
SECRETS D'AUTHENTIFICATION

Épisode II

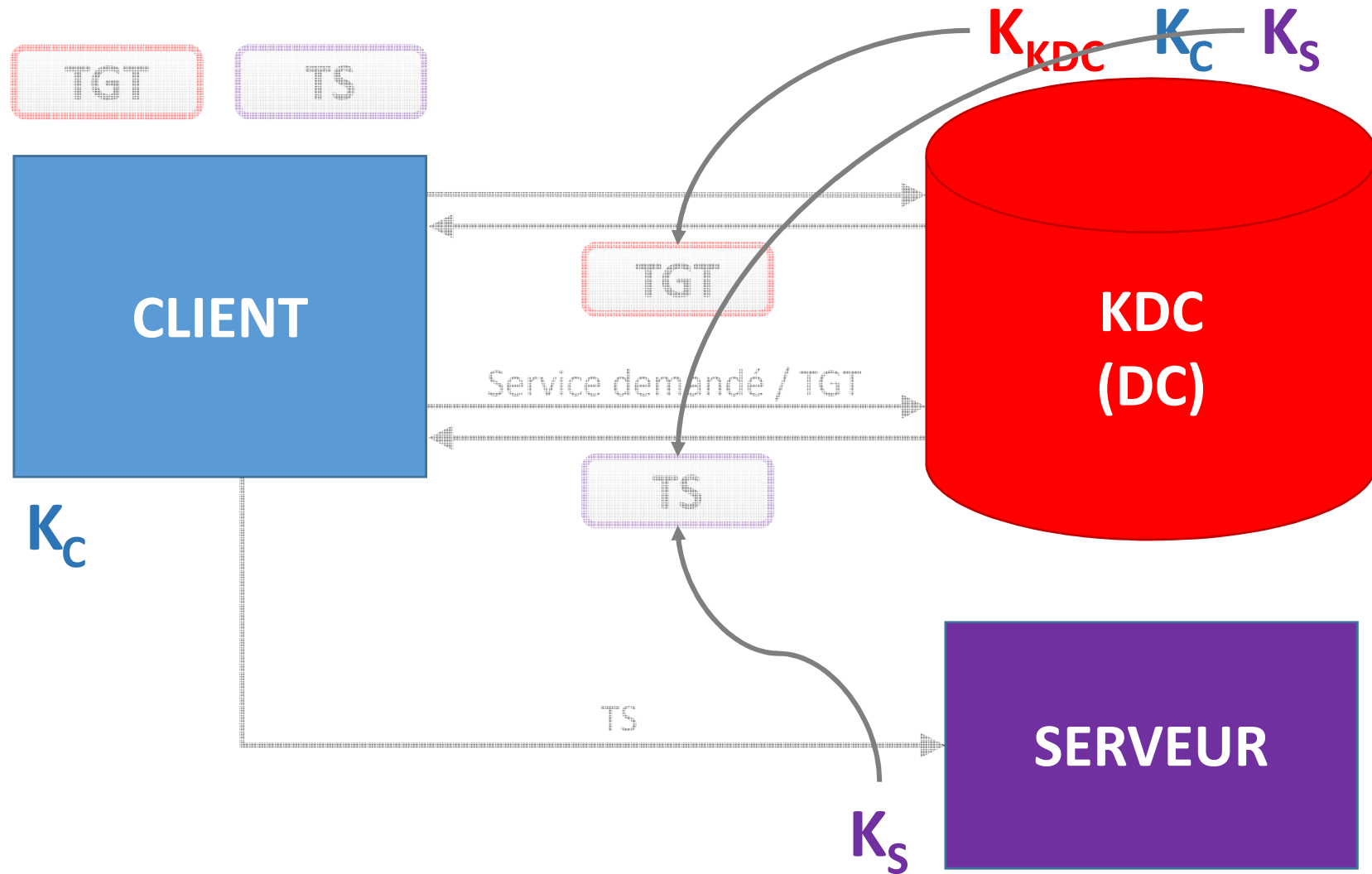
KERBEROS CONTRE-ATTAQUE

Aurélien Bordes
SSTIC – 4 juin 2014

Objectifs

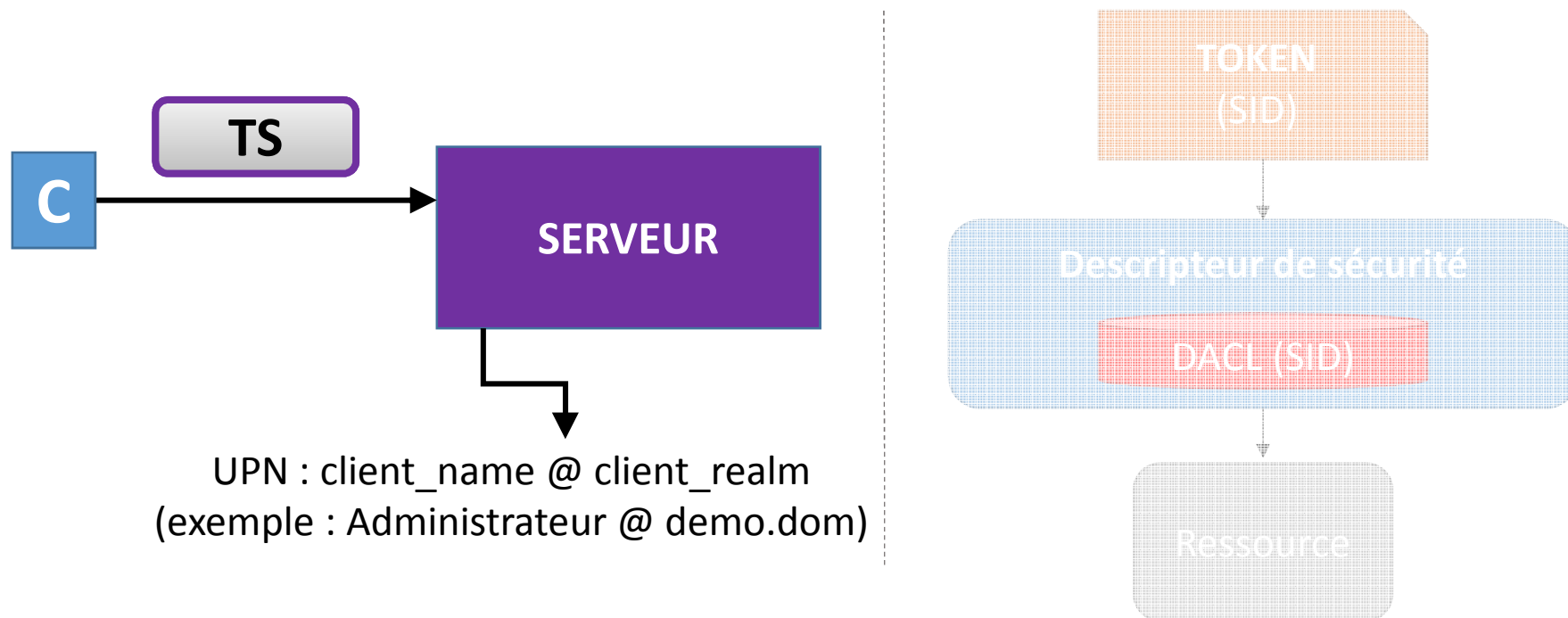
- Détailler le fonctionnement et les spécificités de Kerberos en environnement Active Directory :
 - **Autorisation (PAC)**
 - **Fonctionnement du compte krbtgt**
 - **Relations d'approbation**
 - **Journalisation des évènements Kerberos**
 - Délégation
 - Sélection des algorithmes de chiffrement
 - Gestion des cartes à puce avec PKINIT
 - Service for User (S4U)
- Montrer les problématiques liées à une compromission d'un domaine Active Directory (*pwdump*) :
 - Actions possibles de l'attaquant
 - Problèmes de remédiation

