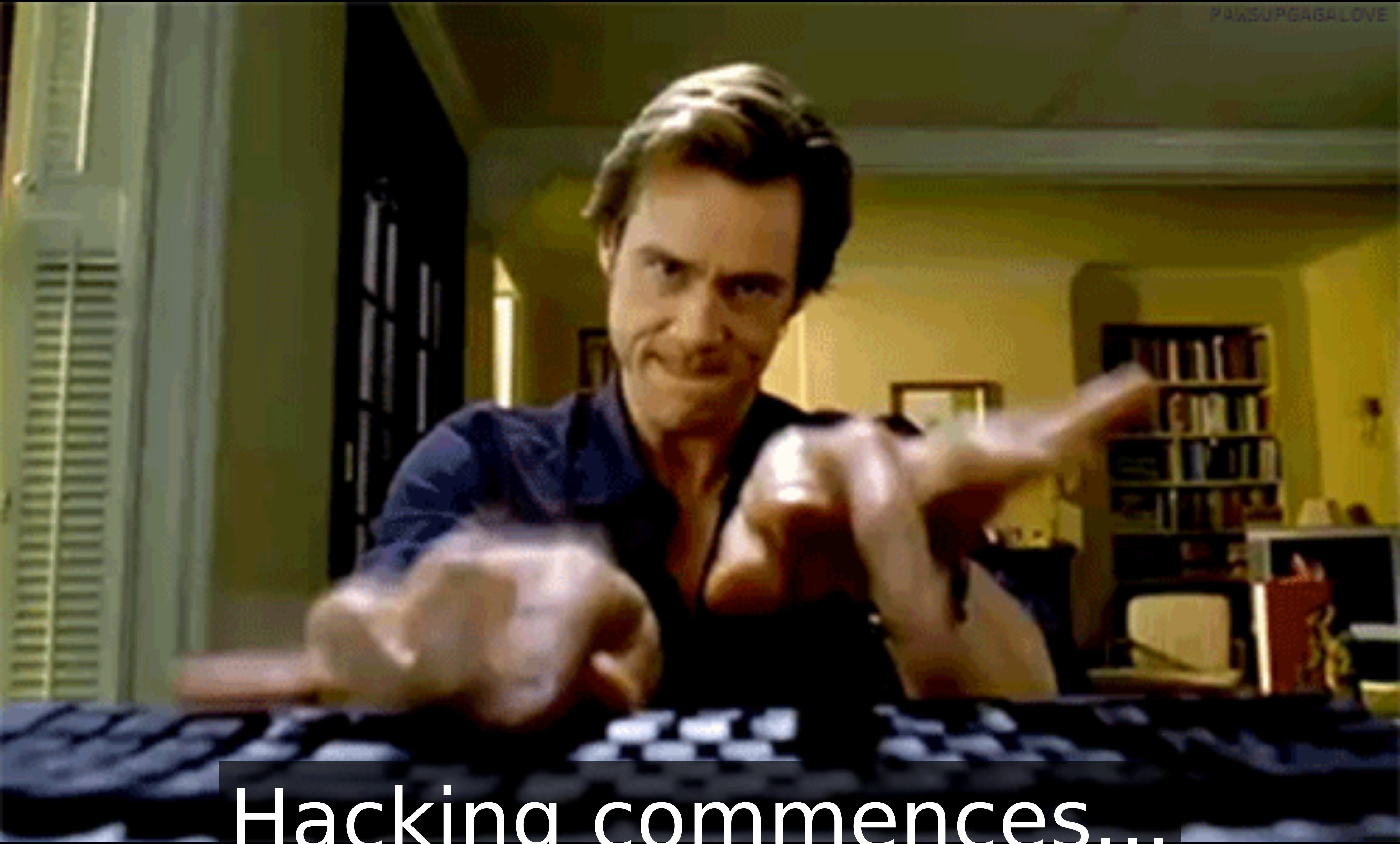
Leveraging Linux Platform for Identity Management

in Enterprise Web Applications

Nathan Kinder
nkinder@redhat.com
http://blog-nkinder.rhcloud.com

Development of a typical web application...

Great idea!



Hacking commences...

Add a login form and
a user database!

The application now needs to deal with account management

- User creation
- User deletion
- Password reset
- ...and on and on

Enterprises typically have an existing identity management solution

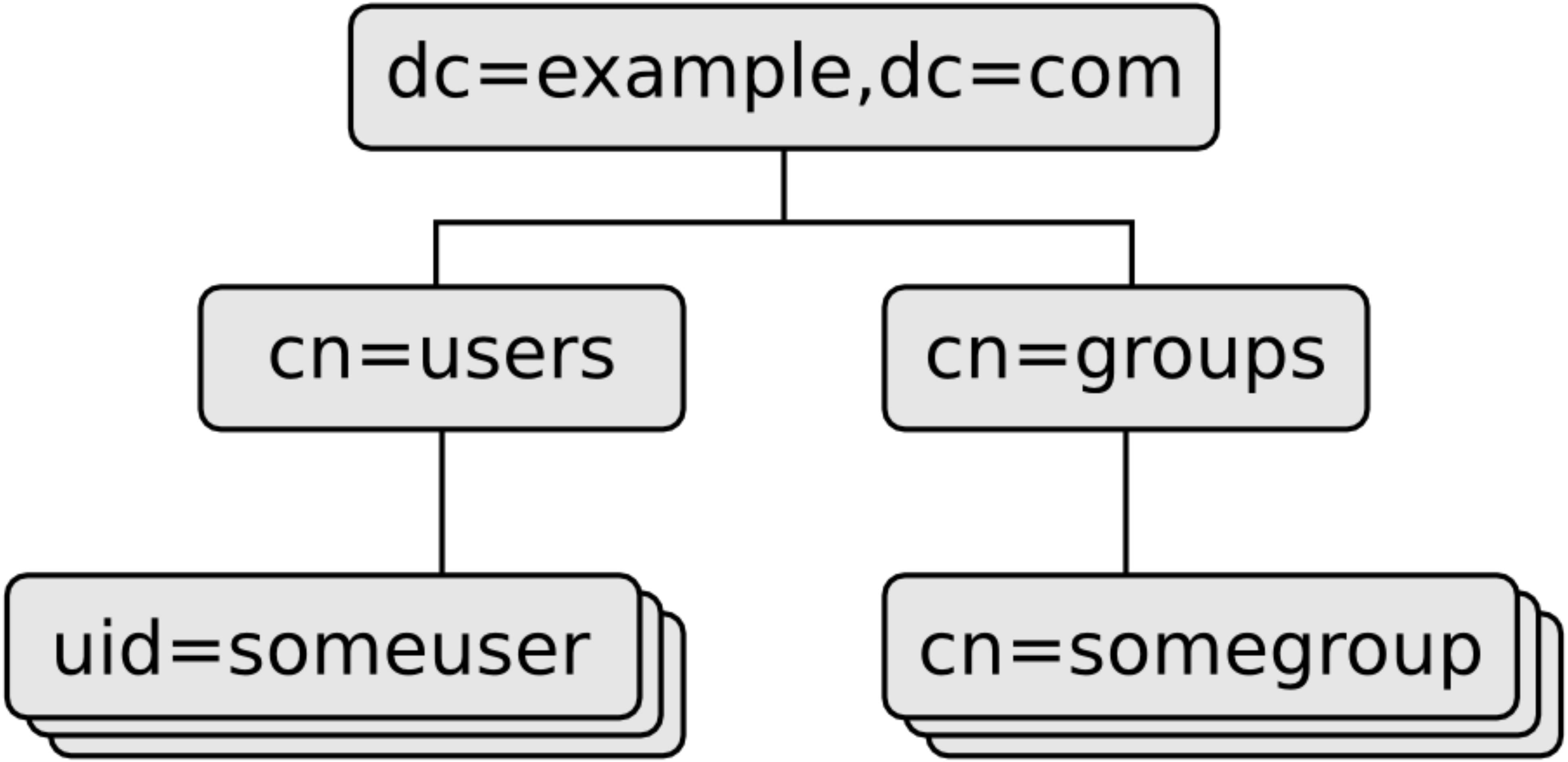
Using an existing identity source allows for improved security:

