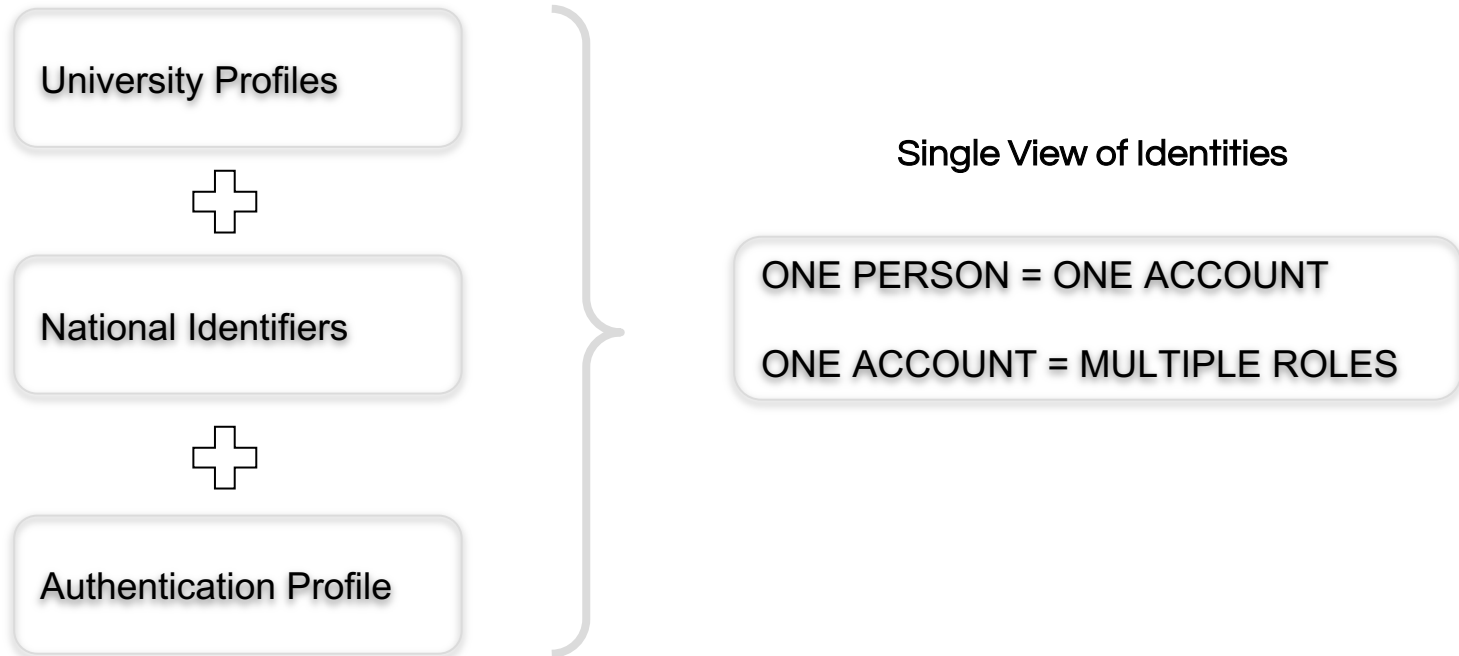# The system architecture behind the universities idm infrastructure
