Computer Security

Authentication

Prof. Jean-Noël Colin
jean-noel.colin@unamur.be
Office #306

UNIVERSITÉ DE NAMUR

Agenda

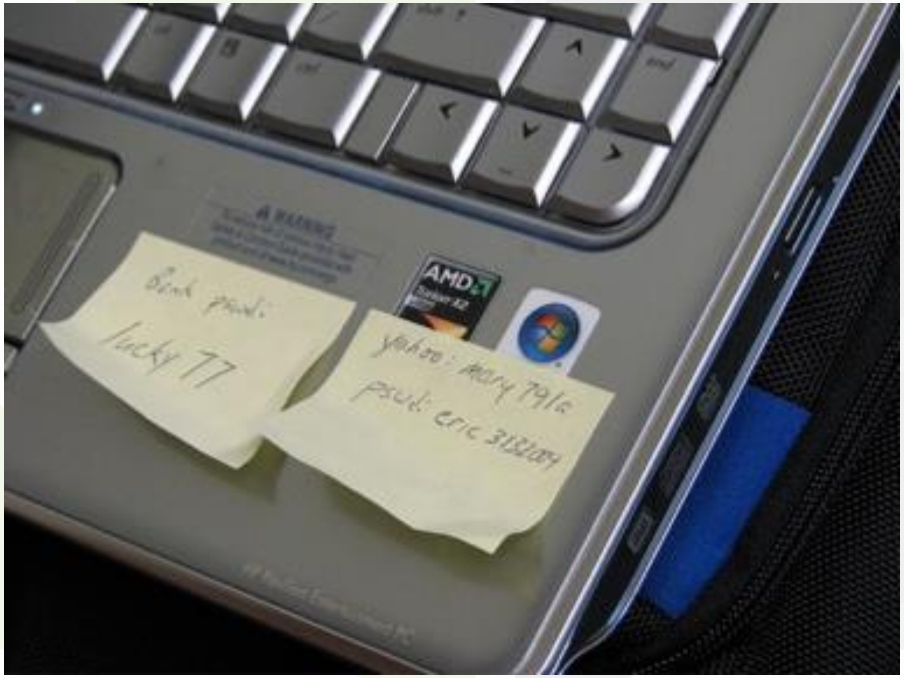
- Introduction
- Passwords
- One-Time Passwords
- Certificates
- Biometry
- Social engineering
- Identity management

Introduction

- Authentication = verification of an entity's identity (≠ identification)
- Two main reasons
  - access control/authorization
  - accounting/traceability/auditability
- Establish my identity with
  - something I know
    - password, PIN
  - something I own
    - token, smartcard
  - something I am
    - biometry
  - multifactor authentication
    - bank card,ItsMe

Password

- Most common authentication means. . .



Password

- Most common authentication means. . .

alphabet size	10 symbols (0-9)			26 symbols(a-z)			62 symbols(a-z,A-Z,0-9)			90 symbols (a-z,A-Z,0-9, symbols)		
password length	4	7	10	8	10	16	8	10	16	8	10	16
equivalent key length (bits)	13	23	33	38	47	75	48	60	95	52	65	104
Brute force possible?	Y	Y	Y	Y	Y	?	Y	Y	N	Y	Y	N
Source: Référentiel Général de Sécurité v2, ANSSI, 2014												

- https://howsecureismypassword.net/

Password policy

- Ensure proper level of quality (length, format, alphabet, avoid weak passwords, limit history…)
- Define secure initial password
- Force regular expiration and reset of passwords
- Limit the number of failed attempts
- Limit attempt rate by imposing a (variable) delay
- Change default passwords
- Password is forgotten if not used regularly
  - do not change password before holidays

Password security

- Storage
  - never in the clear
  - encrypted? hashed!
  - PBKDF2, Bcrypt…
    - <algorithm>$<iterations>$<salt>$<hash>
- Transmission
  - never in the clear
- do not cache password
- do not hardcode password
- prevent login spoofing
  - display connection history
  - safe key activation
  - mutual authentication

Attacks on passwords

- Assumption: authentication server stores hashed passwords and not passwords themselves
- Problem
  - given *h*, a digest, find the corresponding password *p* among *N* possible choices
  - Ex: 10 char. long passwords, with letters U/l and numbers: 62^{10} possibilities = $8{,}4.10^{17}$
- Similar problem
  - given *p* and *c*, find $k \mid c = E(k, p)$
- More generally, invert a one-way function

Attacks on passwords

- Different ways, with variable efficiency
- Parameters
  - T: number of operations (hash or encrypt/decrypt), the time factor
  - M: number of memory words used, the memory factor
  - N: number of possible values (keyspace)

Attacks on passwords

- Method 1: brute force or exhaustive search
  - for all possible passwords, compute the hash, compare to h; if match, p is found
  - on average, password is found in N/2 trials
  - efficiency
    - T=N
    - M=1