Kerberos en 1 planche...



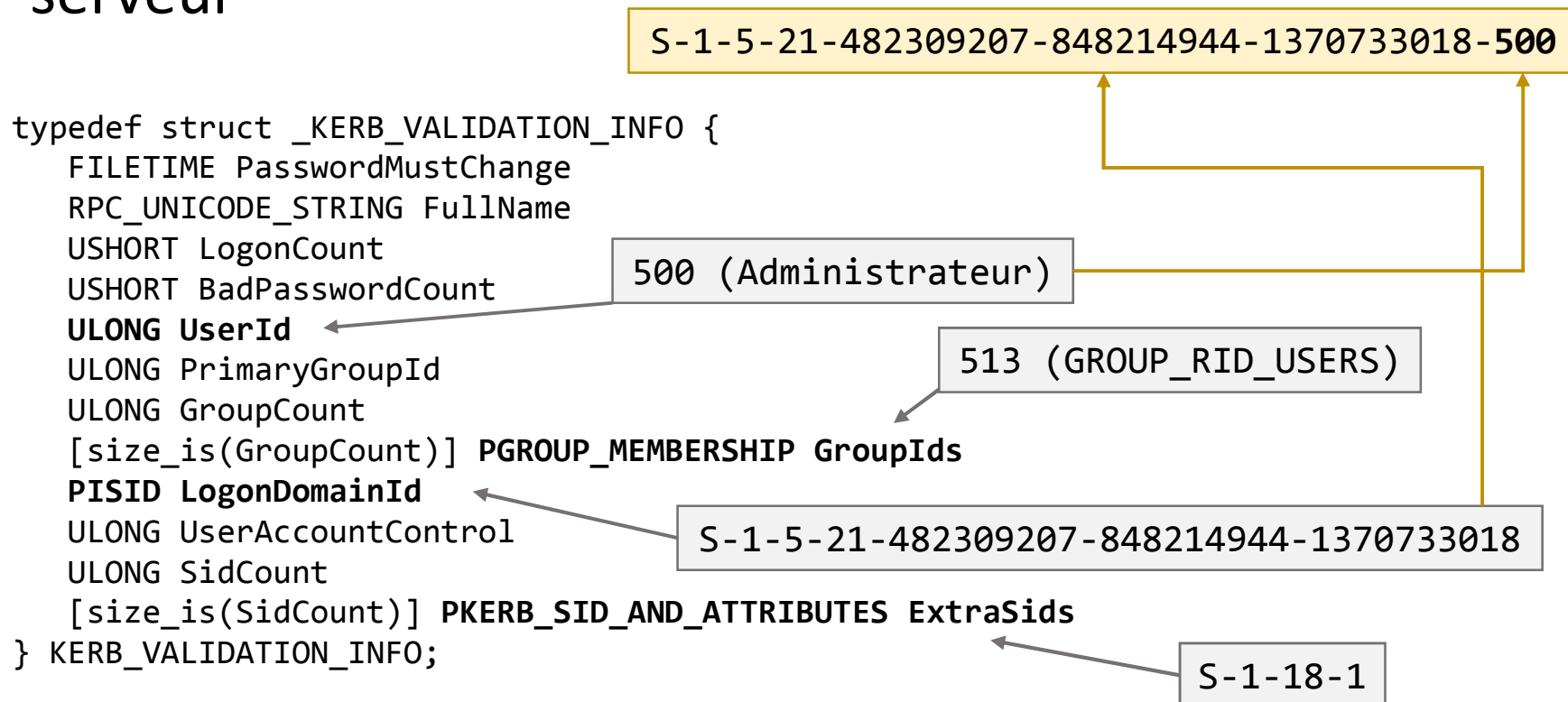
Kerberos et l'autorisation

- De base, Kerberos permet d'authentifier les utilisateurs
- Mais Kerberos reste insuffisant vis-à-vis du contrôle d'accès de Windows (qui repose sur les SID)



