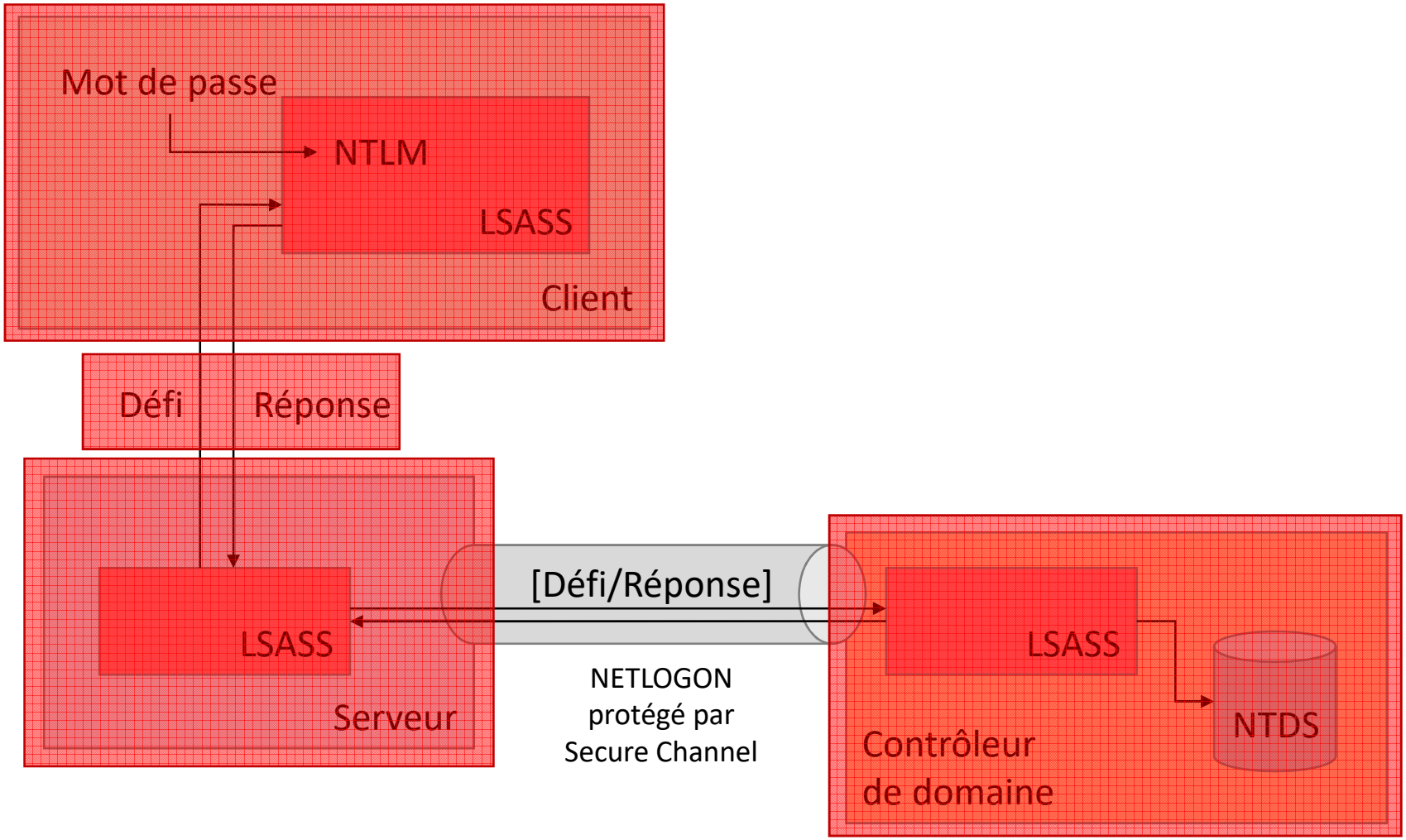
Deux protocoles d'authentification

NTLM (msv1_0)
(LAN Manager)