Attacks on passwords

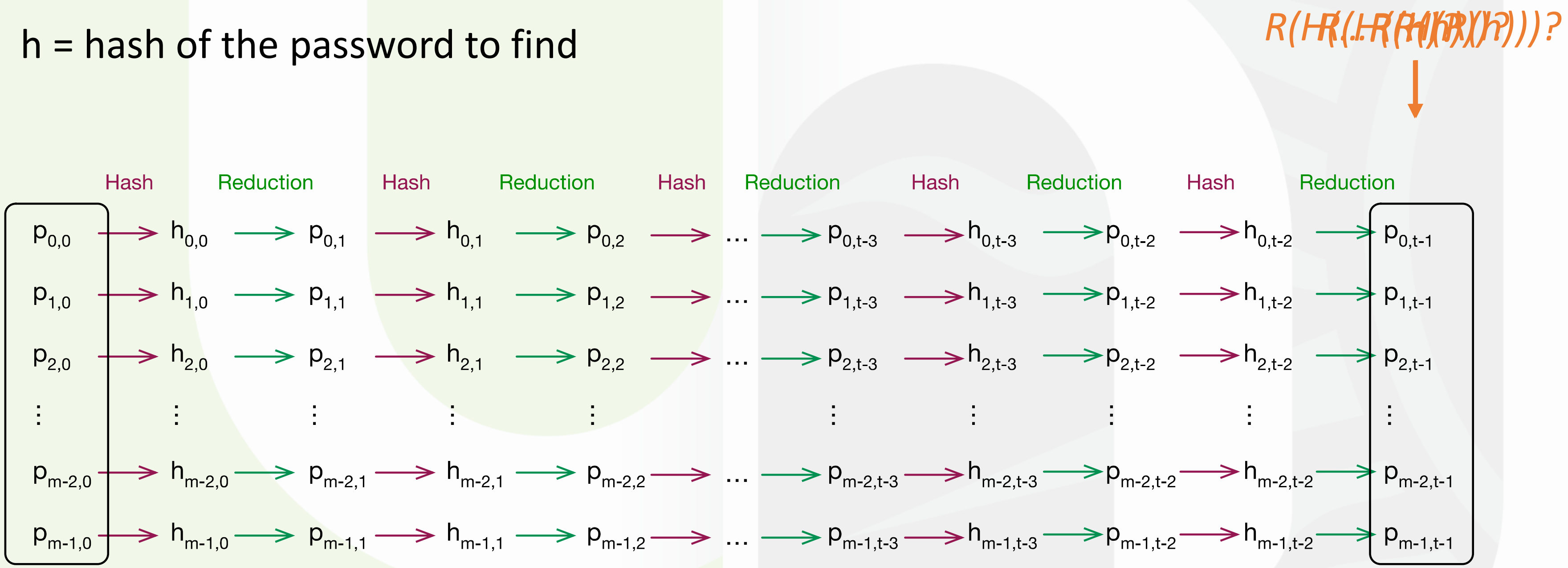
- Method 2: precomputation attack
  - precompute the hash of all possible passwords and store them in a table
  - lookup h in table; return corresponding p
  - efficiency
    - T=1
    - M=N
  - keyspace can be limited to a dictionary of frequent passwords

Time-memory trade-off

- Method 3: time-memory trade-off
  - M. Hellman. A cryptanalytic time-memory trade-off. IEEE Transactions on Information Theory, 26(4):401 – 406, jul 1980.
  - Objective: find p quicker than method 1 and using less memory than method 2
  - Principle
    - create m chains of t passwords
    - i^{th} element in a chain is computed from $(i - 1)^{th}$
    - only first and last elements of the chain are stored

Time-memory trade-off

h = hash of the password to find



Time-memory trade-off

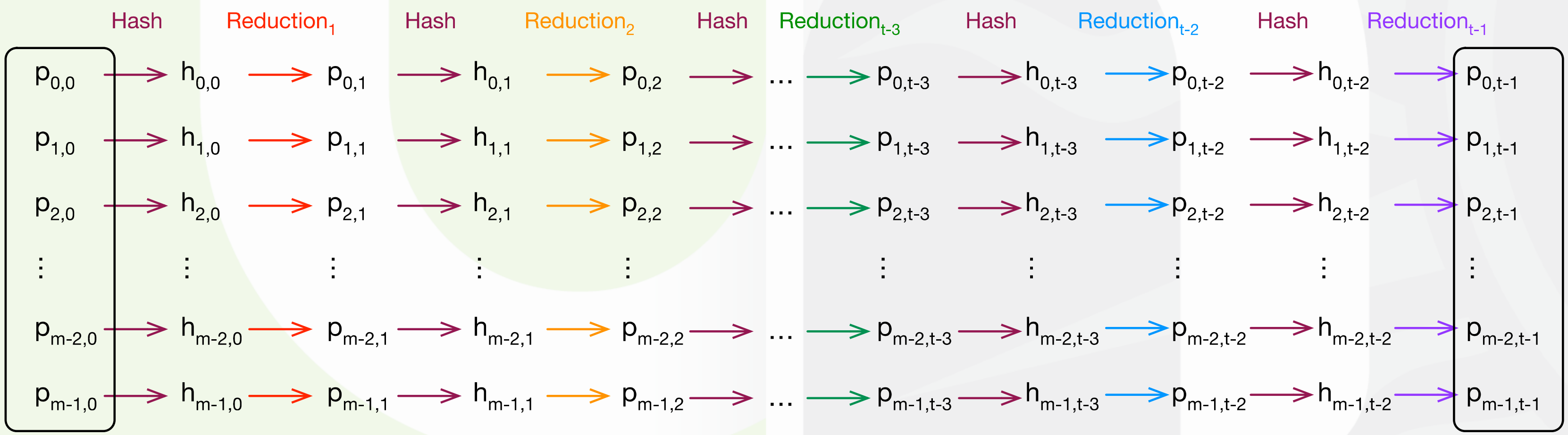
- Efficiency
  - table of m chains of length t, hence m.t elements
  - $M = m.m_0$ where m_0 is the space to store $(p_{i,0}, p_{i,t-1})$
  - worse case: $T = (t - 1)$
  - if all elements are different, $P_{table} = \frac{mt}{N}$
  - Hellman shows that $P_{table} \geq \frac{1}{N} \sum_{i=1}^{m} \sum_{j=0}^{t-1} (1 - \frac{it}{N})^{j+1}$
  - When N increases, efficiency decreases quickly
  - Optimal value for m and t when $mt^2 = N$

