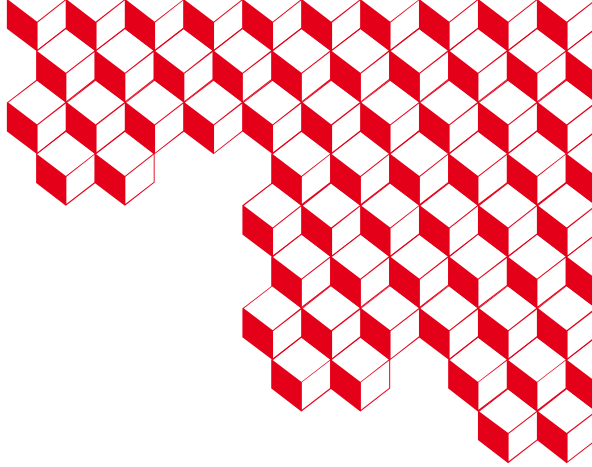


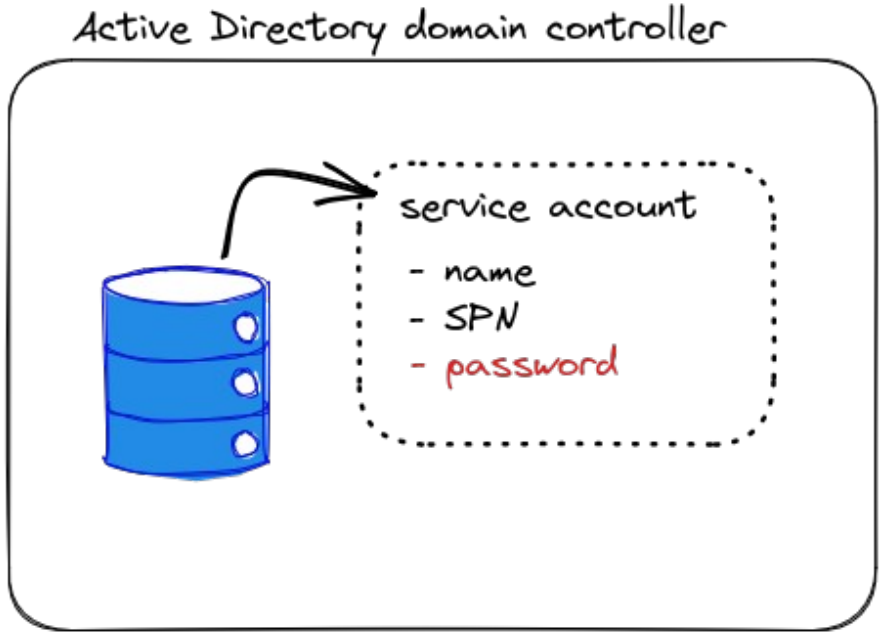
gmsad

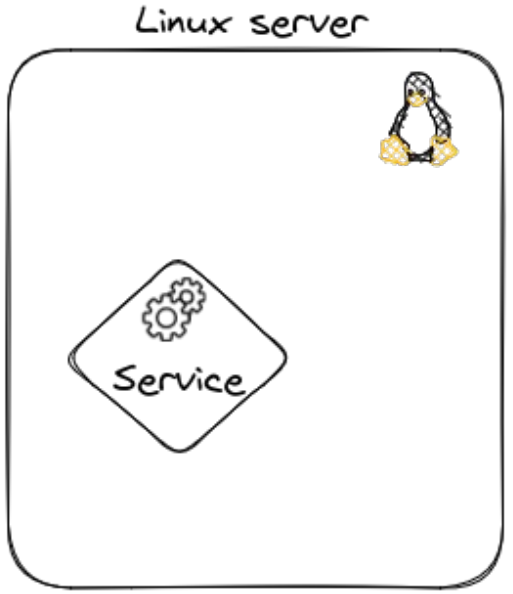
Use « group Managed Service Accounts » (gMSA) on Linux