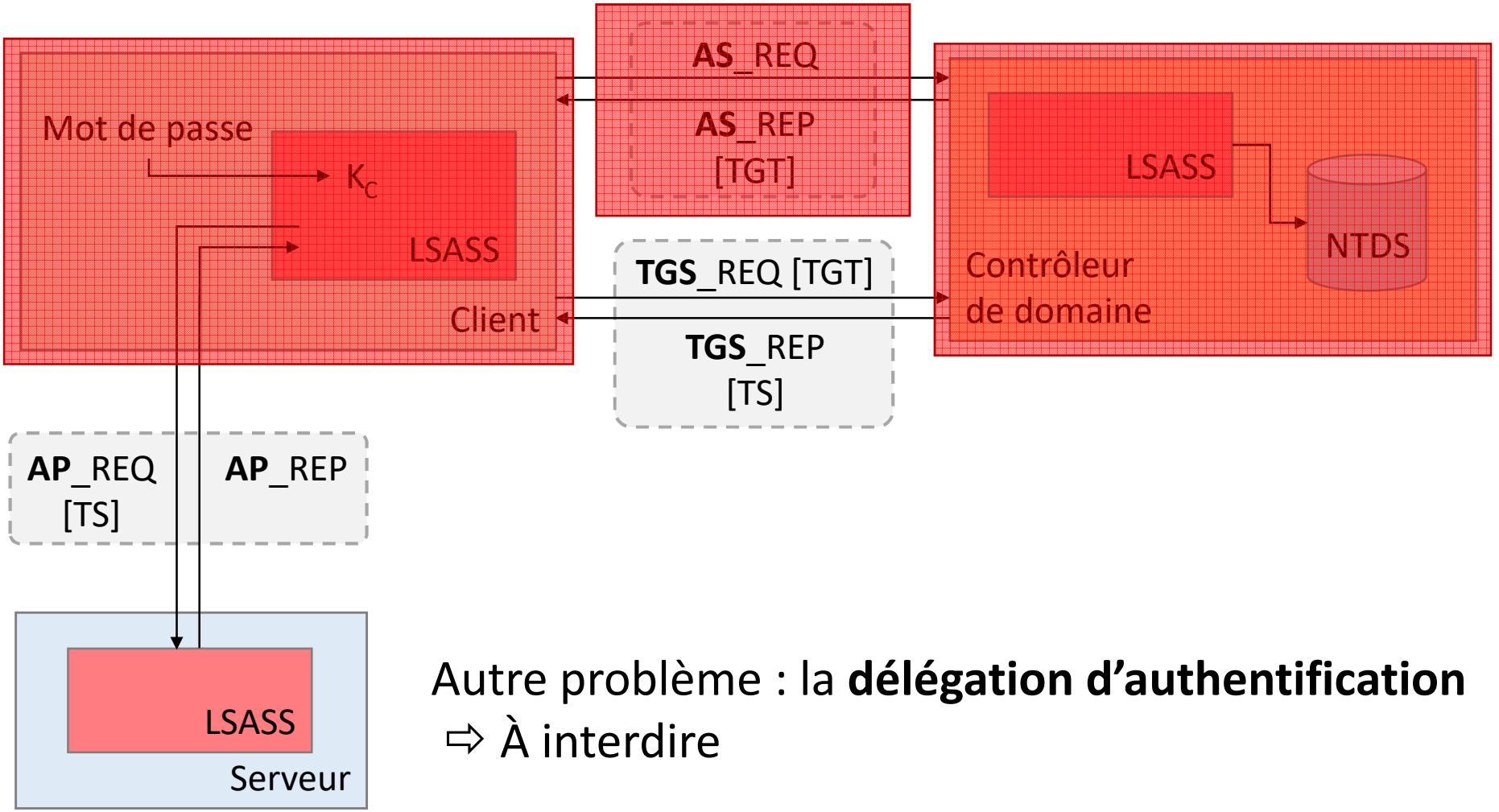


Kerberos
(Windows Server 2000)

NTLM


Mot de passe
NTLM
LSASS
Client
Défi
Réponse
LSASS
Serveur
[Défi/Réponse]
NETLOGON
protégé par
Secure Channel
LSASS
NTDS
Contrôleur
de domaine

Kerberos



Autre problème : la **délégation d'authentification**

⇨ À interdire

Échanges **AS** (AS_REQ/AS_REP) sans blindage

```
[AS-REQ]
  *padata:
    [PA-ENC-TIMESTAMP]
      [PA-ENC-TS-ENC]
        patimestamp: 20170607101242
req-body:
    [KDC-REQ-BODY]
```

K_C

K_C

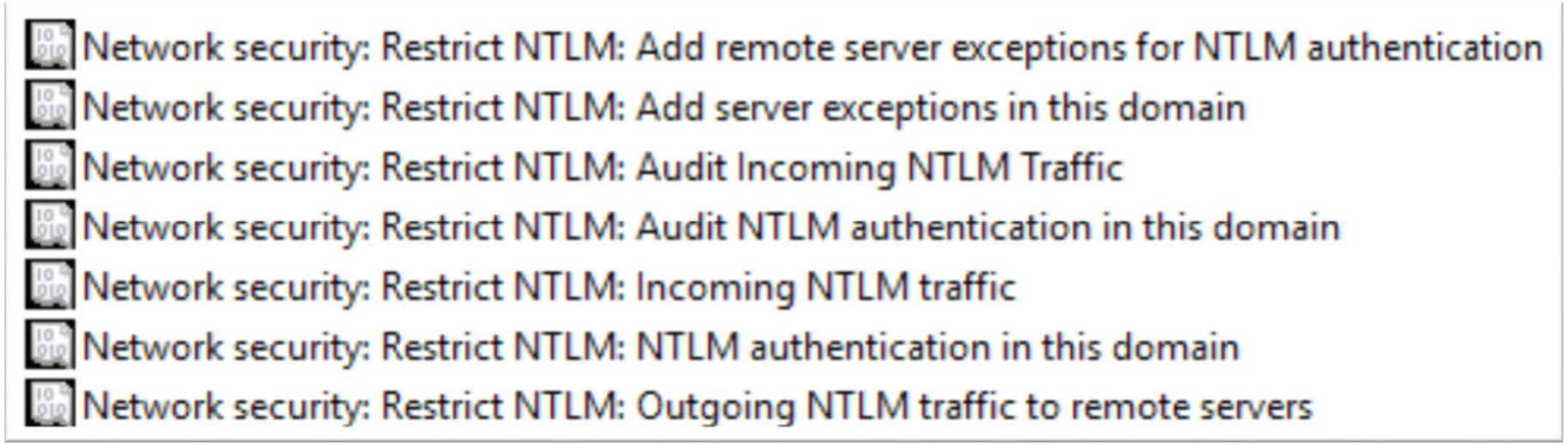
```
[AS-REP]
  ticket:
    [Ticket] (TGT user)
  enc-part:
      [EncKDCRepPart]
```