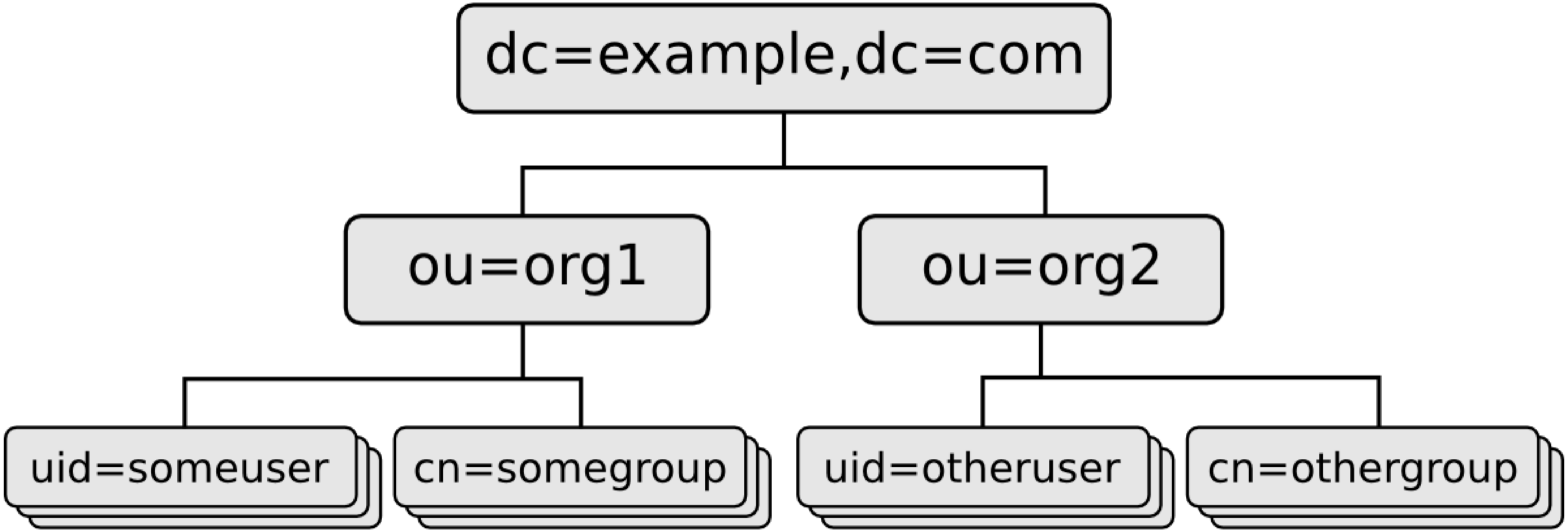
- Centralized authentication
- Account lockout
- Password policies

This leads to adding LDAP support to your web application

Unfortunately, LDAP deployments vary...

The DIT might be flat or nested…


dc=example,dc=com
cn=users
cn=groups
uid=someuser
cn=somegroup


dc=example,dc=com
ou=org1
ou=org2
uid=someuser
cn=somegroup
uid=otheruser
cn=othergroup

Schema differences can lead to very different user entries...

```
dn: uid=someuser,cn=users,dc=example,dc=com
objectclass: inetorgperson
uid: someuser
cn: Some User
mail: someuser@example.com
memberOf: cn=admins,cn=groups,dc=example,dc=com
...
```

```
dn: cn=Some User,cn=users,dc=example,dc=com
objectclass: user
sAMAccountName: someuser
cn: Some User
mail: someuser@example.com
memberOf: cn=admins,cn=users,dc=example,dc=com
...
```

A web application will need to have configuration settings to deal with these differences

You also need to consider how your LDAP code will will perform at scale

- Connection pooling
- Failover
- Caching

This starts to add a lot of complexity into the application

Why not take advantage of the capabilities of the underlying platform?

sssd

fedorahosted.org/sssd

System Security Services Daemon

SSSD provides access to remote authentication and identity resources

FreeIPA, Active Directory, LDAP, Kerberos

Advanced capabilities:

- Caching
- Fail-over
- Multiple identity sources (domains)
- Kerberos ticket aquisition/renewal
- HBAC with FreeIPA

Integrates via PAM, NSS, and DBUS

Available in many distros

- Fedora
- RHEL
- CentOS
- Debian
- Ubuntu
- OpenSUSE
- Gentoo
- Mandriva
- Arch
- ...

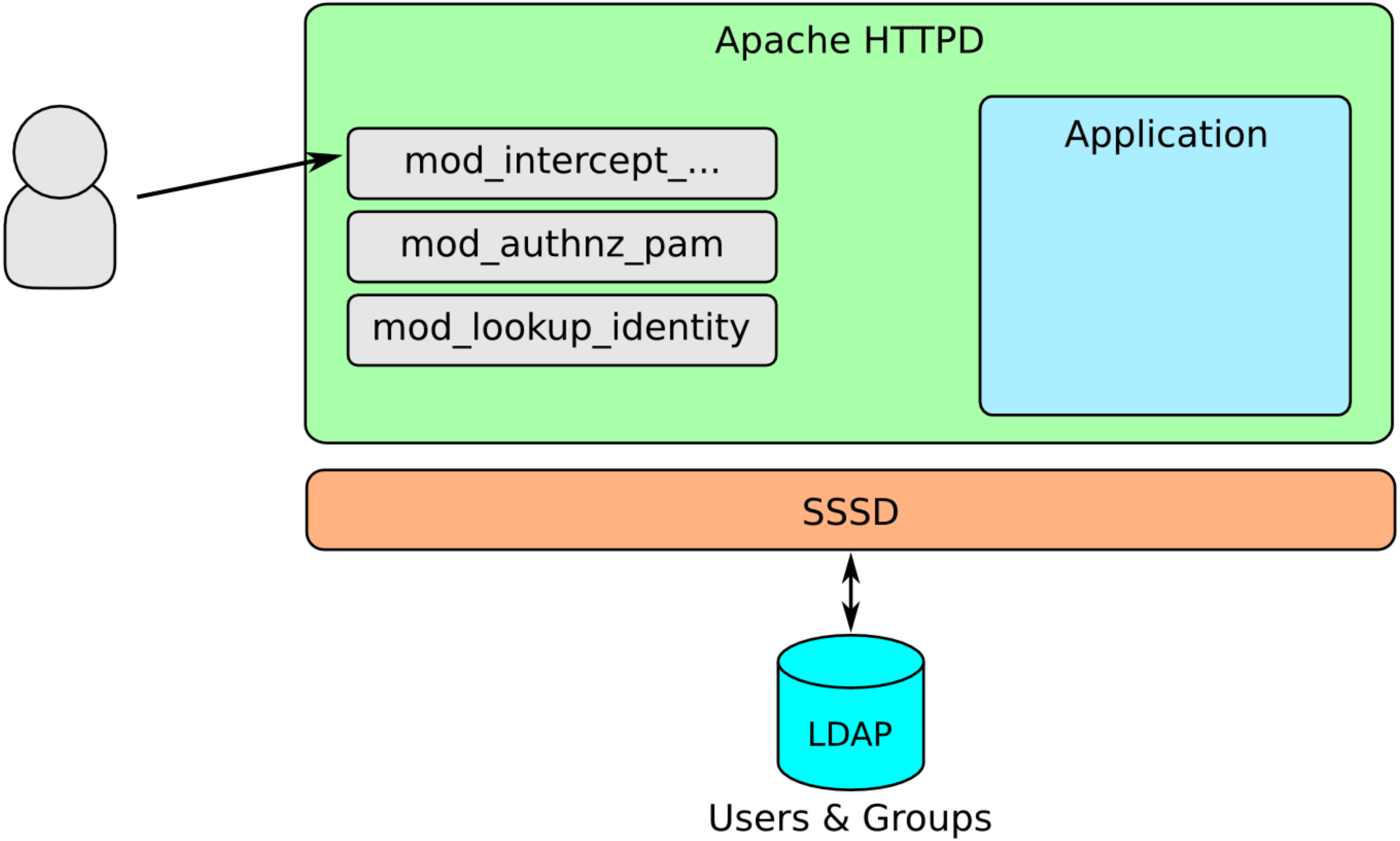
Meet the HTTPD modules...

mod_intercept_form_submit

- Intercepts login and password from login form POST request
- Uses PAM to perform authentication
- Sets REMOTE_USER environment variable

mod_authnz_pam

- Allows PAM to be used for authorization
- Handles PAM authentication for mod_intercept_form_submit
- Particularly useful with FreeIPA HBAC to allow authorization to be handled centrally


Apache HTTPD

mod_intercept_...