Time-memory trade-off

- Limitations
  - collision and chain merge
    - collision: $\exists\ p, q | (p \neq q)\ \wedge$ (R(p)=R(q))
    - two identical values in the table ⇒ two chains merge
    - the larger the table, the greater the probability of chain merge
    - table efficiency decreases when its size increases
    - solution: use l tables with different reduction functions $R_0, R_1, \ldots R_{l-1}$
    - in this case: $P_{table} \geq 1 - (1 - \frac{1}{N} \sum_{i=1}^{m} \sum_{j=0}^{t-1} (1 - \frac{it}{N})^{j+1})^{l}$

Rainbow tables

- Use a different reduction function at each step



Oechslin, P. *Making a Faster Cryptanalytic Time-Memory Trade-Off*, Advances in Cryptology - CRYPTO 2003: 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003. Proceedings, Springer Berlin Heidelberg, 2003, 617-630

Rainbow tables

- Advantage
  - worse case: $T = \frac{t(t-1)}{2}$
  - more efficient than Hellman: let's use t tables m.t (Hellman) and 1 table mt.t (Rainbow table), thus mt2 passwords in both cases
    - success probabilities are approximately equal
    - $T = t^2$(Hellman) vs $T = \frac{t(t-1)}{2}$ (Rainbow tables)
- Go and check the price of rainbow tables

One-time password

- Password is generated when needed and used only once
- Renders any attack on the password itself useless
- No need to remember password
- Password could be exchanged in the clear
- Requires some kind of synchronized state and shared secret between client and server
- OTP generation
  - OTP = f(shared secret, clock)
  - OTP = f(shared secret, sequence number)
  - OTP = f(shared secret, random number)
- Other solutions
  - list of codes
  - password matrix
  - asymmetric crypto instead of shared secret

Certificats

- Certificate
  - (issuer, subject, public key, signature)
  - Authentication through
    - certificate validation
    - challenge/response with asymmetric encryption

Biometry

- Physiological or behavioral data
  - fingerprint, iris or retina scan, voice authentication, keyboard hit
- collect models
  - identification: find 1 sample among n models
  - authentication: check match for 1 sample
  - threshold algorithms

Social engineering

- Set of techniques used to manipulate, influence or lure someone into doing something he shouldn’t normally do. Often, this involves disclosing confidential information
- Human factor is the weak link
  - sensitive to authority, emergency, similarity, sense of responsibility, kindness
- Typical targets
  - people with little security concern
  - people in support roles
  - people with privileged roles
  - people with specific knowledge
  - people with access to valuable assets

Social engineering attack

- Physical data collection
  - dumpster diving, theft, blackmail, bribary, extortion, desktop hacking…
- Often complex and hybrid attacks
  - ex: (spear) phishing, CEO fraud

Protection against social engineering

- Education
  - Main challenges
    - differentiate between good and evil, true and false
    - define clear criteria and reporting lines
  - Know how and when report a potential problem
  - Define clear policies
  - Define clear lines of communication
  - Coordinate between all security actors

Identity Management

- Identity = set of information related to an entity (person, system)
- In a complex IS, there are often multiple sources of identity
  - multiple applications
  - multiple levels (OS, applications. . .)
- How to maintain those sources consistent?
- Strong impact on global security

Where to store identity data?

- File
  - simple to implement
  - limited expressiveness
  - sensitive data can be encrypted
  - control access to sensitive data
- Database
  - simple to implement
  - flexible and extensible datamodel
  - sensitive data can be encrypted
  - control access to sensitive data
  - often application specific

