SCADA Praha 2026

Vaclav Samsa
CEO & CTO
TDP LLC

Jana Dvorakova
Sales
TDP LLC

Authenticaton

Focus on users, not technologies

EU – whatever includes „a card“ is considered as a 2FA ☺

Machine to machine (M2M) authentications are ignored

M2M auths are outnumbering human beings auths

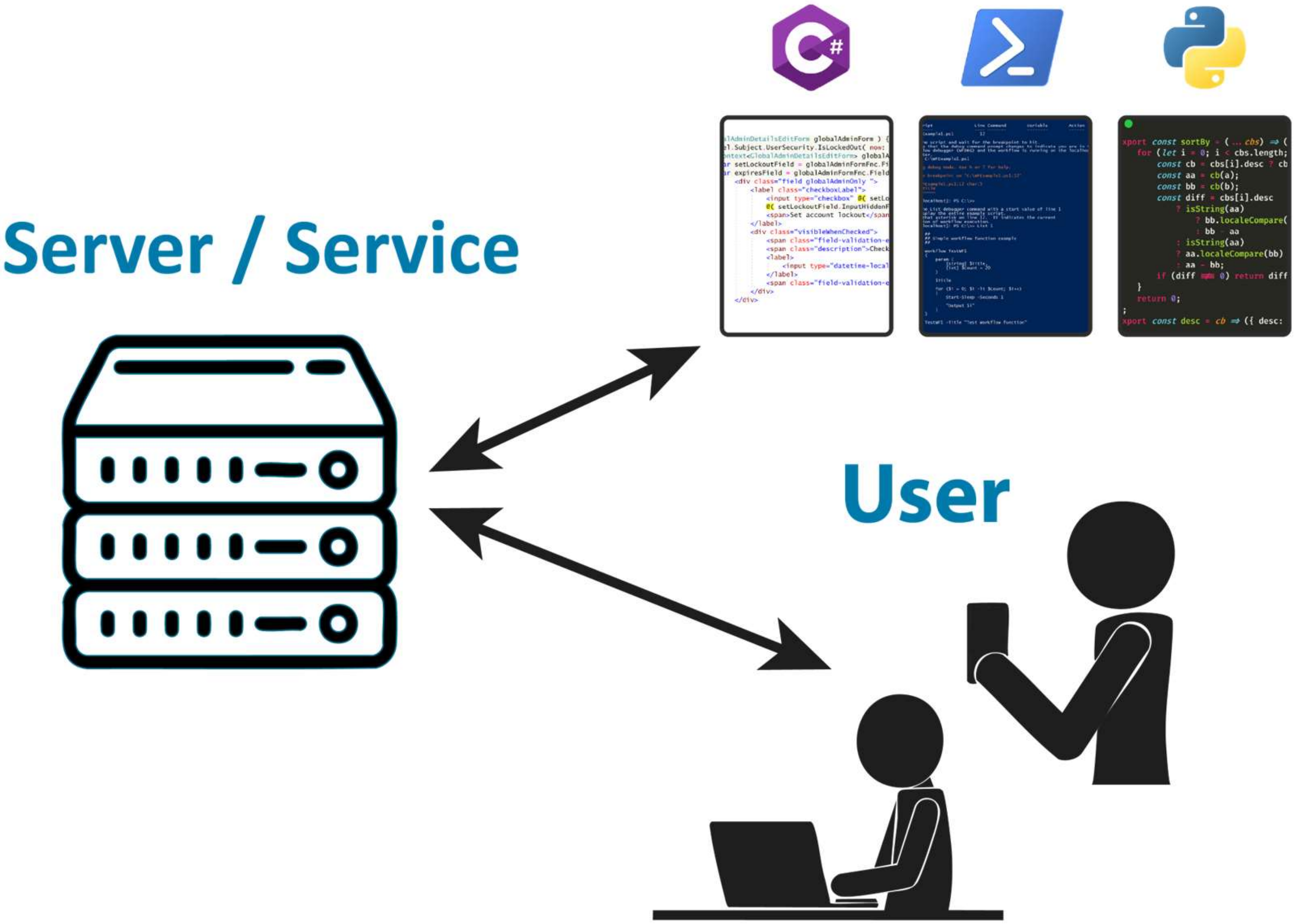
A typical IT clerk can lost their job because some mission critical automated process failed to start. Poor security is unseen and not considered a problem – at least till something happens.