Sécurisation de l'authentification
Objectifs de sécurité

- NTLM :
  - interdire son utilisation
- Kerberos :
  - ne pas autoriser la délégation d'authentification
- Kerberos :
  - protéger les échanges **AS** (AS_REQ/AS_REP)
- Kerberos :
  - limiter les ordinateurs depuis lesquels les utilisateurs peuvent s'authentifier

Interdire NTLM – Stratégie globale

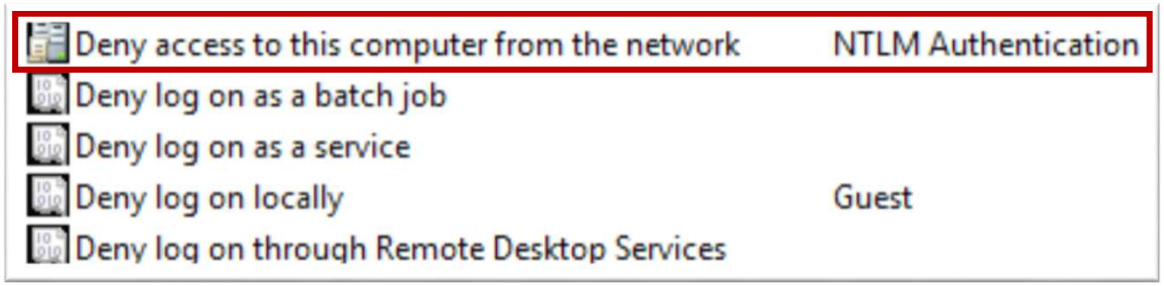
- Les restrictions NTLM, apparues avec Windows 7, permettent d'interdire globalement NTLM au niveau d'un système

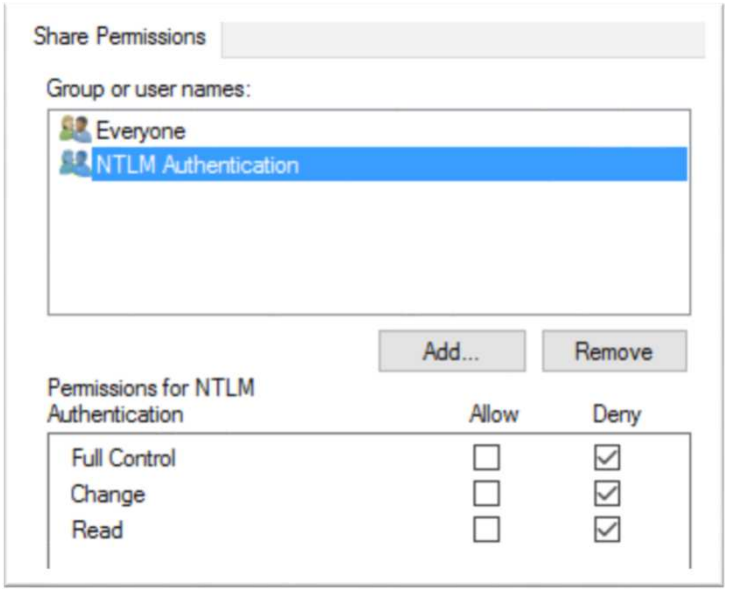


Interdire NTLM - Utilisation du SID **S-1-5-64-10** (AUTORITE NT\NTLM Authentication)

- Le SID « NTLM » est ajouté dans le jeton de sécurité en cas d'authentification d'un utilisateur via NTLM
- Ce SID peut alors être utilisé pour interdire des accès

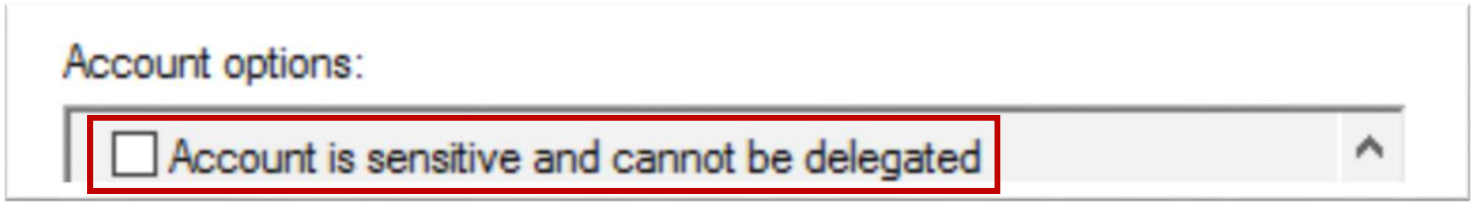
```
Block-SmbShareAccess -Name ShareName -AccountName "*S-1-5-64-10"
```