mod_authnz_pam

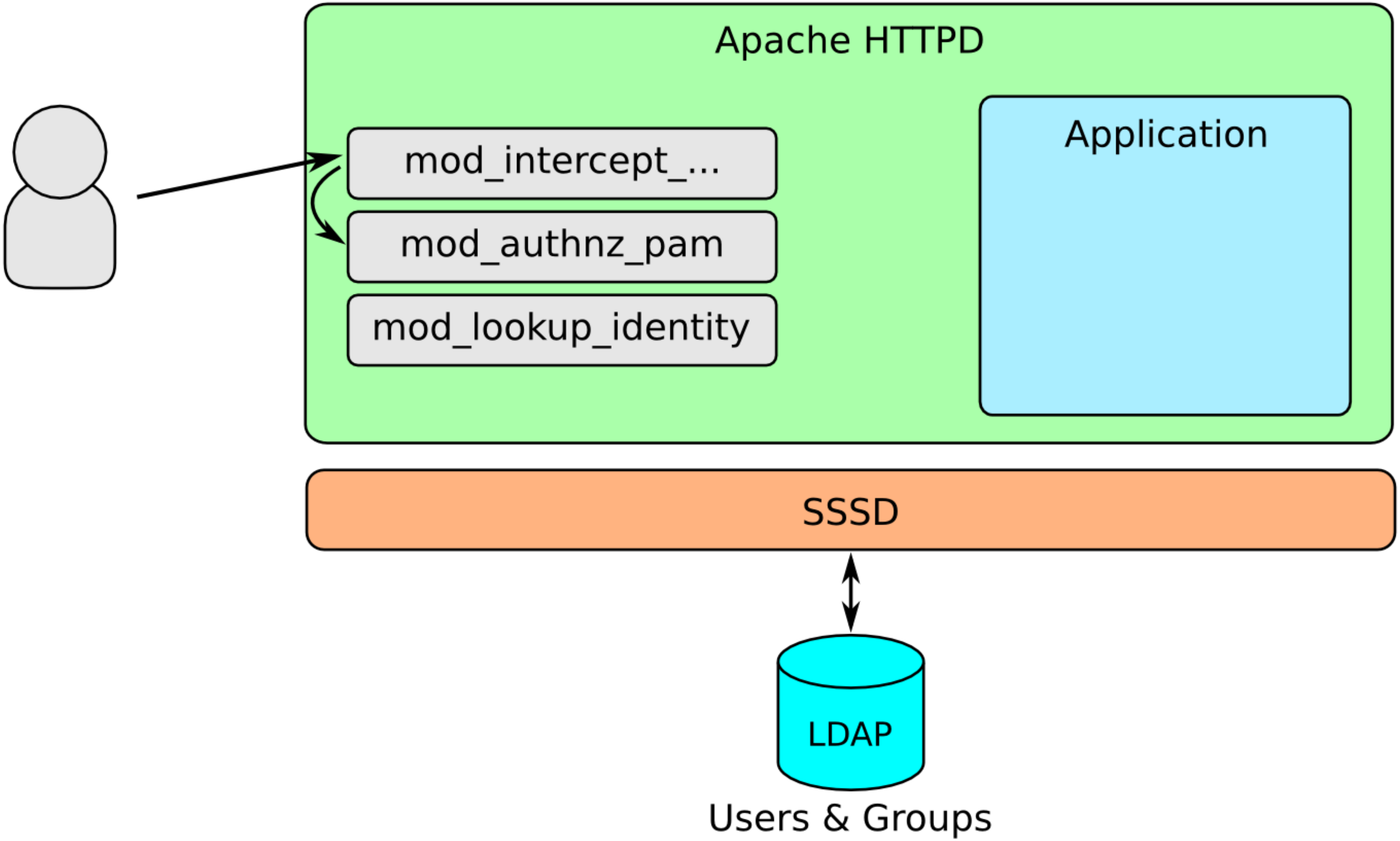
mod_lookup_identity

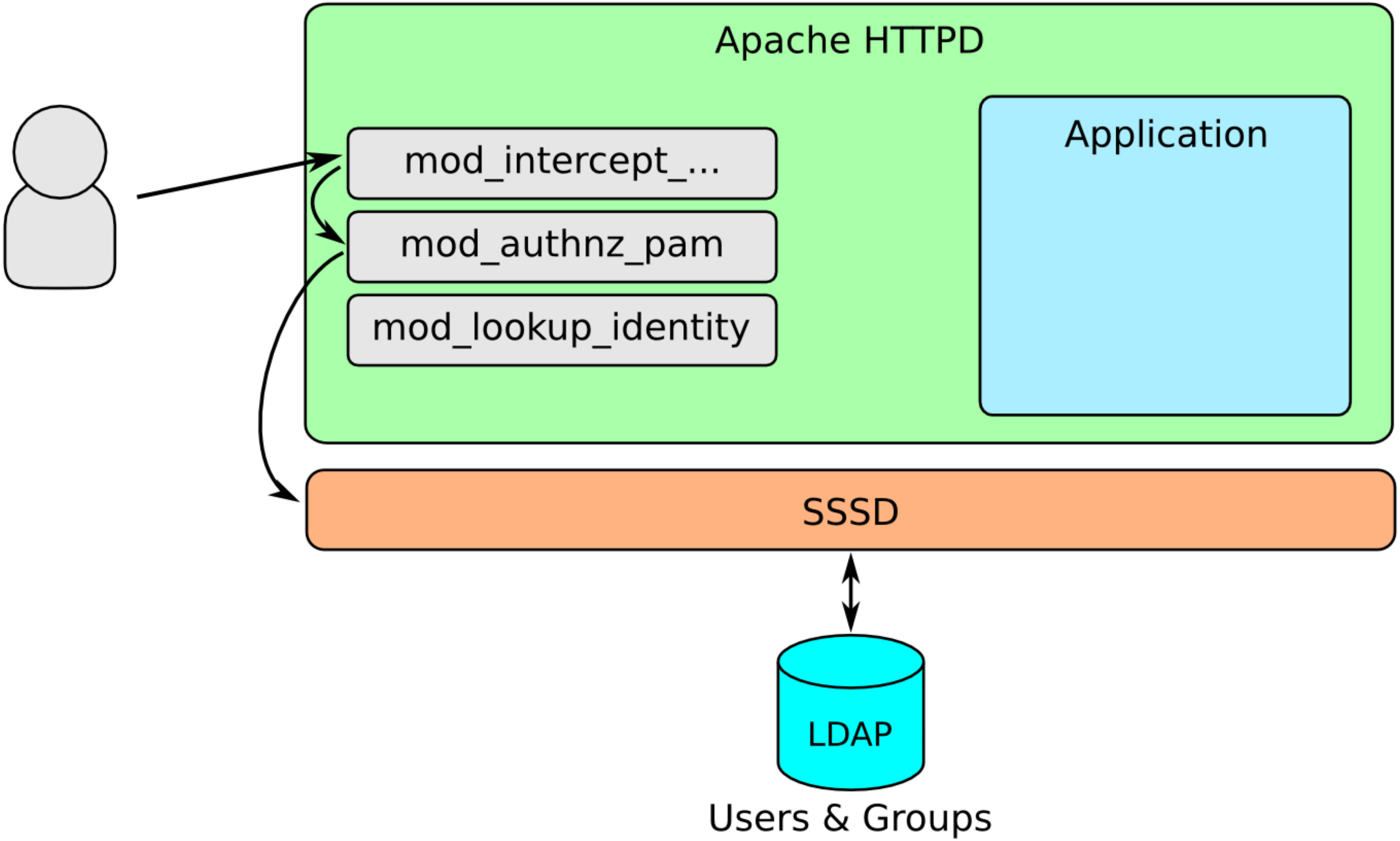
Application

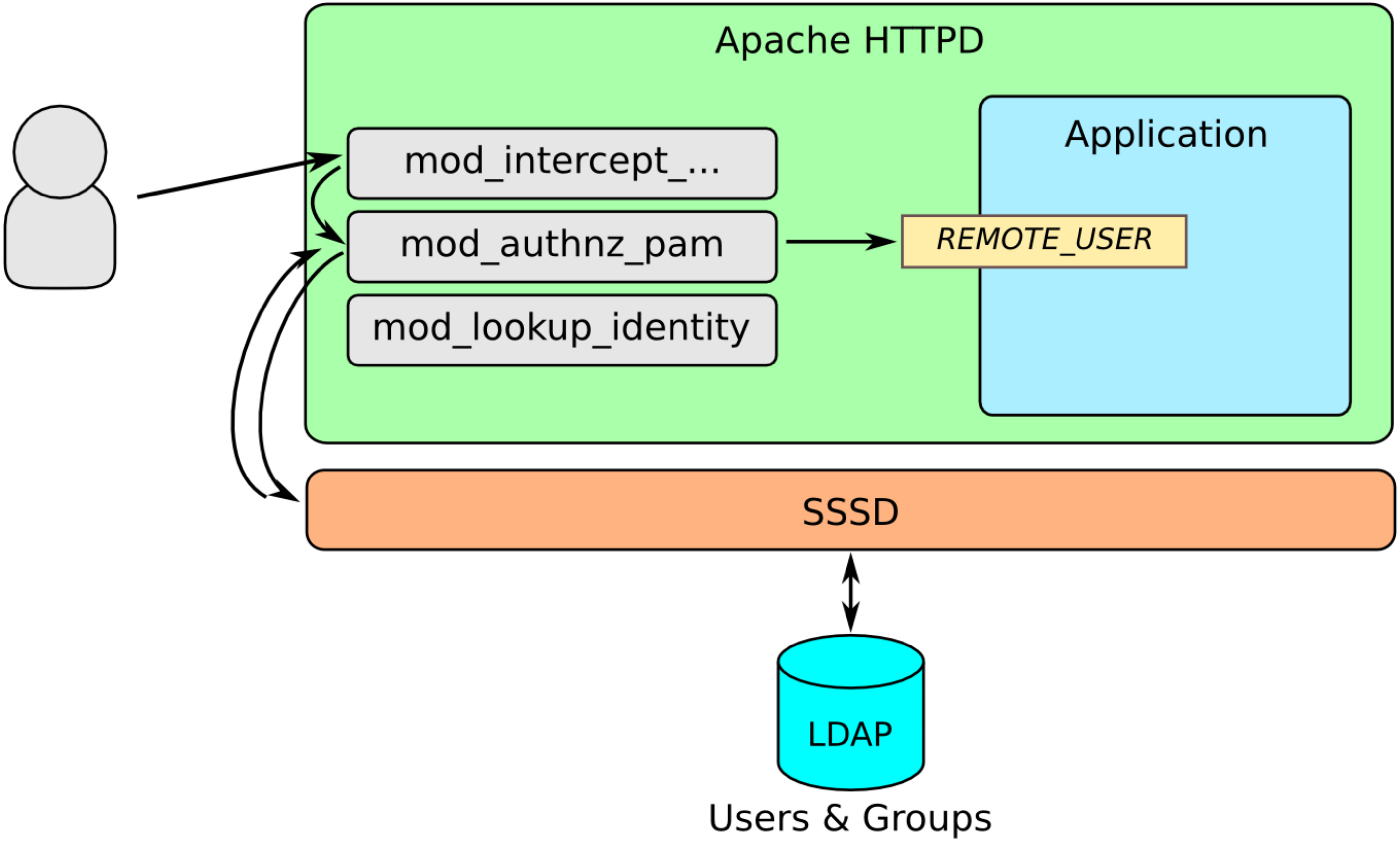
SSSD

LDAP

Users & Groups


Apache HTTPD
mod_intercept_...
mod_authnz_pam
mod_lookup_identity
Application
SSSD