Machines (programs) have no card, no mobile phone, no finger tip, no eye scan, no face.

Language problem -> mindset problem

Security	X	Safety
Hacker		Easy recovery after any failure
Evil admin		Access without user source Entra ID
NO master password		Enterprise class BIN management

Authentication reality all around the world



Server / Service

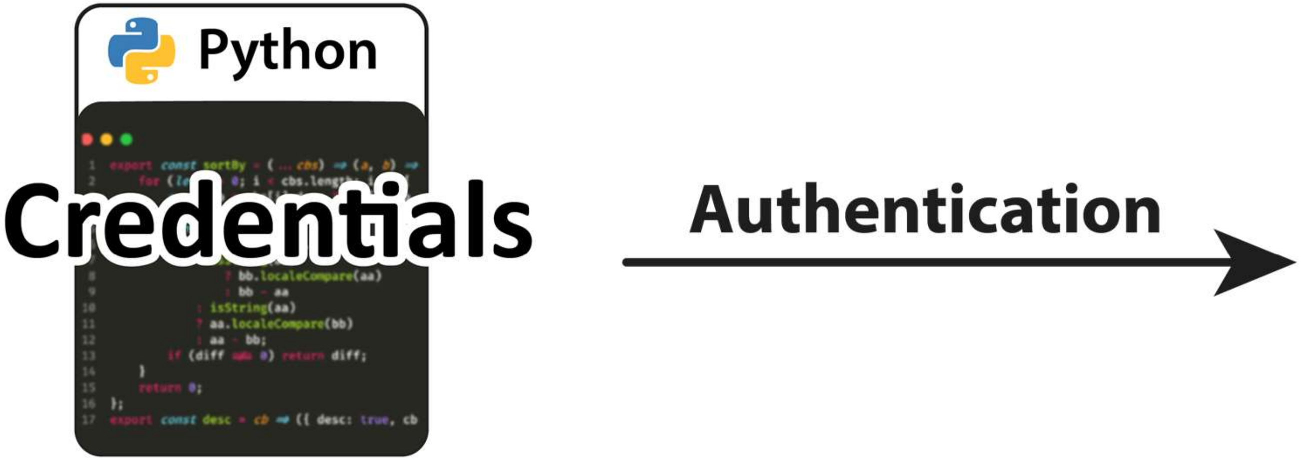
User

```
lAdminDetailsEditForm globalAdminForm ) {
el.Subject.UserSecurity.IsLockedOut( now:
ntext<GlobalAdminDetailsEditForm> globalA
ar setLockoutField = globalAdminFormFnc.Fi
ar expiresField = globalAdminFormFnc.Field
   <div class="field globalAdminOnly ">
       <label class="checkboxLabel">
           <input type="checkbox" @( setLo
           @( setLockoutField.InputHiddenF
           <span>Set account lockout</span
       </label>
       <div class="visibleWhenChecked">
           <span class="field-validation-e
           <span class="description">Check
           <label>
               <input type="datetime-local
           </label>
           <span class="field-validation-e
       </div>
   </div>
```

```
ript                   Line Command        Variable       Action
----                   ---- -------        --------       ------
Example1.ps1             12

he script and wait for the breakpoint to hit.
e that the debug command prompt changes to indicate you are in
low debugger (WFDBG) and the workflow is running on the localhost
ter.
 C:\WFExample1.ps1

g debug mode; Use h or ? for help.

t breakpoint on 'C:\WFExample1.ps1:12'

WFExample1.ps1:12 char:3
$Title
------

localhost]: PS C:\>>

he List debugger command with a start value of line 1
splay the entire example script.
that asterisk on line 12.  It indicates the current
ion of workflow execution.
localhost]: PS C:\>> List 1

 ##
 ## Simple workflow function example
 ##

 workflow TestWF1
 {
     param (
         [string] $Title,
         [int] $Count = 20
     )

     $Title

     for ($i = 0; $i -lt $Count; $i++)
     {
         Start-Sleep -Seconds 1

         "Output $i"
     }
 }

 TestWF1 -Title "Test workflow function"
```