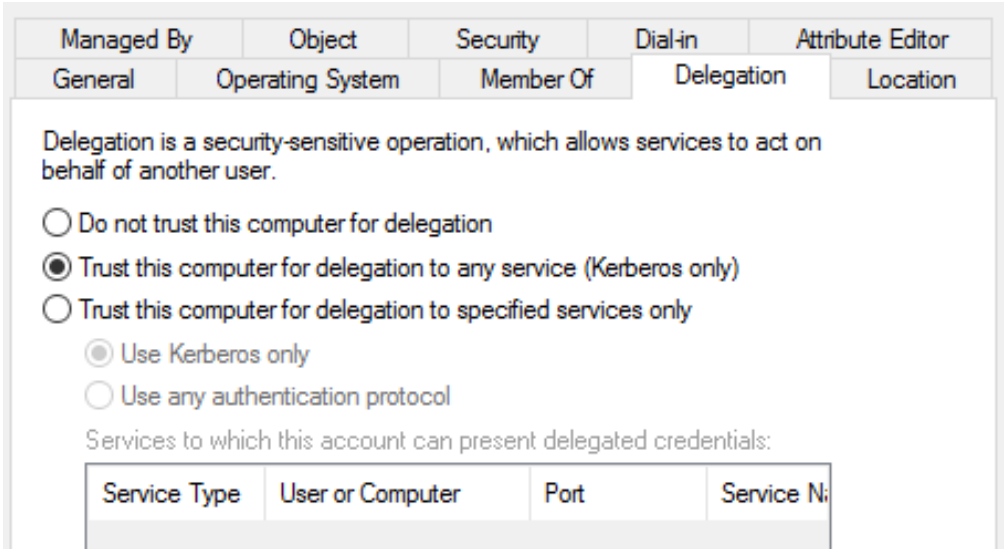




Interdire la délégation

- Pour être mise en œuvre, la délégation nécessite :
  - d'être activée sur les services
  - de ne pas être interdite au niveau des utilisateurs





Nouveaux mécanismes de protection avec Windows ou l'Active Directory

- *Protected Users Security Group*
- Blindage Kerberos *(Kerberos Armoring)*
- Revendications *(Claims)* :
  - Revendications utilisateurs *(User Claims)*
  - Revendications périphériques *(Device Claims)*
  - Attributs de ressource *(Resource Attributes)*
- Stratégies d'authentification *(Authentication Policies)*
- Silos d'authentification *(Authentication Policy Silos)*
- Authentification composée *(Compound Authentication)*

Protected Users Security Group
Windows 8.1 / Windows Server 2012 R2

- **Côté client :**
  - Désactivation de la mise en cache des secrets d'authentification (NTLM, CredSSP et Wdigest)
  - Désactivation de la mise en cache des clés Kerberos
    - Renouvellement de TGT impossible
- **Côté KDC (contrôleur de domaine) :**
  - Désactivation de NetLogon (validation NTLM)
  - Kerberos : désactivation de DES et RC4
  - Kerberos : interdiction de la délégation d'authentification

⇨ Ajouter à ce groupe les comptes ROUGE

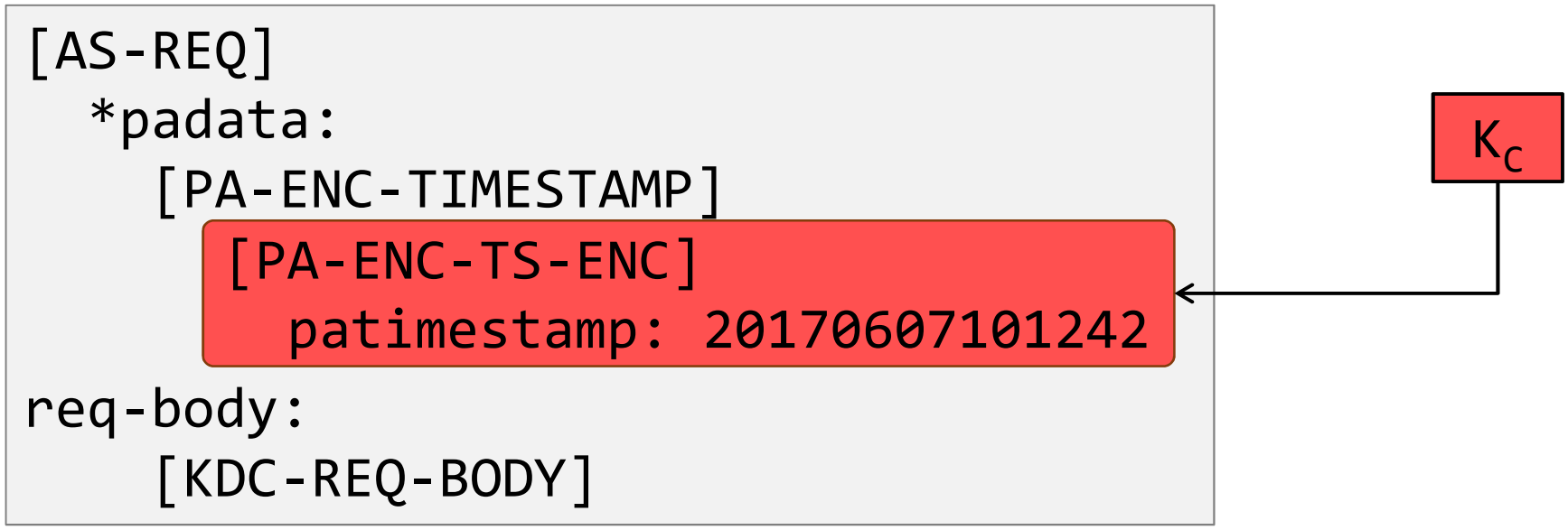
Sécurisation de l'authentification
Objectifs de sécurité

