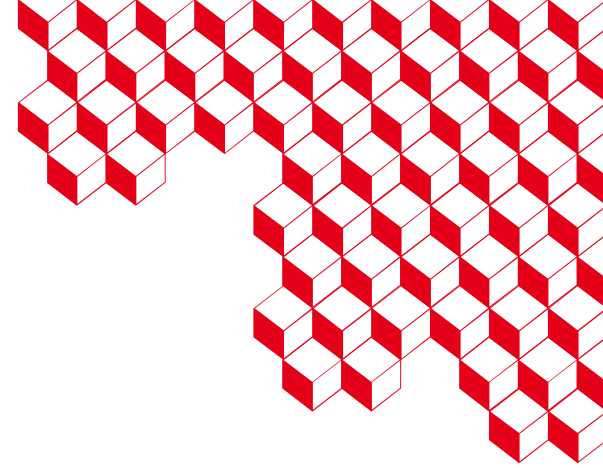




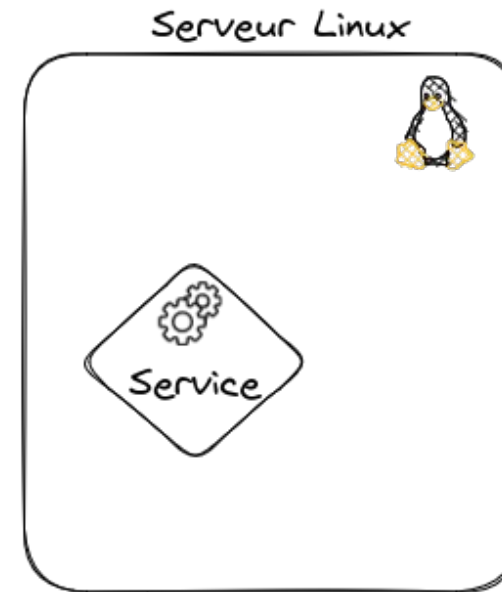
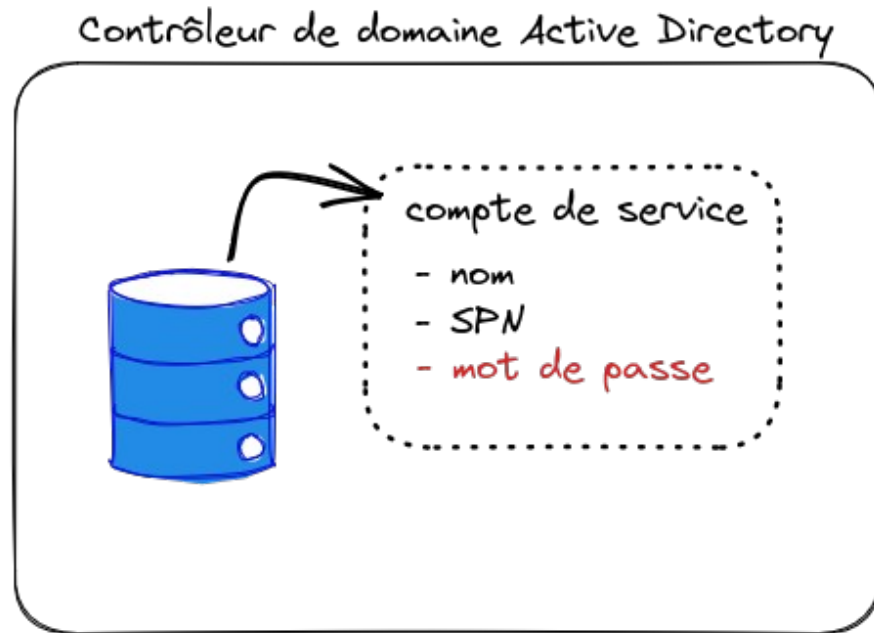
gmsad

Utilisation de « group Managed Service Accounts » (gMSA) sous Linux

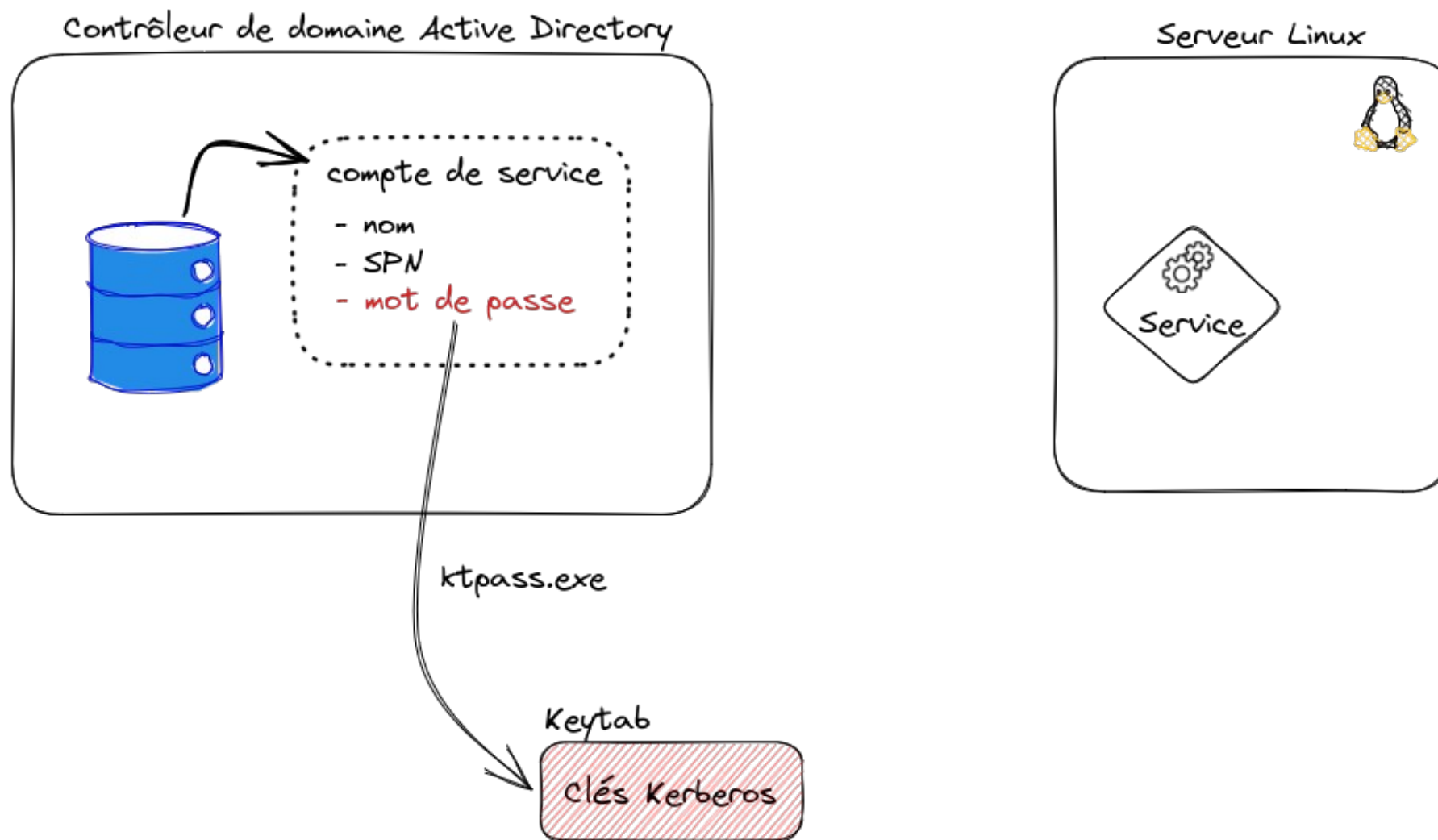


1 ■ Service kerberisé sous Linux

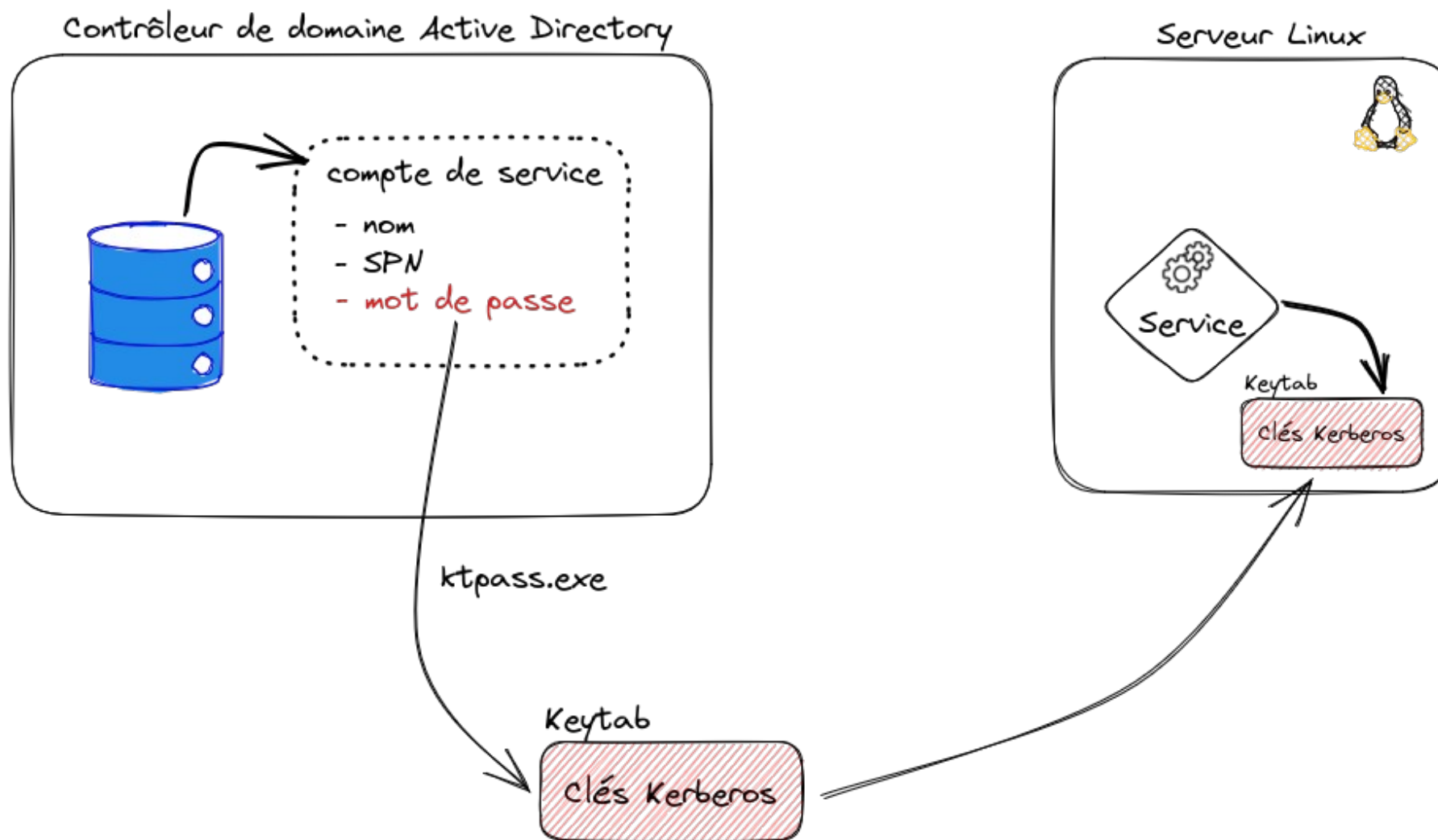
Service kerberisé sous Linux



Service kerberisé sous Linux



Service kerberisé sous Linux



Exemple de configuration

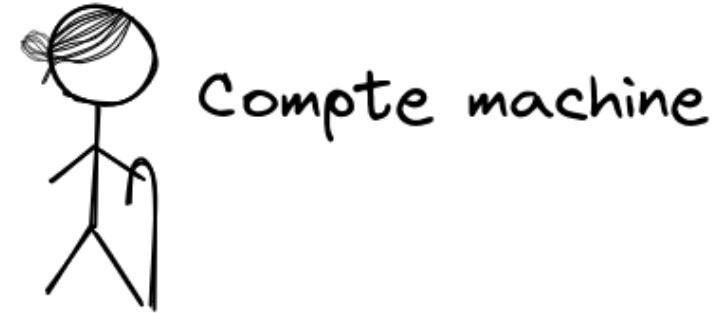
Configuration Apache avec le module mod_auth_kerb :

```
<VirtualHost 10.1.2.3:443>  
  ServerName super.domaine.fr
```