William BRUNEAU & Vincent RUELLO – SSTIC 2023

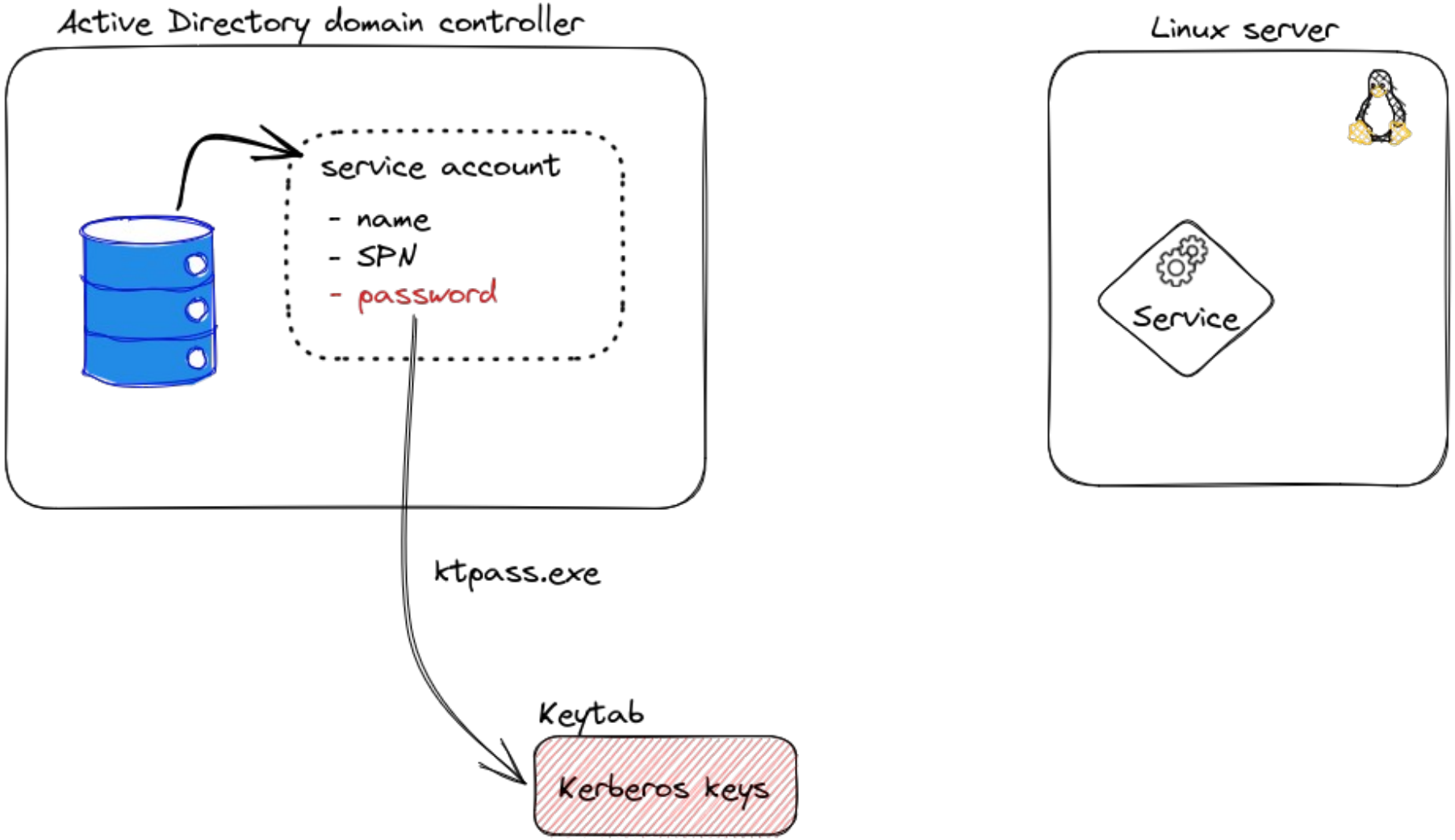
1. Kerberised service on Linux

Kerberised service on Linux

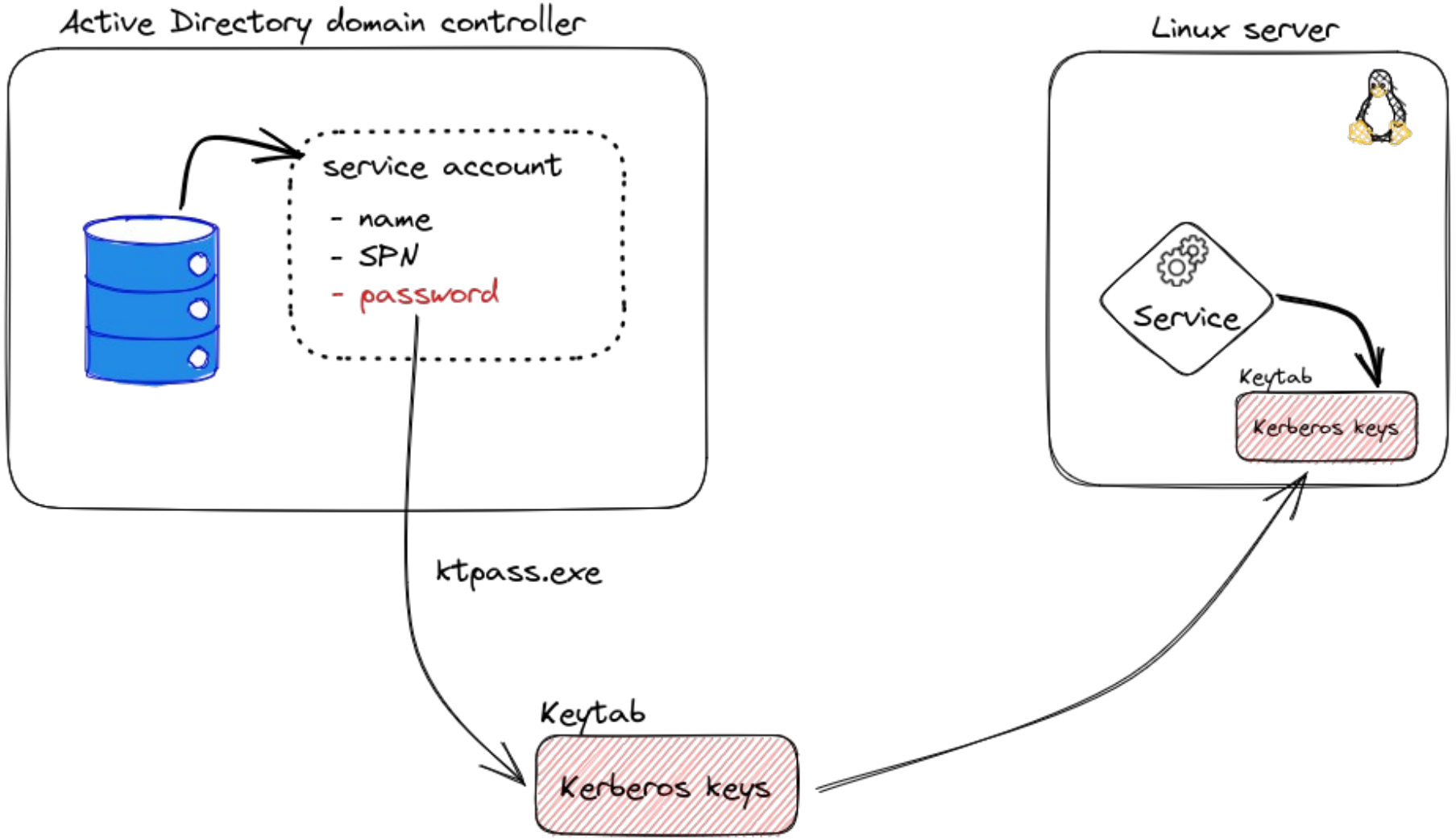




Kerberised service on Linux



Kerberised service on Linux

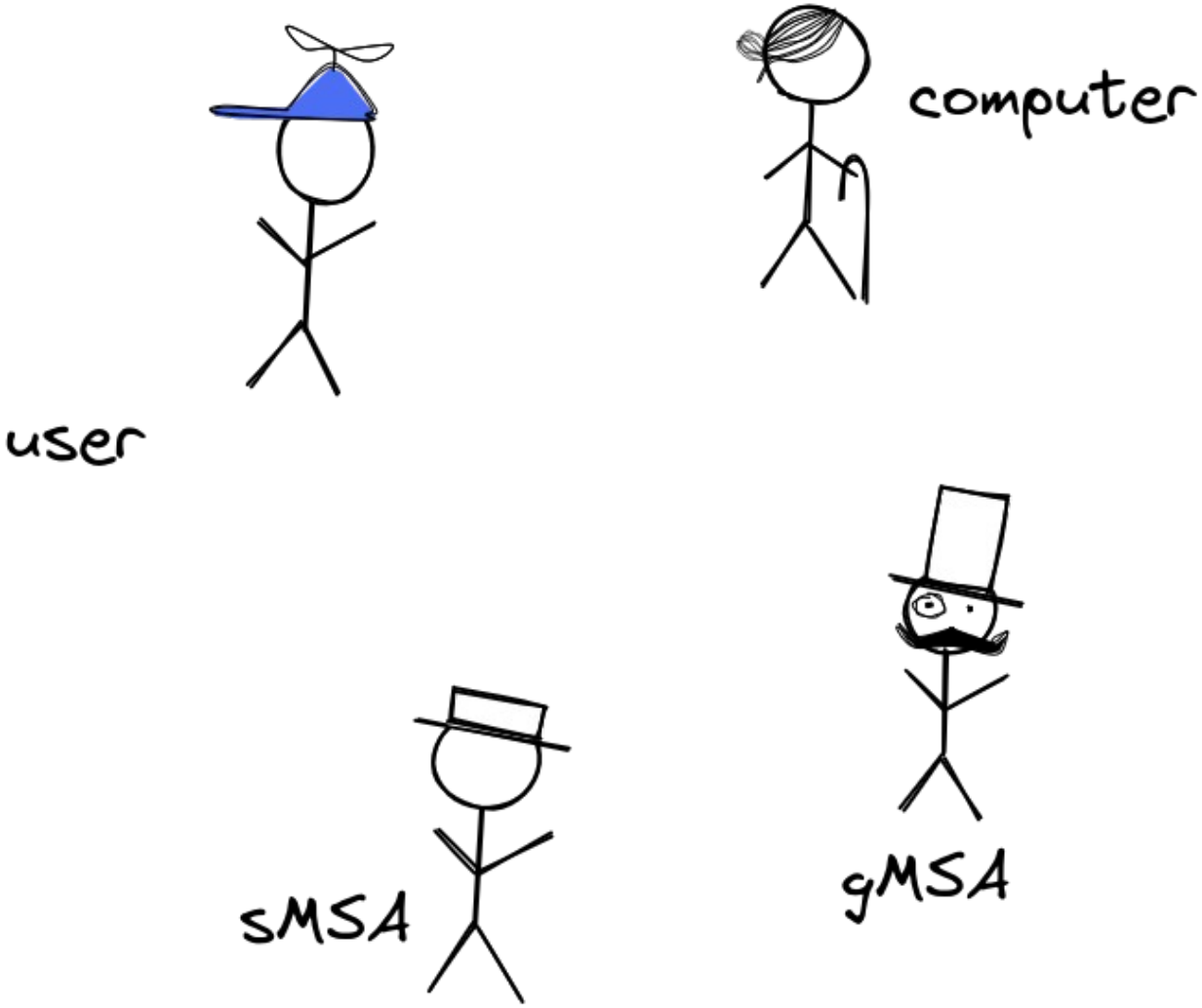


Configuration example

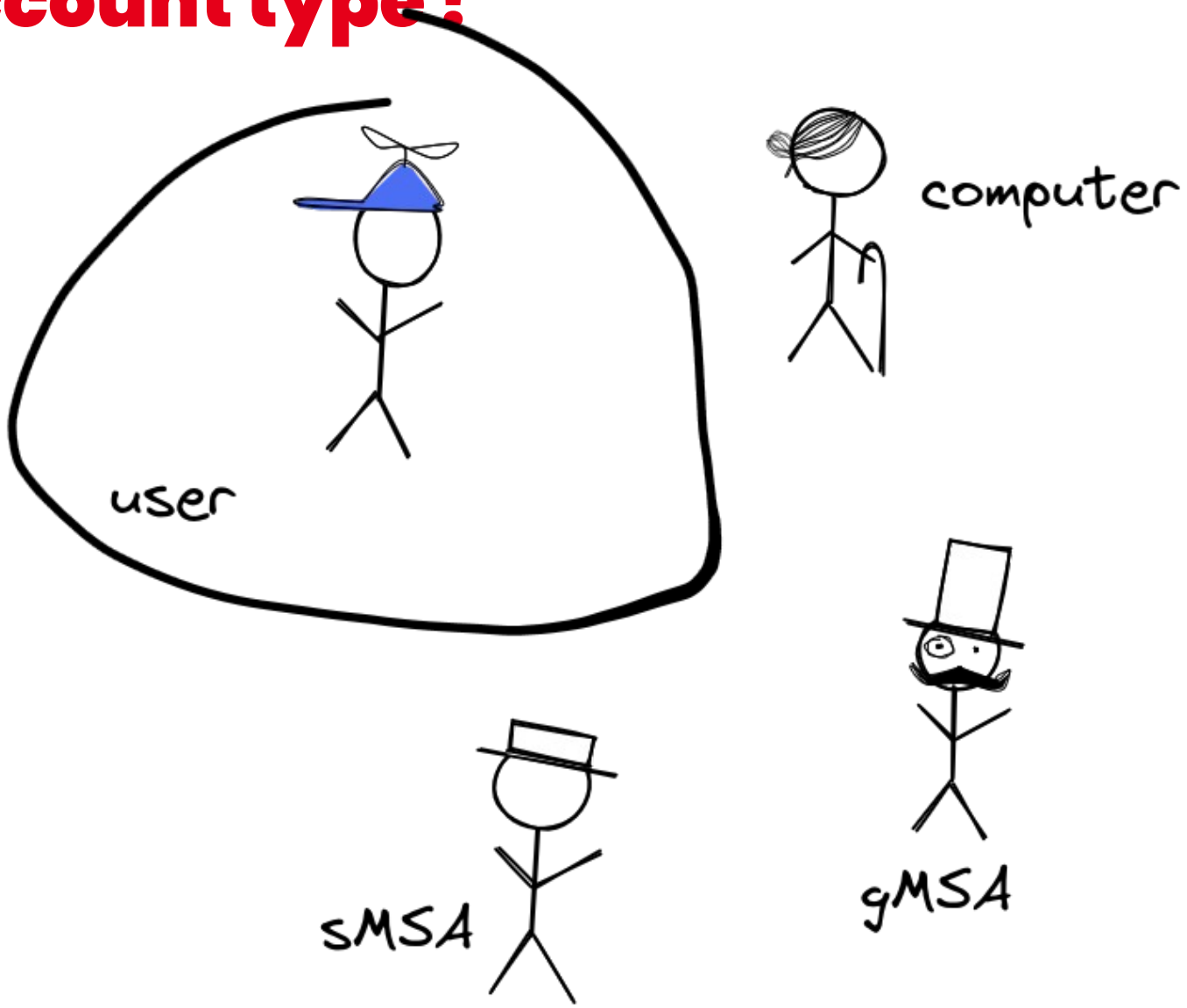
Apache configuration using `mod_auth_kerb` module:

```
<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>
```

Which account type ?



Which account type ?

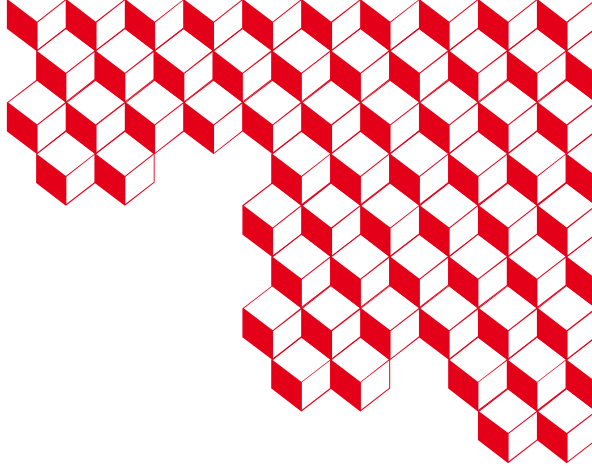


Legacy user account

- Setup
  - User account with a password which **never expires**
  - Use `ktpass.exe` to generate a **keytab**
- Issues
  - Not good to have a ”never expire” password
  - The password can be (poorly) chosen by the administrator

Legacy user account v2.0

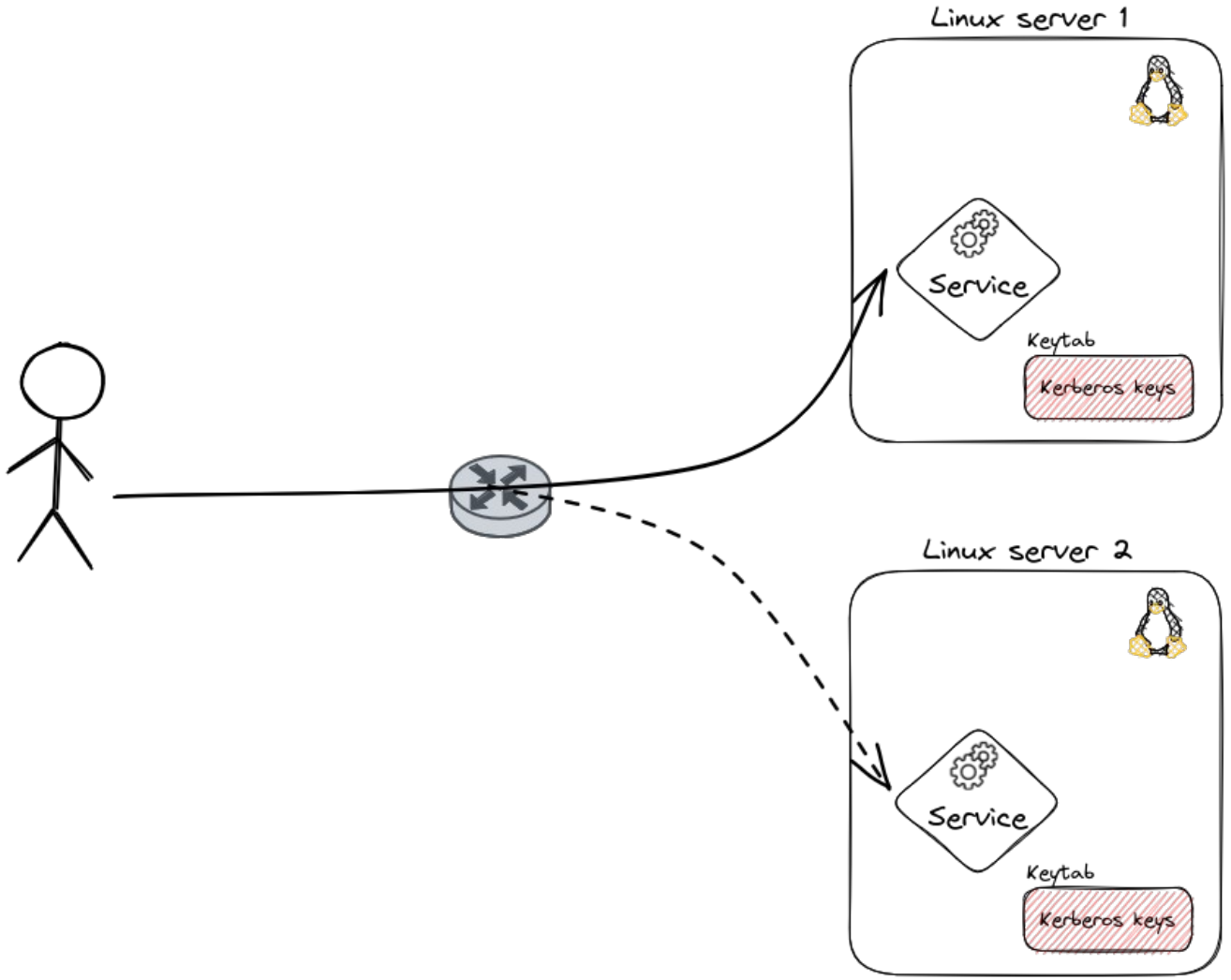
- Setup
  - User account with a password which **expires**
    - Renew password and keytab using `msktutil` (or equivalent)
  - Use `ktpass.exe` to generate the keytab with **option +rndPass**
- Works well !