Autorisation

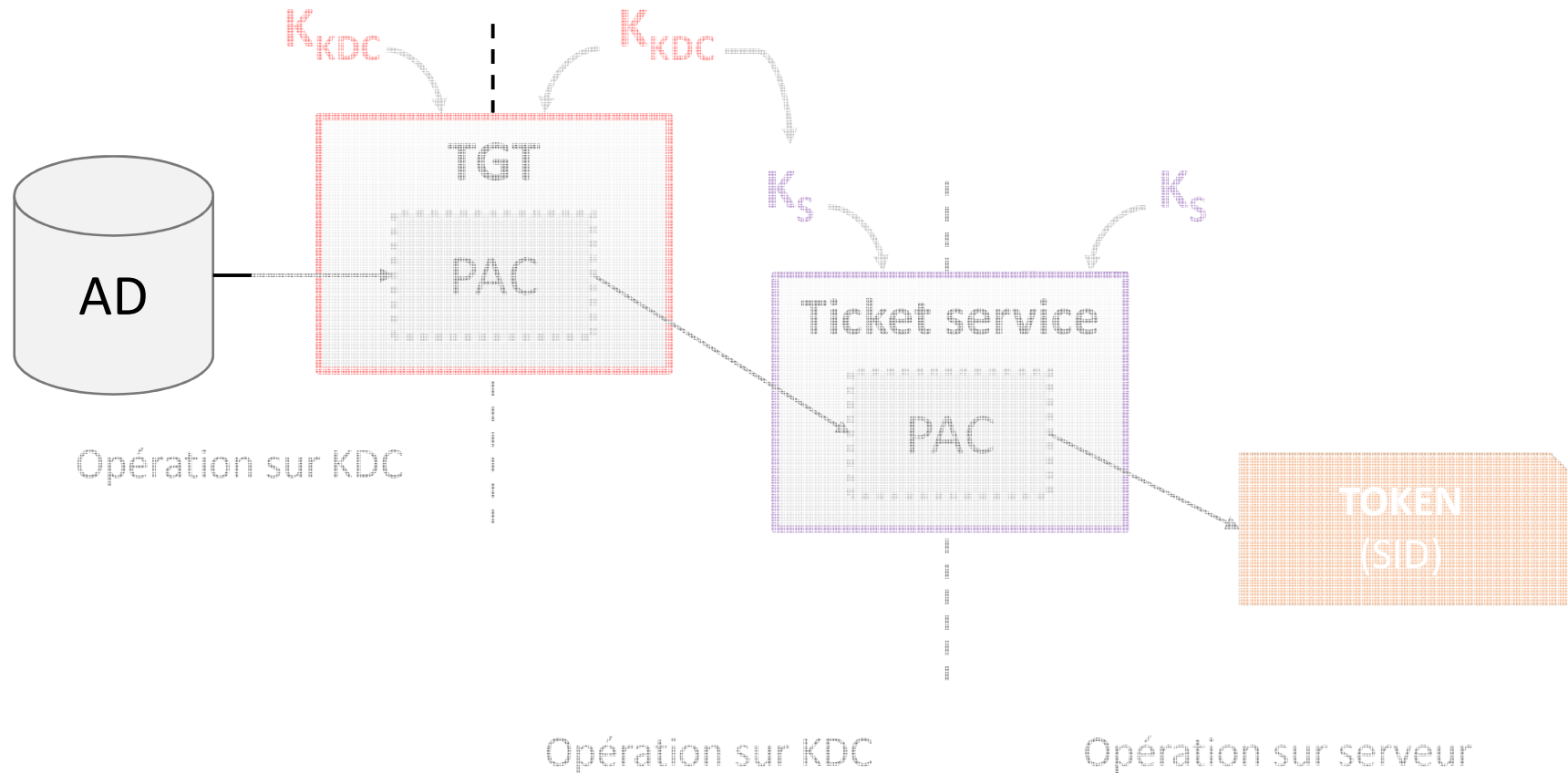
- Microsoft utilise le champ **authorization-data** des tickets pour transporter les données d'autorisation (PAC pour *Privilege Attribute Certificate*) d'un DC vers un serveur



ExtraSids

- Possibilité d'ajouter des SID arbitraires :
 - S-1-18-1 : « Identité déclarée par une autorité d'authentification »
 - S-1-5-21-0-0-0-497 : « Revendications valides »
 - **Historique des SID** : utilisé dans la migration d'utilisateurs d'un domaine à un autre :
 - Nouveau SID → `objectSID`
 - Anciens SID (*user, groups*) → `sIDHistory`