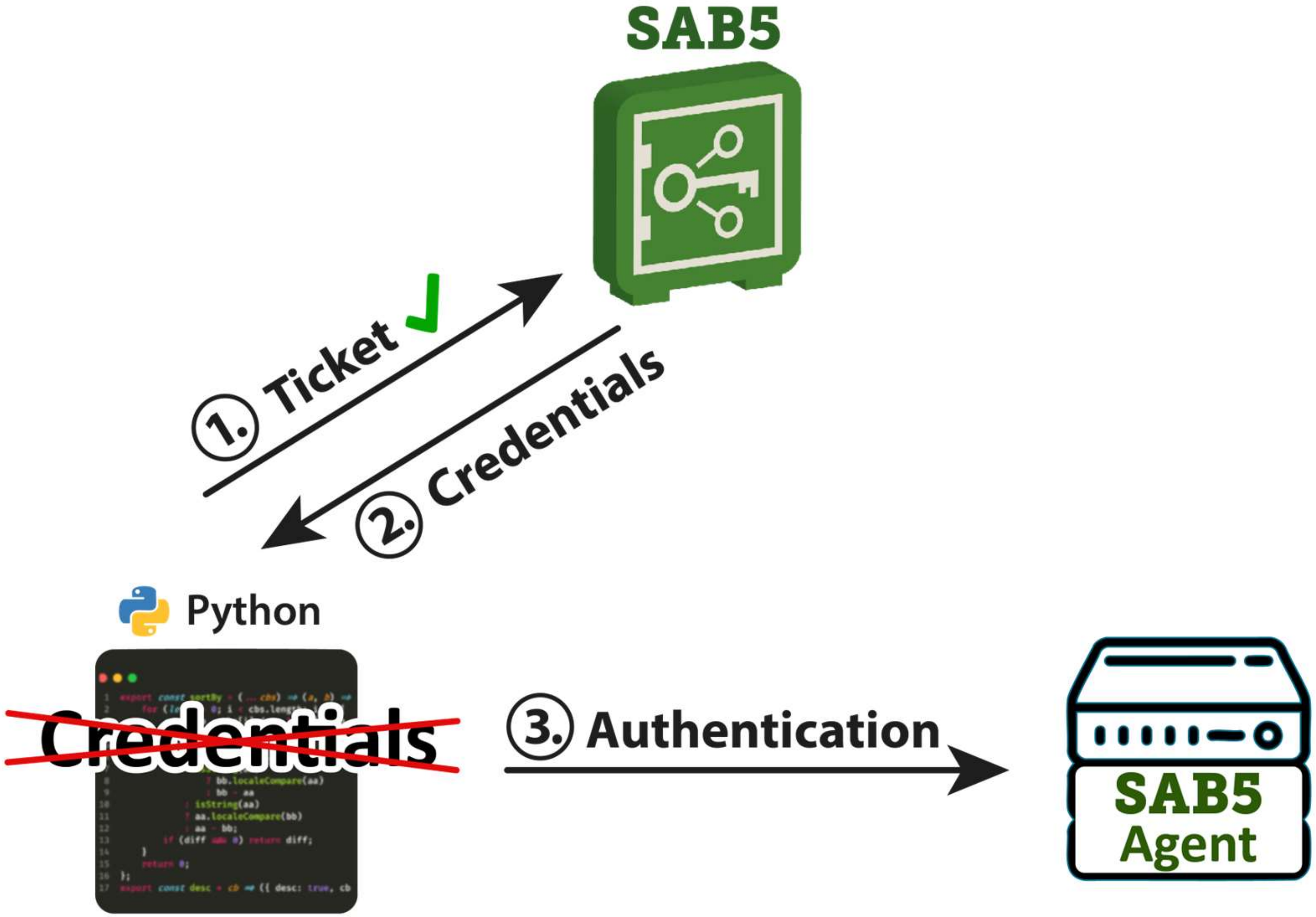
```
xport const sortBy = (...cbs) => (
  for (let i = 0; i < cbs.length;
      const cb = cbs[i].desc ? cb
      const aa = cb(a);
      const bb = cb(b);
      const diff = cbs[i].desc
          ? isString(aa)
              ? bb.localeCompare(
              : bb - aa
          : isString(aa)
          ? aa.localeCompare(bb)
          : aa - bb;
      if (diff !== 0) return diff
  }
  return 0;
;
xport const desc = cb => ({ desc:
```

Typical unsecure machine authentication



```
export const sortBy = (...cbs) => (a, b) =>
    for (le[illegible] 0; i < cbs.length; i[illegible]
[illegible]
                        ? bb.localeCompare(aa)
                        : bb - aa
                    : isString(aa)
                    ? aa.localeCompare(bb)
                    : aa - bb;
            if (diff !== 0) return diff;
        }
    return 0;
};
export const desc = cb => ({ desc: true, cb
```