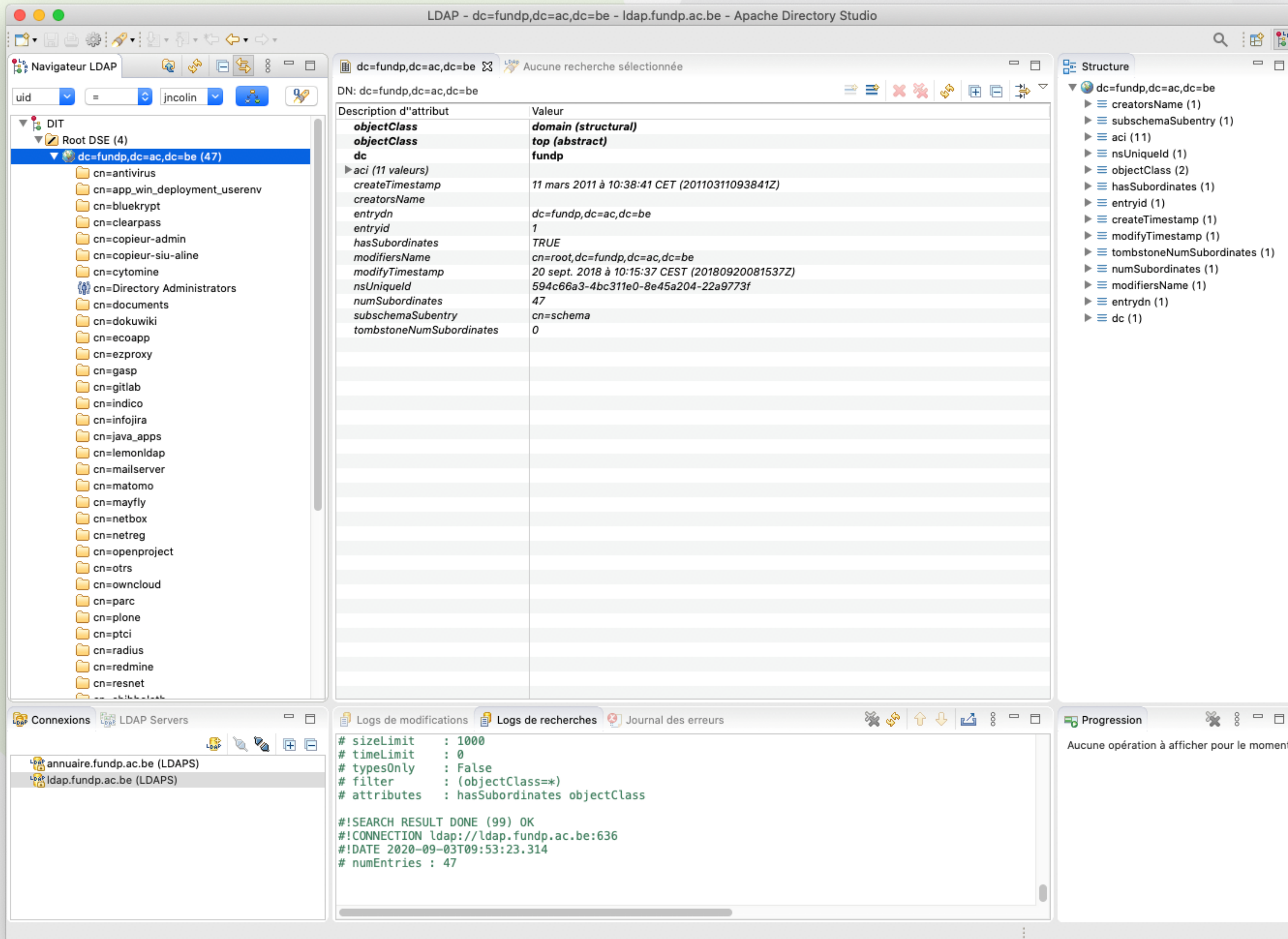
Where to store identity data?

- LDAP – Lightweight Directory Access Protocol
  - defines both a datamodel and a data access protocol
  - derived from X.500 standard
  - data is organized as a tree: DIT – Directory Information Tree
  - data stored in tree nodes
    - node structure defined in an extensible schema
    - all schema elements identified by unique Object Identifier (OID)
  - root node identified by a root suffix
    - i.e.: `dc=unamur, dc=be`