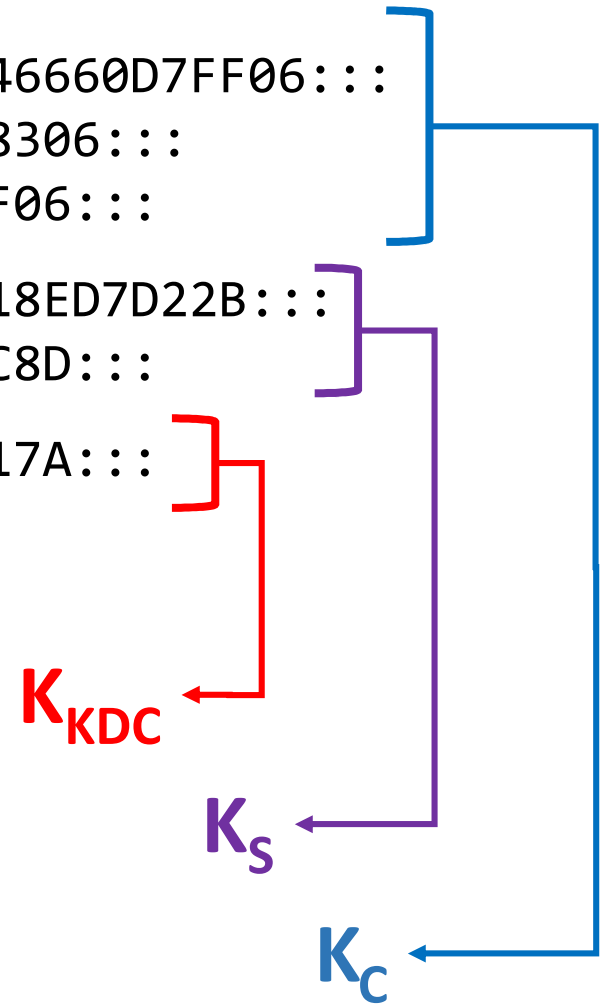
Gestion des PAC



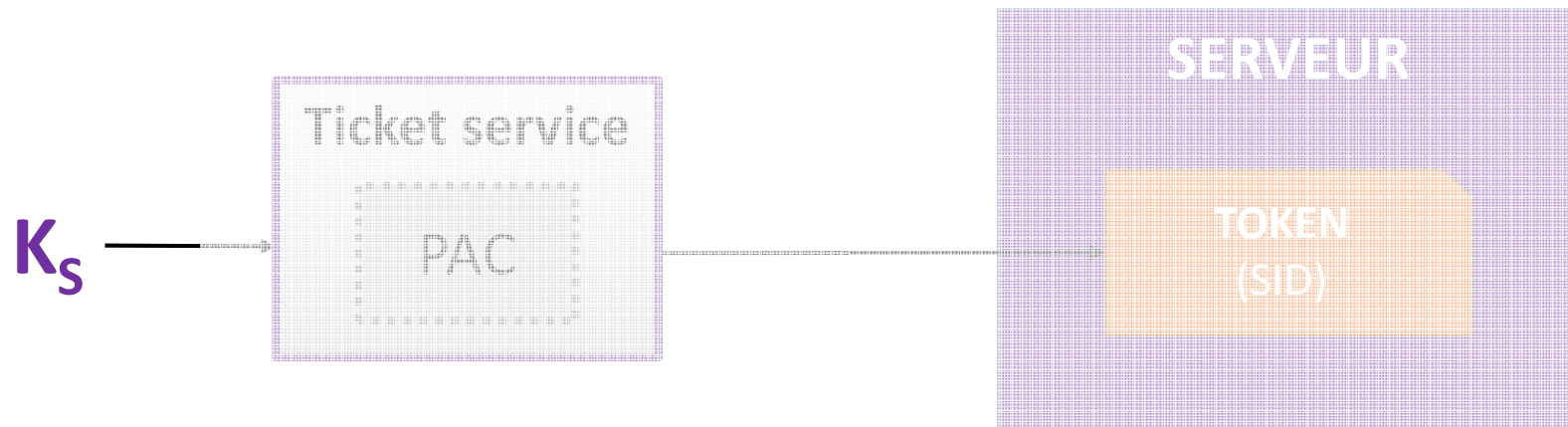
Comptes dans l'AD

```
Administrateur:500:95771430787A7B69EACAD46660D7FF06:::  
client:1105:213237F95870261048372AF7658E8306:::  
test2:1106:95771430787A7B69EACAD46660D7FF06:::  
  
DC-2012-01$:1001:8512349A72DE9A2D25C320B18ED7D22B:::  
WIN8$:1104:B0970CA0BEE6F99936A6139A136ADC8D:::  
  
krbtgt:502:396E0B9A4FC017022B71D9E4B2A5517A:::
```

- Les comptes machine et krbtgt n'ont pas de droit particulier sur l'AD et les systèmes
- Le compte krbtgt est désactivé (sert juste de conteneur de clés)



Utilisation des comptes machine (K_s)