Machine auth with SAB5 privileged accounts management – easy to implement, very safe



```
export const sortBy = (...cbs) => (a, b) =>
    for (let i = 0; i < cbs.length; i++) {
                ? bb.localeCompare(aa)
                : bb - aa
            : isString(aa)
            ? aa.localeCompare(bb)
            : aa - bb;
        if (diff !== 0) return diff;
    }
    return 0;
};
export const desc = cb => ({ desc: true, cb
```

Multi Factor Auth Chain

Factor	Action	Note
1	Ticket	Aka passkey
2	Location	IP addr/network
3	Time of the day	Auto run by cron

AGENTS

Windows

Linux

Raspberry

Active Directory

eDirectory

Generic LDAP

OS authenticated services, tasks

When OS starts a service or a task, it makes it running under an existing account

Account is used to define access to resources. Local or network

Such accounts are quite often used in a general way

Such accounts are privileged

The challenges:

- Protection against unauthorised use of remembered credentials
- Password rotation – synchronised update of OS configuration and security environment (eg MS AD)

Can authenticaton protect your data?

Meta data driven systems (ACL) do not provide any protection for your data. They increase an identity trust level

The only functional data protection is encryption

Cloud or hosting owner/provider, your administrator, persons with physicall access to the storage – they all can access the data unless you use an encryption

With encryption, who has the key has access to the data

Key logistics is then the crucial part of your security. The best for encryption key management is – encryption

1F

Credentials
(Local or UserSource account)

or

KeyShield SSO
(Included for Enterprise)

2F

TOTP
(Optional)

Access

to unencrypted data

Access

~ to unencrypted data

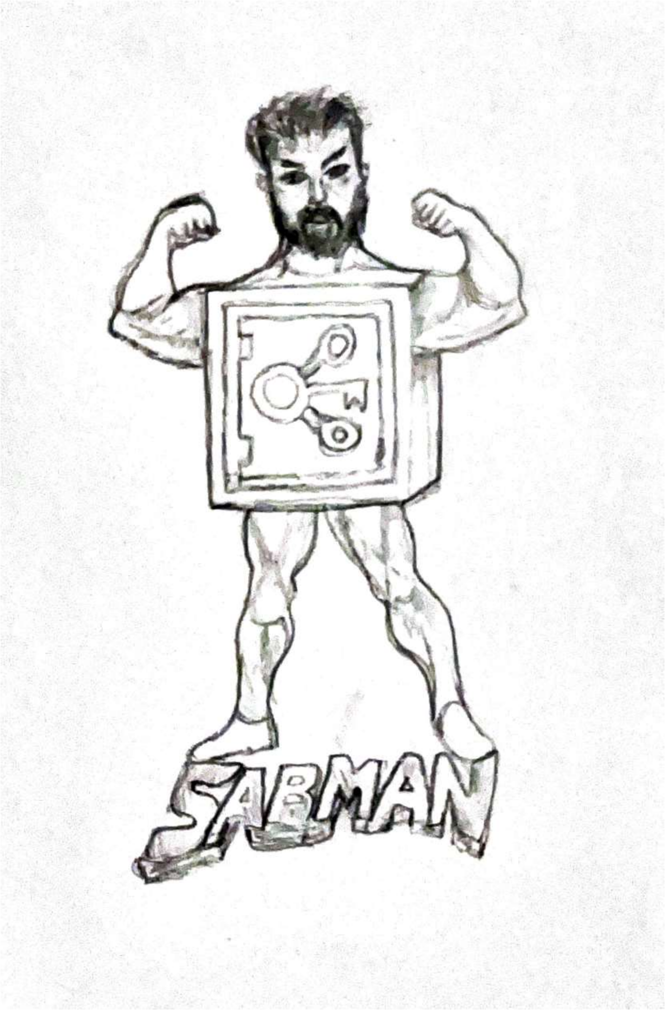
3F

Access code

(Mandatory)