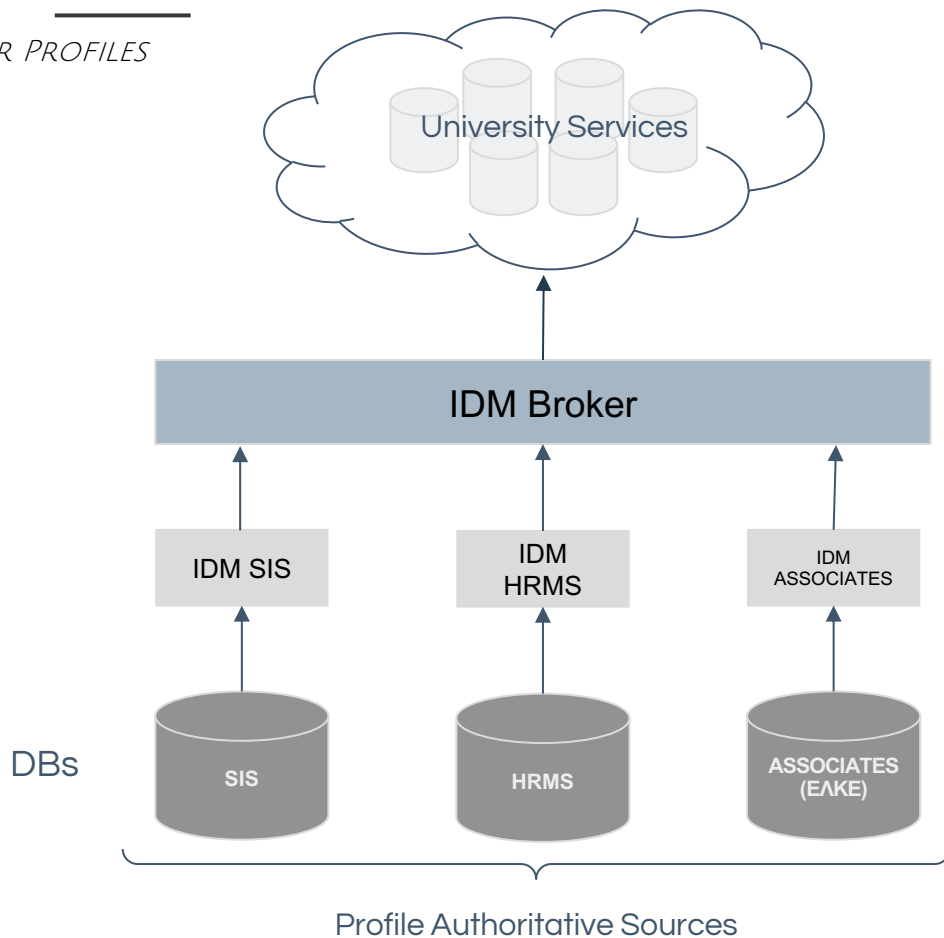
by GUNET
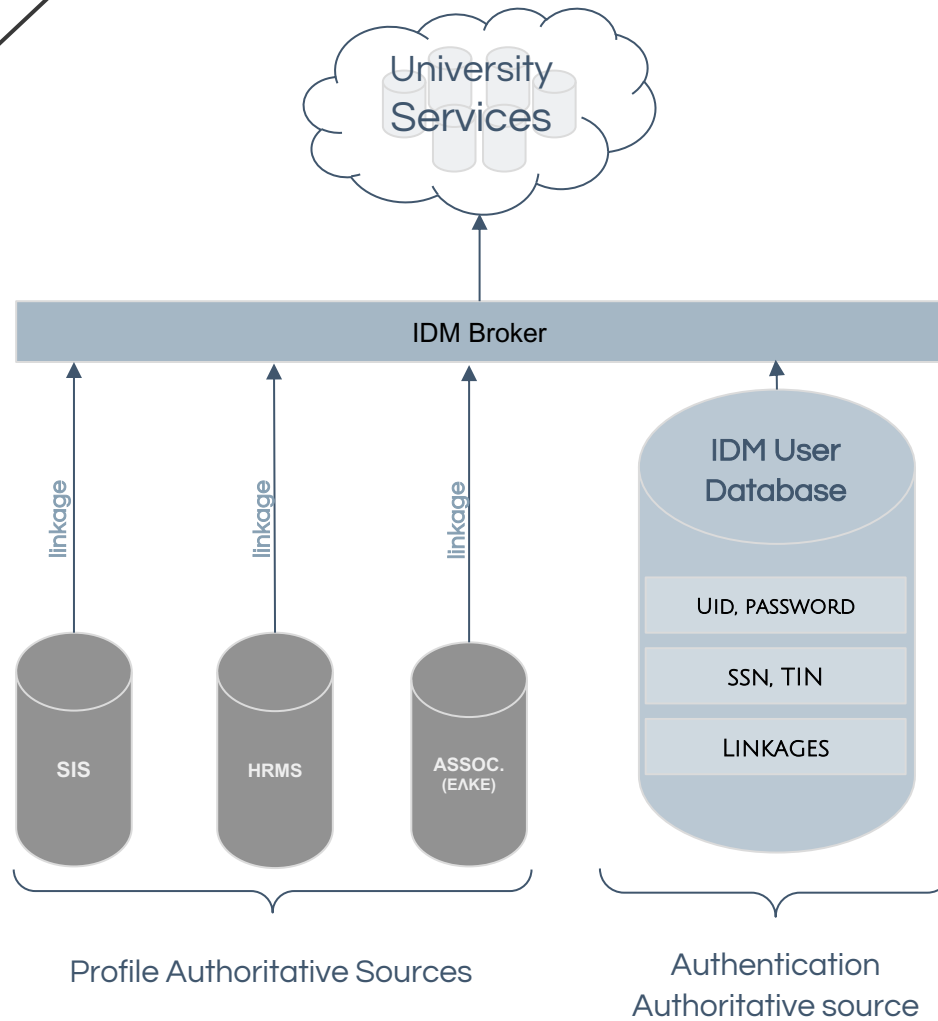
IDM BASIC PRINCIPLES