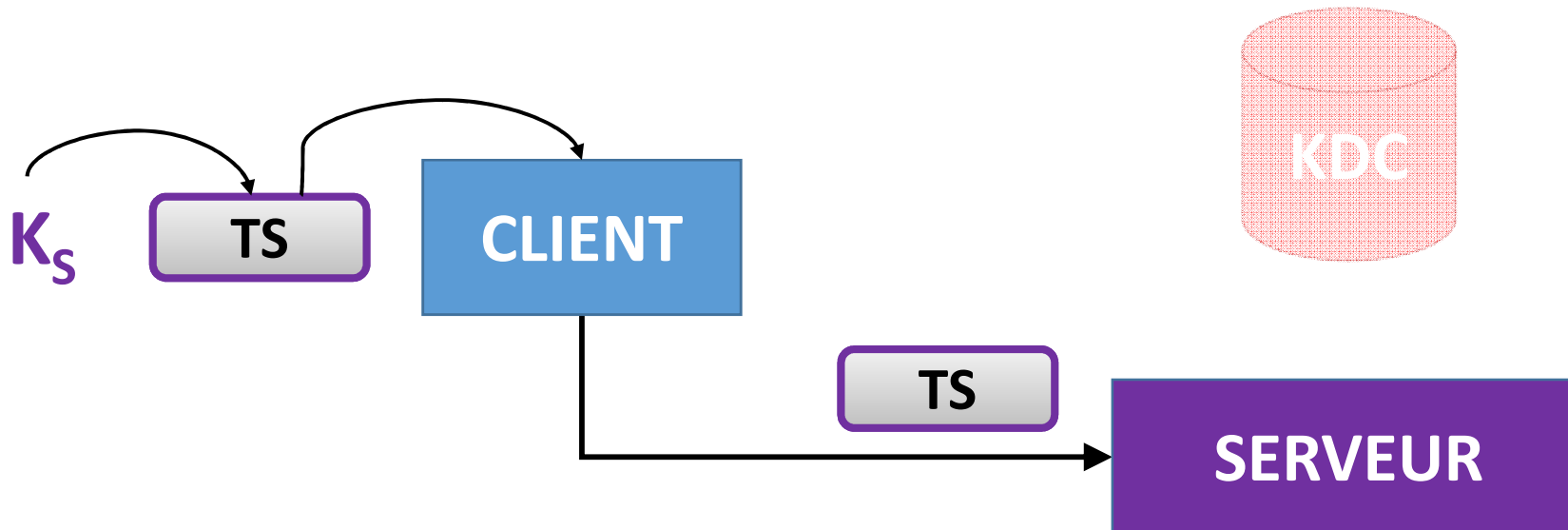
Maîtrise de K_s

⇒ Maîtrise de la PAC d'un ticket de service

⇒ Maîtrise du *token* généré sur le serveur

Démo 1

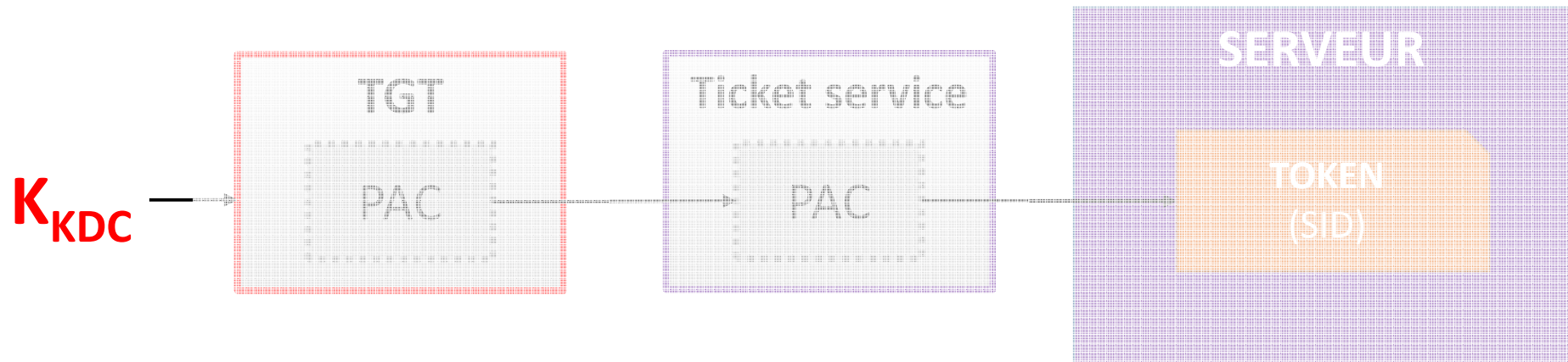
- Prérequis : empreinte d'un compte machine (K_s) [Vidéo](#)
- Étapes :
 - Création d'un ticket avec une PAC représentant un administrateur du domaine (DOMAIN_GROUP_RID_ADMINS)
 - Authentification auprès de la machine et présentation du ticket



Conclusion sur les comptes machine

- La compromission des secrets d'un compte machine de l'AD permet d'avoir le contrôle sur la machine associée
- Les mots de passe des comptes machine doivent être changés en cas de compromission de la base des comptes d'un domaine :
 - Contrôleurs de domaine
 - Serveurs
 - Postes d'administration
 - Postes utilisateur

Utilisation du compte `krbtgt` (K_{KDC})



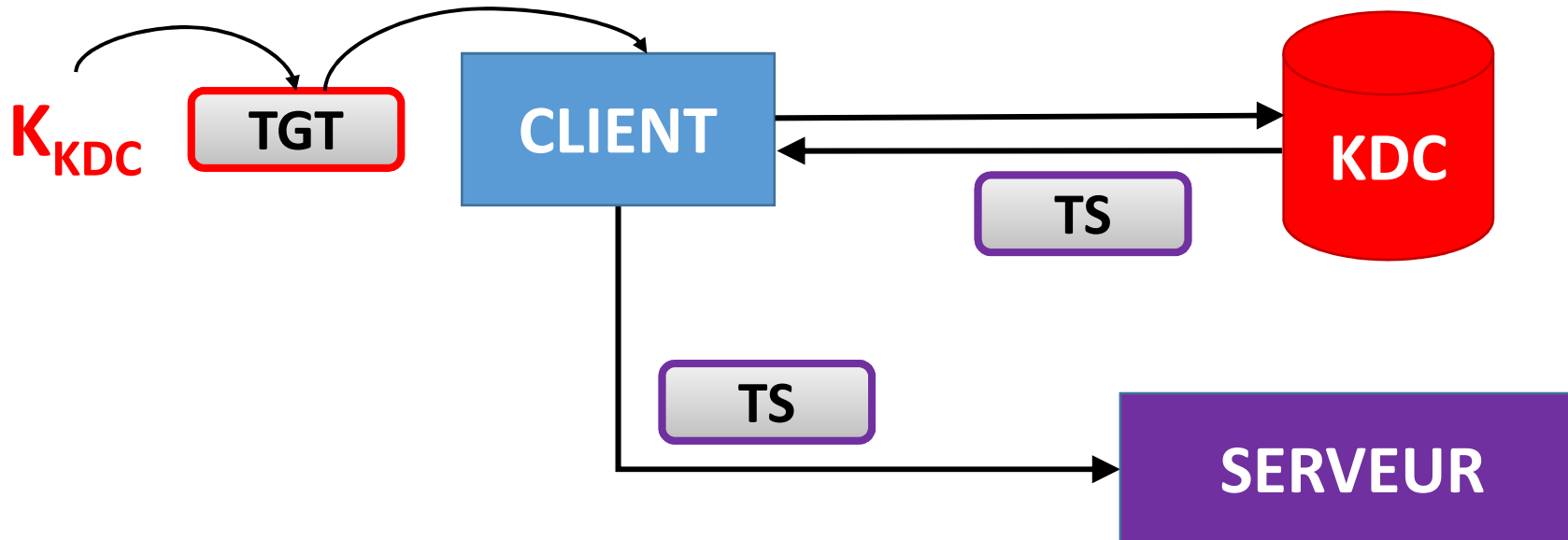
Maîtrise de K_{KDC}

- ⇒ Maîtrise de la PAC d'un TGT
- ⇒ Maîtrise de la PAC d'un ticket de service
- ⇒ Maîtrise du *token* généré sur le serveur

Démo 2

- Prérequis : empreinte du compte krbtgt (K_{KDC})
- Étapes :
 - Création d'un ticket TGT avec une PAC
 - Authentification auprès d'un serveur
 - Récupération d'un ticket de service
 - Présentation du ticket au serveur

[Vidéo](#)