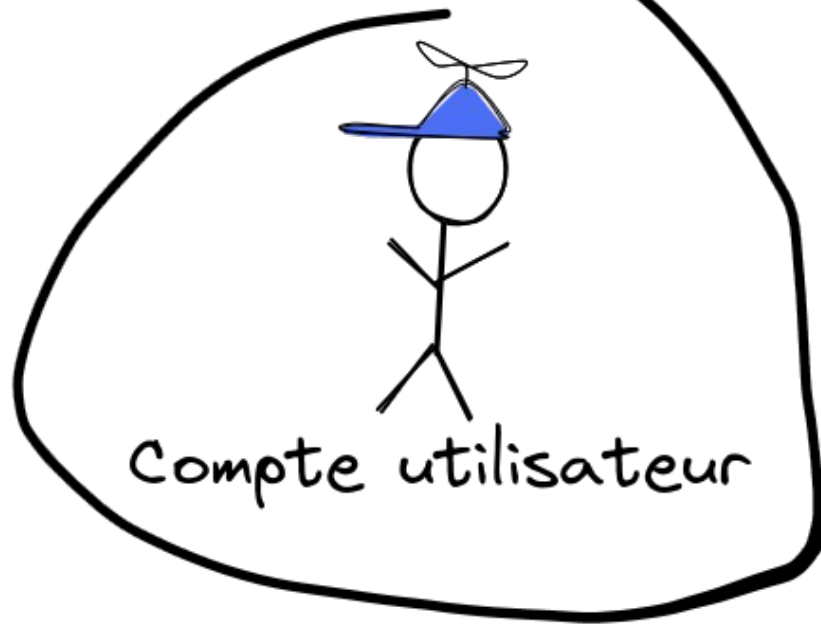
```
  <Location "/service">  
    Require valid-user  
    AuthType Kerberos  
  </Location>
```

```
  KrbAuthRealms DOMAINE.FR  
  Krb5Keytab /etc/service.keytab  
  KrbServiceName HTTP  
</VirtualHost>
```

Quel type de compte ?



Quel type de compte ?



Compte machine



gMSA



sMSA

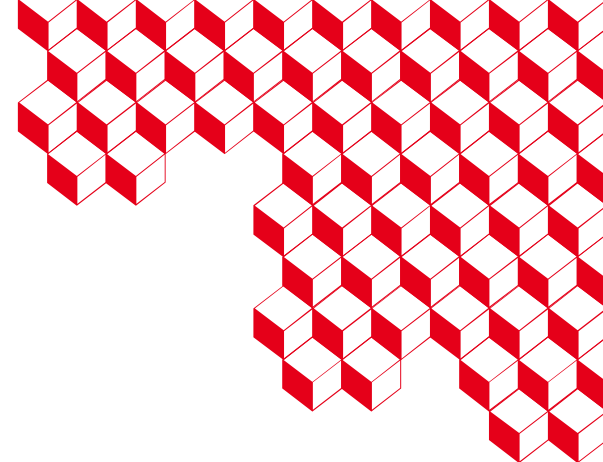
Compte utilisateur classique

- Mise en place
 - Compte utilisateur avec mot de passe qui **n'expire pas**
 - Utilisation de `ktpass.exe` pour générer la **keytab**
- Problèmes
 - C'est mal d'avoir un mot de passe qui n'expire pas
 - Le mot de passe peut être (mal) choisi par l'administrateur

Compte utilisateur classique v2

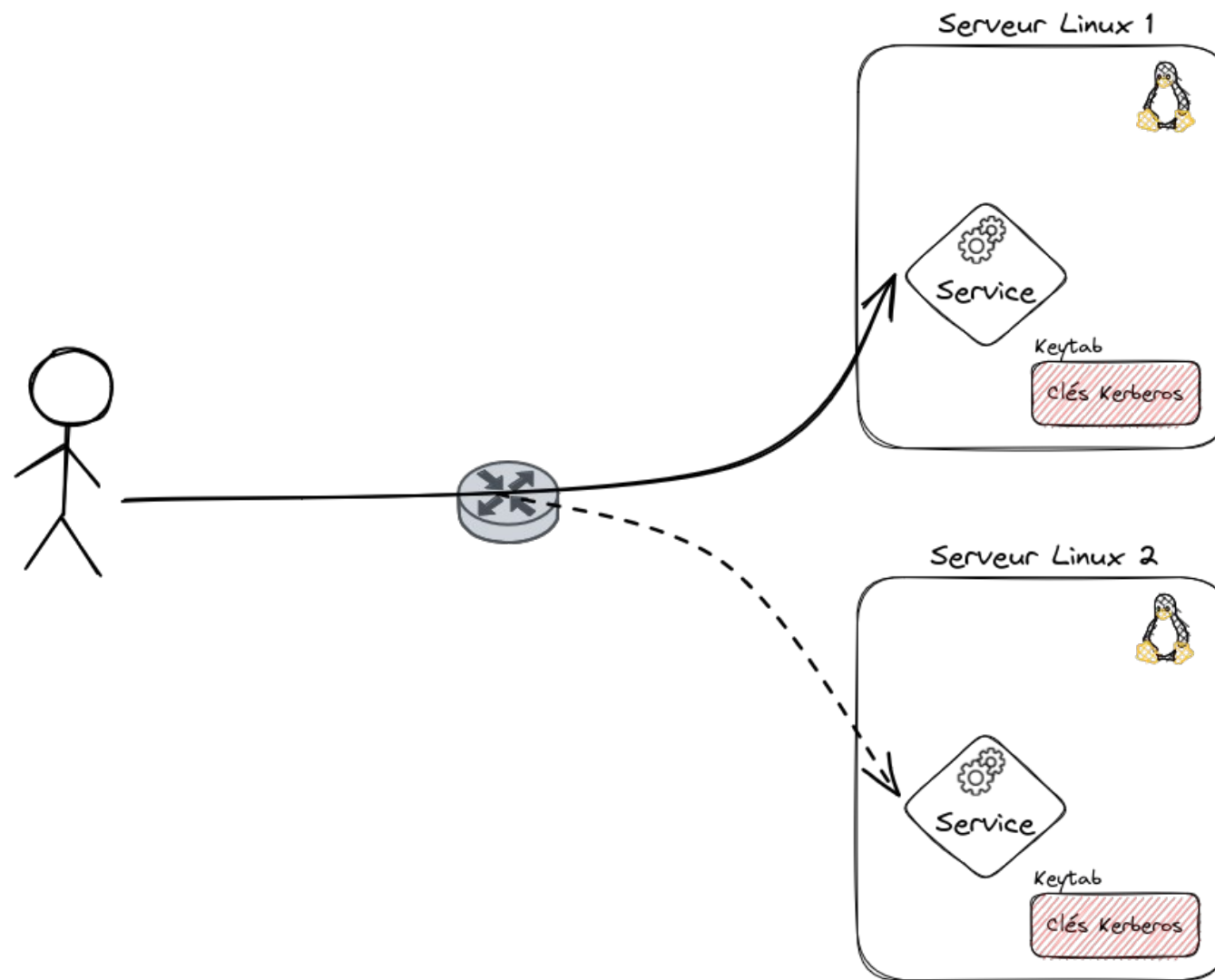
- Mise en place
 - Compte utilisateur avec mot de passe qui **expire**
 - Renouvellement du mot de passe et de la keytab avec `msktutil` (ou équivalent)
 - Utilisation de `ktpass.exe` pour générer la keytab avec l'**option +rndPass**
- Et ça marche bien !