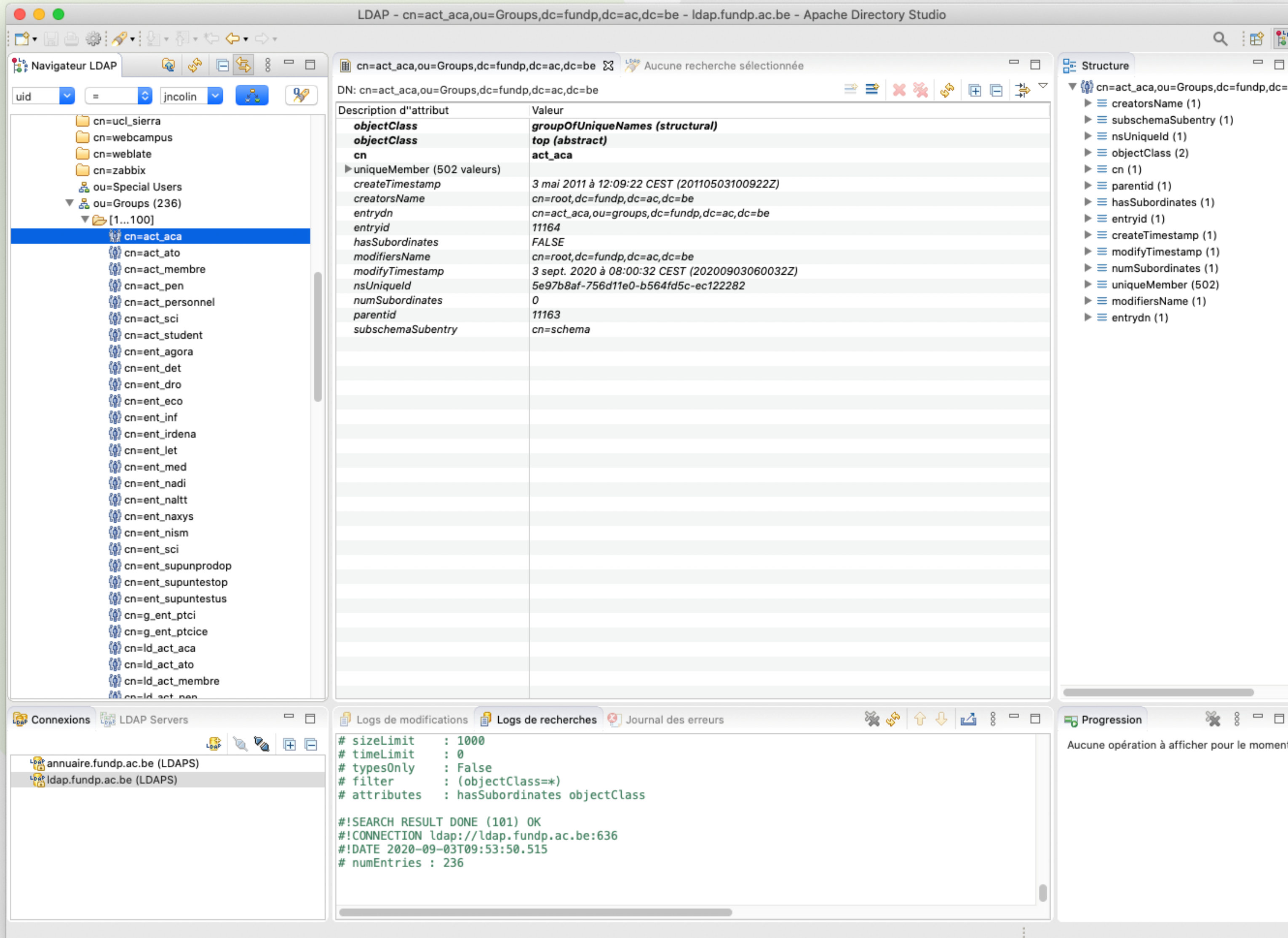
Where to store identity data?

- LDAP – Lightweight Directory Access Protocol
  - node = DSE – Directory Service Entry
    - identified by a node name (DN & RDN)
    - instantiates one or more classes – ObjectClass, which define mandatory and optional node attributes, and can inherit from one another
  - node represents a user, a group (static or dynamic)
    - or any entity: just define the appropriate ObjectClass