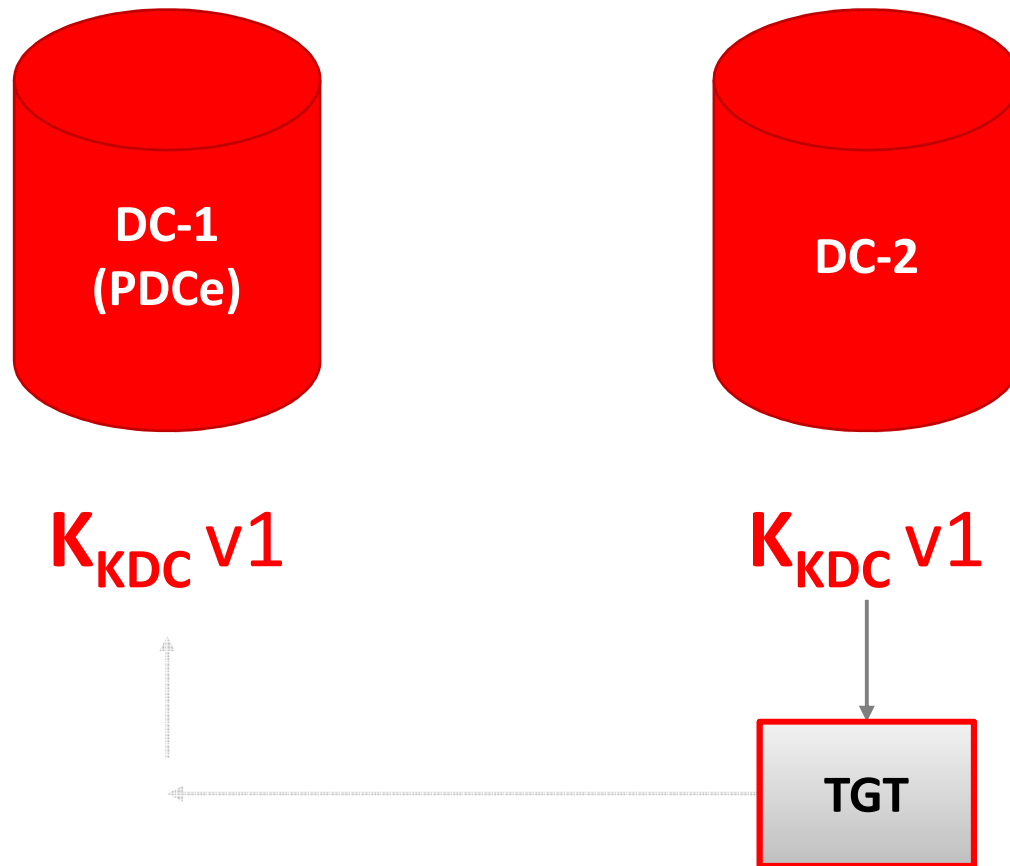
Conclusion sur le compte krbtgt

- La compromission des secrets d'authentification du compte krbtgt (K_{KDC}) permet d'avoir le contrôle sur toutes les ressources du domaine
- Ce compte doit être changé en cas de compromission de la base des comptes de l'AD

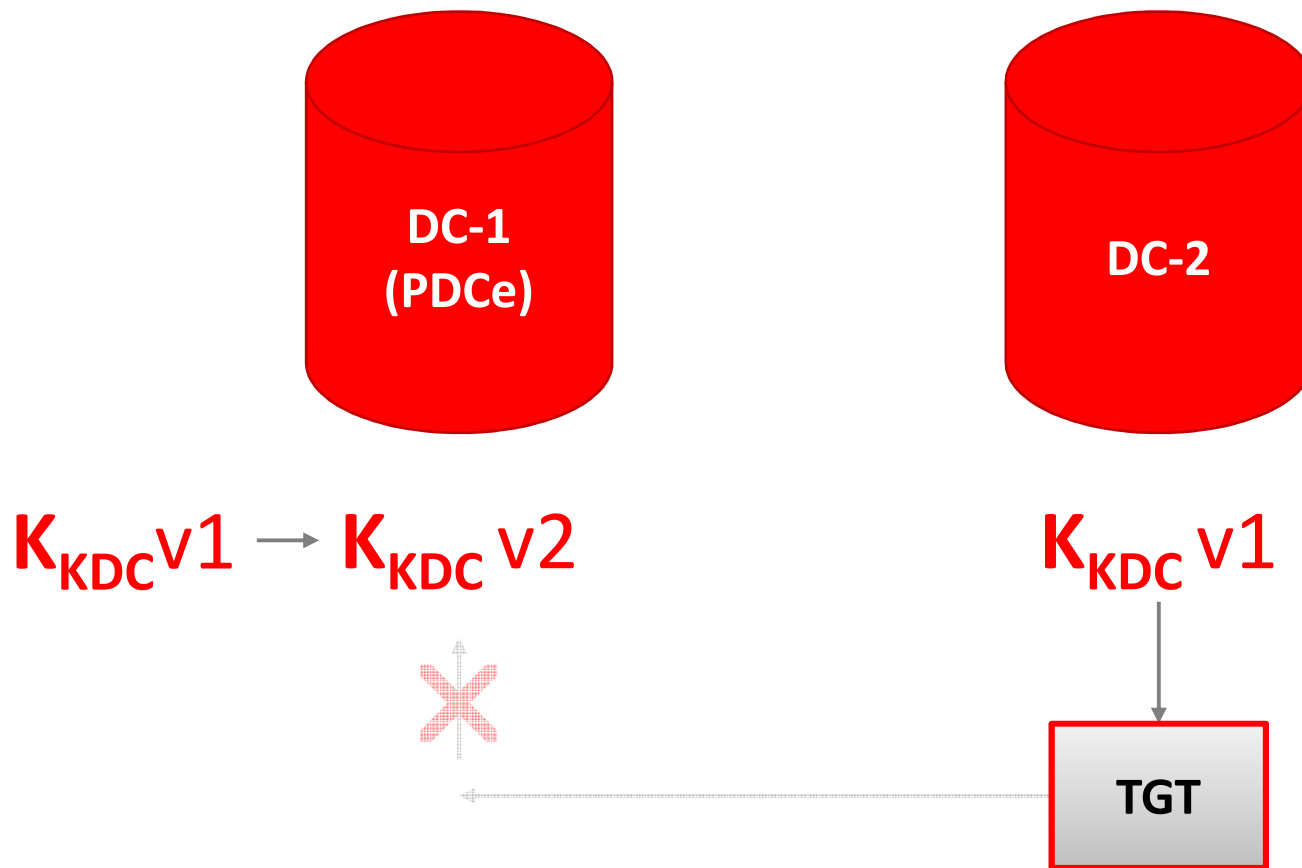
Problématique du compte krbtgt

- Le mot de passe associé au compte krbtgt (donc K_{KDC}) doit pouvoir être changé
- Le mécanisme de réplication de l'Active Directory (`drsuapi`) assure la réplication de K_{KDC} sur tous les DC
- Or, le changement de K_{KDC} entraîne :
 - L'invalidité des TGT déjà émis
 - L'impossibilité des DC à s'authentifier auprès du PDCE et donc l'impossibilité de récupérer la nouvelle clé K_{KDC}

Problème de réplication des DC (1/2)



Problème de réplication des DC (2/2)