Access

to encrypted data



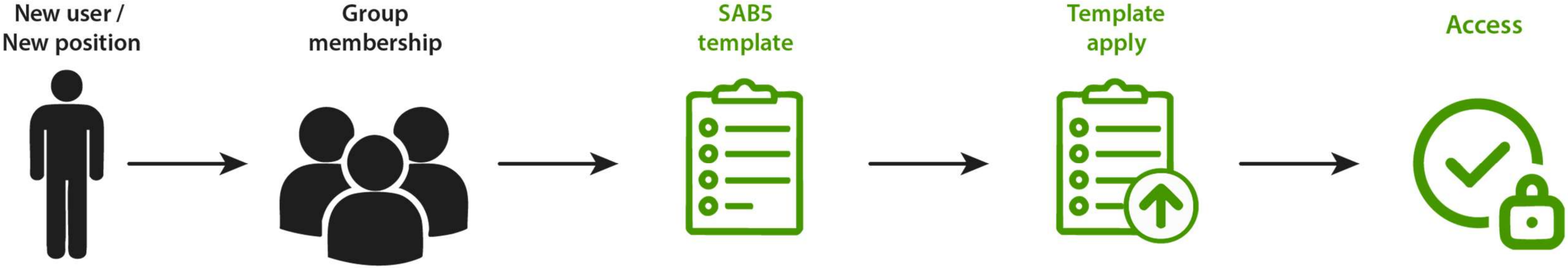
LastPass

1Password

Keeper

BitWarden

Passbolt



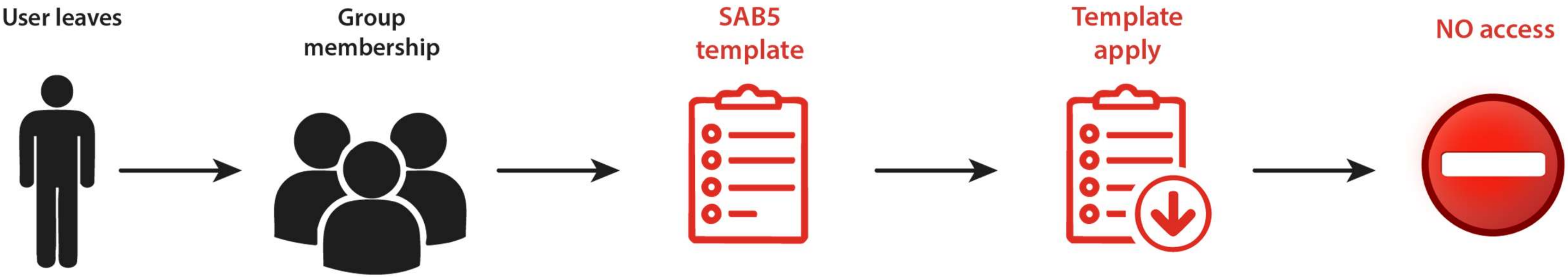
New user / New position

Group membership

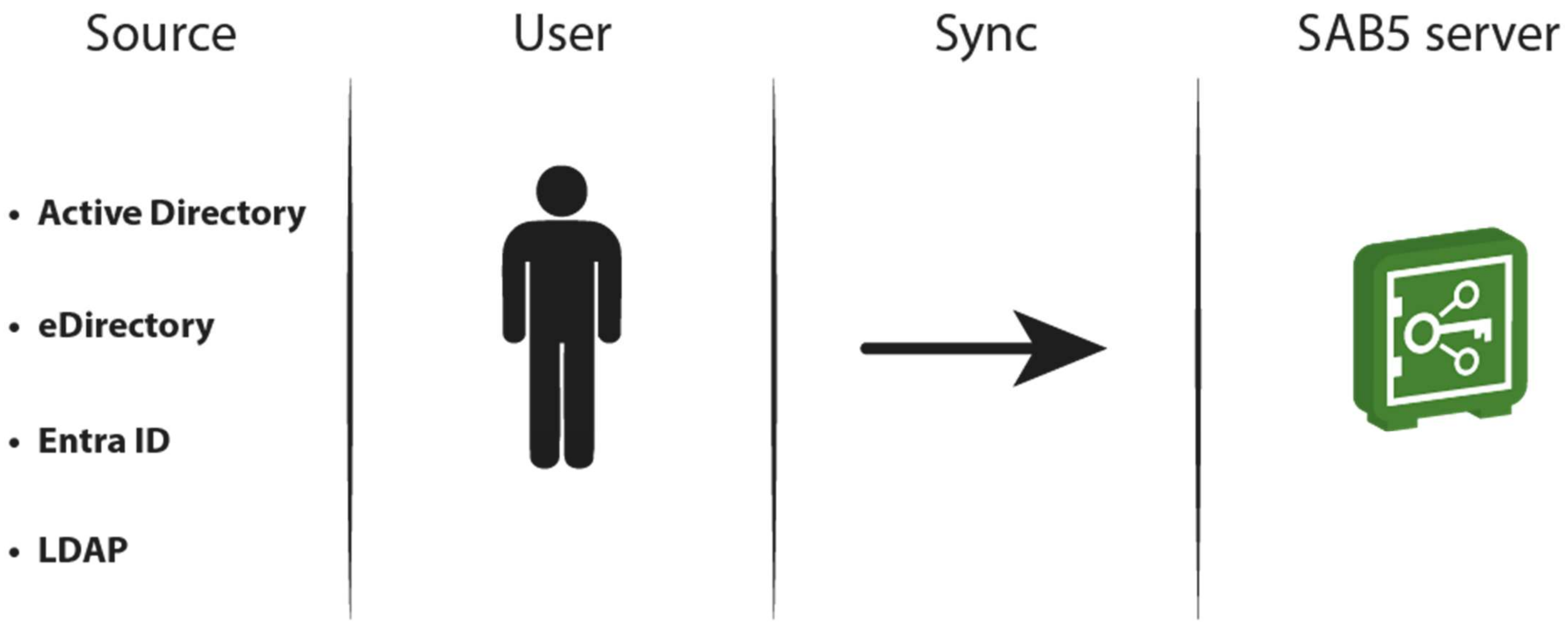
SAB5 template

Template apply

Access



User leaves → Group membership → SAB5 template → Template apply → NO access