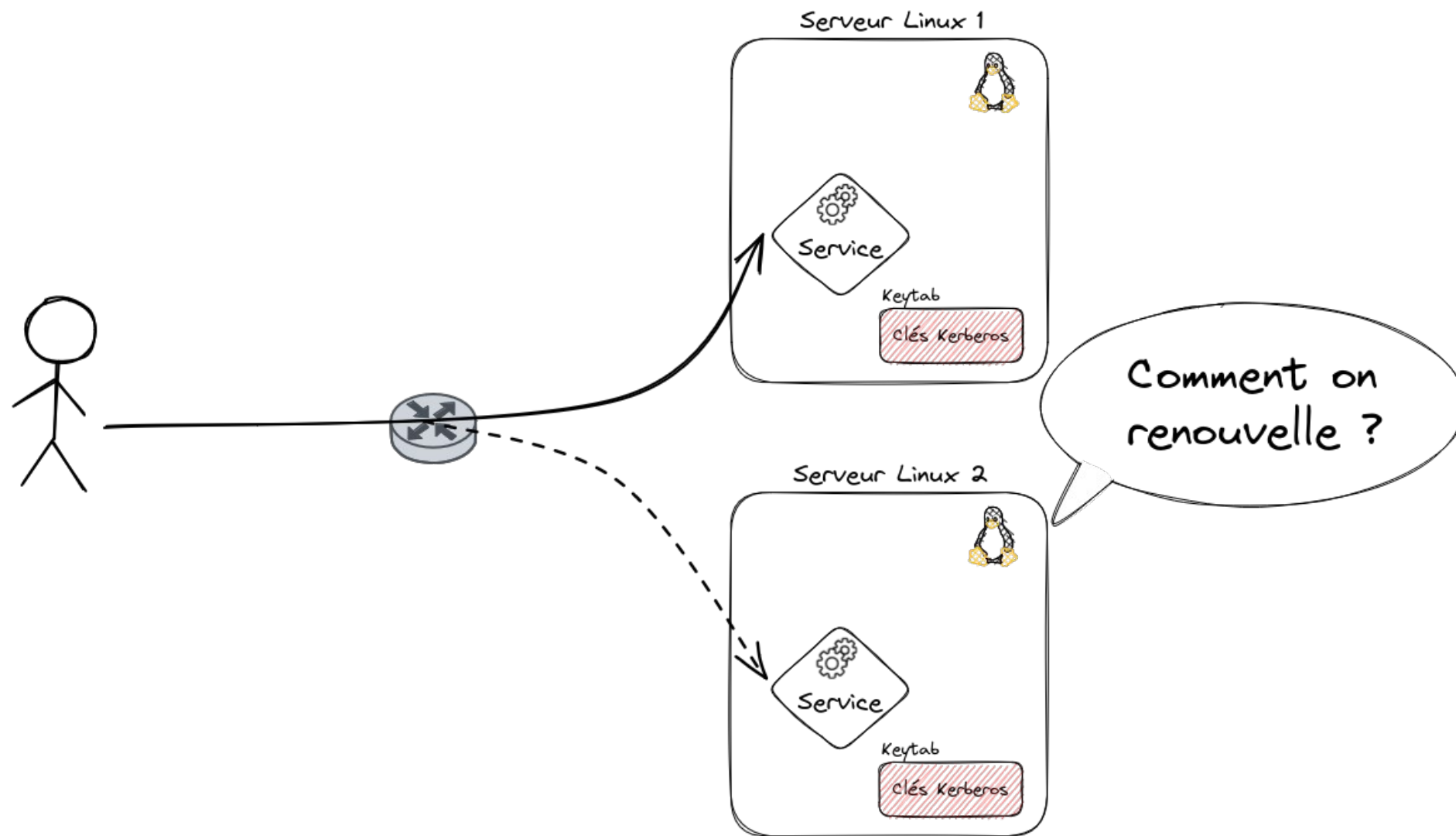


Fin

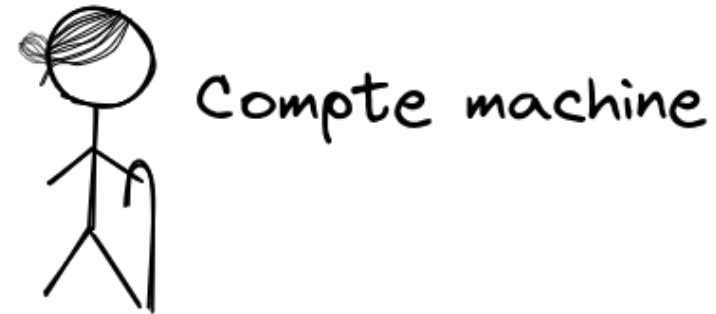
Et la redondance ?!



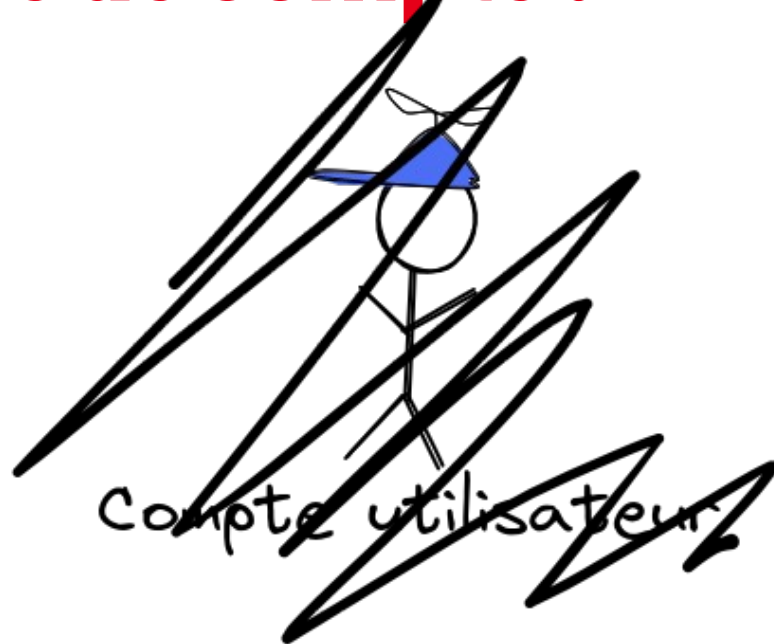
Et la redondance ?!



Quel type de compte ?



Quel type de compte ?



Compte machine





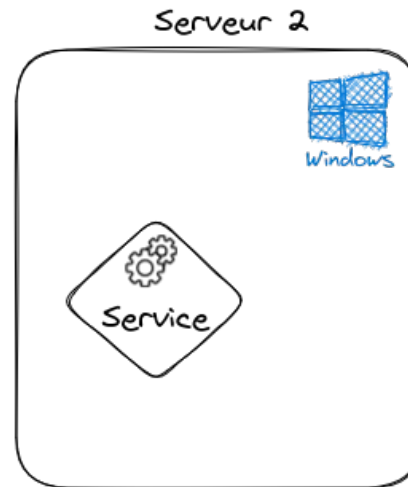
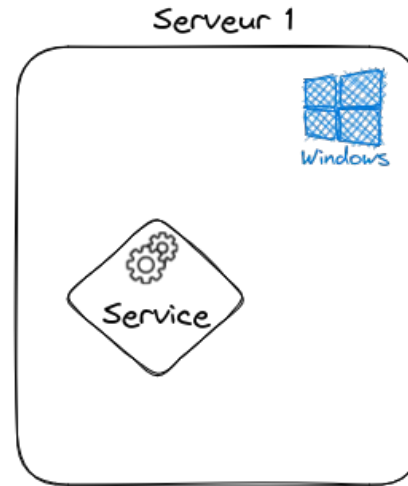
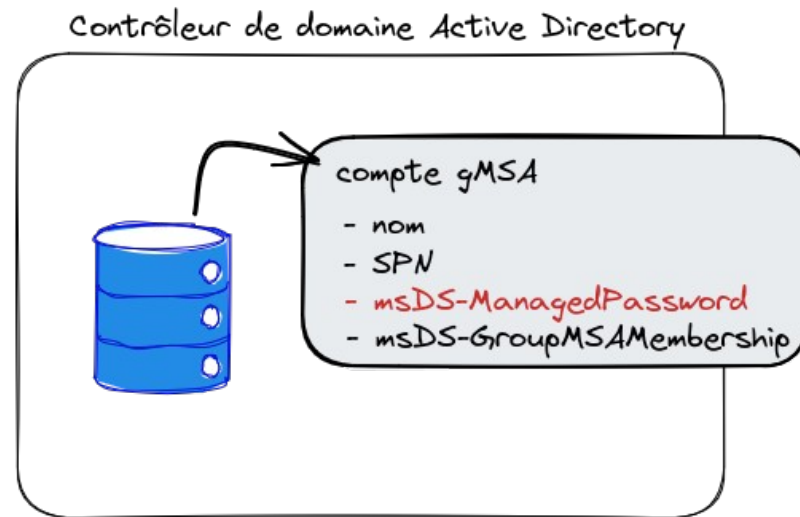
2. group Managed Service Account

ou « Compte de service administré de groupe »

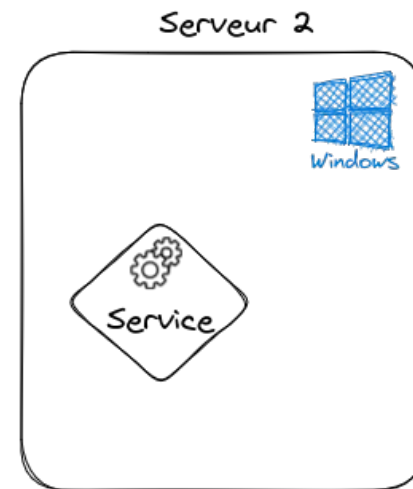
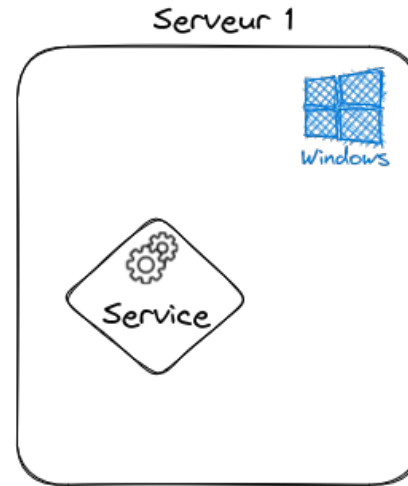
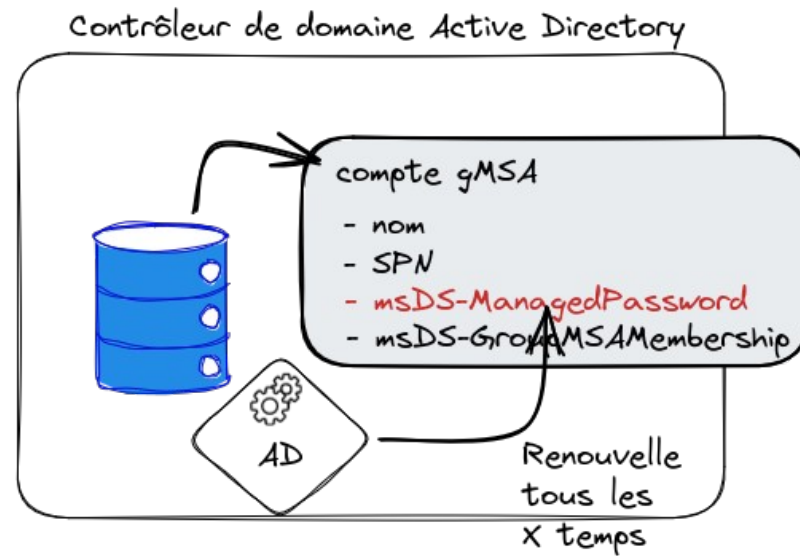
group Managed Service Account

- Mécanisme Active Directory
- Permet l'utilisation d'un **compte de service sur plusieurs machines**
- Prérequis :
 - Clé racine du KDS déployée
 - Schéma mis à jour en Windows Server 2012