LDAP
Users & Groups


Apache HTTPD
mod_intercept_...
mod_authnz_pam
mod_lookup_identity
Application
SSSD
LDAP
Users & Groups

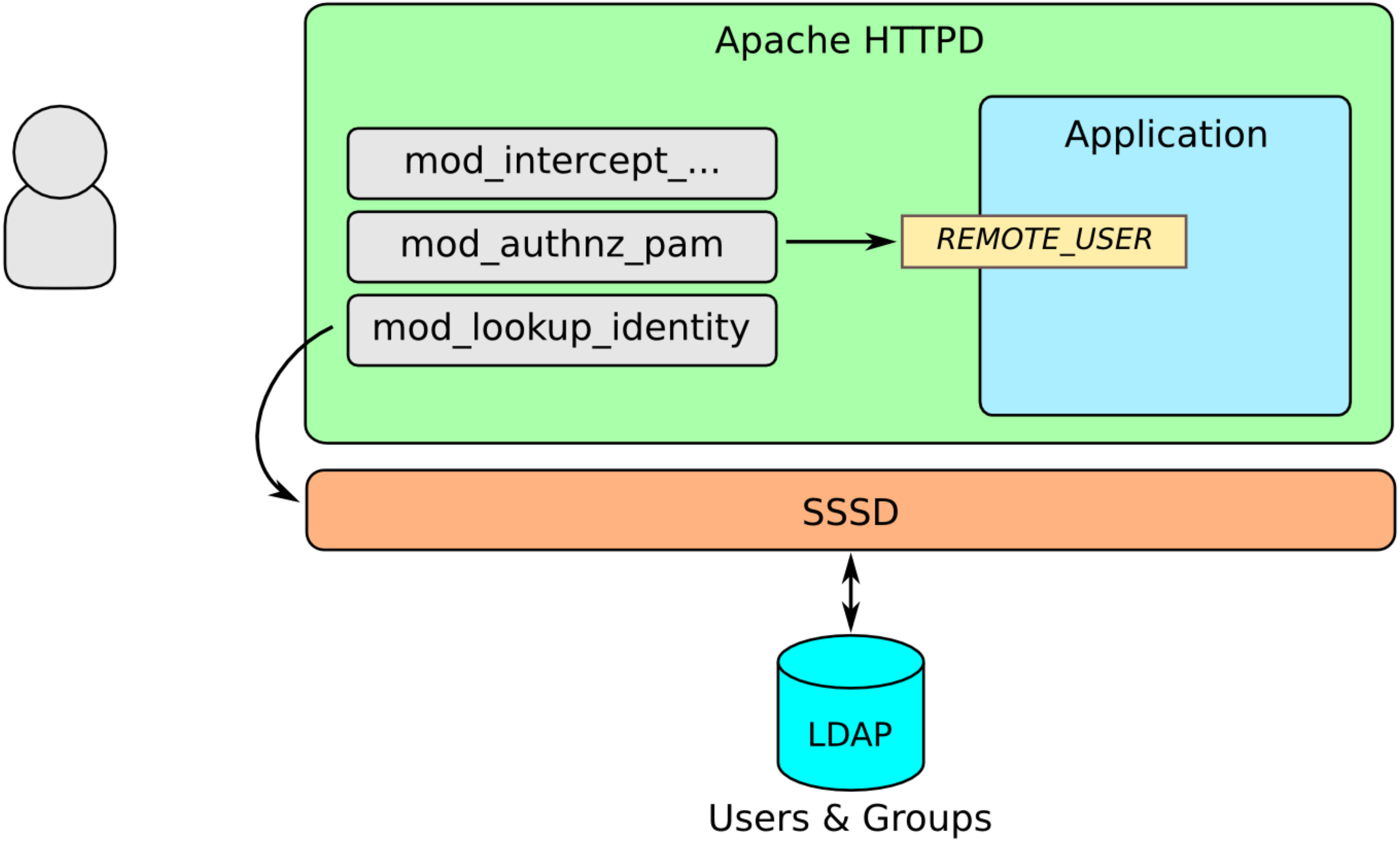

Apache HTTPD
Application
mod_intercept_...
mod_authnz_pam
mod_lookup_identity
REMOTE_USER
SSSD
LDAP
Users & Groups