A University IDM account comprises of multiple parts originated from distinct sources
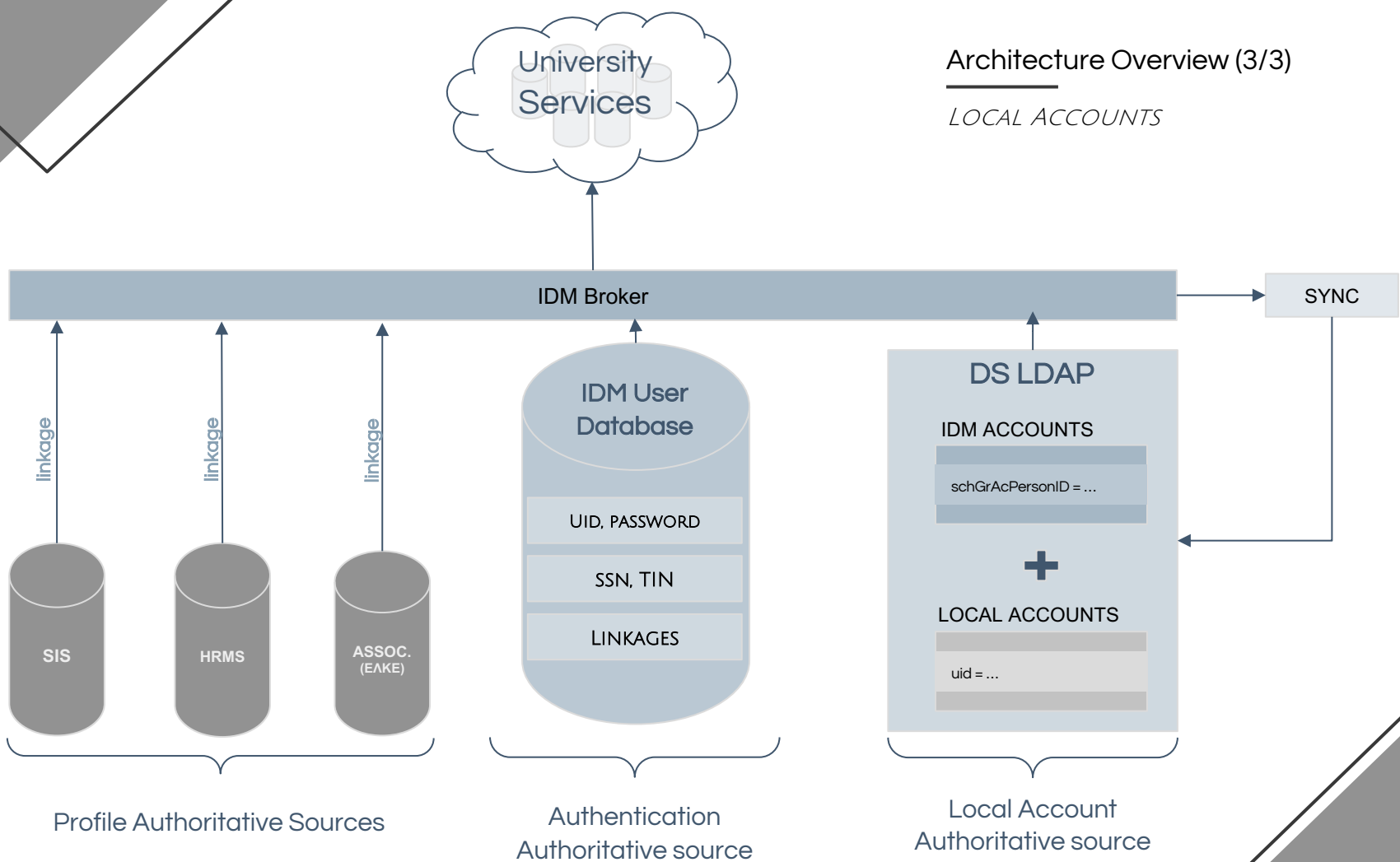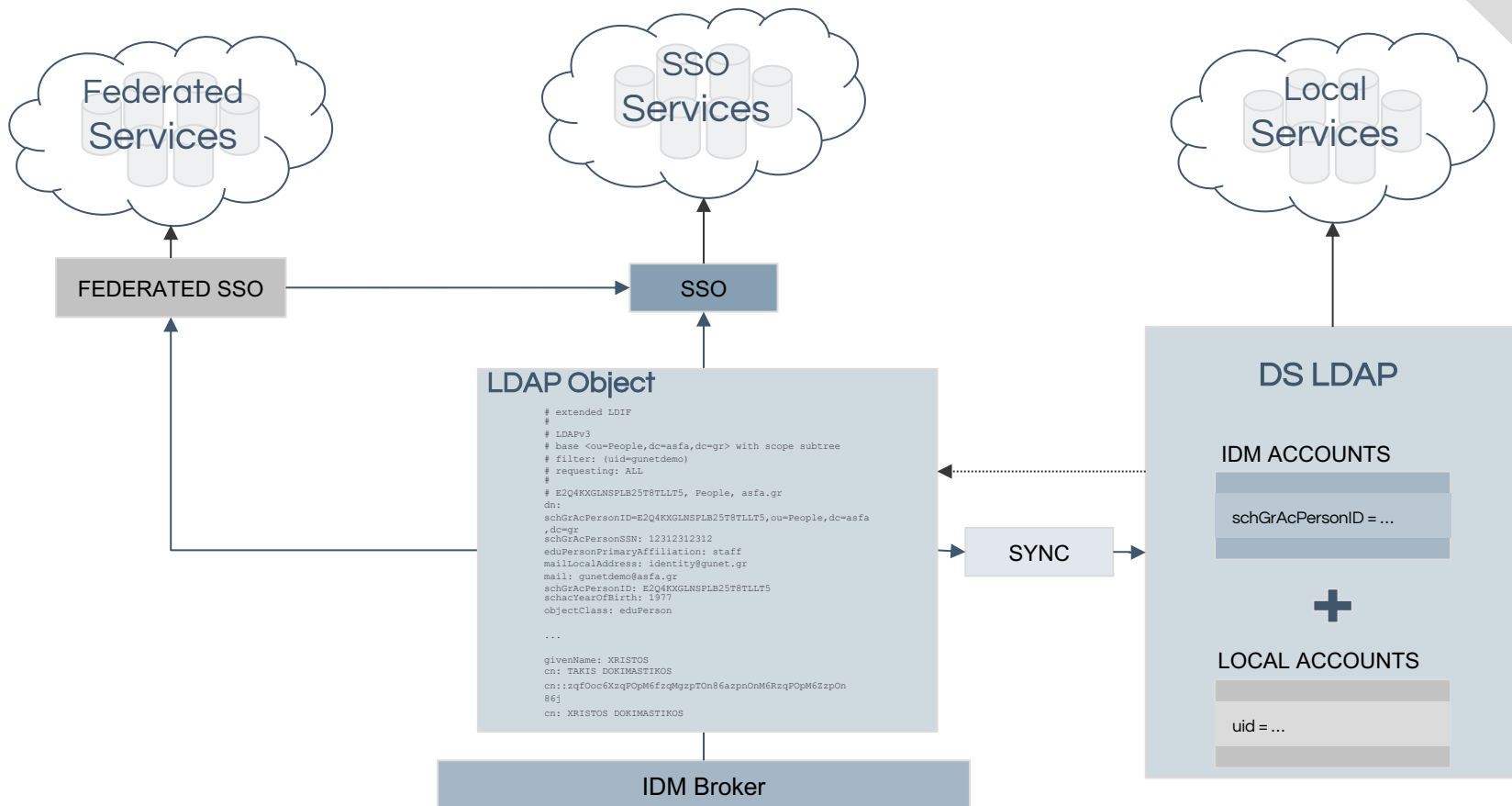
University Profiles