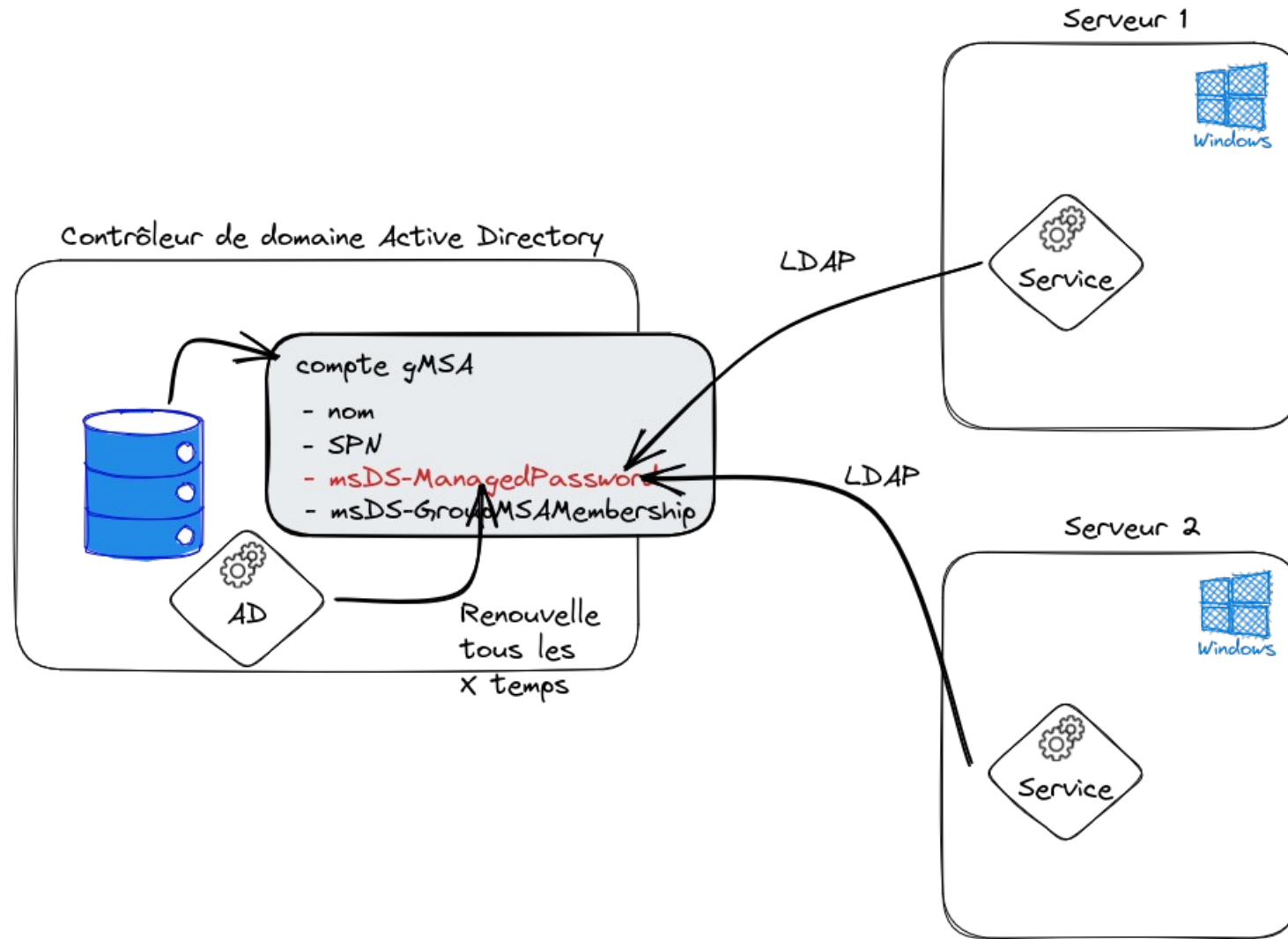
Utilisation d'un gMSA



Utilisation d'un gMSA



Utilisation d'un gMSA

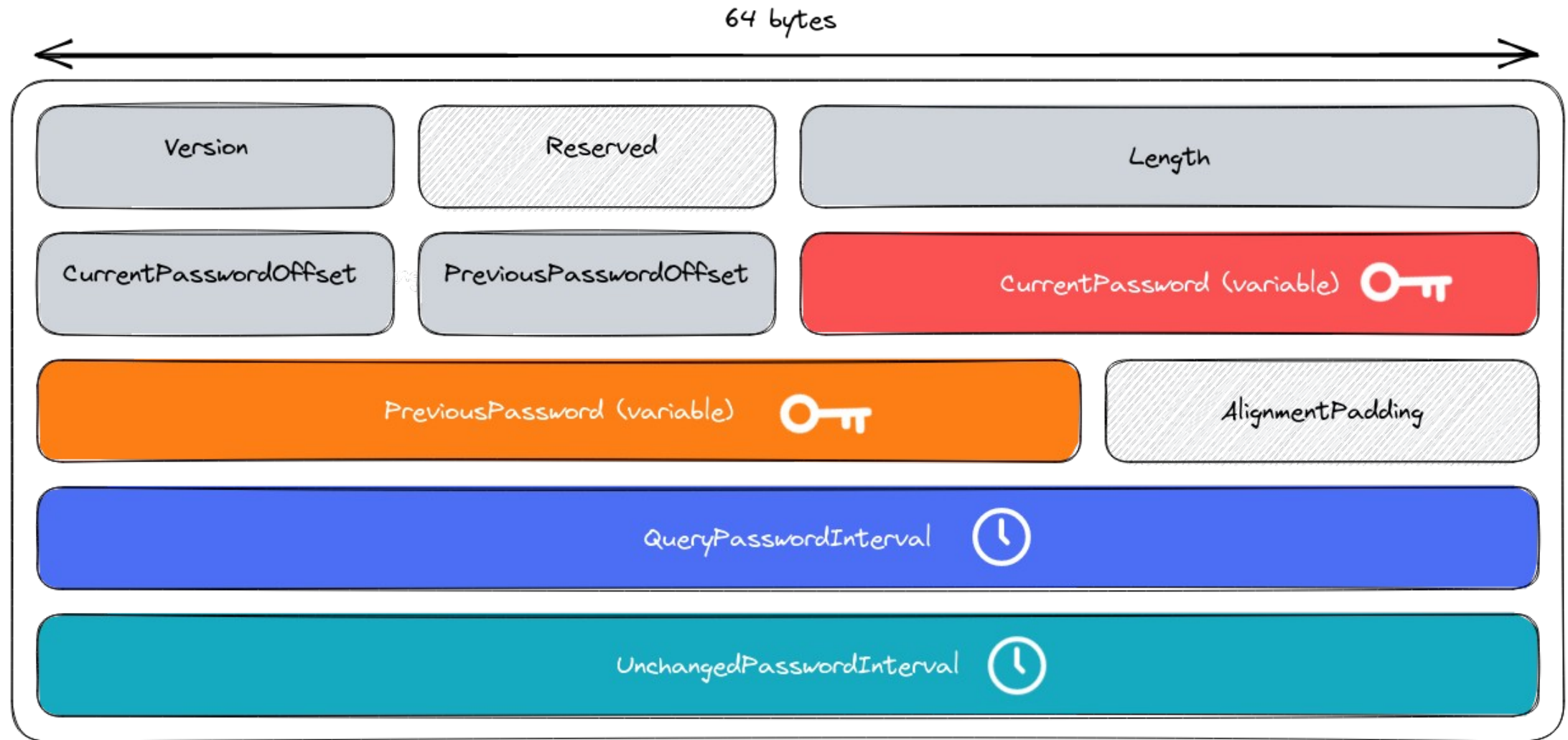


Objet gMSA



- L'attribut **msDS-ManagedPassword**
 - Permet de récupérer le mot de passe du compte et des métadonnées
 - Accessible en **LDAP** via une connexion chiffrée (LDAPS ou LDAP chiffré avec Kerberos)
- L'attribut **msDS-GroupMSAMembership**
 - Définit quelles machines ont accès à l'attribut msDS-ManagedPassword
 - Contient un descripteur de sécurité Windows

msDS-ManagedPassword



MSDS-MANAGEDPASSWORD_BLOB

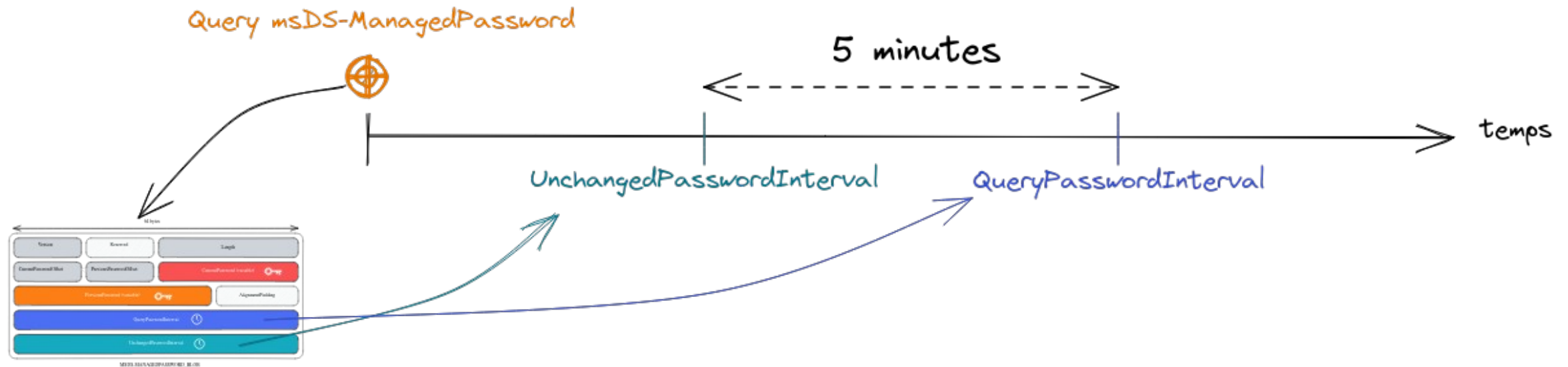
« Documentation » Microsoft

- a. Let StaleCount be zero.
- b. Let NewKeyStartTime = CurrentKeyExpirationTime.
- c. Let NewKeyStartTime = NewKeyStartTime + GDKIRolloverInterval and StaleCount = StaleCount + 1 until NewKeyStartTime is greater than the current time.
- d. Call GetPasswordBasedOnTimestamp() where:
 - *Timestamp* contains NewKeyStartTime.
 - *AccountSID* contains the TO!objectSid attribute ([MS-ADA3] section 2.45).

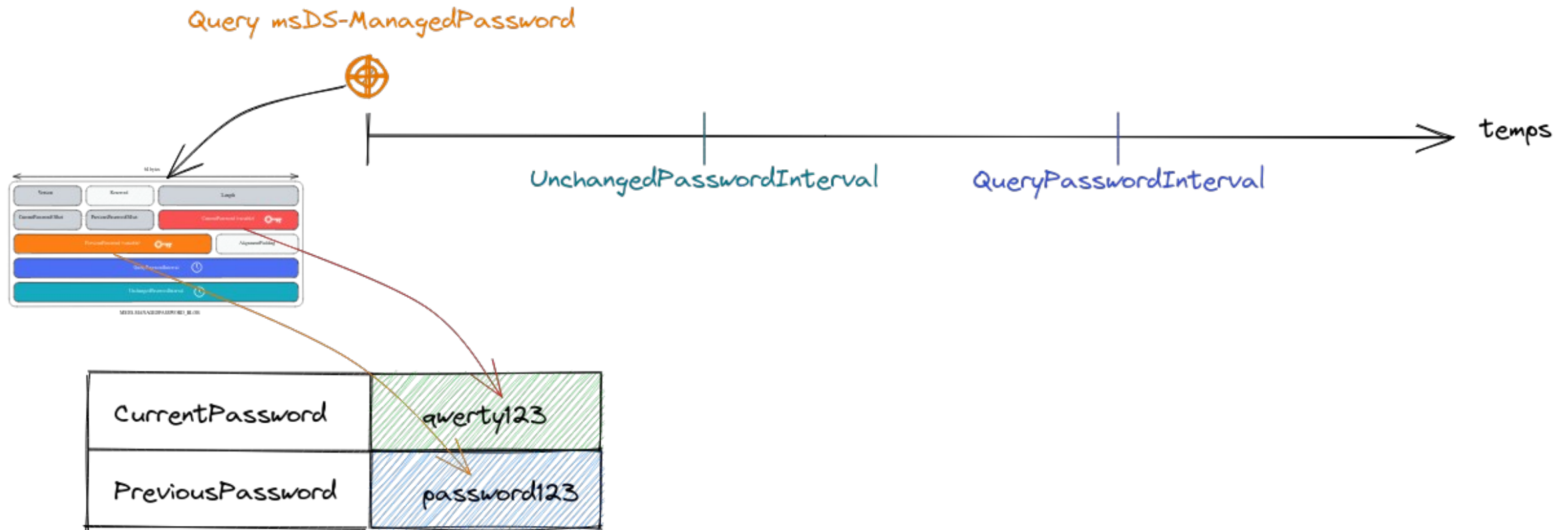
Let NewKeyID be the returned KeyID. Let NewPassword be the returned password.