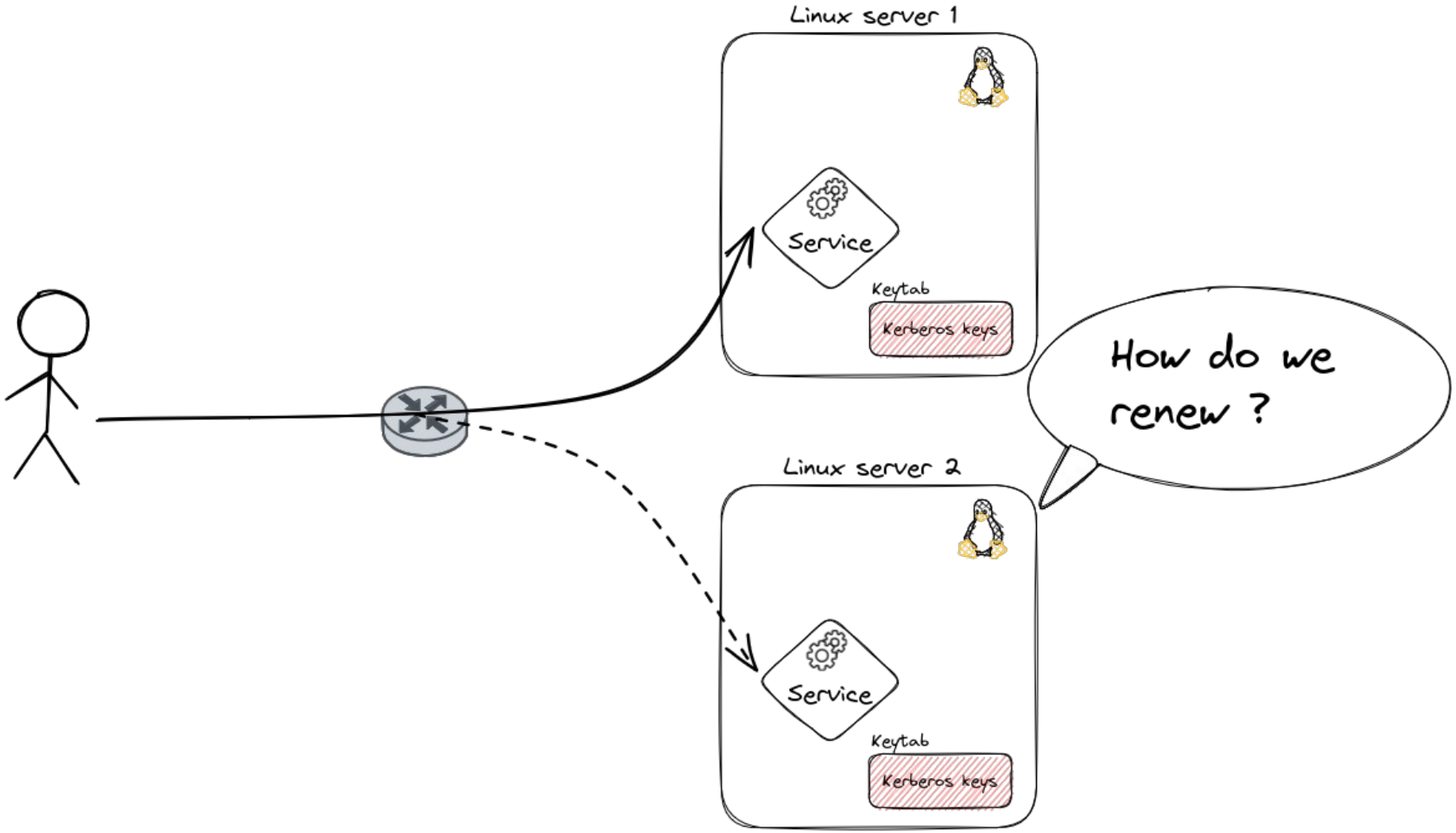
The end

William BRUNEAU et Vincent RUELLO – SSTIC 2023

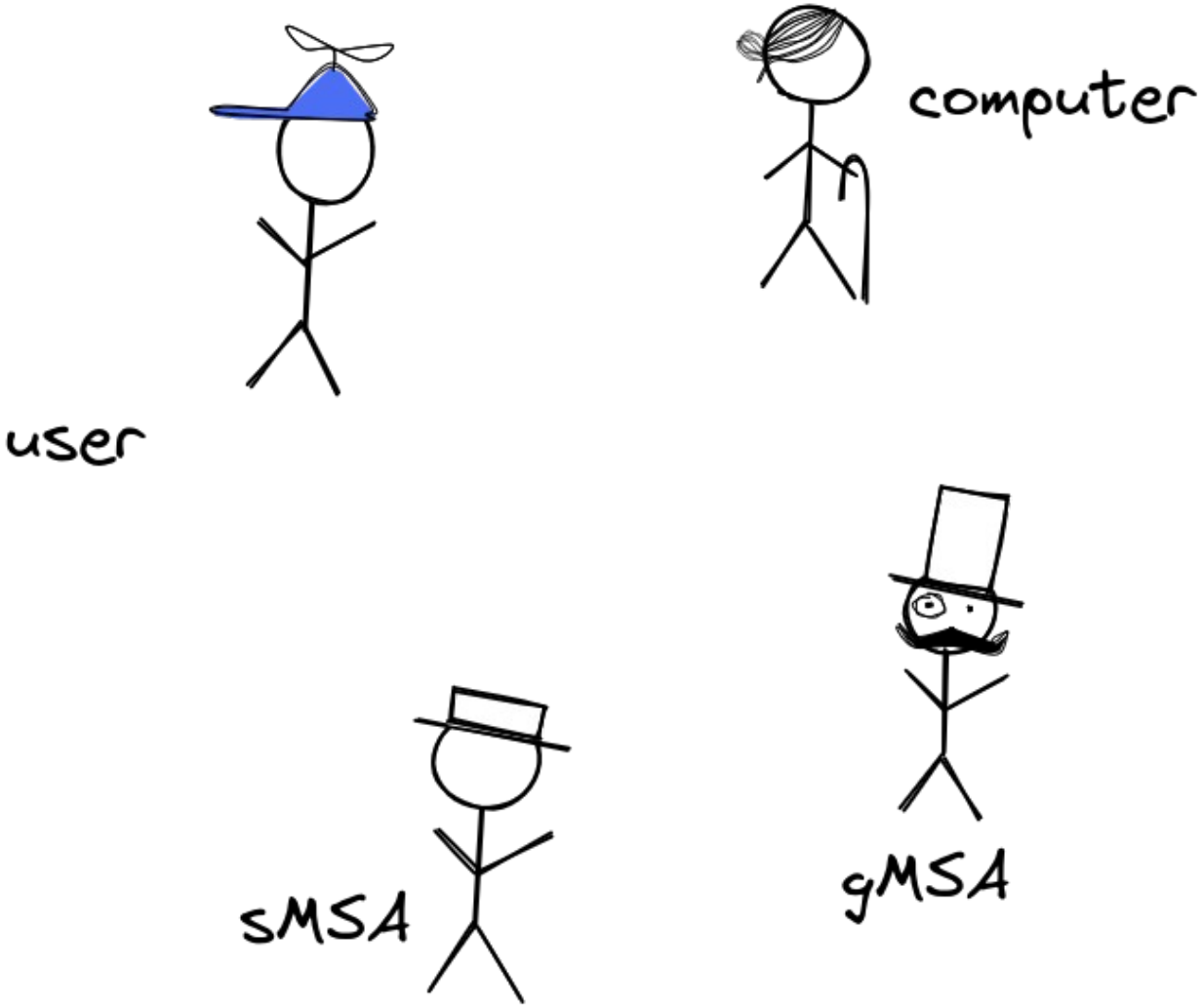
What about redundancy ?!



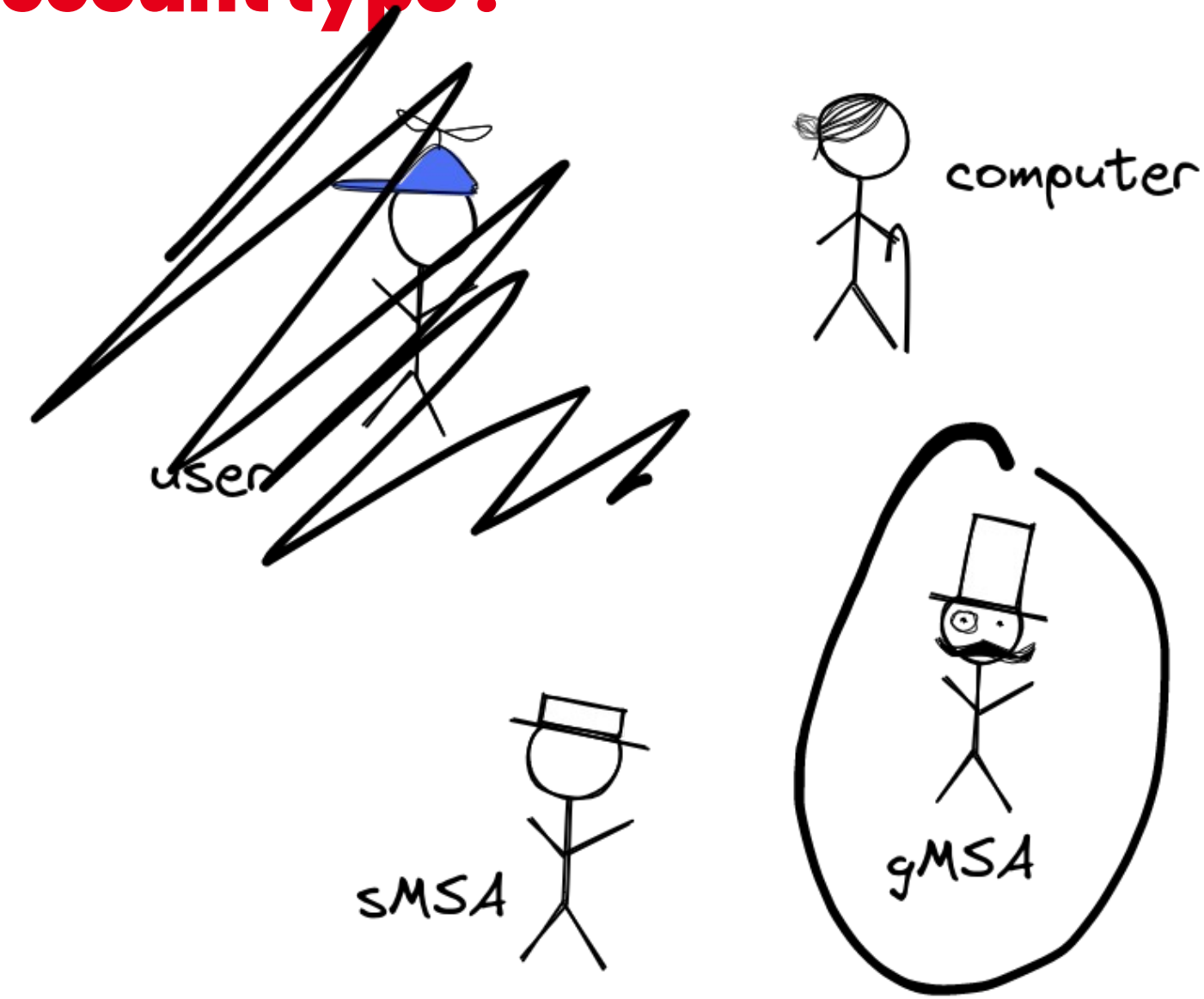
What about redundancy ?!



Which account type ?



Which account type ?