+

National Identifiers

+

Authentication Profile

Single View of Identities

ONE PERSON = ONE ACCOUNT

ONE ACCOUNT = MULTIPLE ROLES

IDM Upper Layers

Federated Services

SSO Services

Local Services

FEDERATED SSO

SSO

LDAP Object

```
# extended LDIF
#
# LDAPv3
# base <ou=People,dc=asfa,dc=gr> with scope subtree
# filter: (uid=gunetdemo)
# requesting: ALL
#
# E2Q4KXGLNSPLB25T8TLLT5, People, asfa.gr
dn:
schGrAcPersonID=E2Q4KXGLNSPLB25T8TLLT5,ou=People,dc=asfa
,dc=gr
schGrAcPersonSSN: 12312312312
eduPersonPrimaryAffiliation: staff
mailLocalAddress: identity@gunet.gr
mail: gunetdemo@asfa.gr
schGrAcPersonID: E2Q4KXGLNSPLB25T8TLLT5
schacYearOfBirth: 1977
objectClass: eduPerson

...

givenName: XRISTOS
cn: TAKIS DOKIMASTIKOS
cn::zqfOoc6XzqPOpM6fzqMgzpTOn86azpnOnM6RzqPOpM6ZzpOn
86j
cn: XRISTOS DOKIMASTIKOS
```

DS LDAP

IDM ACCOUNTS

schGrAcPersonID = ...

➕

LOCAL ACCOUNTS

uid = ...

SYNC

IDM Broker

uRegister

External email = ?
or
Mobile = ?

uRegister

Retrieve (RegistrationID, SSN)

IDM User
Database

SET PERSON ID

registrationalId = ...

registrationalId = ...

registrationalId = ...