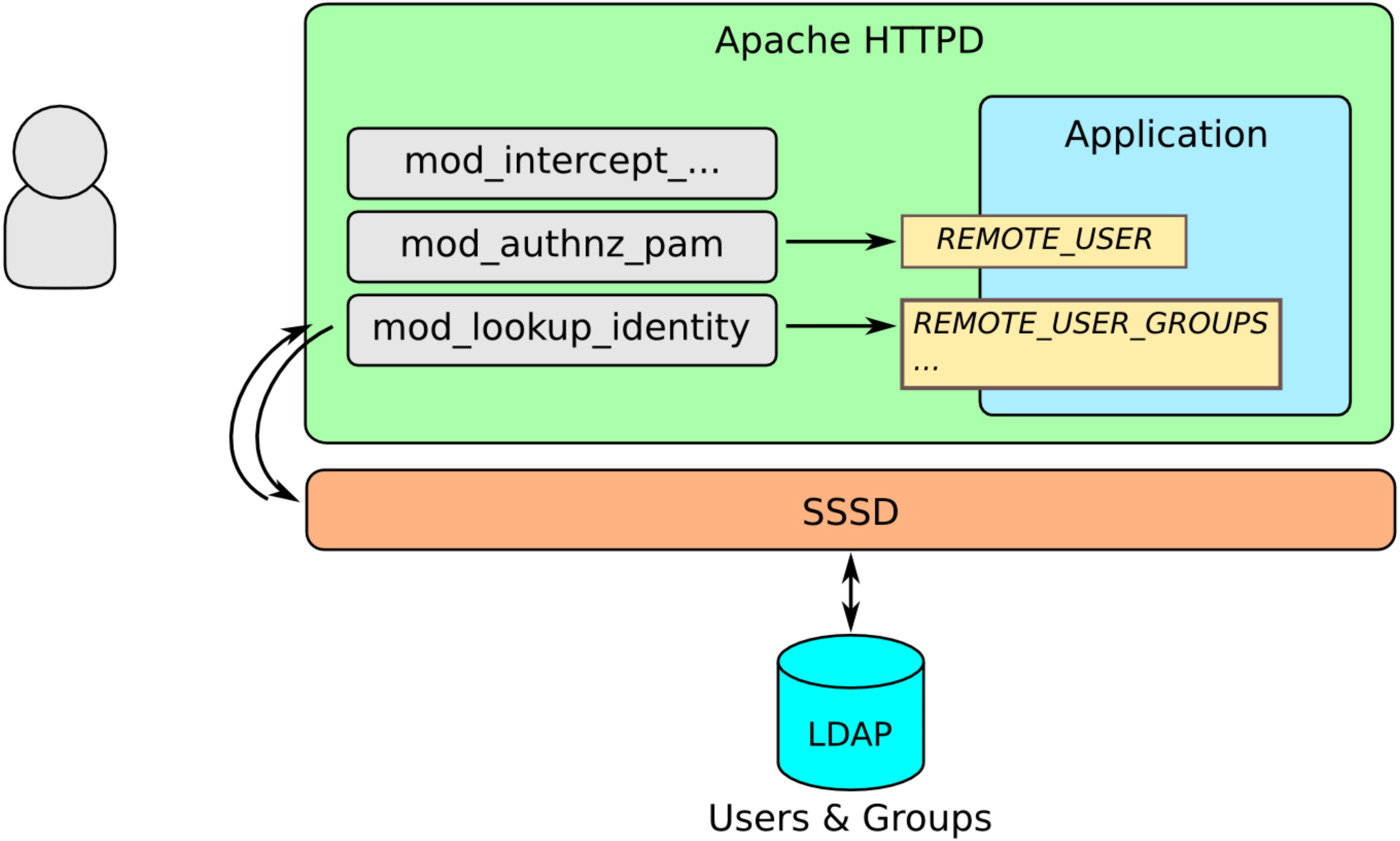
mod_intercept_form_submit config

mod_authnz_pam config

mod_lookup_identity

- Allows additional user information to be provided to the application
- Useful for things like e-mail addresses or group membership for role-based authorization
- Information is retrieved from SSSD via DBUS


Apache HTTPD
mod_intercept_...
mod_authnz_pam
mod_lookup_identity
Application
REMOTE_USER
SSSD
LDAP
Users & Groups



Apache HTTPD

mod_intercept_...

mod_authnz_pam

mod_lookup_identity

Application

REMOTE_USER

REMOTE_USER_GROUPS
...

SSSD

LDAP

Users & Groups

SSSD Infopipe Config

```
[domain/example.test]
ldap_user_extra_attrs = mail, givenname, sn
...

[sssd]
services = nss, pam, ssh, ifp
...

[ifp]
allowed_uids = apache, root
user_attributes = +mail, +givenname, +sn
```

mod_lookup_identity config

Application Changes

REMOTE_USER needs to be accepted
for authentication, then fallback
to normal form processing

This may already exist to support HTTP
Basic or Digest authentication

Mapping of additional user info variables needs to be handled

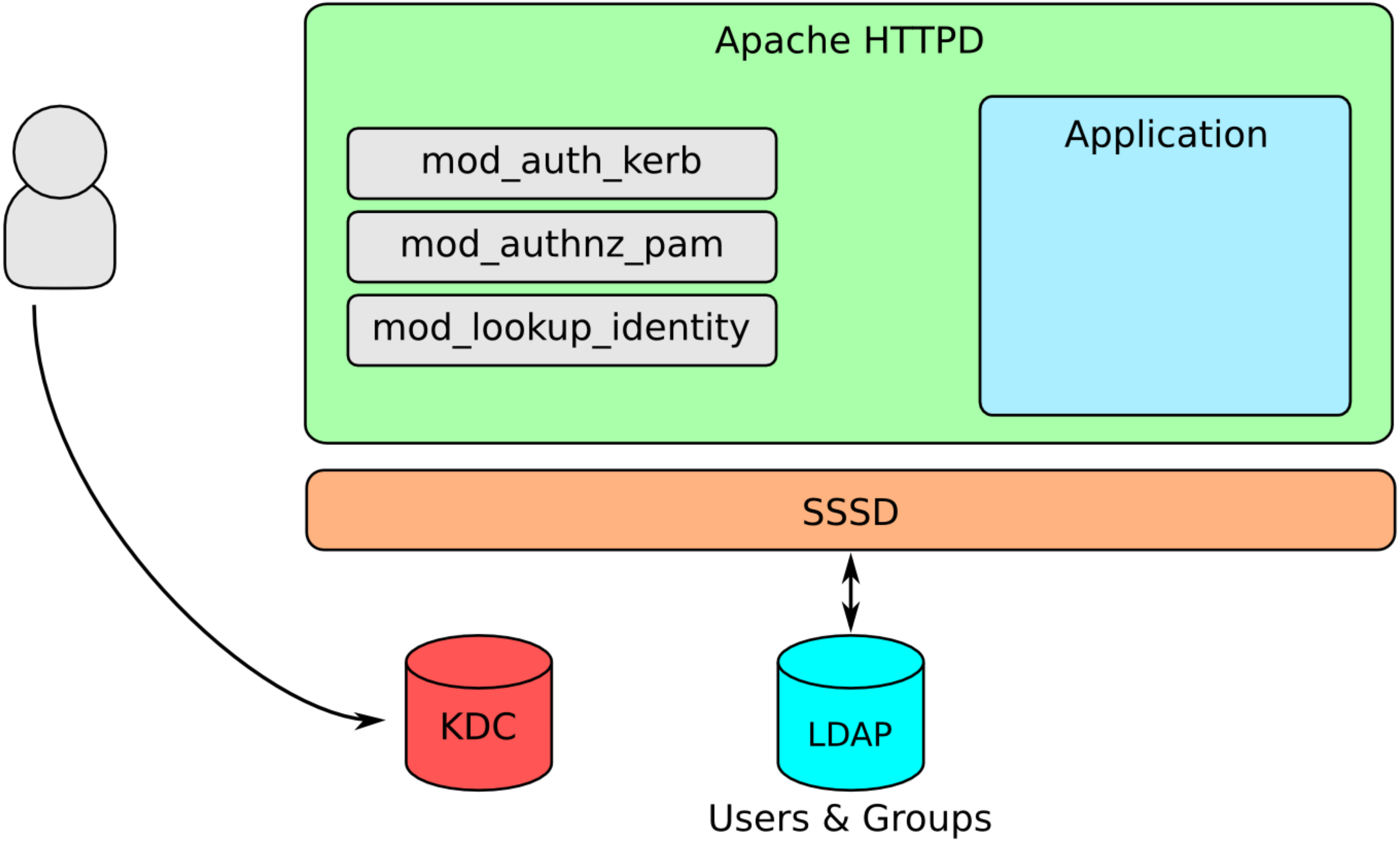
If the application needs to store application specific data associated with the user, it should do so when a user first authenticates

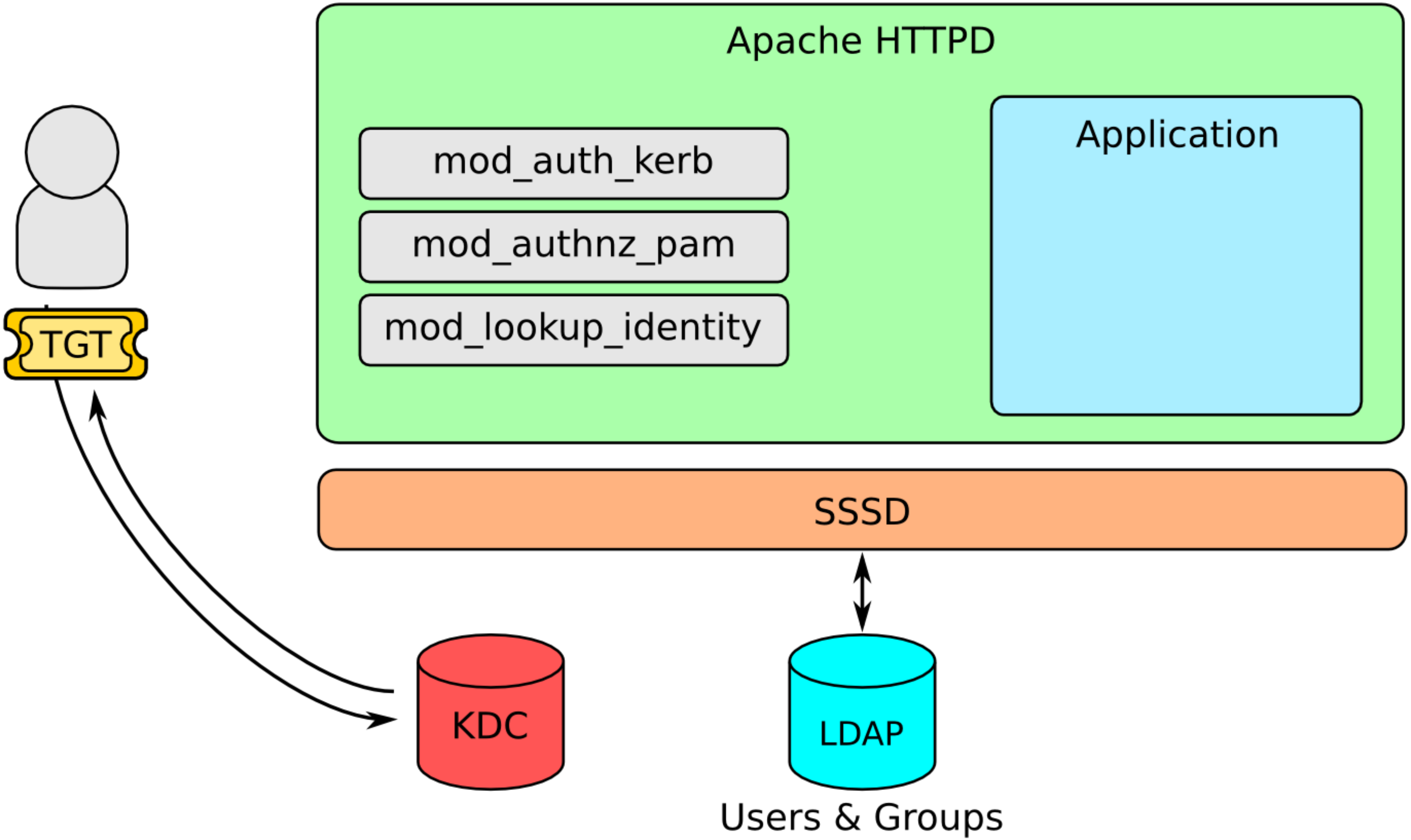
If fine-grained authorization is needed, group membership can be mapped to application specific roles (admin, user, etc.)