- ~~NTLM :~~ ✓ *Protected Users*
  - ~~interdire son utilisation~~
- ~~Kerberos :~~ ✓ *Protected Users*
  - ~~ne pas autoriser la délégation d'authentification~~
- Kerberos :
  - protéger les échanges **AS** (AS_REQ/AS_REP)
- Kerberos :
  - limiter les ordinateurs depuis lesquels les utilisateurs peuvent s'authentifier

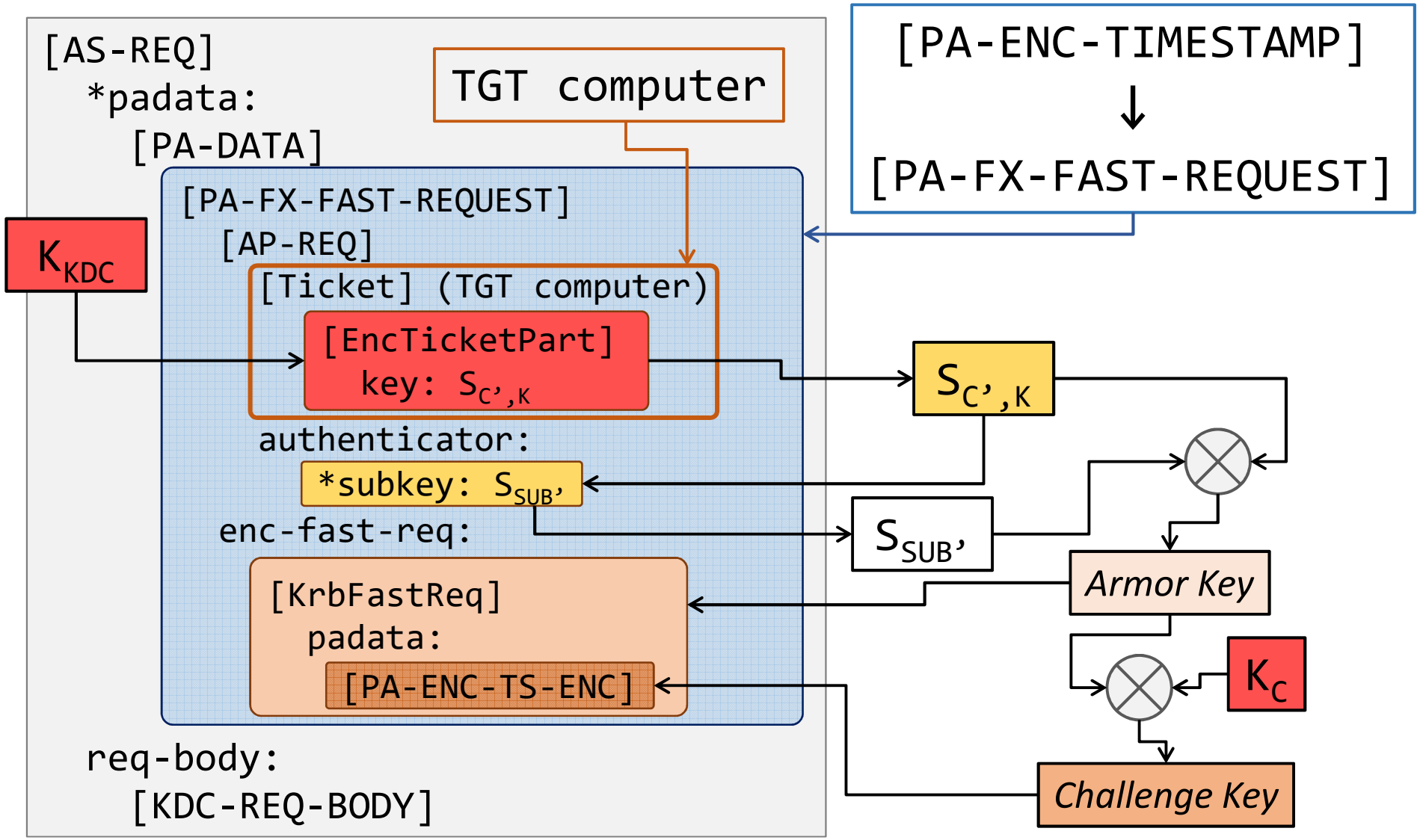
Blindage Kerberos
Windows 8 / Windows Server 2012

- Implémentation du protocole FAST *(Flexible Authentication via Secure Tunneling)*
- Permet de renforcer la protection des échanges :
  - **AS** (AS_REQ/AS_REP)
  - **TGS** (TGS_REQ/TGS_REP)
- Nécessite un TGT et la clé de session associée pour la protection
  - Utilisation de celui de la machine

Requêtes AS_REQ sans blindage



Requête AS_REQ avec blindage



Conséquences du blindage

- L'utilisateur ne peut plus générer de requêtes AS_REQ (pas d'accès au TGT de la machine et à $S_{C'}, _{K}$)
  - Seul LSASS peut le faire

- Il n'y a plus bloc directement chiffré par K_C
  - Les messages **AS** (AS_REQ/AS_REP) ne sont plus vulnérables

- Le KDC dispose du TGT de la machine depuis laquelle l'utilisateur s'authentifie