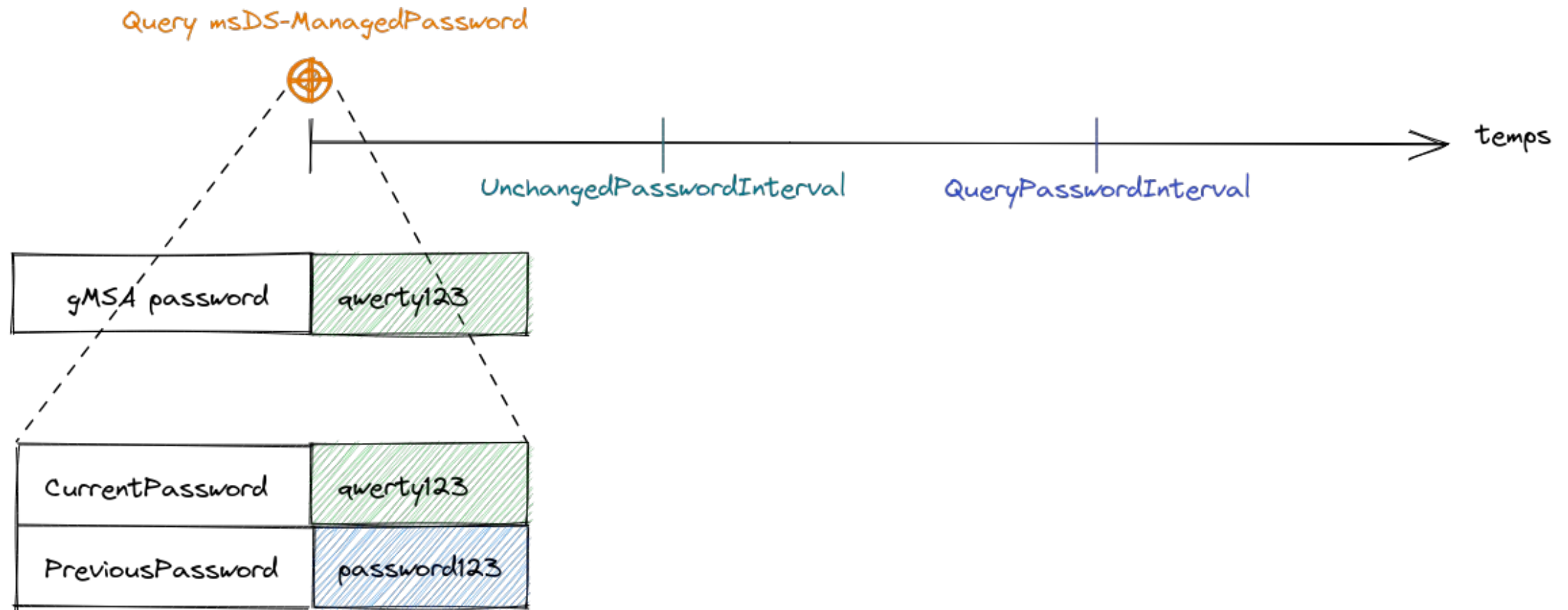
Mécanisme de mise à jour



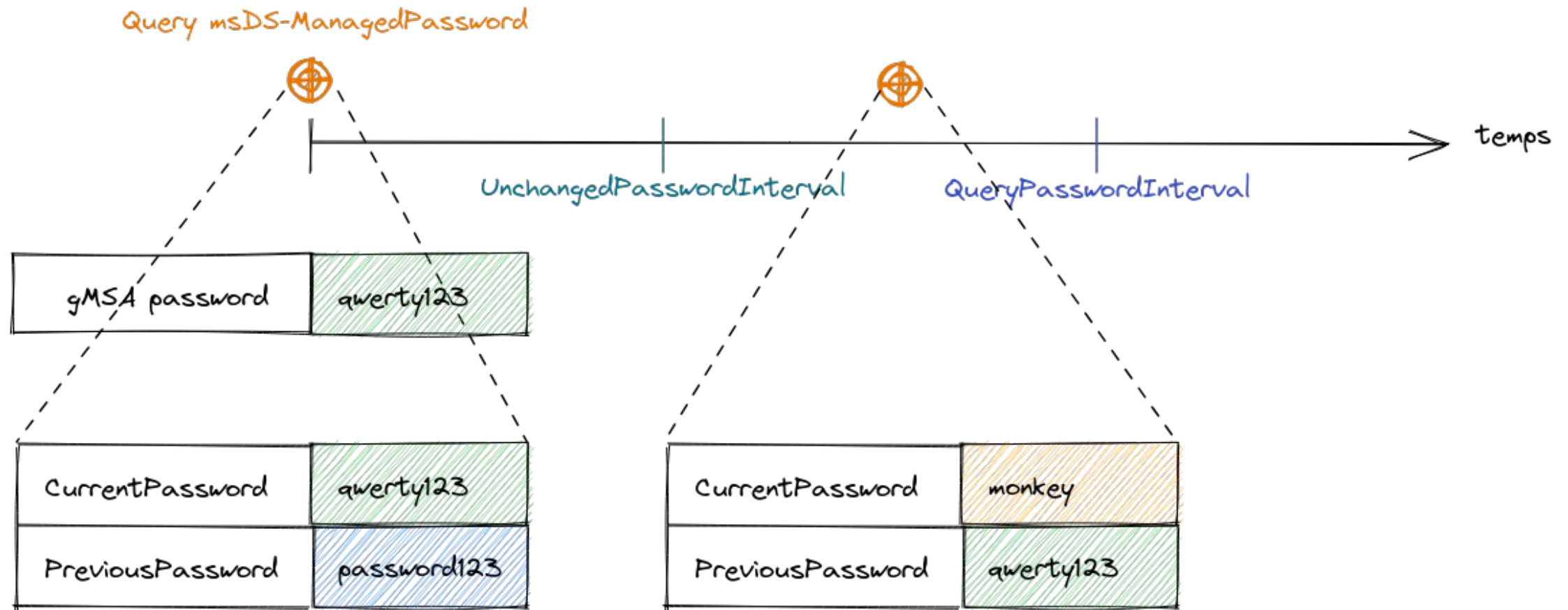
Mécanisme de mise à jour



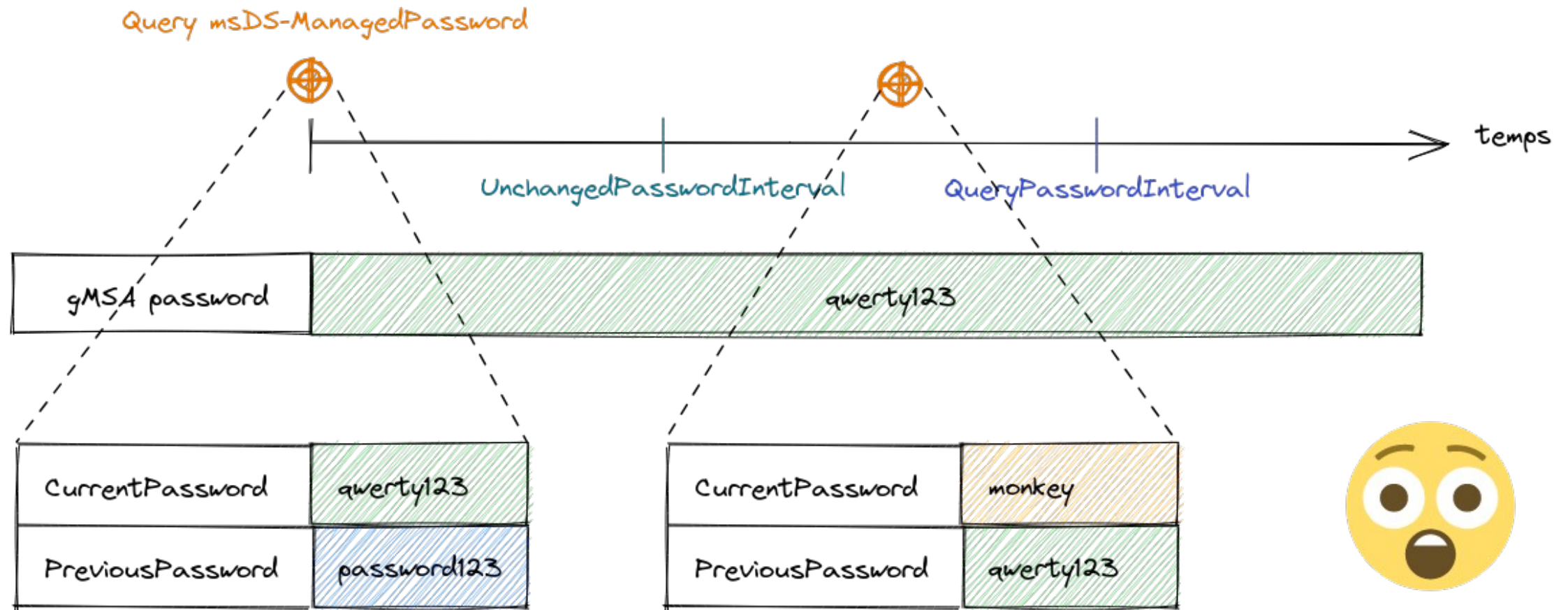
Mécanisme de mise à jour



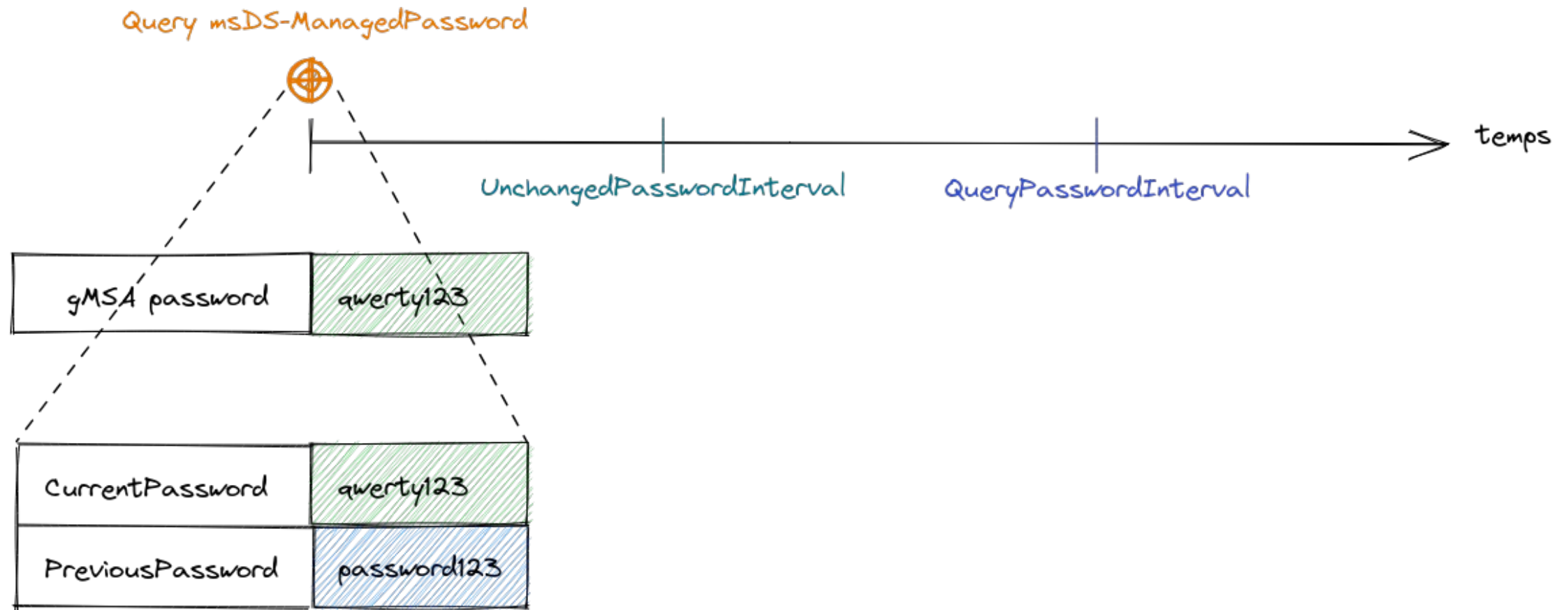
Mécanisme de mise à jour



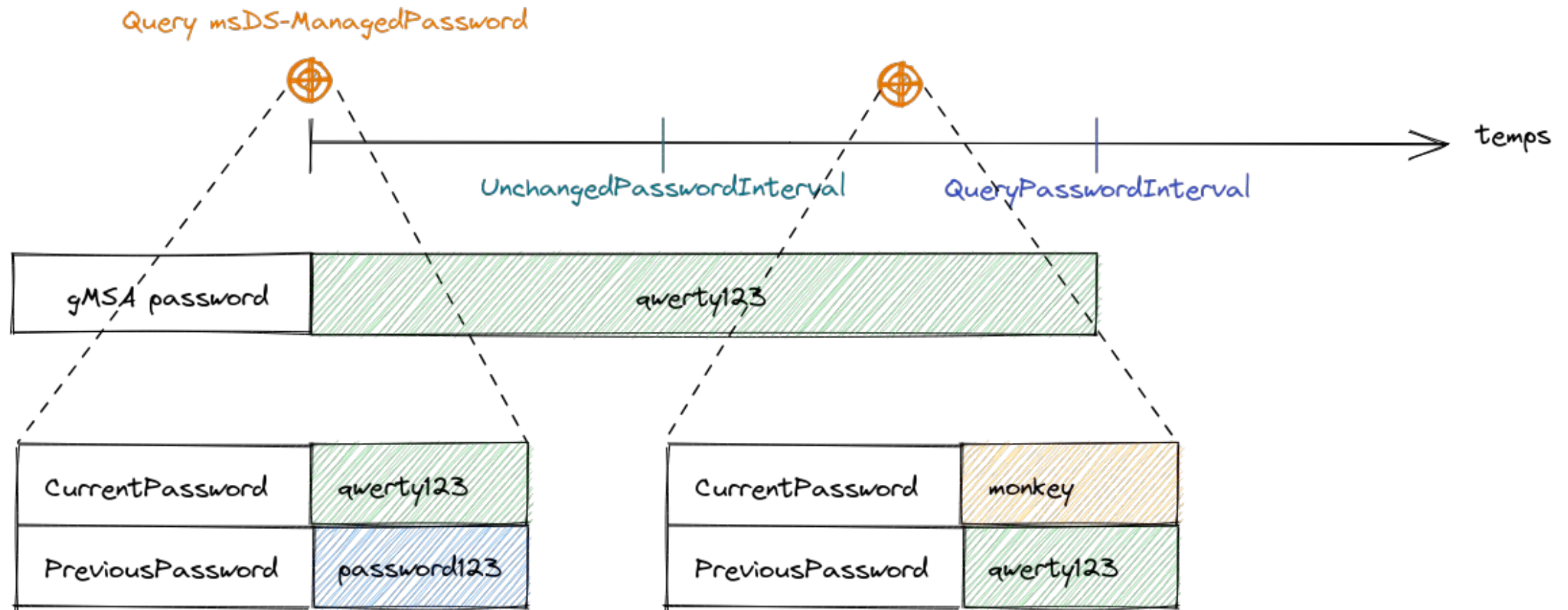
Mécanisme de mise à jour



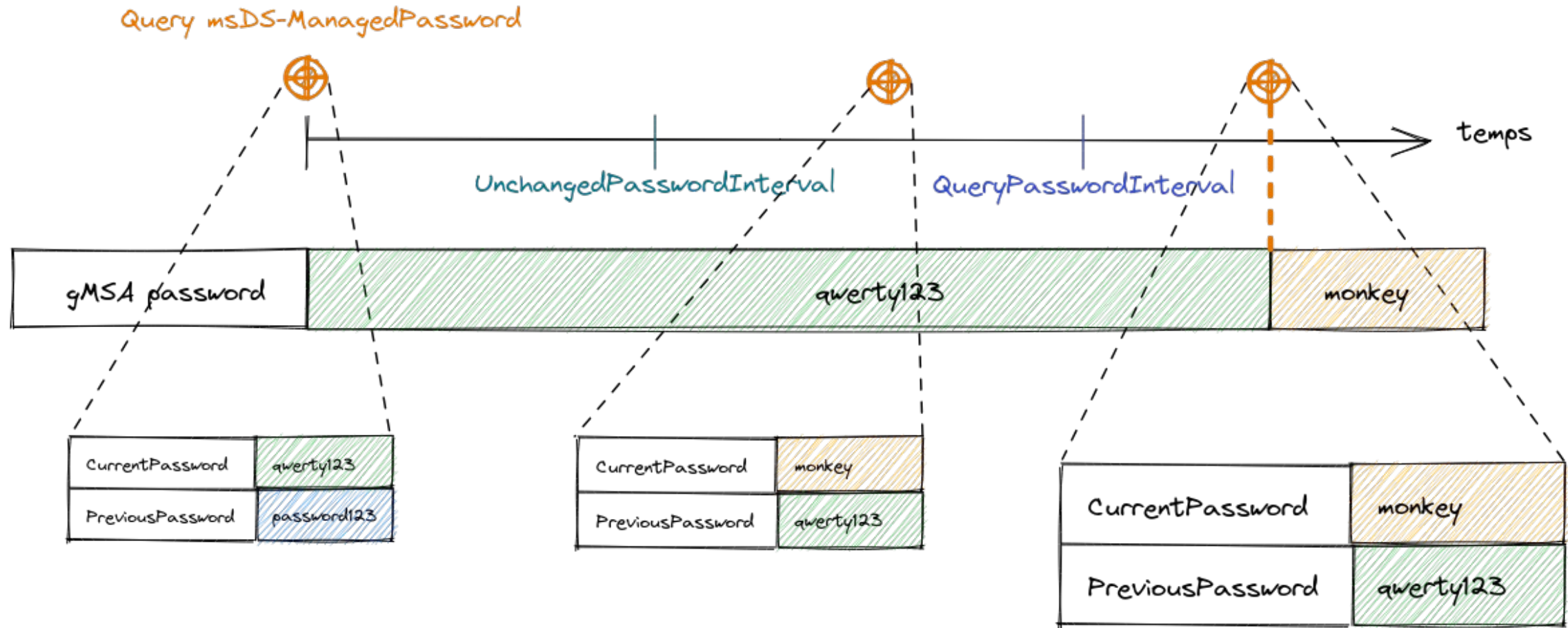
Mécanisme de mise à jour