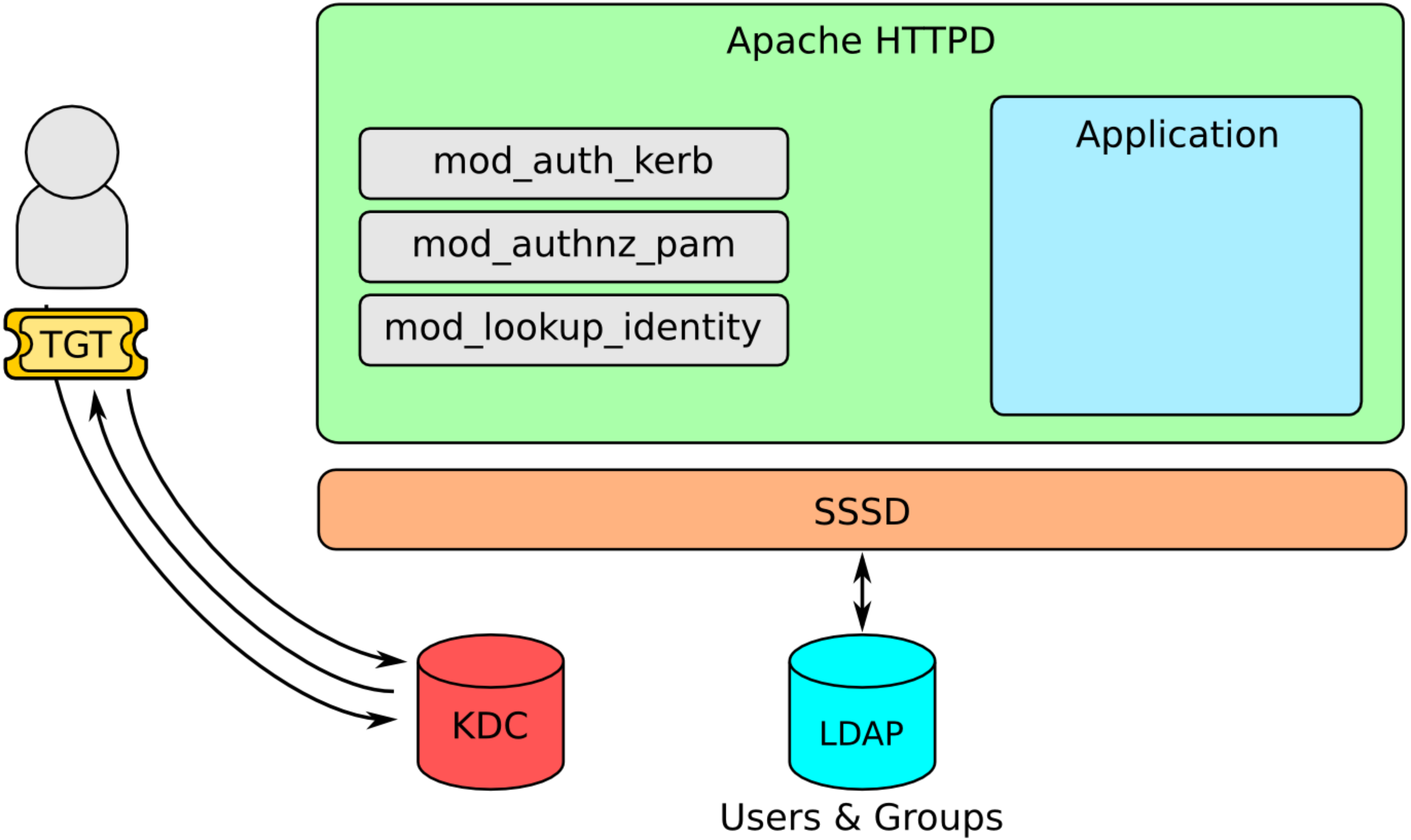
Advanced authentication methods can easily be added by using other HTTPD modules

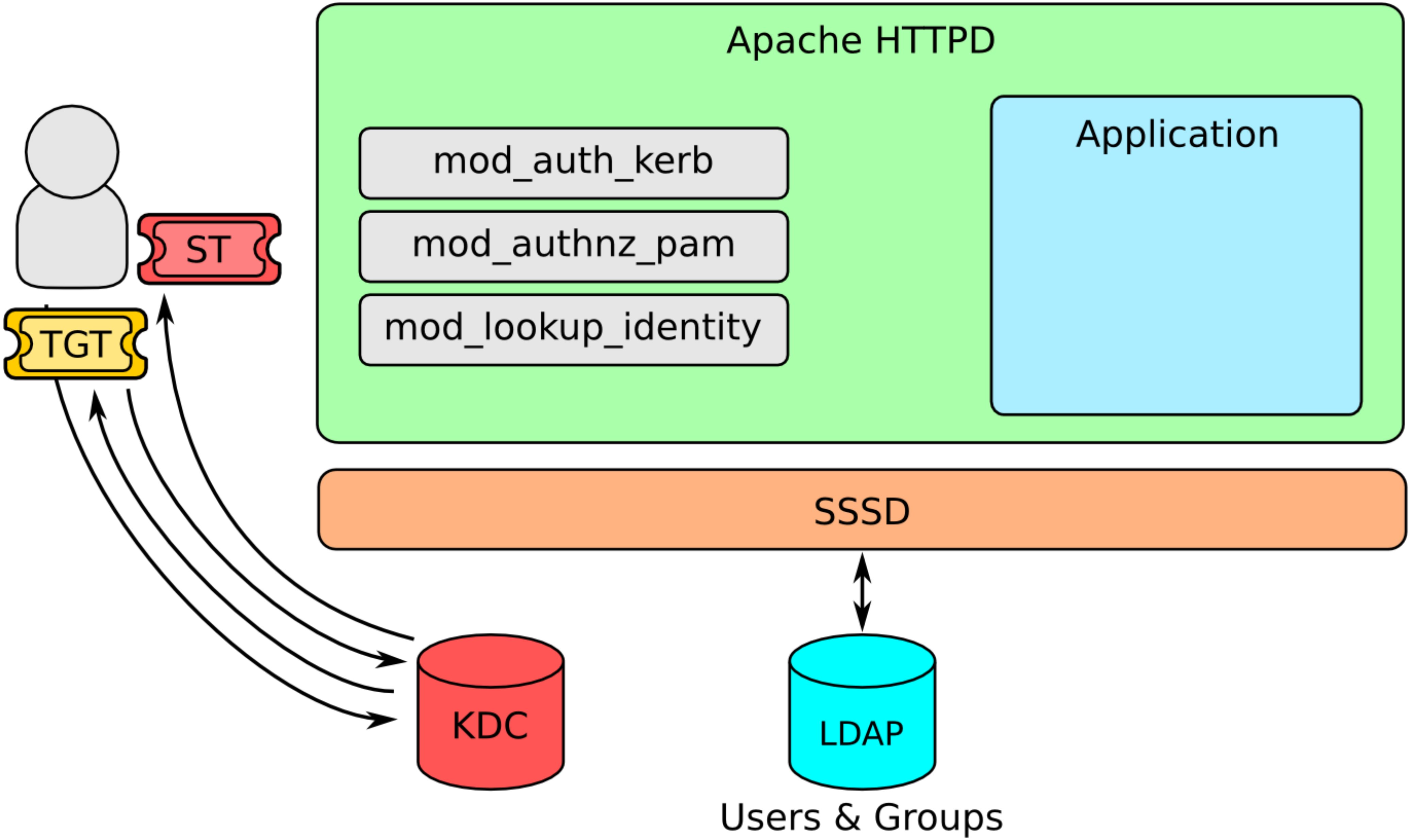
- mod_auth_gssapi/mod_auth_kerb
- mod_ssl/mod_nss
- mod_auth_mellon/mod_shib