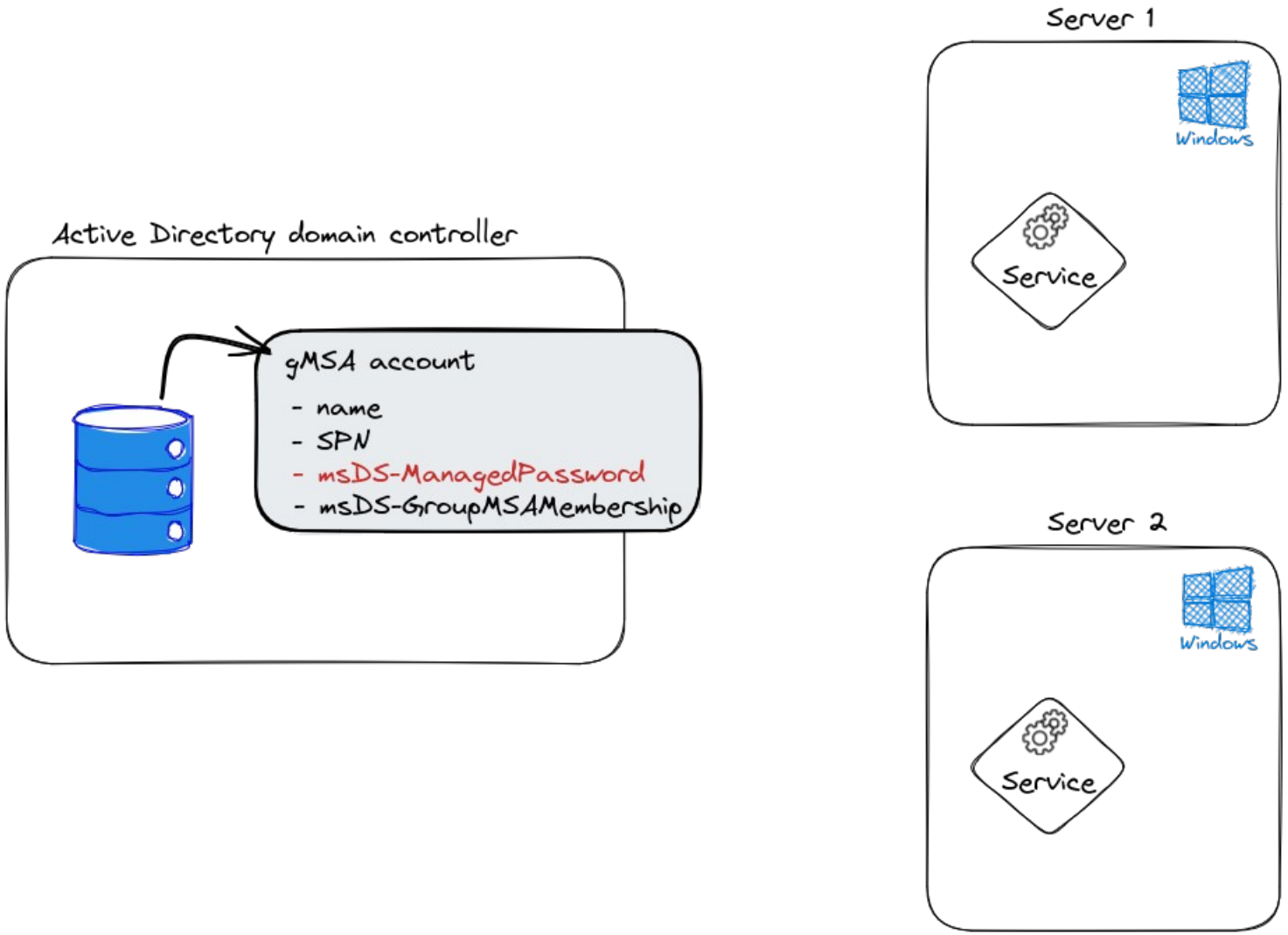
2. group Managed Service Account

group Managed Service Account

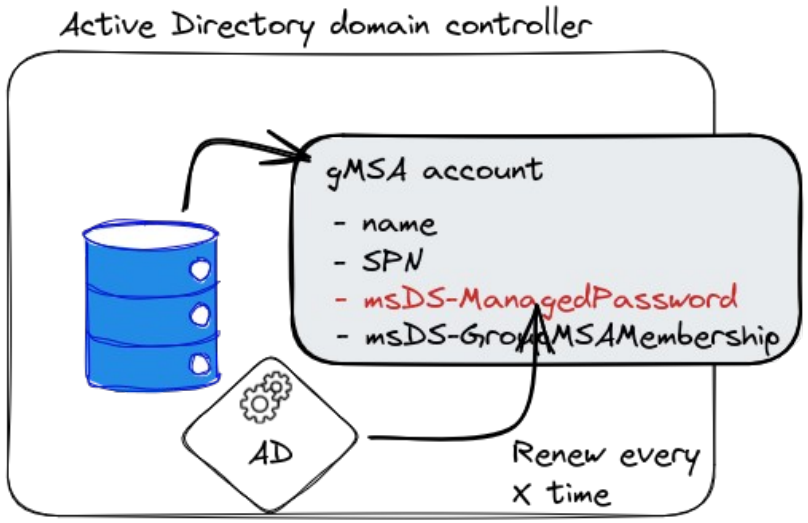
- Active Directory mechanism
- Enable the use of **one account on multiple computers**

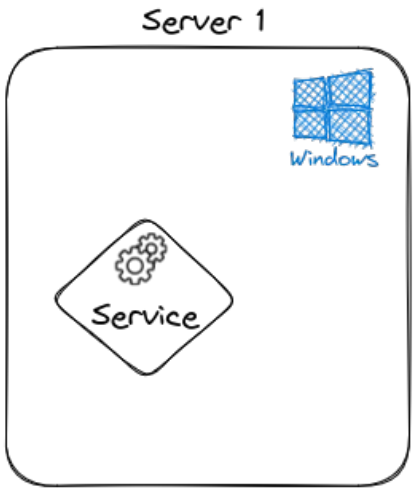
- Prerequisite:
  - KDS root key deployed
  - Schema updated to Windows Server 2012

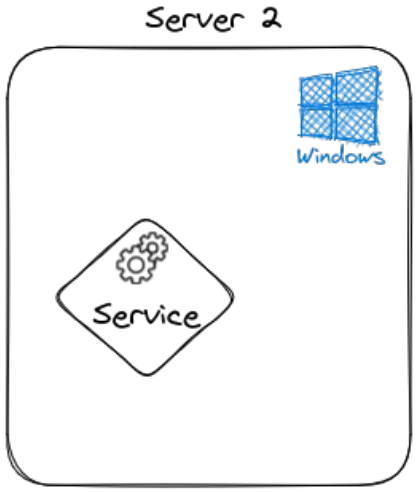
Basic gMSA life cycle



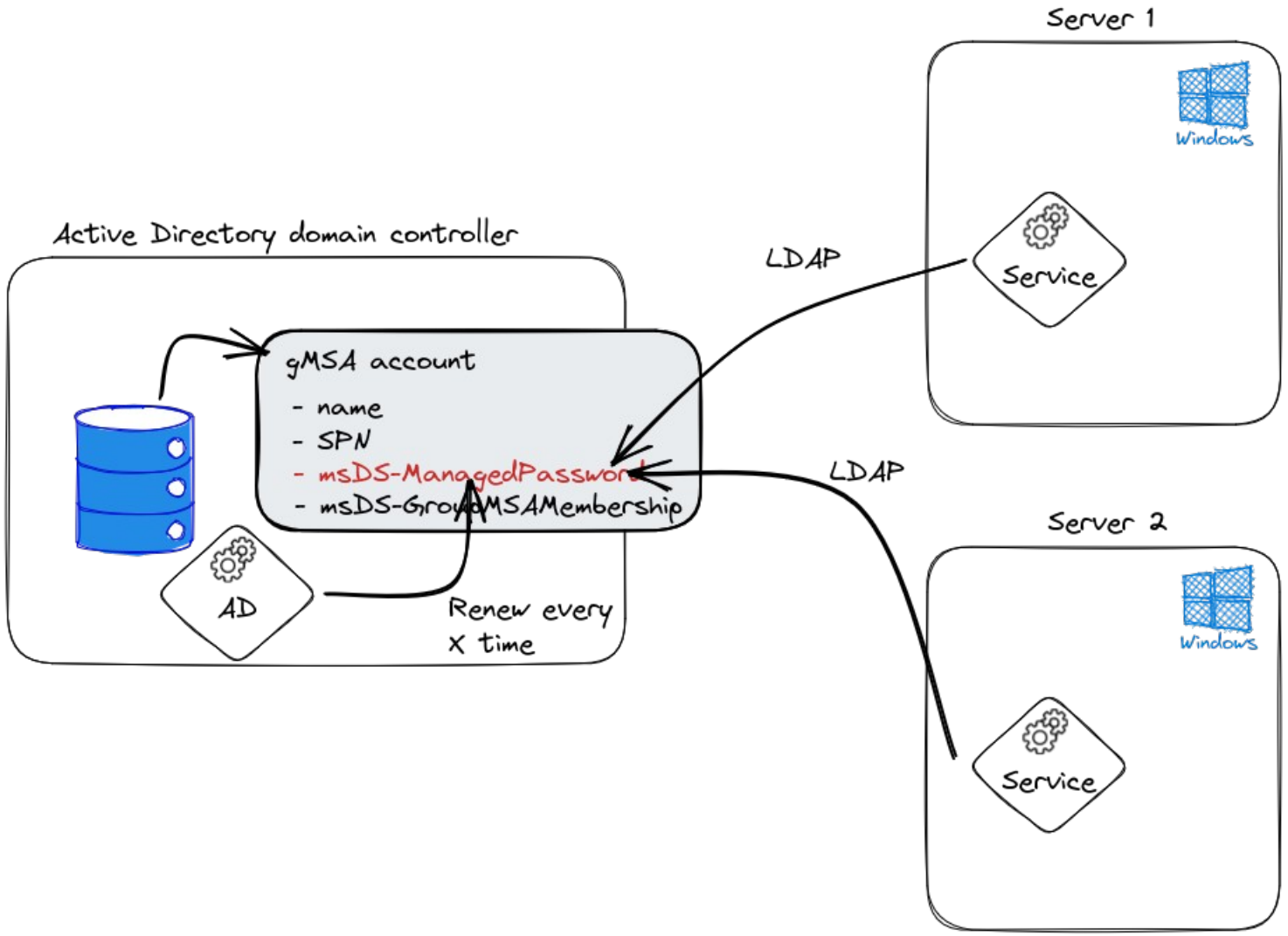
Basic gMSA life cycle







Basic gMSA life cycle

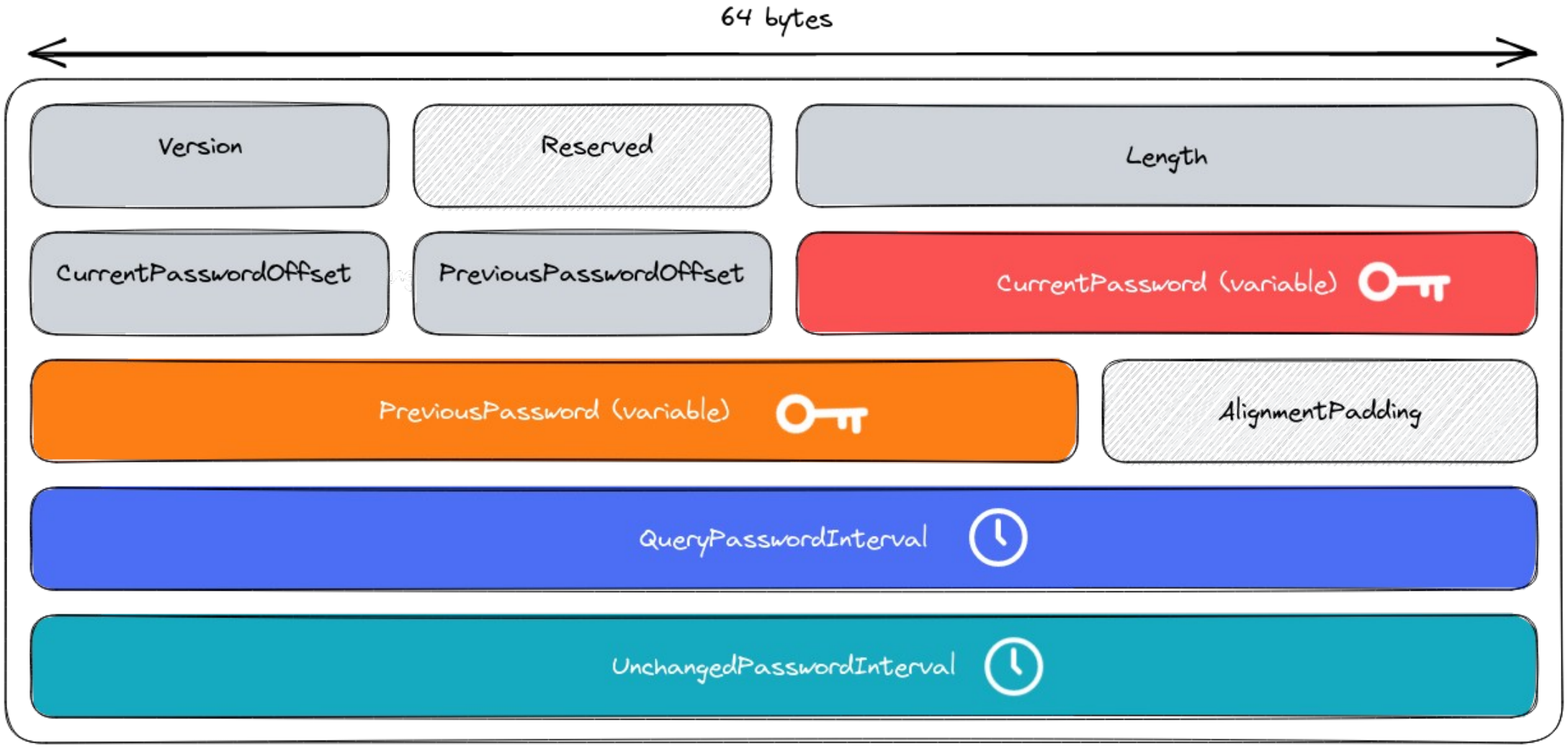


gMSA object

- **msDS-ManagedPassword** attribute
  - Gives access to the account password and some metadata
  - Accessible through an encrypted **LDAP** connection (LDAPs or Kerberos encrypted LDAP)

- **msDS-GroupMSAMembership** attribute
  - Contains the list of account who has access to msDS-ManagedPassword
  - Windows security descriptor format

msDS-ManagedPassword



MSDS-MANAGEDPASSWORD_BLOB

Microsoft « documentation »

a. Let StaleCount be zero.

b. Let NewKeyStartTime = CurrentKeyExpirationTime.