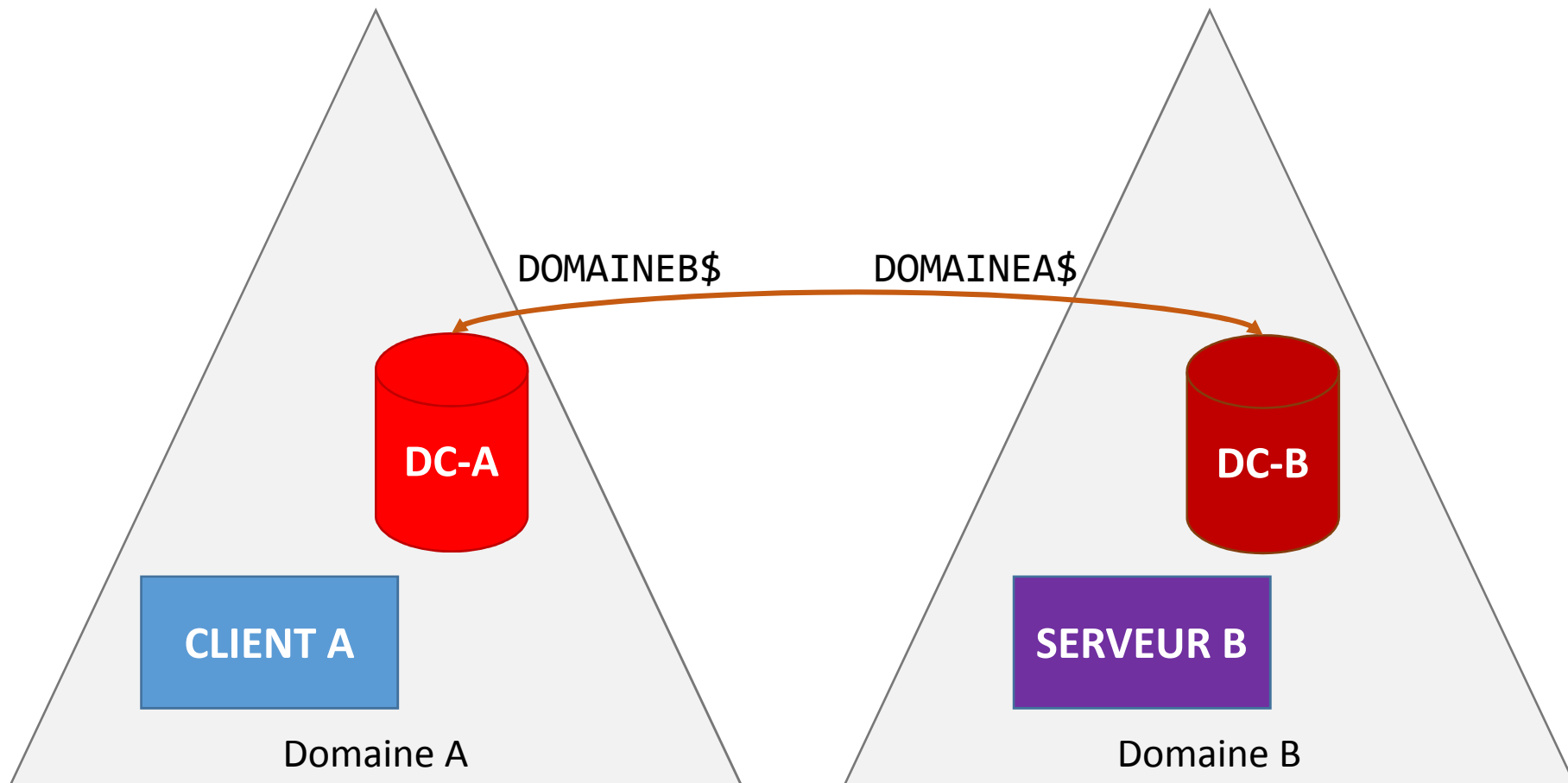
Solution

- Pour les tickets chiffrés avec K_{KDC} , les contrôleurs de domaine tentent un premier déchiffrement avec la version actuelle de K_{KDC}
- Si le déchiffrement échoue, un nouveau déchiffrement est tenté avec la version précédente de K_{KDC}
- Ainsi, deux générations de clé K_{KDC} sont valables

Changement de mot de passe de krbtgt

- Pour être réellement efficace, le changement du mot de passe de krbtgt doit être effectué deux fois
- Le délai entre des deux changements est fondamental :
 - **Trop court** : casse la réplication entre les DC
 - **Trop long** : permet à un attaquant de s'authentifier avec l'ancienne clé K_{KDC} afin de récupérer la nouvelle clé

Relations d'approbation Kerberos (*Cross-realm Authentication*)