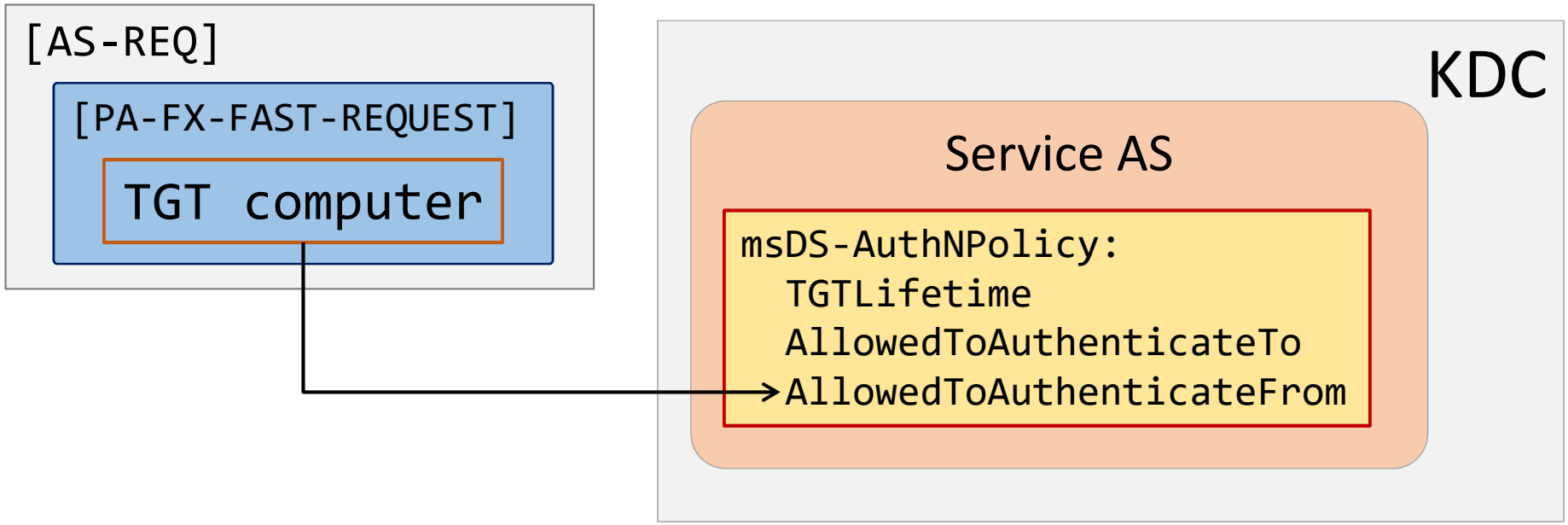
Sécurisation de l'authentification
Objectifs de sécurité

- ~~NTLM :~~ ✓ *Protected Users*
  - ~~interdire son utilisation~~
- ~~Kerberos :~~ ✓ *Protected Users*
  - ~~ne pas autoriser la délégation d'authentification~~
- ~~Kerberos :~~ ✓ Blindage Kerberos
  - ~~protéger les échanges **AS** (AS_REQ/AS_REP)~~
- Kerberos :
  - limiter les ordinateurs depuis lesquels les utilisateurs peuvent s'authentifier

Stratégies d'authentification
Windows Server 2012 R2

- Les stratégies d'authentification permettent d'appliquer des restrictions lors des demandes de TGT et ticket de service :
  - TGT : limite de la durée de vie du TGT
  - TS : restriction du *To*
  - **TGT : restriction du *From***