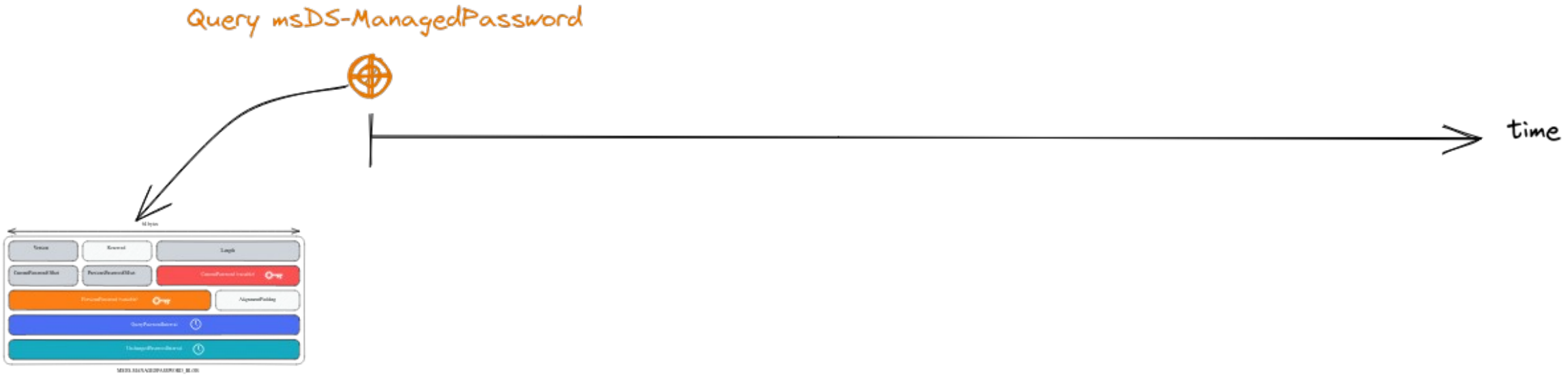
c. Let NewKeyStartTime = NewKeyStartTime + GDKIRolloverInterval and StaleCount = StaleCount +1 until NewKeyStartTime is greater than the current time.

d. Call GetPasswordBasedOnTimestamp() where:

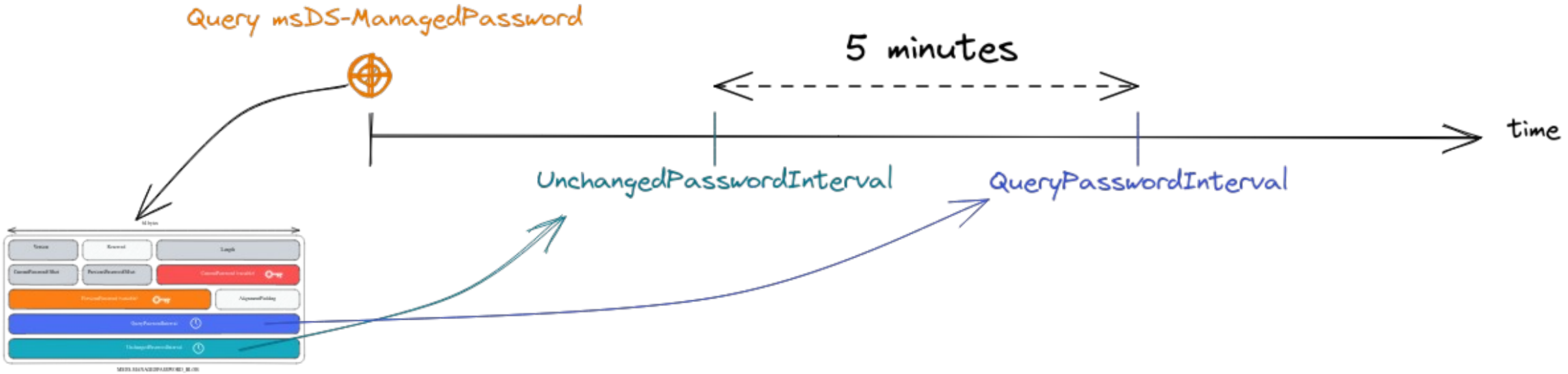
- *Timestamp* contains NewKeyStartTime.
- *AccountSID* contains the TO!objectSid attribute ([MS-ADA3] section 2.45).