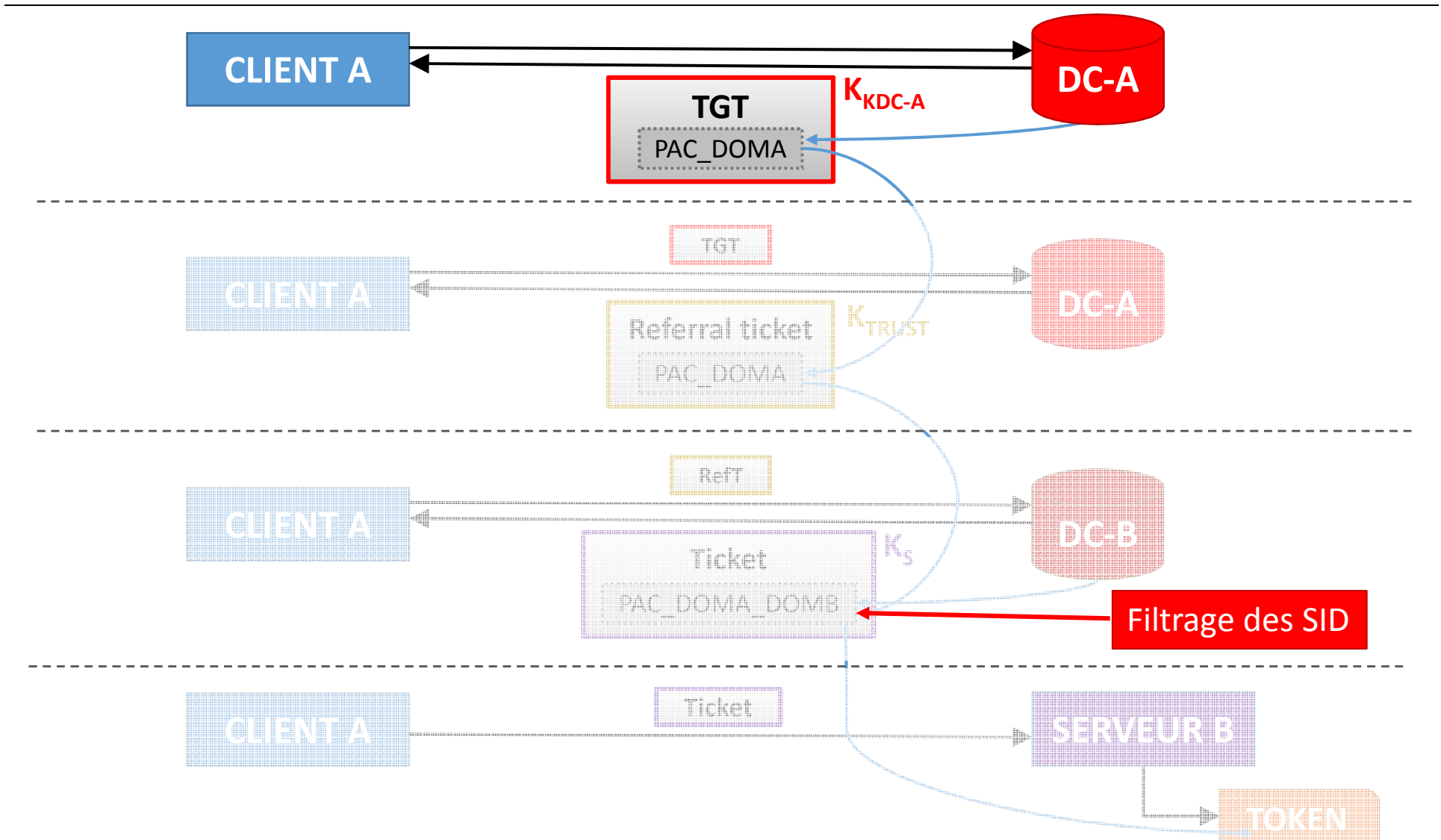
Comptes dans l'AD

Administrateur:500:95771430787A7B69EACAD46660D7FF06:::
client:1105:213237F95870261048372AF7658E8306:::
test2:1106:95771430787A7B69EACAD46660D7FF06:::
DC-2012-01\$:1001:8512349A72DE9A2D25C320B18ED7D22B:::
WIN8\$:1104:B0970CA0BEE6F99936A6139A136ADC8D:::
krbtgt:502:396E0B9A4FC017022B71D9E4B2A5517A:::
DOMAINEB\$:1045:B54DEF823AE34209E944B6594462AB4F:::

Secret du *trust* ←



Tickets et PAC dans les relations



Politique de filtrage inter-domaines

Type de relation \ Type de SID	<i>Within Forest</i>	<i>Quarantined Within Forest</i>	<i>CrossForest*</i>	<i>External</i>	<i>Quarantined External</i>
<i>AlwaysFilter</i> S-1-5-18, S-1-5-32-544 (Adm.)	Filtré	Filtré	Filtré	Filtré	Filtré
<i>NeverFilter</i>					
<i>ForestSpecific</i> RID < 500 RID = 518 (AS), RID = 519 (AE)		Filtré	Filtré	Filtré	Filtré
<i>DomainSpecific†</i> 500 ≤ RID < 1000	Filtré	Filtré	Filtré	Filtré	Filtré
<i>Domain</i> RID ≥ 1000			Filtré		Filtré
SID en quarantaine		Filtré			Filtré

* : les SID doivent également appartenir à la forêt distante

† : traité comme *ForestSpecific* depuis Windows Server 2012

Politique de filtrage *Within Forest*

- Exemple de la politique de filtrage entre domaines d'une même forêt (sous Windows Server 2012) :
 - **S-1-5-18 : SYSTEM** → **Filtré**
 - **S-1-5-21-<Domain>-R avec R<500** → **Non filtré**
 - **S-1-5-21-<Domain>-R avec $500 \leq \text{RID} < 1000$** → **Non filtré**
 - 512 : DOMAIN_ALIAS_RID_ADMINS
 - 519 : DOMAIN_GROUP_RID_ENTERPRISE_ADMINS
 - **S-1-5-21-<Domain>-R avec $R \geq 1000$** → **Non filtré**

Démo 3

- Prérequis : empreinte du compte de *trust*
- Étapes :
 - Création d'un *referral ticket* avec une PAC contenant le SID administrateur du domaine B
 - Authentification, depuis le domaine A, auprès d'un serveur du domaine B

[Vidéo](#)

Conclusion sur la relation d'approbation

- La compromission d'un domaine peut entraîner la compromission des domaines qui l'approuvent
- En intra-forêt, le filtrage des SID est structurellement limité :
 - Compromission d'un domaine → Compromission de la forêt
- La frontière d'administration est le domaine AD
- La frontière de sécurité est toute la forêt

Conclusion

- La compromission d'un domaine a des conséquences bien plus graves qu'il n'y paraît :
 - Comptes machine → prise de contrôle des machines
 - Compte `krbtgt` → prise de contrôle de tout le domaine
 - Comptes de *trust* → prise de contrôle des domaines qui l'approuvent
- Le changement du mot de passe du compte `krbtgt` n'est pas chose aisée
- *Idem* pour comptes *trust* et contrôleurs de domaine

Recommandations (1/2)

- ~~Utiliser NTLM~~ 😊

- **Prévention :**

- Assainissement de l'annuaire
 - Minimisation des comptes privilégiés
 - Vérification des chemins de prise de contrôle
- Amélioration des pratiques d'administration
- Limitation des authentifications des comptes d'administration
- Sécurisation des contrôleurs de domaine
- Mise en place de RODC
- Utilisation des nouveaux mécanismes de sécurité (*protected users, restricted admins, protected process, etc.*)

- **Détection et supervision :**

- Collecte, centralisation et traitement des journaux Windows

Recommandations (2/2)

- **Réaction :**

- Ne pas minimiser la tâche
- 2 solutions :
 - **Forêt vierge** : tout recréer
 - Haut niveau de sécurité
 - Très couteux
 - Migration des données d'autorisation
 - « **Active Directory Forest Recovery** »¹
 - Isolation de tous les contrôleurs de domaine pendant la phase de remédiation

¹ <http://www.microsoft.com/en-us/download/details.aspx?id=16506>

Questions ?