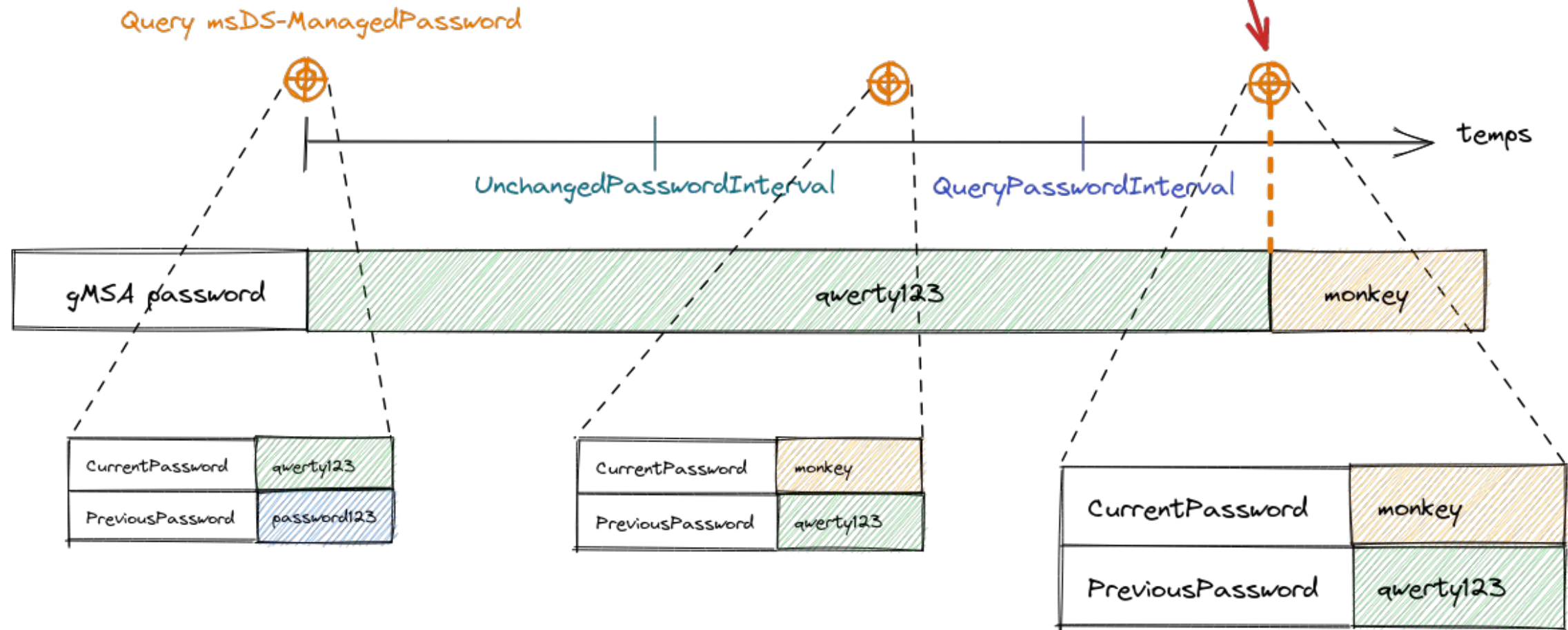
Mécanisme de mise à jour



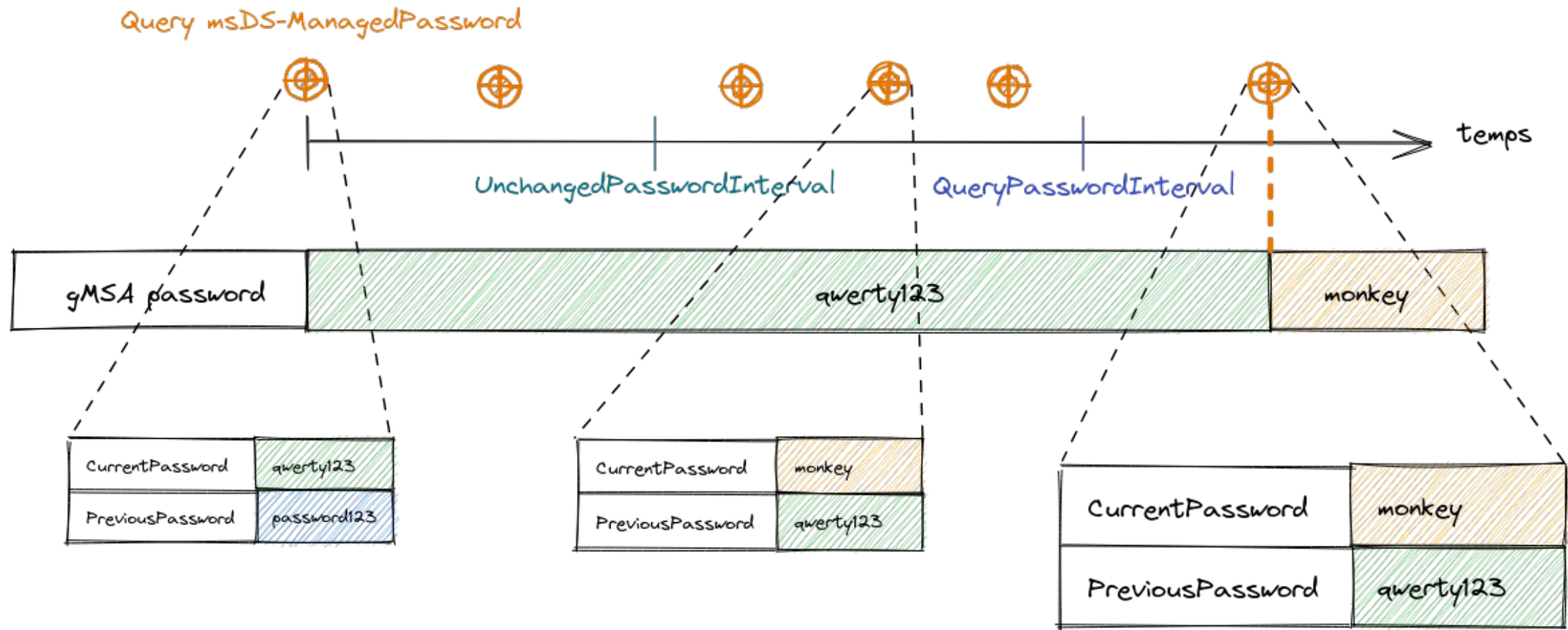
Mécanisme de mise à jour



Mécanisme de mise à jour

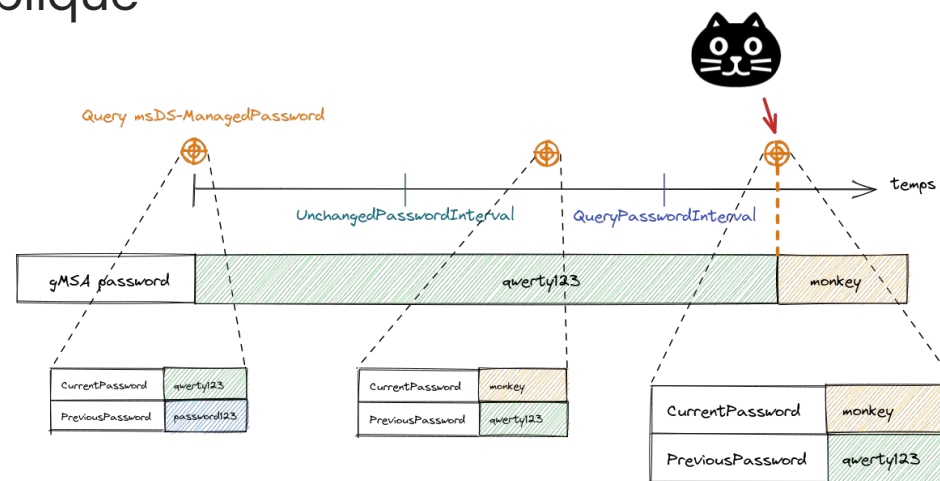


Mécanisme de mise à jour



En résumé

- À partir de **UnchangedPasswordInterval** :
 - On a accès au prochain mot de passe
 - Mais il n'est pas encore changé pour le compte !