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

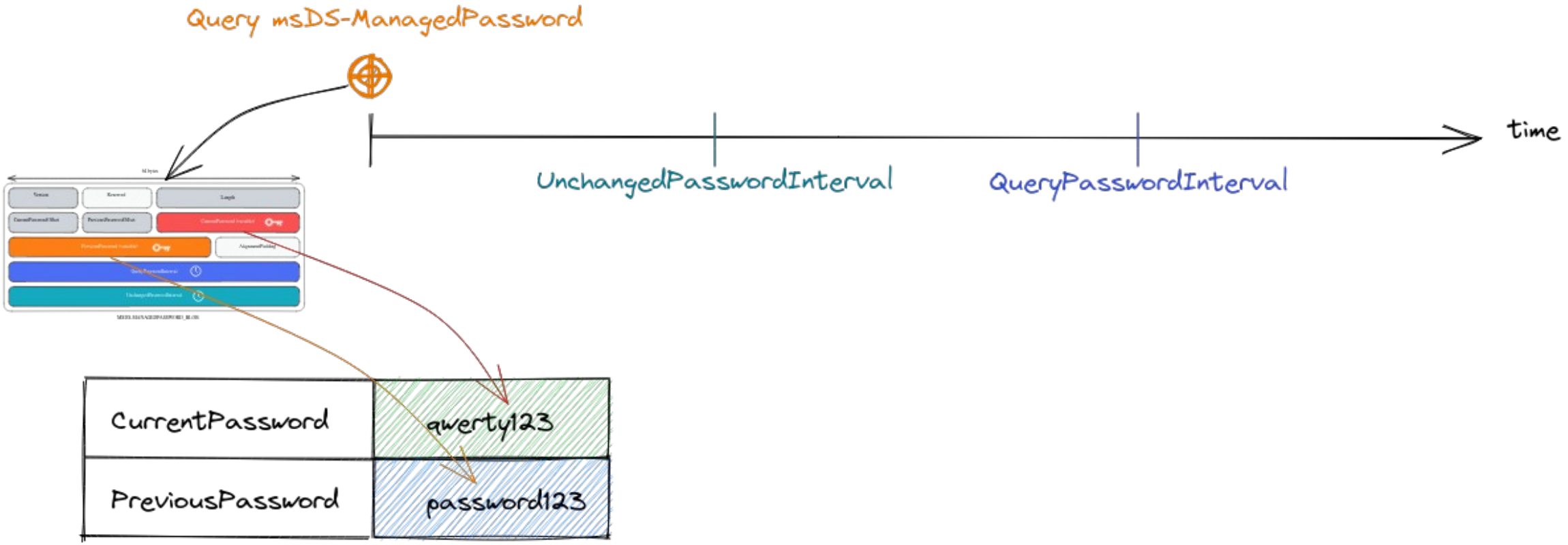
Update mechanism



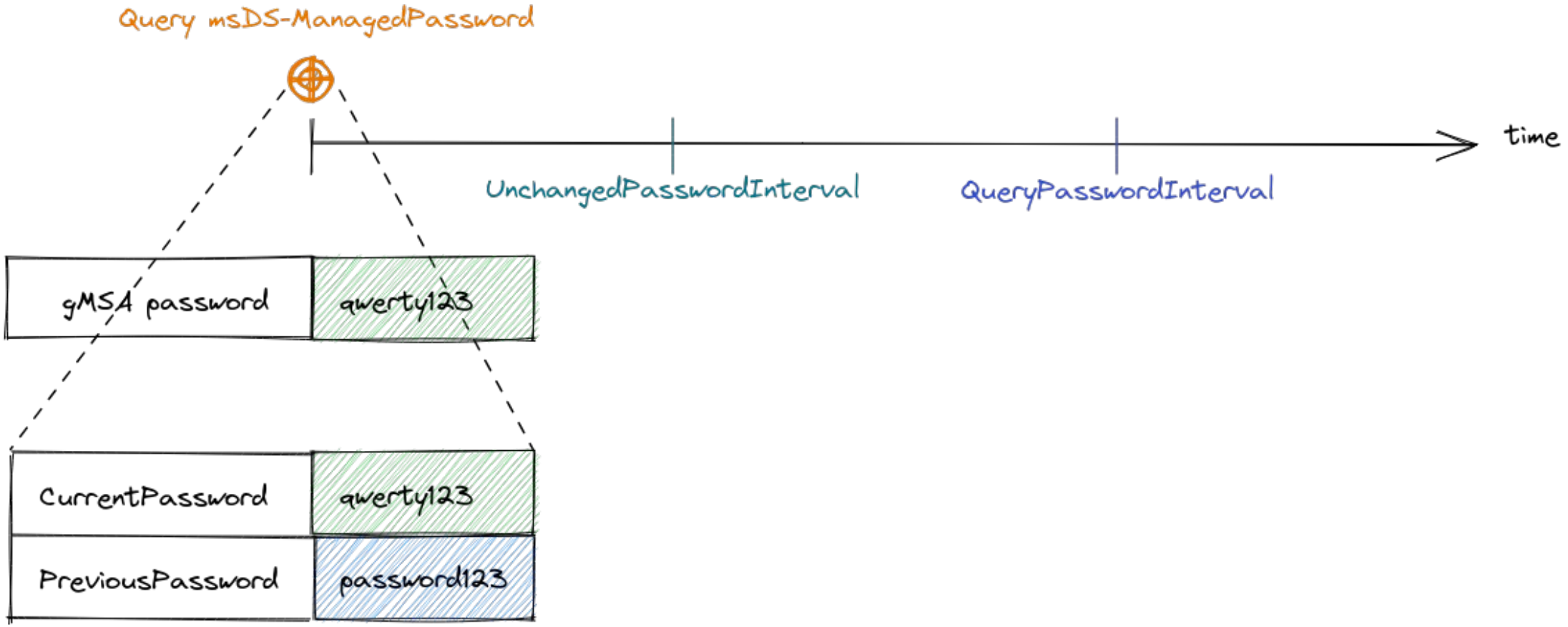
Update mechanism



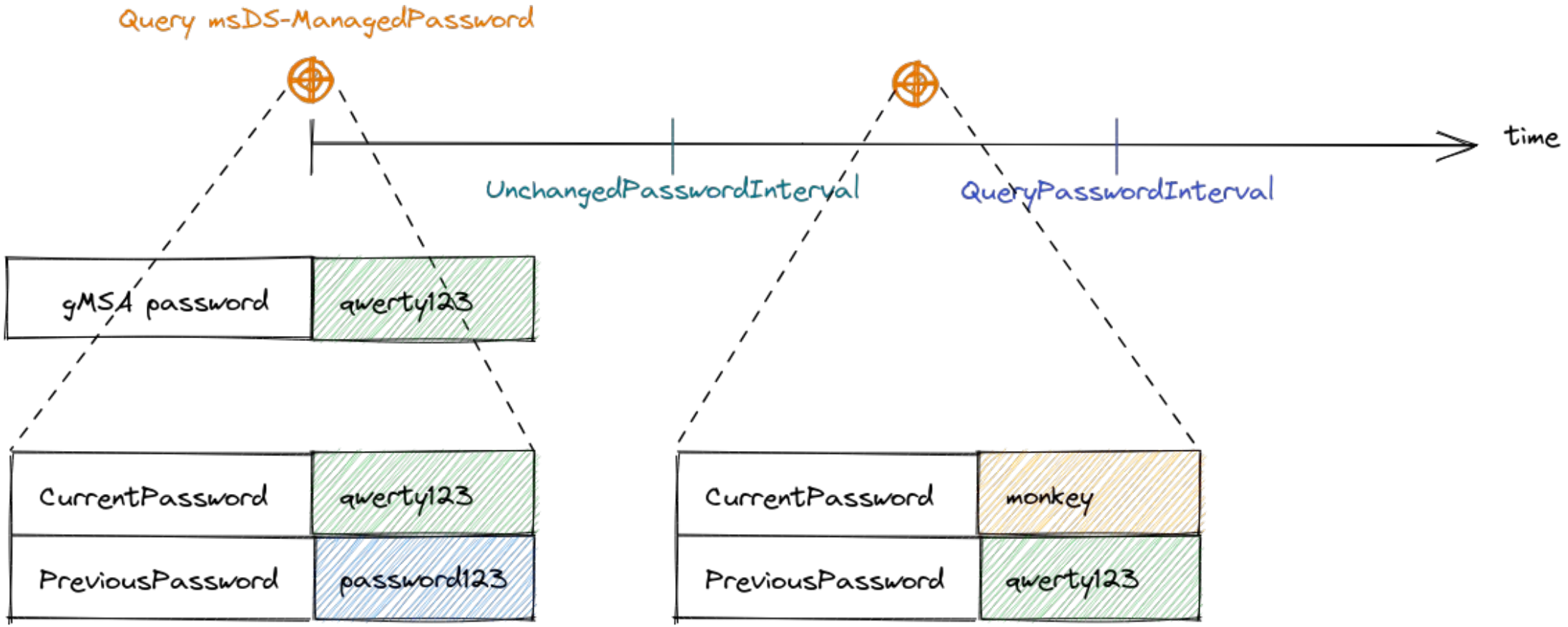
Update mechanism



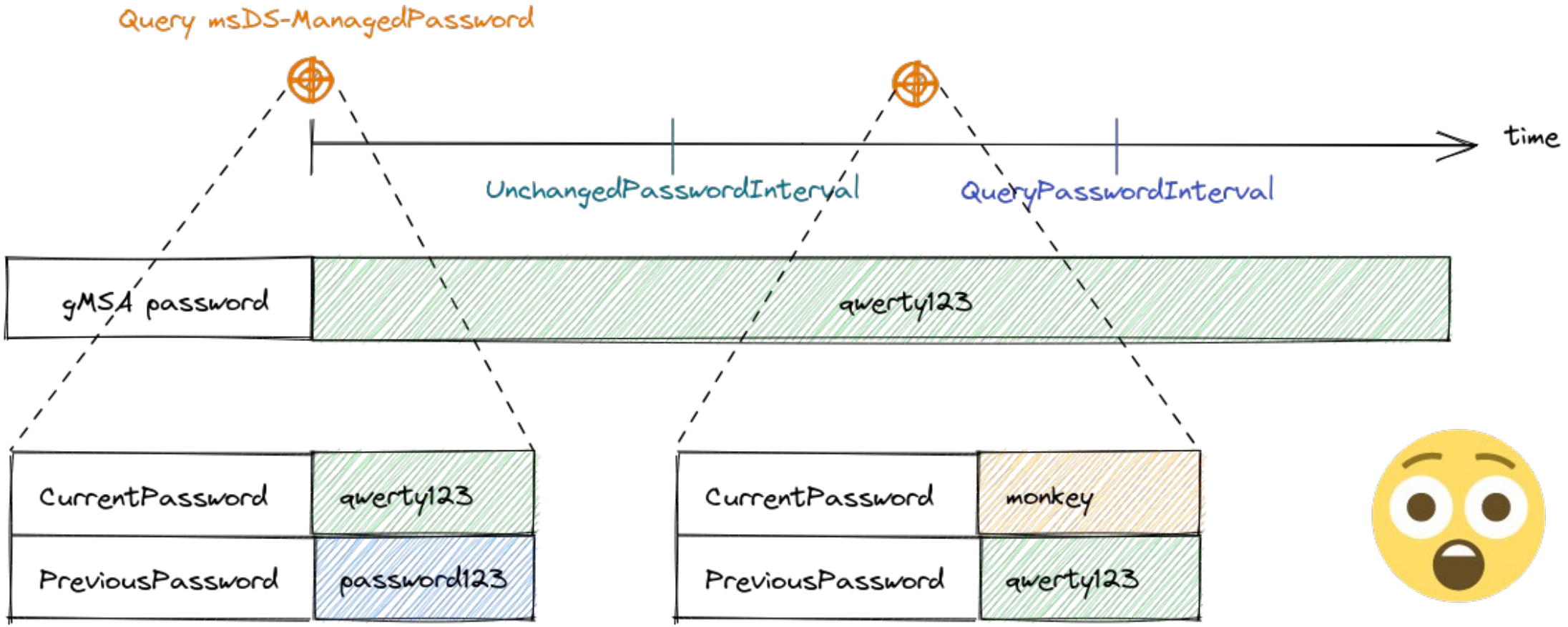
Update mechanism



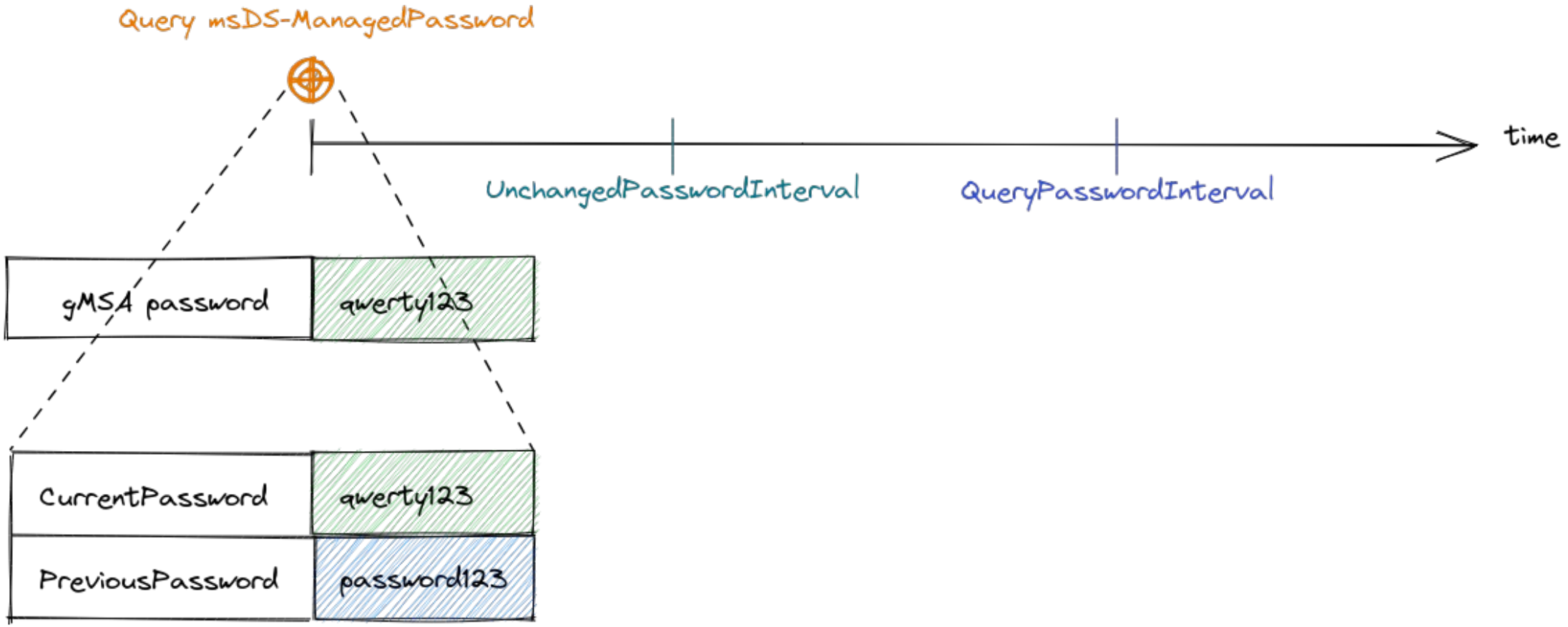
Update mechanism



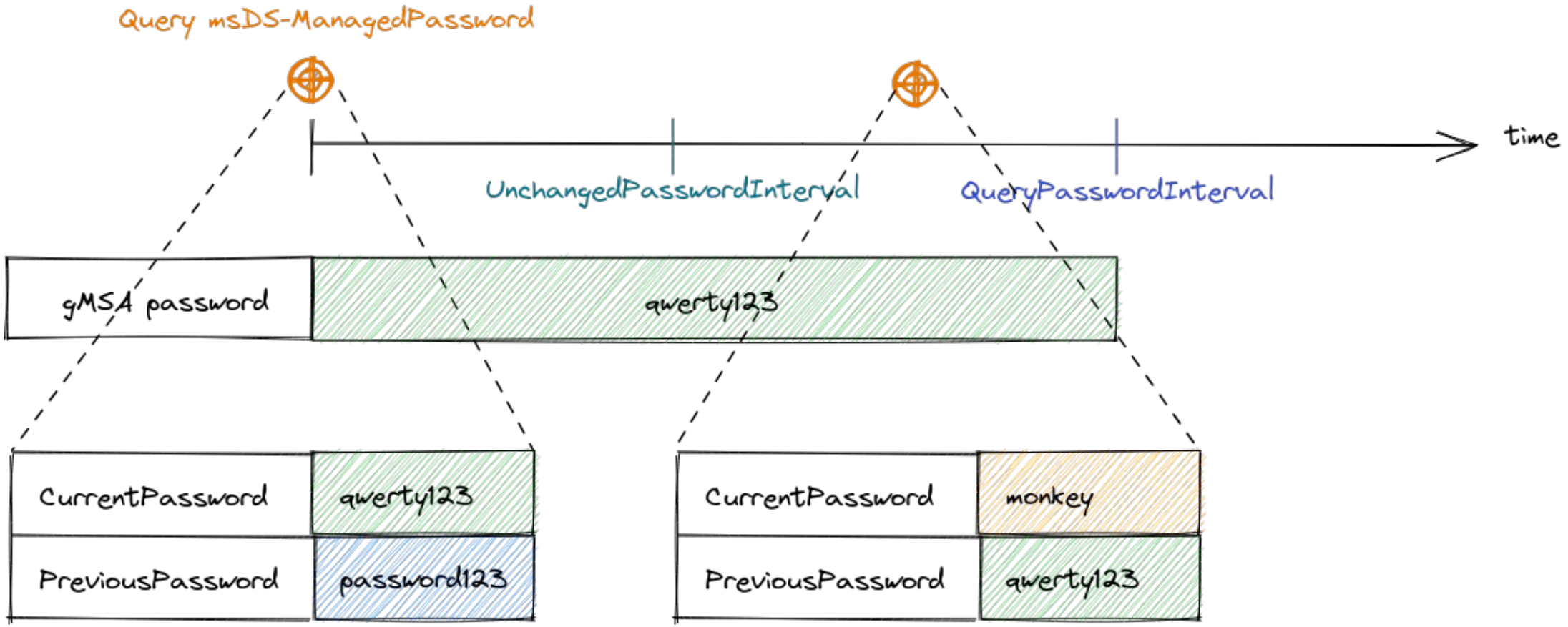
Update mechanism



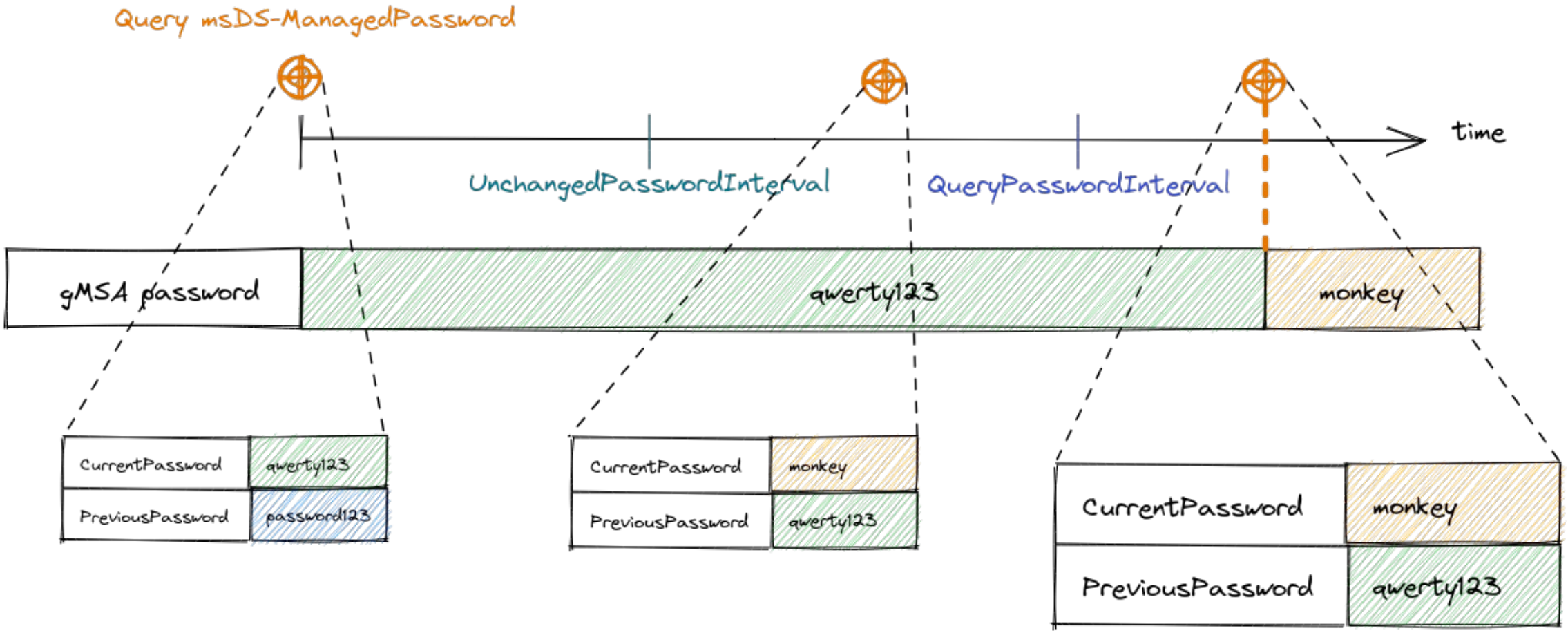
Update mechanism



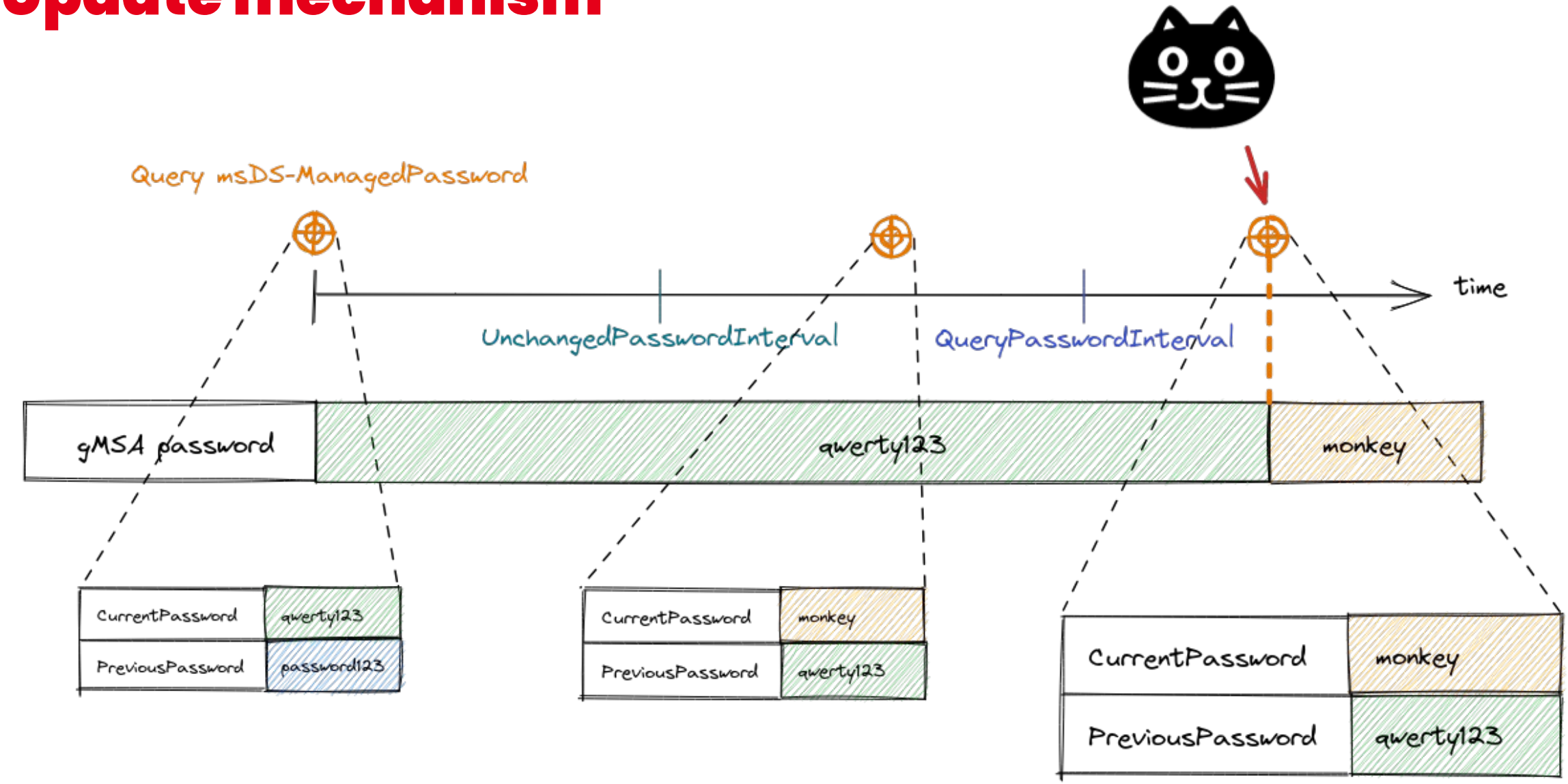
Update mechanism



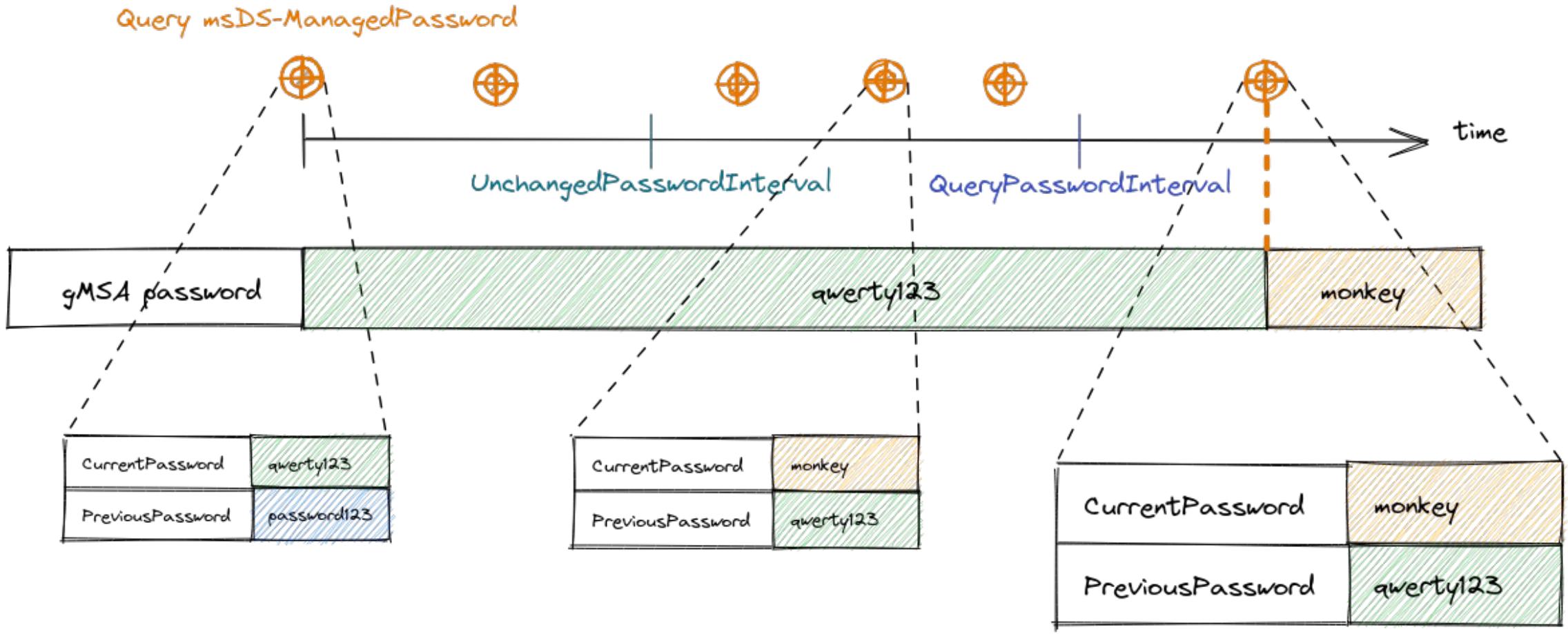
Update mechanism



Update mechanism

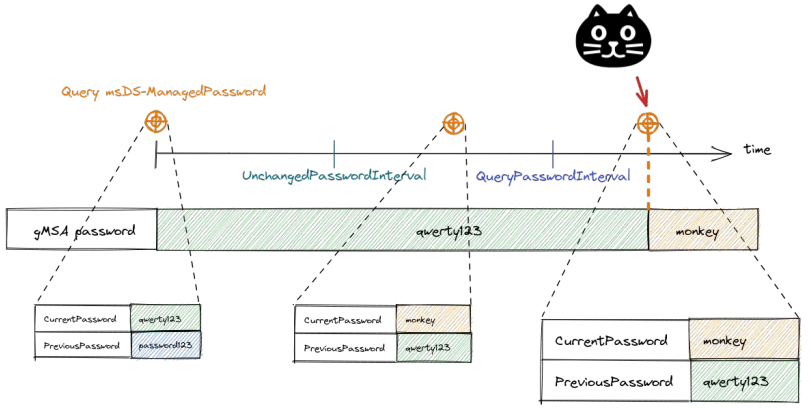


Update mechanism



Wrapping it up