Utilise le TGT de l'ordinateur présenté grâce au blindage Kerberos

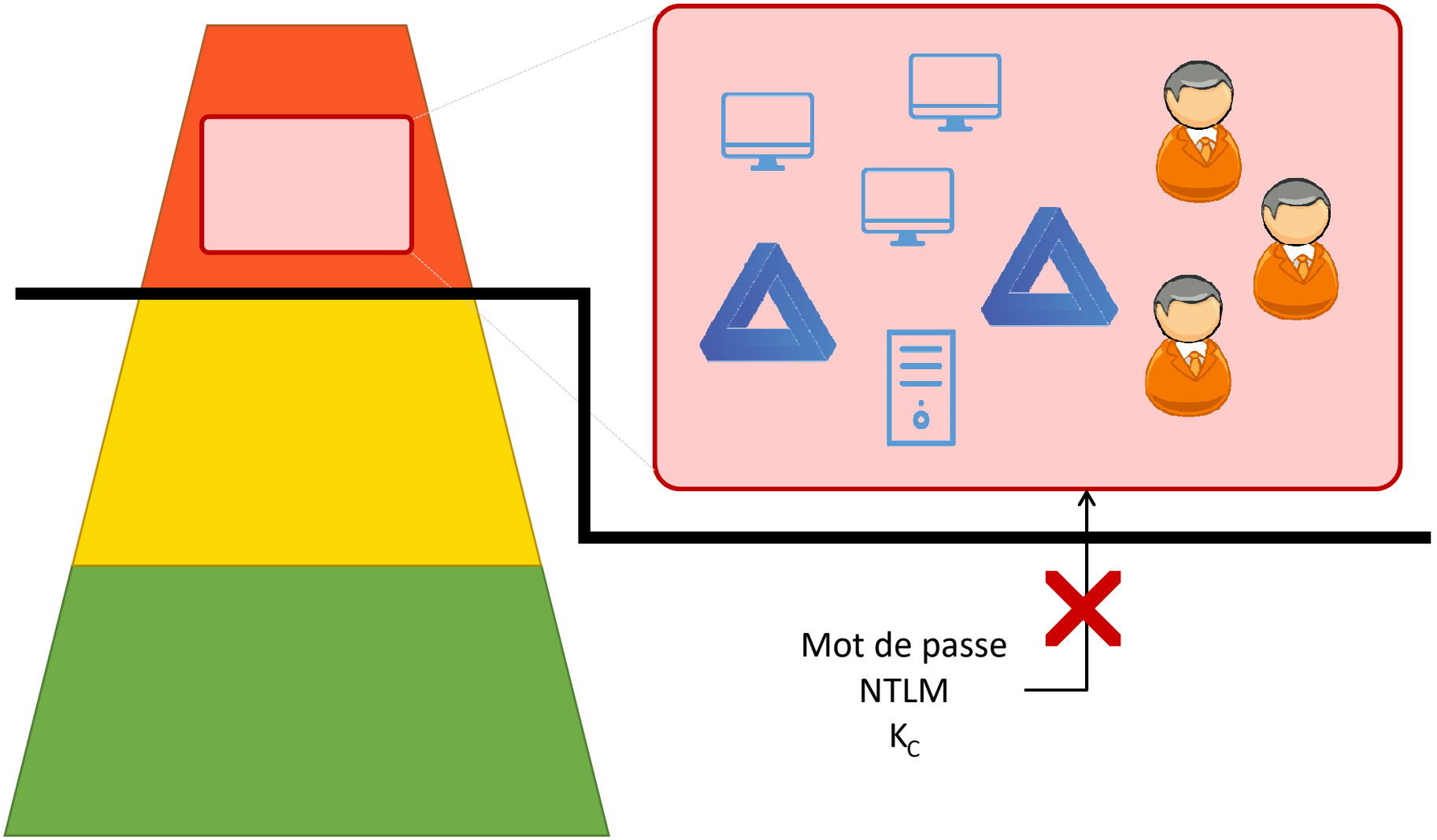


Démo 1

Silo d'authentification
Windows Server 2012 R2

- Un silo d'authentification permet de simplifier la mise en place des stratégies d'authentification
- Un silo d'authentification est caractérisé par :
  - Un ensemble de machines et d'utilisateurs
  - Une stratégie d'authentification
- La stratégie d'authentification doit autoriser l'authentification des utilisateurs du silo uniquement depuis les machines du silo