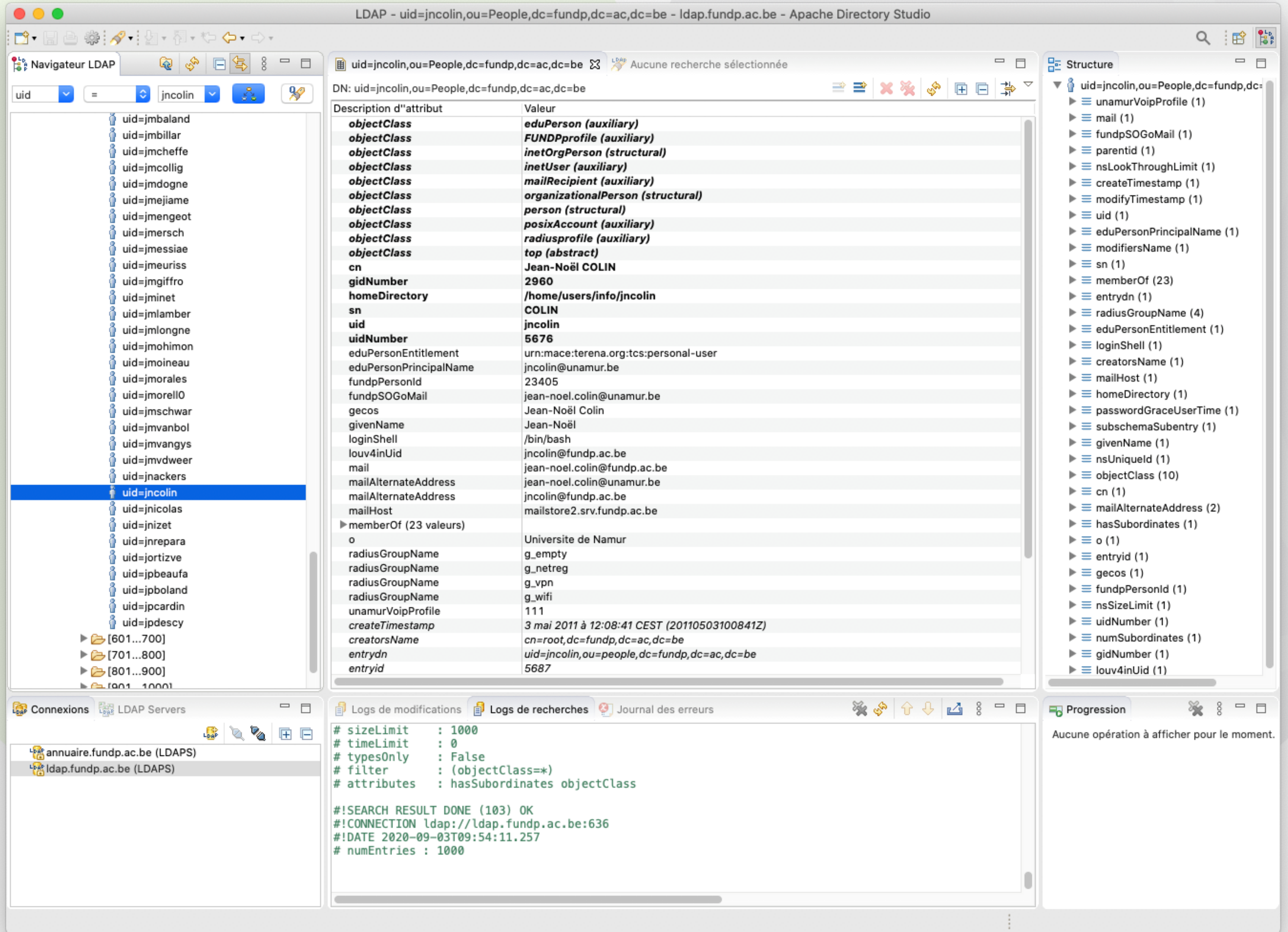
LDAP


LDAP - dc=fundp,dc=ac,dc=be - ldap.fundp.ac.be - Apache Directory Studio
Navigateur LDAP
uid
=
jncolin
DIT
Root DSE (4)
dc=fundp,dc=ac,dc=be (47)
cn=antivirus
cn=app_win_deployment_userenv
cn=bluekrypt
cn=clearpass
cn=copieur-admin
cn=copieur-siu-aline
cn=cytomine
cn=Directory Administrators
cn=documents
cn=dokuwiki
cn=ecoapp
cn=ezproxy
cn=gasp
cn=gitlab
cn=indico
cn=infojira
cn=java_apps
cn=lemonldap
cn=mailserver
cn=matomo
cn=mayfly
cn=netbox
cn=netreg
cn=openproject
cn=otrs
cn=owncloud
cn=parc
cn=plone
cn=ptci
cn=radius
cn=redmine
cn=resnet
dc=fundp,dc=ac,dc=be
Aucune recherche sélectionnée
DN: dc=fundp,dc=ac,dc=be
Description d''attribut
Valeur
objectClass
domain (structural)
objectClass
top (abstract)
dc
fundp
aci (11 valeurs)
createTimestamp
11 mars 2011 à 10:38:41 CET (20110311093841Z)
creatorsName
entrydn
dc=fundp,dc=ac,dc=be
entryid
1
hasSubordinates
TRUE
modifiersName
cn=root,dc=fundp,dc=ac,dc=be
modifyTimestamp
20 sept. 2018 à 10:15:37 CEST (20180920081537Z)
nsUniqueId
594c66a3-4bc311e0-8e45a204-22a9773f
numSubordinates
47
subschemaSubentry
cn=schema
tombstoneNumSubordinates
0
Structure
dc=fundp,dc=ac,dc=be
creatorsName (1)
subschemaSubentry (1)
aci (11)
nsUniqueId (1)
objectClass (2)
hasSubordinates (1)
entryid (1)
createTimestamp (1)
modifyTimestamp (1)
tombstoneNumSubordinates (1)
numSubordinates (1)
modifiersName (1)
entrydn (1)
dc (1)
Connexions
LDAP Servers
annuaire.fundp.ac.be (LDAPS)
ldap.fundp.ac.be (LDAPS)
Logs de modifications
Logs de recherches
Journal des erreurs
sizeLimit : 1000
timeLimit : 0
typesOnly : False
filter : (objectClass=*)
attributes : hasSubordinates objectClass
#!SEARCH RESULT DONE (99) OK
#!CONNECTION ldap://ldap.fundp.ac.be:636
#!DATE 2020-09-03T09:53:23.314
numEntries : 47
Progression
Aucune opération à afficher pour le moment.