- After **UnchangedPasswordInterval :**
  - We have access to the new password
  - But it is not yet changed for the account !
- After **QueryPasswordInterval**, we need to query the msDS-ManagedPassword attribute to **trigger** the password roll
- The time between these « interval » allow each computer using the gMSA to retrieve the new password before it is changed



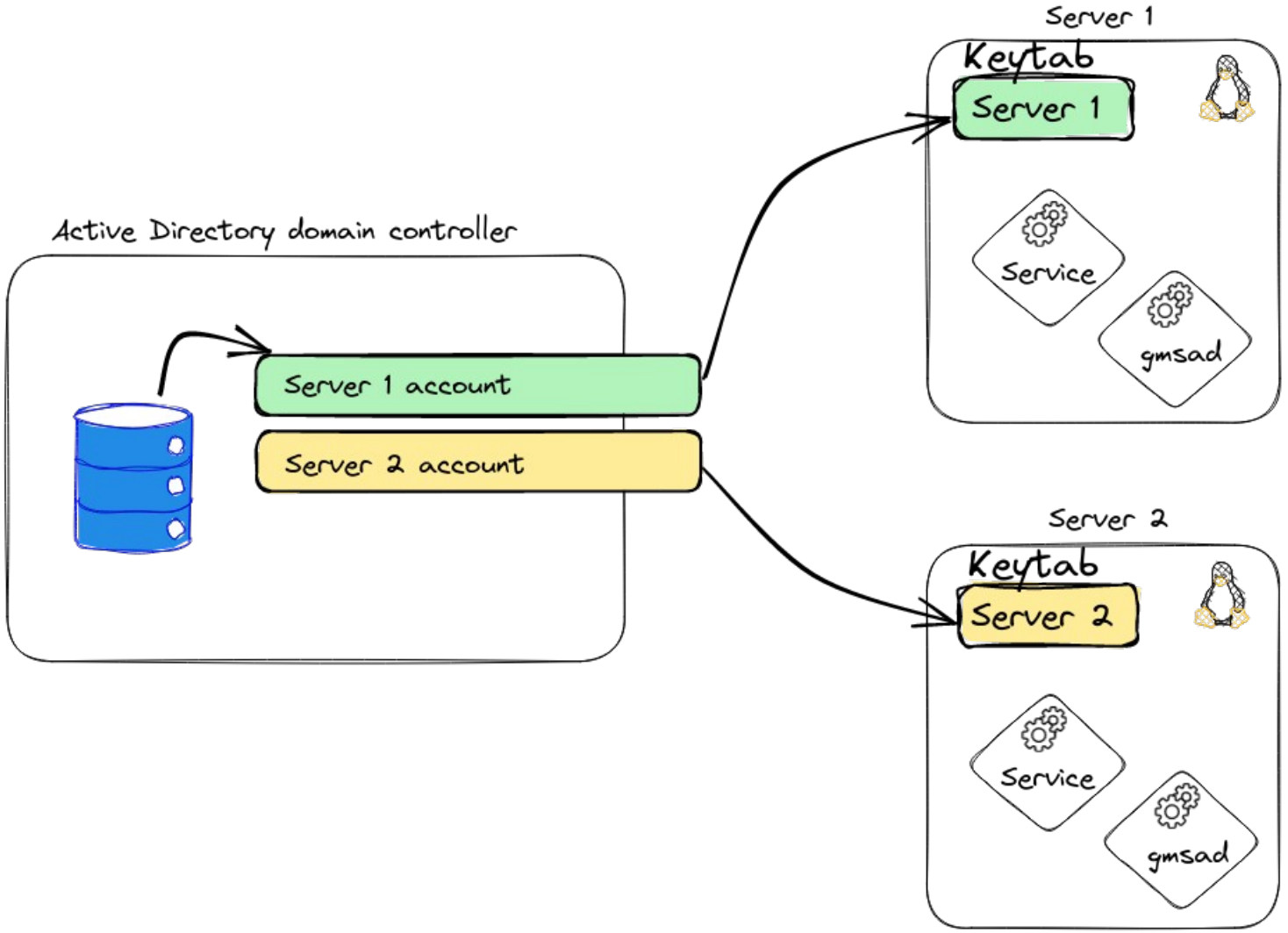
3. gmsad

gmsad

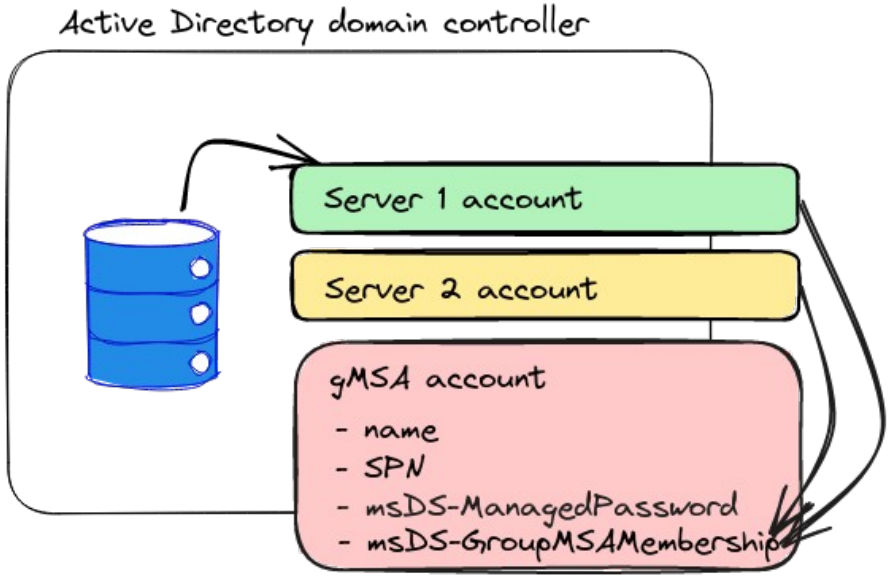
- Features :
  - Retrieve a gMSA password
  - Update mechanism
  - Manage a keytab
- Intended for use as a Linux service
- ~1000 lines of (typed) Python

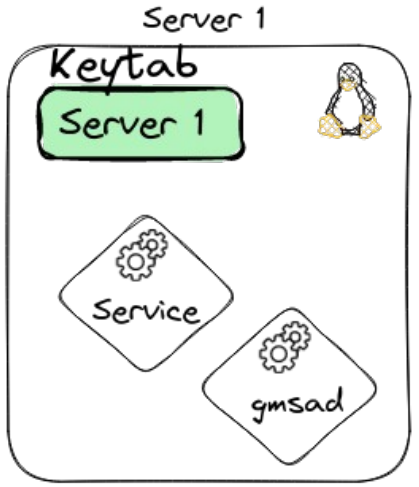
- Github: https://github.com/cea-sec/gmsad