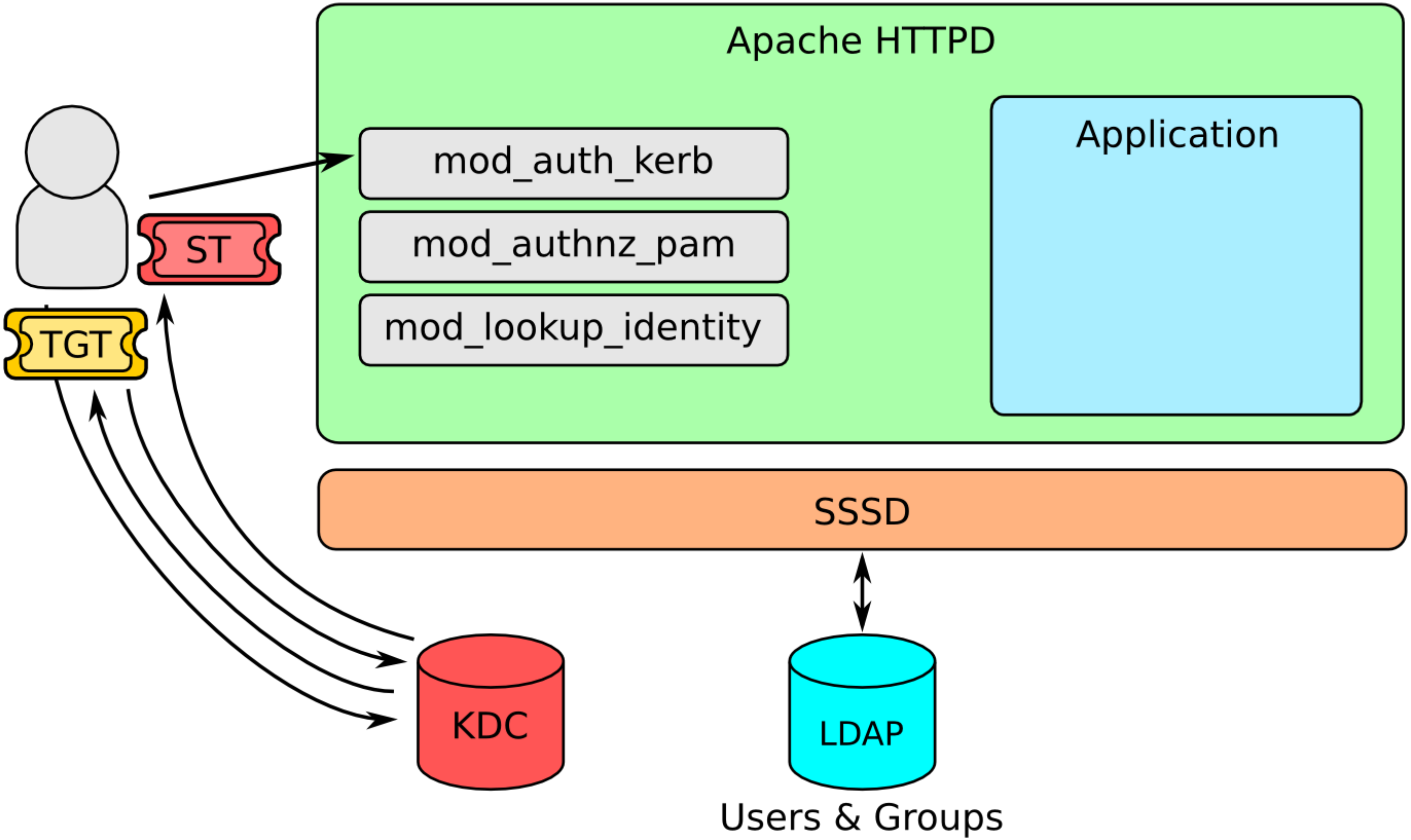
Kerberos workflow

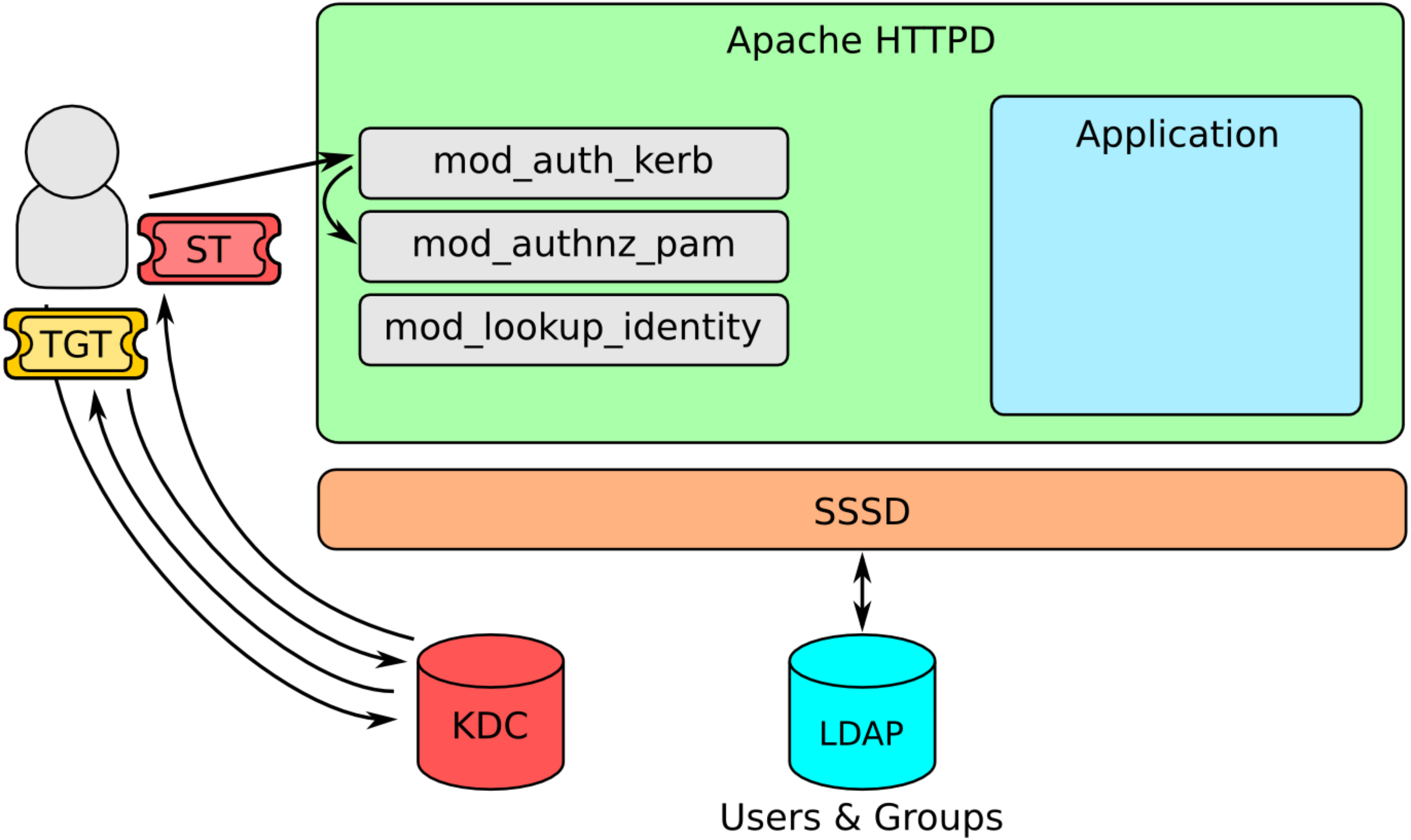

Apache HTTPD
mod_auth_kerb
mod_authnz_pam
mod_lookup_identity
Application
SSSD
KDC
LDAP
Users & Groups