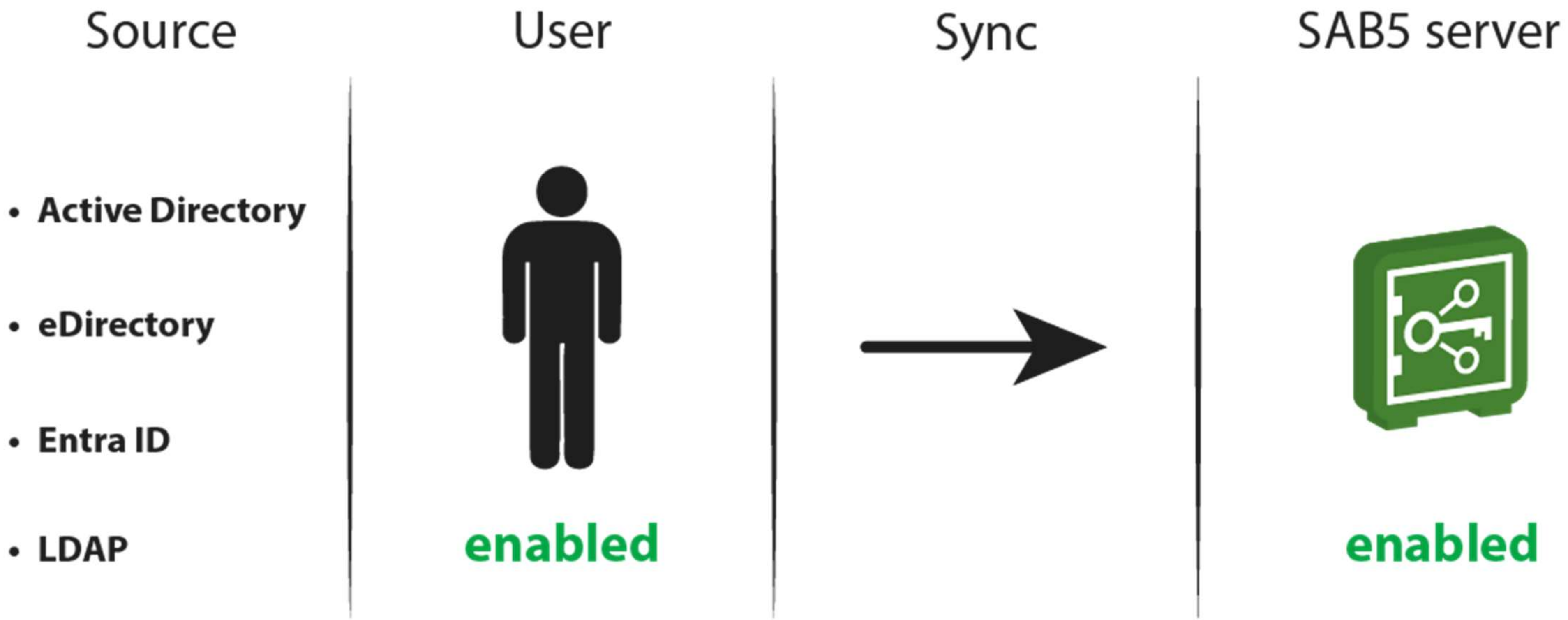
Source

- Active Directory
- eDirectory
- Entra ID
- LDAP

User

Sync

SAB5 server



Source

- Active Directory
- eDirectory
- Entra ID
- LDAP

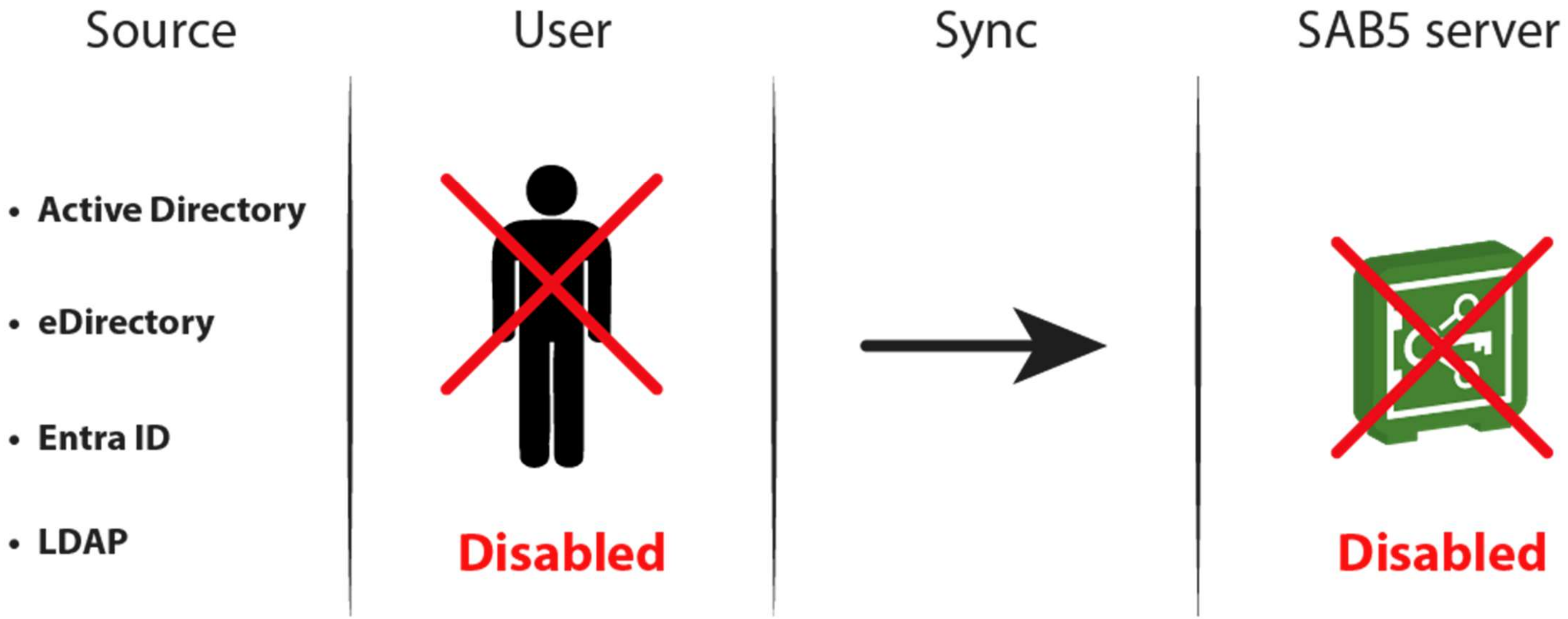
User

enabled

Sync

SAB5 server

enabled



Source

- Active Directory
- eDirectory
- Entra ID
- LDAP

User

Disabled

Sync

SAB5 server

Disabled

- Audit to DB
- SIEM integration (audit and diagnostic)
- Watching - aggregated email notification
- TOTP provider

- API

SAB5

- Entra ID
- Active Directory
- eDirectory
- Generic LDAP

- Sensitive Docs
- Configurations
- Outside sharing
- Valuables - lic etc
- Keys, certs

SAB5

...

Q&A

(Answers Free of Charge today)