Le silo ROUGE



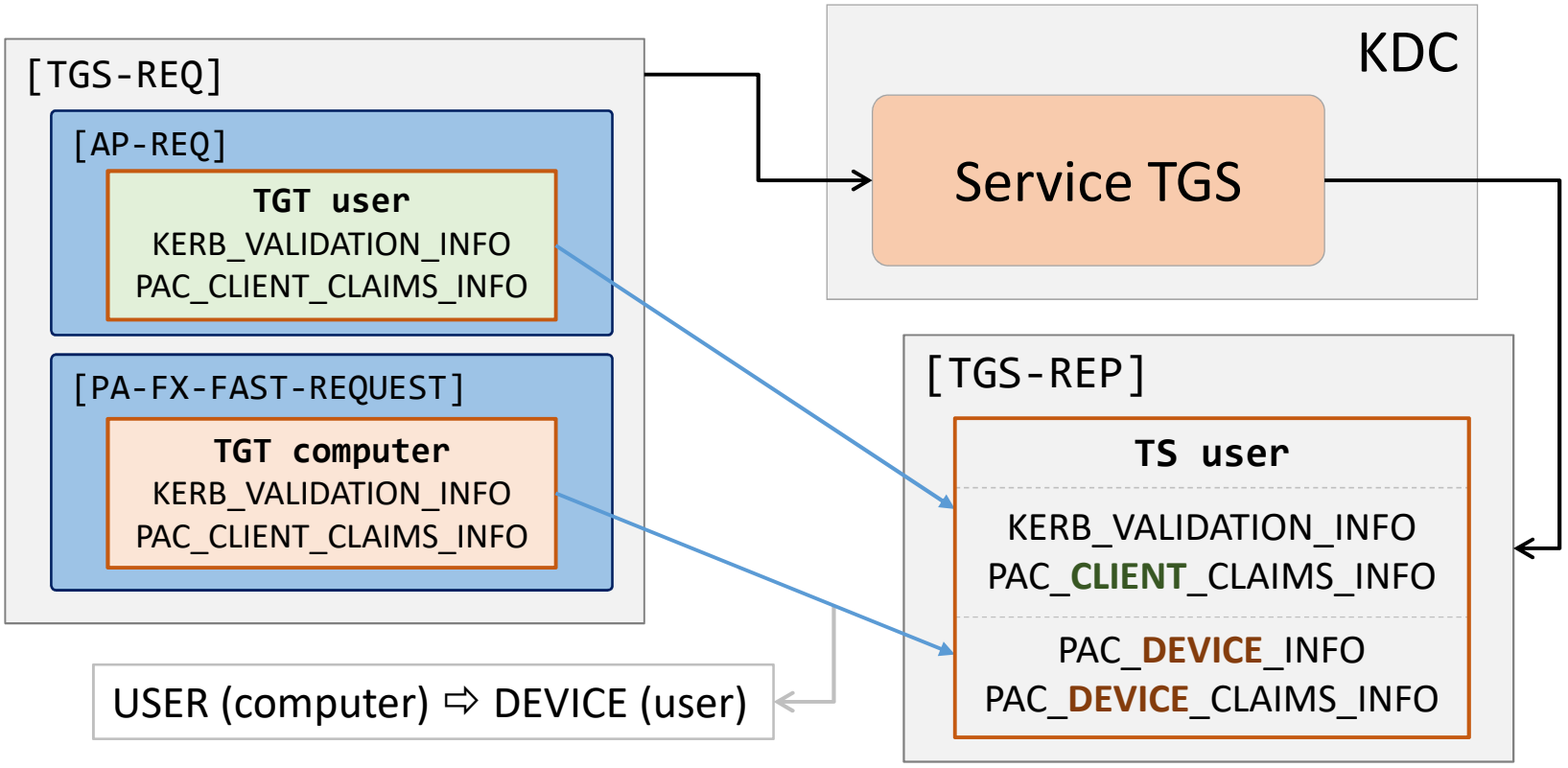
Démo 2

Sécurisation de l'authentification
Objectifs de sécurité

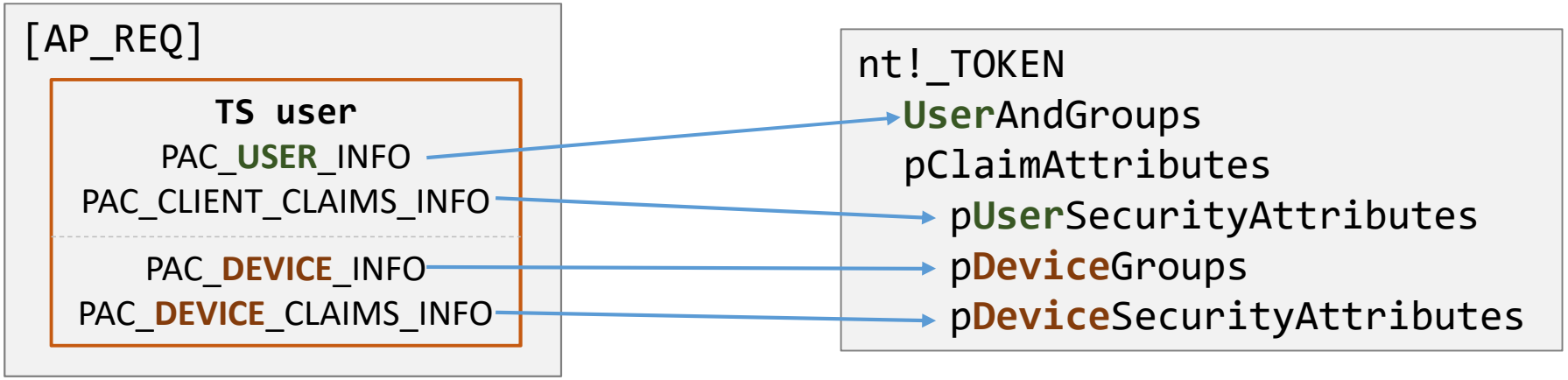
- ~~NTLM :~~ ✓ *Protected Users*
  - ~~interdire son utilisation~~
- ~~Kerberos :~~ ✓ *Protected Users*
  - ~~ne pas autoriser la délégation d'authentification~~
- ~~Kerberos :~~ ✓ Blindage Kerberos
  - ~~protéger les échanges **AS** (AS_REQ/AS_REP)~~
- ~~Kerberos :~~ ✓ Stratégies d'authentification
  - ~~limiter les ordinateurs depuis lesquels les utilisateurs peuvent s'authentifier~~

Authentification composée
Windows 8 / Windows Server 2012

- Mise en œuvre par le blindage des messages TGS
- Les données d'autorisation contenues dans le TGT de la machine sont fusionnées avec celles de l'utilisateur



Utilisation dans le contrôle d'accès




```
SECURITY DESCRIPTOR
  (A;;FA;;;WD)
```
Filtrage sur les SID de l'utilisateur

```
  (XA;;FA;;;WD;(@USER.ad://ext/AuthenticationSilo Any_of {"ROUGE"}))
```
Filtrage sur les revendications de l'utilisateur

```
  (XA;;FA;;;WD;(Device_Member_of_any {SID(DD)}))
```
Filtrage sur les SID de la machine

```
  (XA;;FA;;;WD;(@DEVICE.ad://ext/AuthenticationSilo Any_of {"ROUGE"}))
```
Filtrage sur les revendications de la machine

Démo 3

Conclusions

- Protections :
  - 5 ans après, toujours méconnues et peu utilisées
  - Simples à mettre en œuvre
    - Mais reposant sur des concepts et des mécanismes de sécurité de plus en plus complexes
  - Permettent de cloisonner efficacement les niveaux d'authentification (en particulier le ROUGE)
- Nécessite une hygiène minimum
  - Windows Server 2012 / Windows 8
  - Peu de comptes de niveau ROUGE
- Ne sont pas une protection absolue
  - Ne peut rien contre la perte du compte krbtgt

Kerberos *samples* :

http://aurelien26.free.fr/kerberos/

TS (Terminal Service) Security Editor :

https://github.com/aurel26/TS-Security-Editor

Questions ?

aurelien26 (at) free.fr