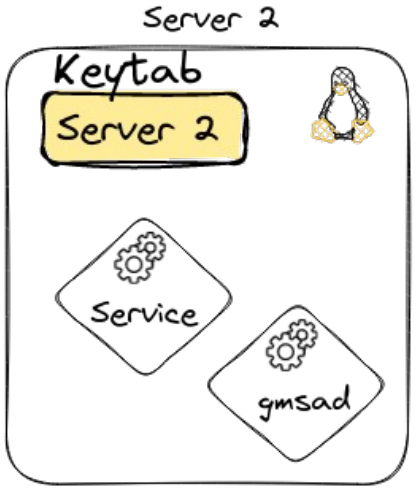
gmsad


Server 1
Keytab
Server 1
Service
gmsad
Active Directory domain controller
Server 1 account
Server 2 account
Server 2
Keytab
Server 2
Service
gmsad

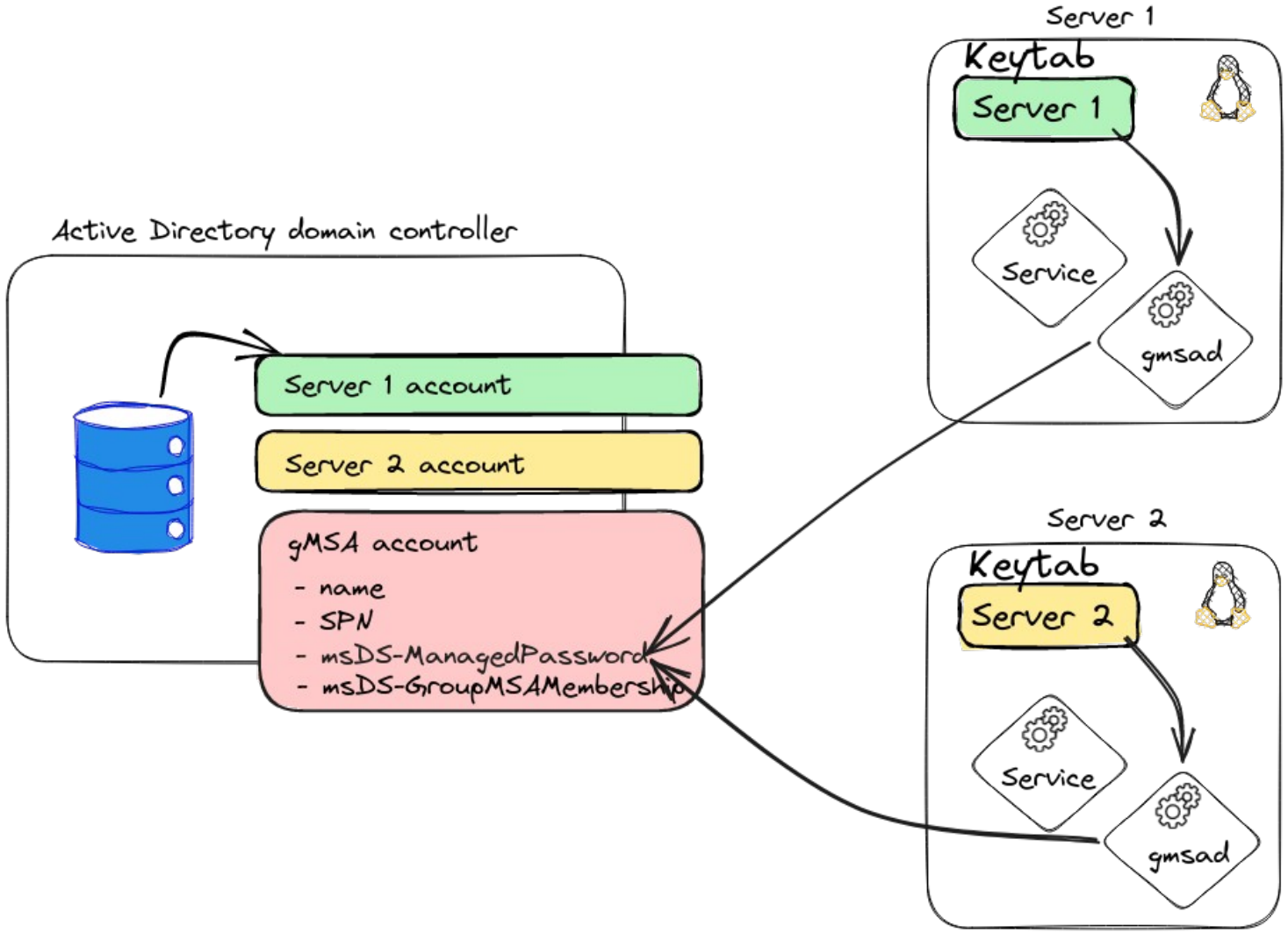
gmsad


Active Directory domain controller
Server 1 account
Server 2 account
gMSA account
- name
- SPN
- msDS-ManagedPassword
- msDS-GroupMSAMembership

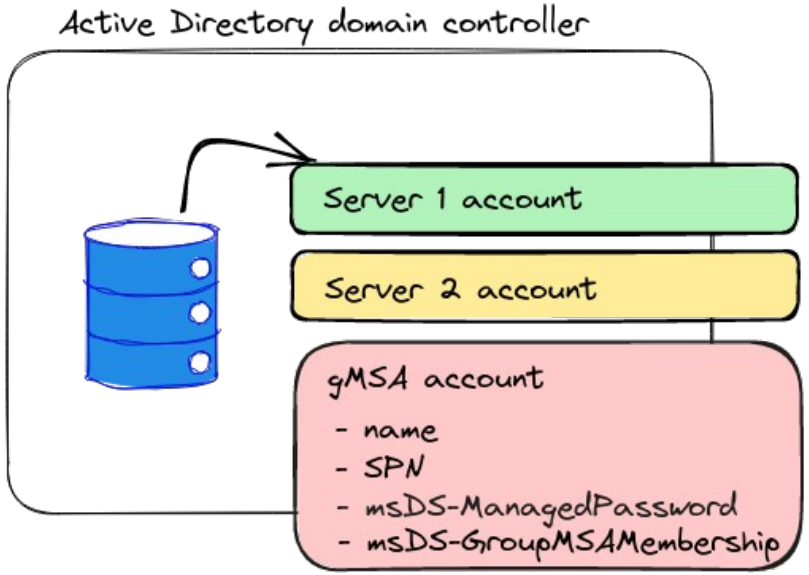

Server 1
Keytab
Server 1
Service
gmsad

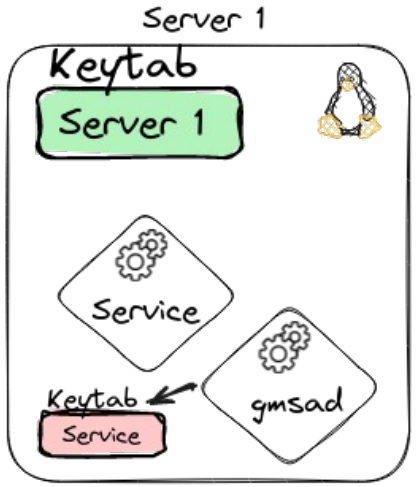

Server 2
Keytab
Server 2
Service
gmsad

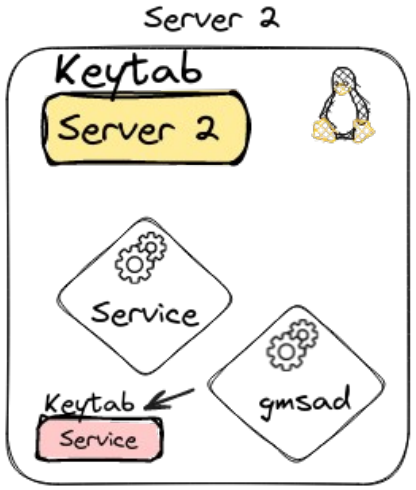
gmsad


Server 1
Keytab
Server 1
Service
gmsad
Active Directory domain controller
Server 1 account
Server 2 account
gMSA account
- name
- SPN
- msDS-ManagedPassword
- msDS-GroupMSAMembership
Server 2
Keytab
Server 2
Service
gmsad

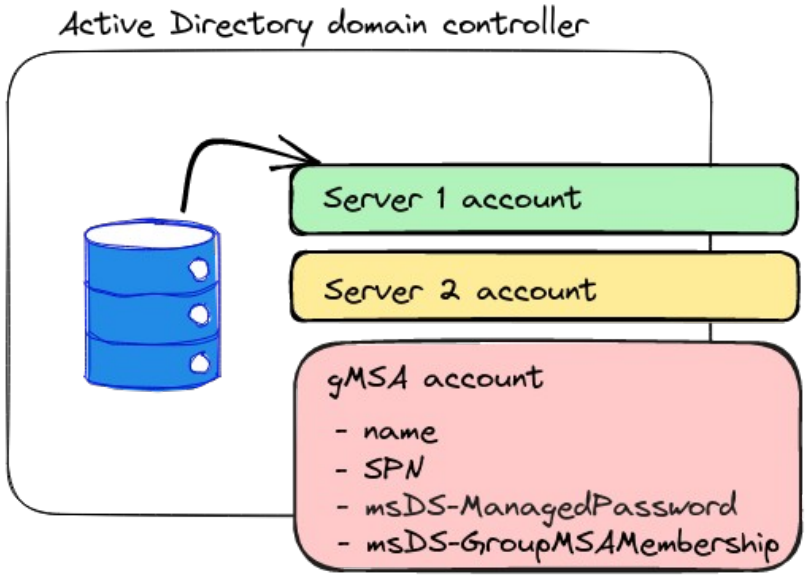
gmsad

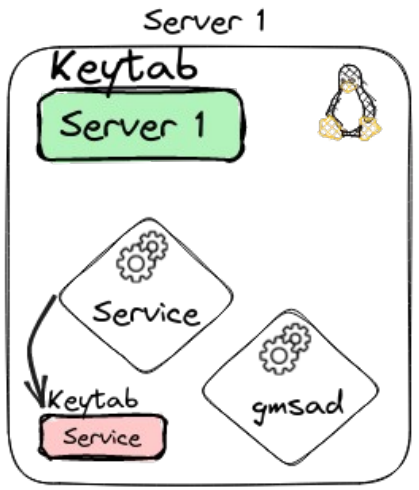

Active Directory domain controller
Server 1 account
Server 2 account
gMSA account
- name
- SPN
- msDS-ManagedPassword
- msDS-GroupMSAMembership

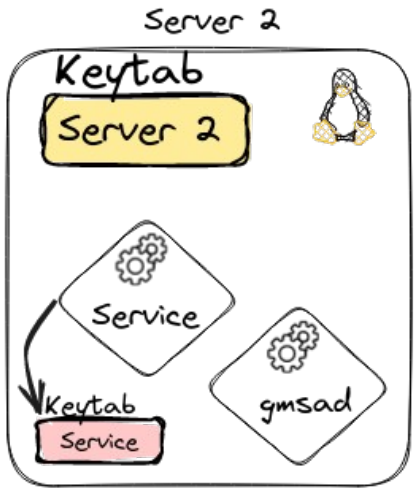

Server 1
Keytab
Server 1
Service
gmsad
Keytab
Service


Server 2
Keytab
Server 2
Service
gmsad
Keytab
Service

gmsad


Active Directory domain controller
Server 1 account
Server 2 account
gMSA account
- name
- SPN
- msDS-ManagedPassword
- msDS-GroupMSAMembership


Server 1
Keytab
Server 1
Service
Keytab
Service
gmsad

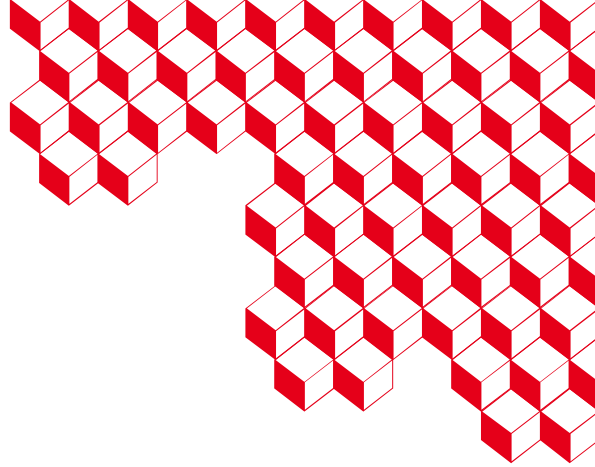

Server 2
Keytab
Server 2
Service
Keytab
Service
gmsad

Use cases

- In production:
  - Host a kerberised service on multiple Linux servers
  - Use an AD account for automated tasks from multiple machines
- In audit:
  - Retrieve the keytab of a gMSA
  - Easily generate and hack keytabs

TODO

- Packaging the tool in main Linux distributions



The end (for real)

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

CEA DAM

Centre de Bruyères-le-Châtel

91297 Arpajon Cedex

Établissement public à caractère industriel et commercial

William BRUNEAU & Vincent RUELLO – SSTIC 2023