LDAP


LDAP - cn=act_aca,ou=Groups,dc=fundp,dc=ac,dc=be - ldap.fundp.ac.be - Apache Directory Studio
Navigateur LDAP
uid
=
jncolin
cn=ucl_sierra
cn=webcampus
cn=weblate
cn=zabbix
ou=Special Users
ou=Groups (236)
[1...100]
cn=act_aca
cn=act_ato
cn=act_membre
cn=act_pen
cn=act_personnel
cn=act_sci
cn=act_student
cn=ent_agora
cn=ent_det
cn=ent_dro
cn=ent_eco
cn=ent_inf
cn=ent_irdena
cn=ent_let
cn=ent_med
cn=ent_nadi
cn=ent_naltt
cn=ent_naxys
cn=ent_nism
cn=ent_sci
cn=ent_supunprodop
cn=ent_supuntestop
cn=ent_supuntestus
cn=g_ent_ptci
cn=g_ent_ptcice
cn=ld_act_aca
cn=ld_act_ato
cn=ld_act_membre
cn=act_aca,ou=Groups,dc=fundp,dc=ac,dc=be
Aucune recherche sélectionnée
DN: cn=act_aca,ou=Groups,dc=fundp,dc=ac,dc=be
Description d''attribut
Valeur
objectClass
groupOfUniqueNames (structural)
objectClass
top (abstract)
cn
act_aca
uniqueMember (502 valeurs)
createTimestamp
3 mai 2011 à 12:09:22 CEST (20110503100922Z)
creatorsName
cn=root,dc=fundp,dc=ac,dc=be
entrydn
cn=act_aca,ou=groups,dc=fundp,dc=ac,dc=be
entryid
11164
hasSubordinates
FALSE
modifiersName
cn=root,dc=fundp,dc=ac,dc=be
modifyTimestamp
3 sept. 2020 à 08:00:32 CEST (20200903060032Z)
nsUniqueId
5e97b8af-756d11e0-b564fd5c-ec122282
numSubordinates
0
parentid
11163
subschemaSubentry
cn=schema
Structure
cn=act_aca,ou=Groups,dc=fundp,dc=a
creatorsName (1)
subschemaSubentry (1)
nsUniqueId (1)
objectClass (2)
cn (1)
parentid (1)
hasSubordinates (1)
entryid (1)
createTimestamp (1)
modifyTimestamp (1)
numSubordinates (1)
uniqueMember (502)
modifiersName (1)
entrydn (1)
Connexions
LDAP Servers
annuaire.fundp.ac.be (LDAPS)
ldap.fundp.ac.be (LDAPS)
Logs de modifications
Logs de recherches
Journal des erreurs
sizeLimit : 1000
timeLimit : 0
typesOnly : False
filter : (objectClass=*)
attributes : hasSubordinates objectClass
#!SEARCH RESULT DONE (101) OK
#!CONNECTION ldap://ldap.fundp.ac.be:636
#!DATE 2020-09-03T09:53:50.515
numEntries : 236
Progression
Aucune opération à afficher pour le moment.

LDAP

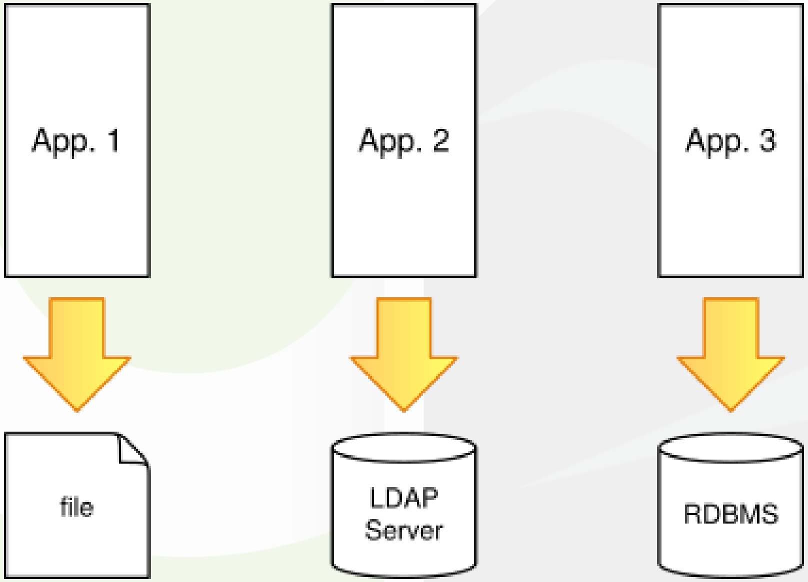

LDAP - uid=jncolin,ou=People,dc=fundp,dc=ac,dc=be - ldap.fundp.ac.be - Apache Directory Studio
Navigateur LDAP
uid=jncolin,ou=People,dc=fundp,dc=ac,dc=be
Aucune recherche sélectionnée
DN: uid=jncolin,ou=People,dc=fundp,dc=ac,dc=be
Description d''attribut
Valeur
objectClass eduPerson (auxiliary)
objectClass FUNDPprofile (auxiliary)
objectClass inetOrgPerson (structural)
objectClass inetUser (auxiliary)
objectClass mailRecipient (auxiliary)
objectClass organizationalPerson (structural)
objectClass person (structural)
objectClass posixAccount (auxiliary)
objectClass radiusprofile (auxiliary)
objectClass top (abstract)
cn Jean-Noël COLIN
gidNumber 2960
homeDirectory /home/users/info/jncolin
sn COLIN
uid jncolin
uidNumber 5676
eduPersonEntitlement urn:mace:terena.org:tcs:personal-user
eduPersonPrincipalName jncolin@unamur.be
fundpPersonId 23405
fundpSOGoMail jean-noel.colin@unamur.be
gecos Jean-Noël Colin
givenName Jean-Noël
loginShell /bin/bash
louv4inUid jncolin@fundp.ac.be
mail jean-noel.colin@fundp.ac.be
mailAlternateAddress jean-noel.colin@unamur.be
mailAlternateAddress jncolin@fundp.ac.be
mailHost mailstore2.srv.fundp.ac.be
memberOf (23 valeurs)
o Universite de Namur
radiusGroupName g_empty
radiusGroupName g_netreg
radiusGroupName g_vpn
radiusGroupName g_wifi
unamurVoipProfile 111
createTimestamp 3 mai 2011 à 12:08:41 CEST (20110503100841Z)
creatorsName cn=root,dc=fundp,dc=ac,dc=be
entrydn uid=jncolin,ou=people,dc=fundp,dc=ac,dc=be
entryid 5687
Structure
Connexions
LDAP Servers
annuaire.fundp.ac.be (LDAPS)
ldap.fundp.ac.be (LDAPS)
Logs de modifications
Logs de recherches
Journal des erreurs
sizeLimit : 1000
timeLimit : 0
typesOnly : False
filter : (objectClass=*)
attributes : hasSubordinates objectClass
#!SEARCH RESULT DONE (103) OK
#!CONNECTION ldap://ldap.fundp.ac.be:636
#!DATE 2020-09-03T09:54:11.257
numEntries : 1000
Progression
Aucune opération à afficher pour le moment.