- À partir de **QueryPasswordInterval**, requêter l'attribut msDS-ManagedPassword **déclenche** le changement du mot de passe
- L'intervalle entre les deux permet à toutes les machines utilisant le gMSA de récupérer le nouveau mot de passe avant qu'il soit appliqué

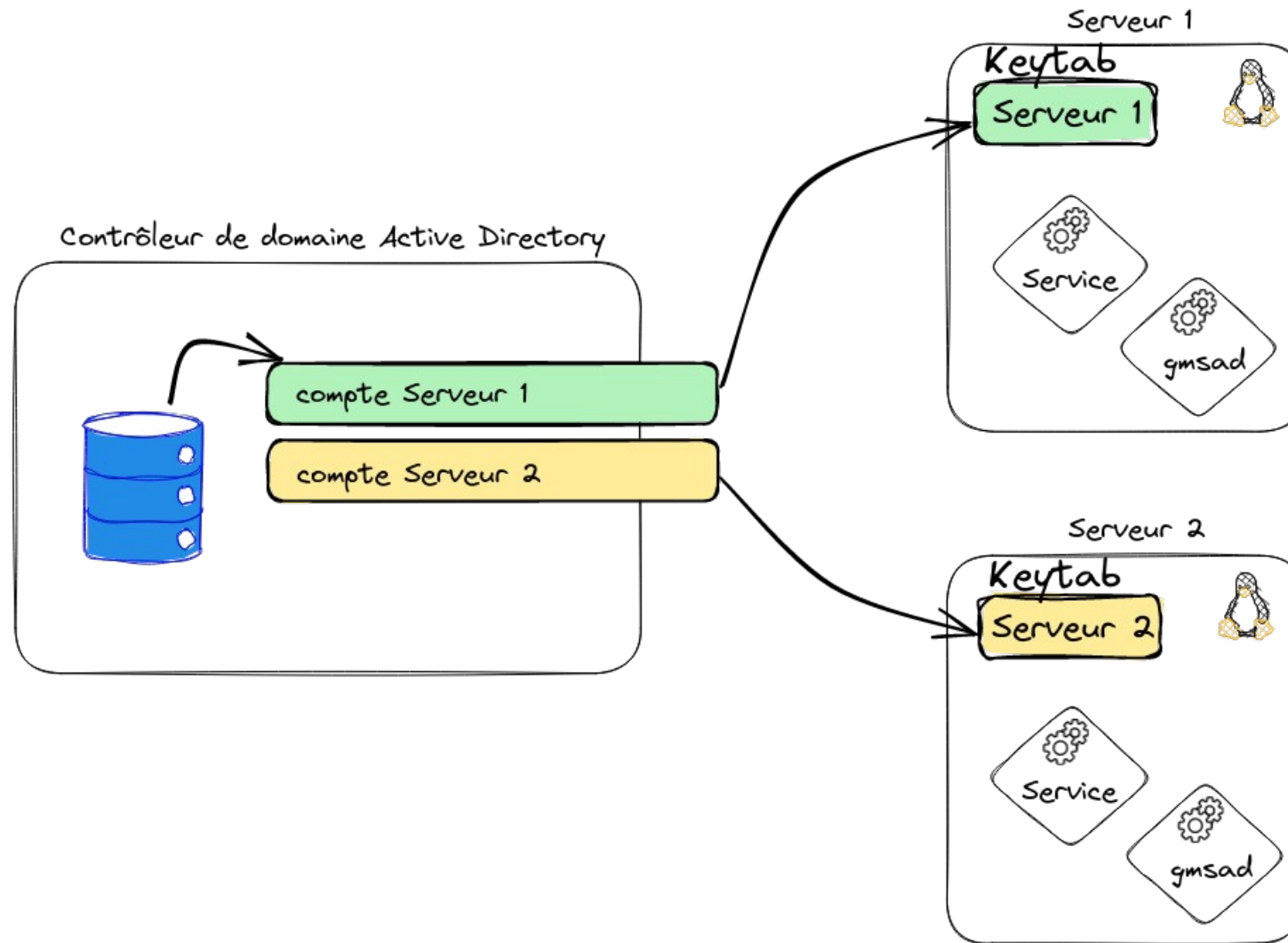




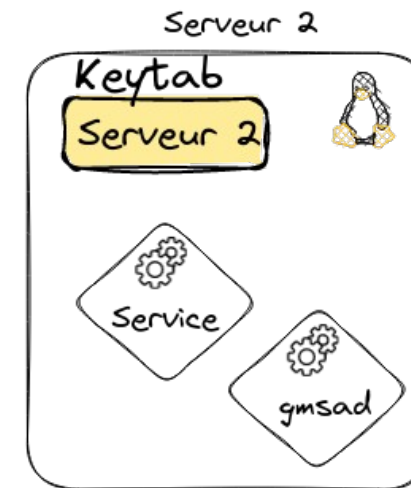
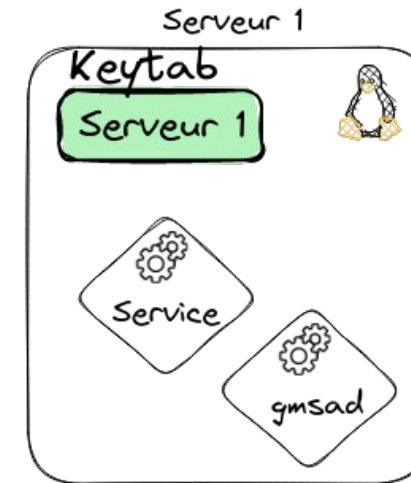
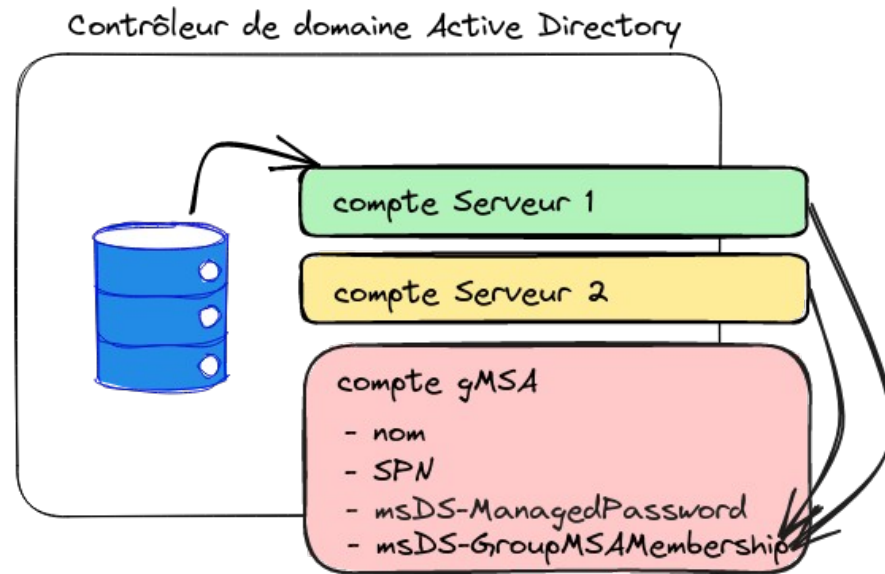
3 ■ gmsad