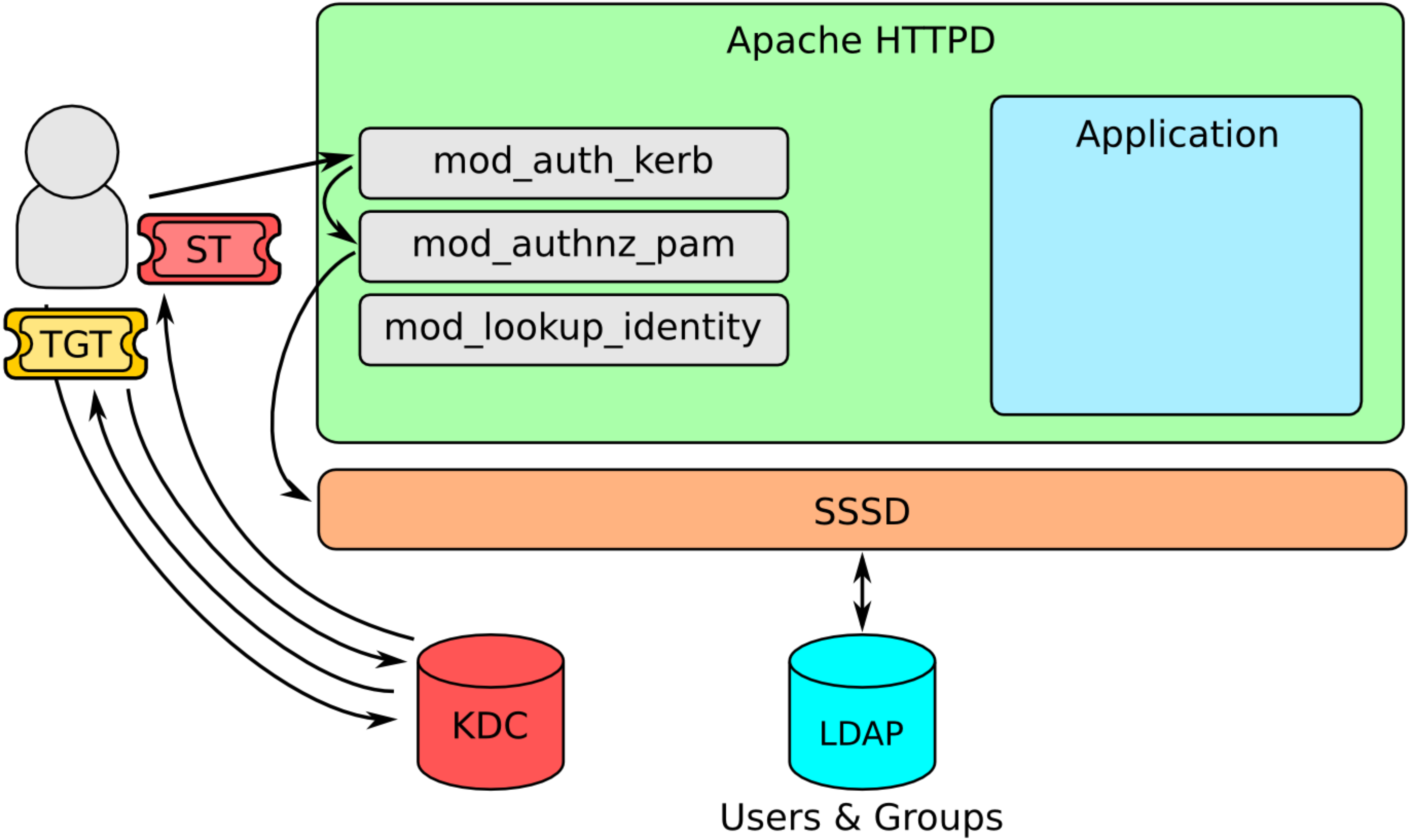

Apache HTTPD
mod_auth_kerb
mod_authnz_pam
mod_lookup_identity
Application
TGT
SSSD
KDC
LDAP
Users & Groups

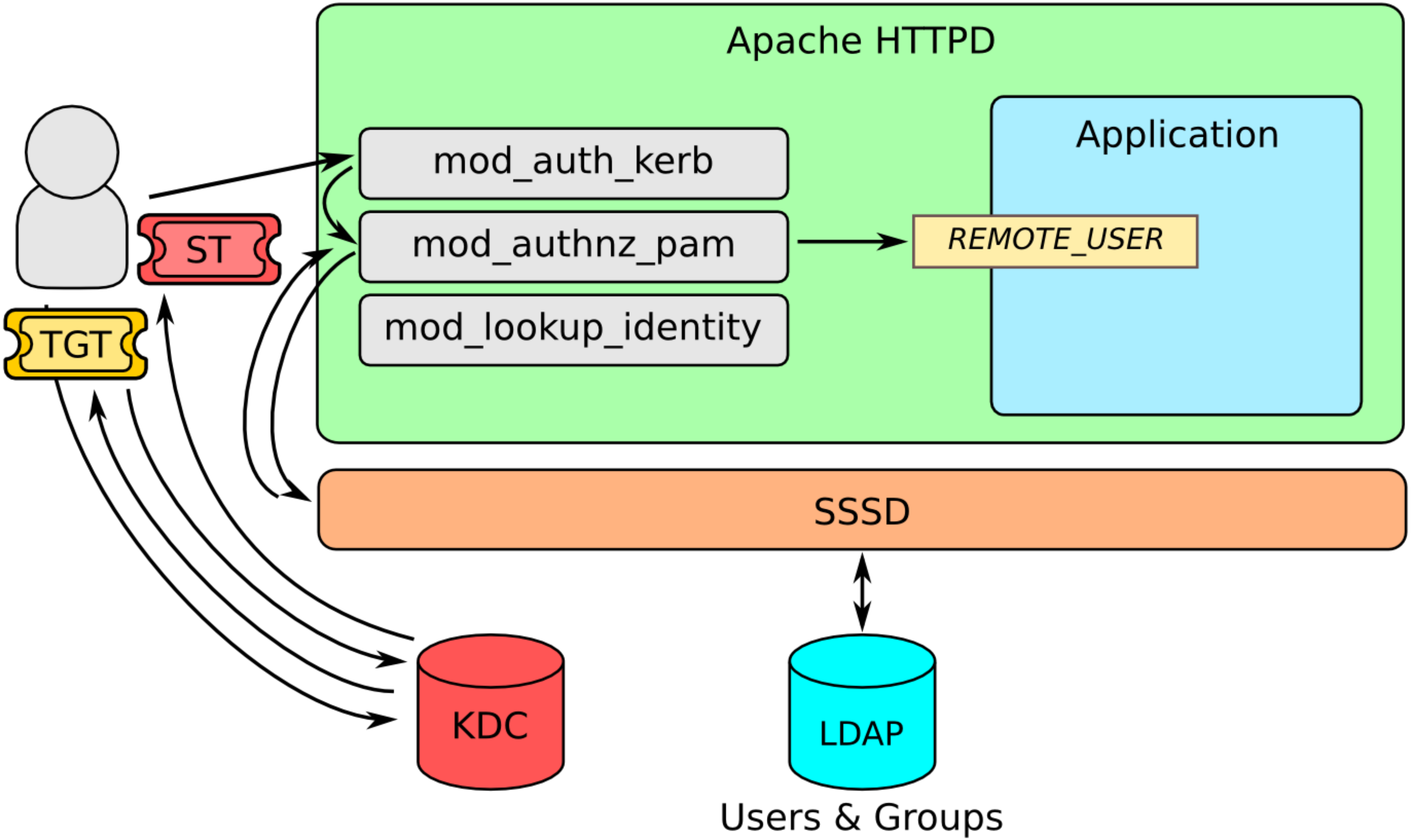

Apache HTTPD
mod_auth_kerb
mod_authnz_pam
mod_lookup_identity
Application
TGT
SSSD
KDC
LDAP
Users & Groups


Apache HTTPD
mod_auth_kerb
mod_authnz_pam
mod_lookup_identity
Application
ST
TGT
SSSD
KDC
LDAP
Users & Groups


Apache HTTPD
mod_auth_kerb
mod_authnz_pam
mod_lookup_identity
Application
ST
TGT
SSSD
KDC
LDAP
Users & Groups


Apache HTTPD
mod_auth_kerb
mod_authnz_pam
mod_lookup_identity
Application
ST
TGT
SSSD
KDC
LDAP
Users & Groups


Apache HTTPD
Application
mod_auth_kerb
mod_authnz_pam
mod_lookup_identity
ST
TGT
SSSD
KDC
LDAP
Users & Groups


Apache HTTPD
mod_auth_kerb
mod_authnz_pam
mod_lookup_identity
Application
REMOTE_USER
ST
TGT
SSSD
KDC
LDAP
Users & Groups

Kerberos config example

Questions?

http://www.freeipa.org/page/Web_App_Authentication
nkinder@redhat.com