gmsad

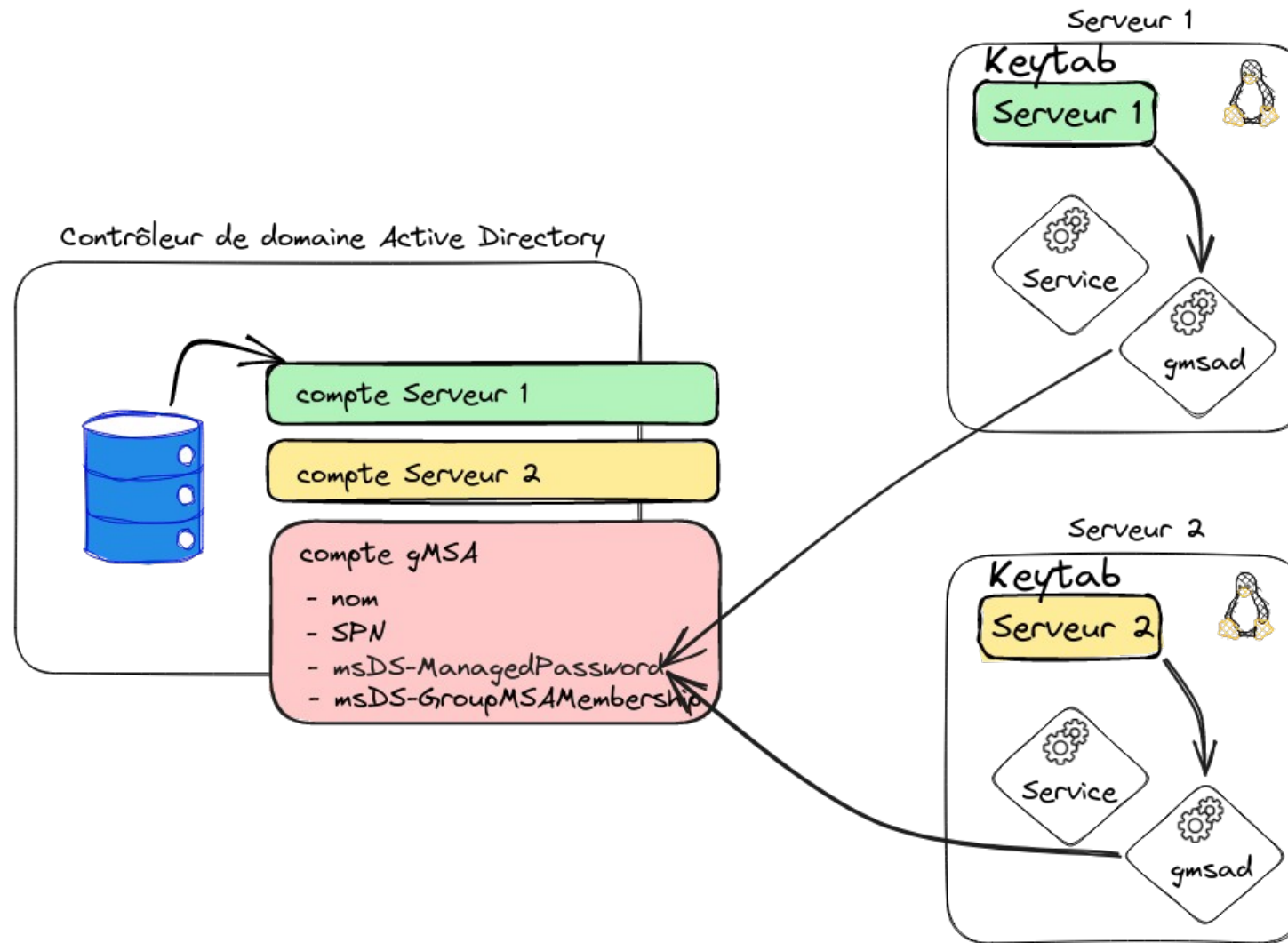
- Fonctionnalités :
 - Mécanisme de récupération du mot de passe d'un gMSA
 - Mécanisme de mise à jour
 - Gestion d'une keytab
- Fait pour s'exécuter en tant que service Linux
- ~1000 lignes de Python (typé)
- Github : <https://github.com/cea-sec/gmsad>



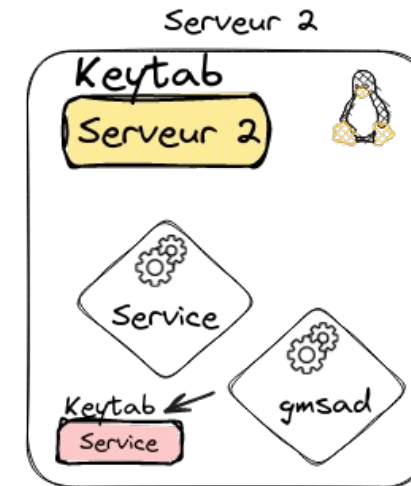
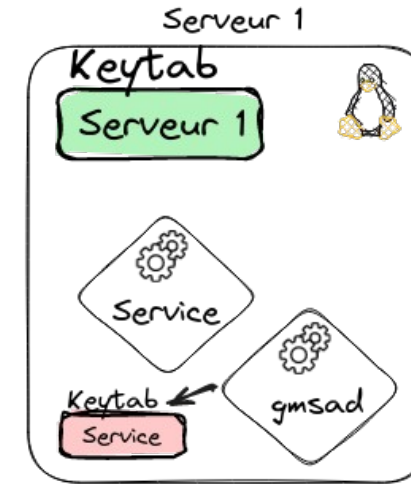
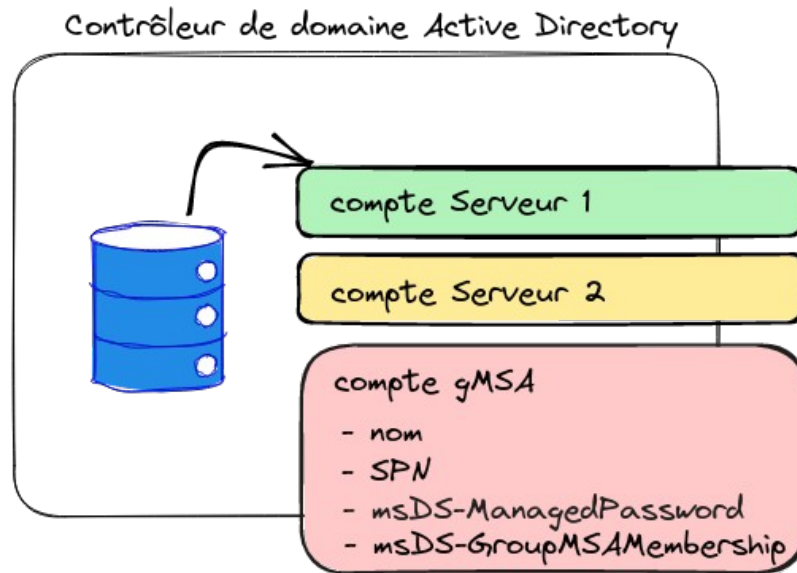
gmsad



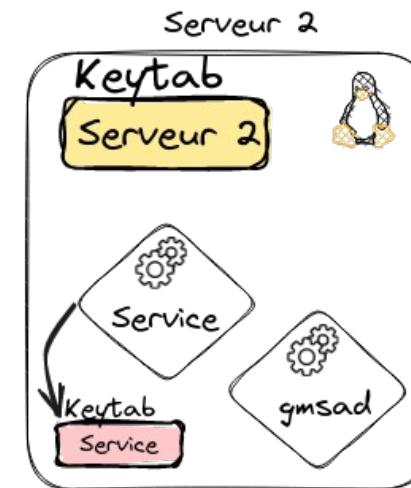
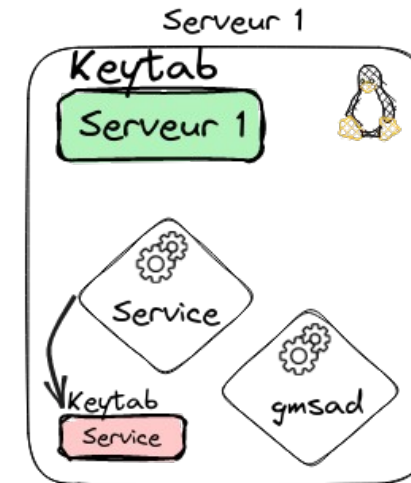
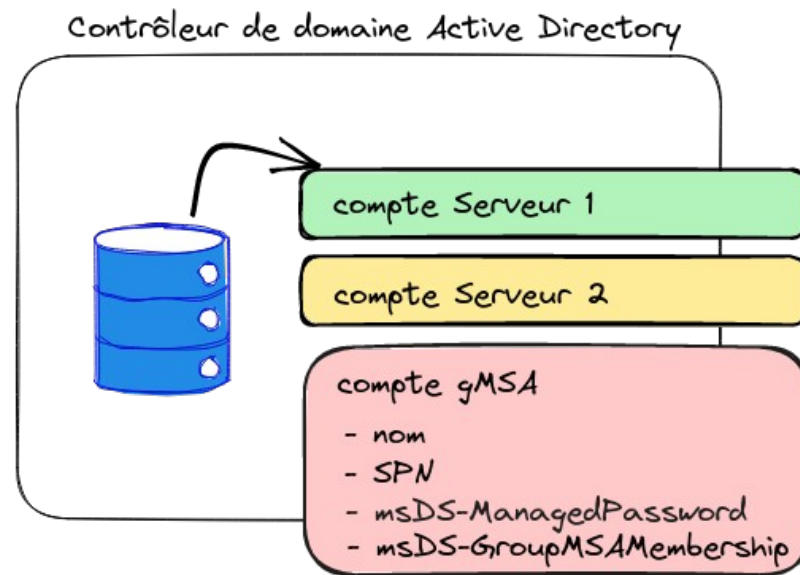
gmsad



gmsad



gmsad



“ **Lorem ipsum dolor sit amet,
consectetur adipiscing elit.
Maecenas porttitor congue
massa** ”

Des mots

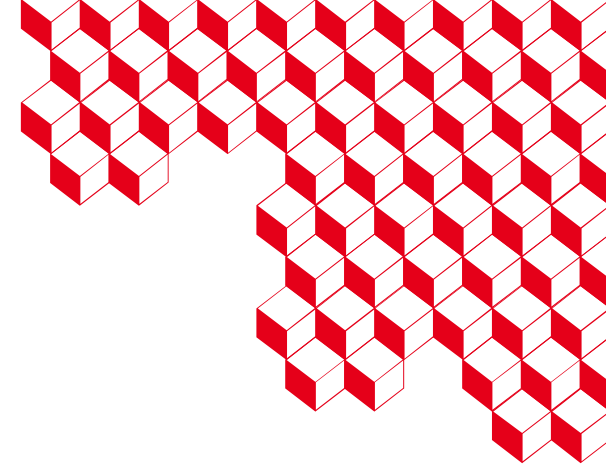
Applications

- En production :
 - Héberger un service kerberisé sur plusieurs machines Linux
 - Utiliser un compte Active Directory pour des tâches automatiques depuis plusieurs machines
- En audit :
 - Récupérer une keytab pour un gMSA
 - Générer et bidouiller des keytabs facilement

TODO

- *Packager* l'outil dans les principales distributions





Fin (vraiment)

<https://github.com/cea-sec/gmsad>

William BRUNEAU & Vincent RUELLO – SSTIC 2023

CEA DAM

Centre de Bruyères-le-Châtel
91297 Arpajon Cedex
Établissement public à caractère
industriel et commercial