Where to store identity data?

- LDAP – Lightweight Directory Access Protocol
  - access protocol
    - bind (session opening): authenticated or anonymous
    - operation(s):
      - search, delete, modify (add or update)
    - unbind (session closing)
  - access control - Access Control List (ACL)
    - defines name, target, permission, bind rules
    - often server specific

```
aci: (target="ldap:///uid=jnc,dc=example,dc=com")
(targetattr="*")(version 3.0; acl "example aci"; allow
(write) userdn="ldap:///self";)
```

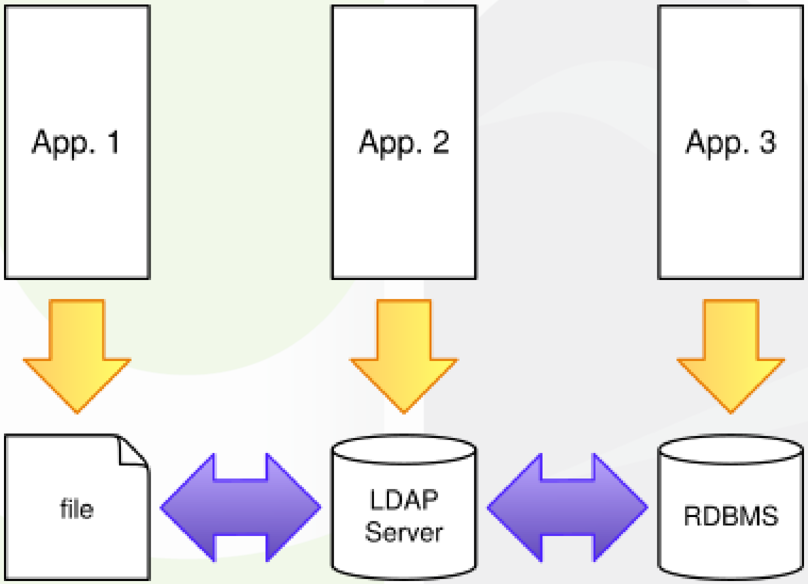
Various identity sources?



<u>Independent sources</u>

- Simple
- Isolation
- Multiple identities
- Risk of inconsistent data

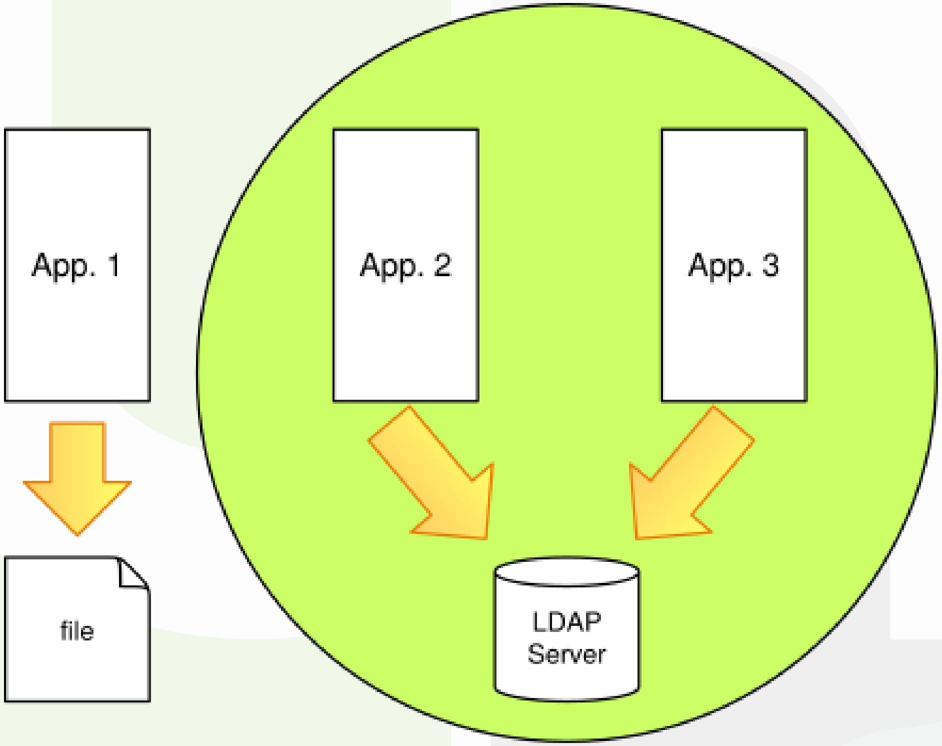
Various identity sources?



Synchronized sources

- One single identity
- Synchronization cost
- Not scalable
- Application specific
- No isolation

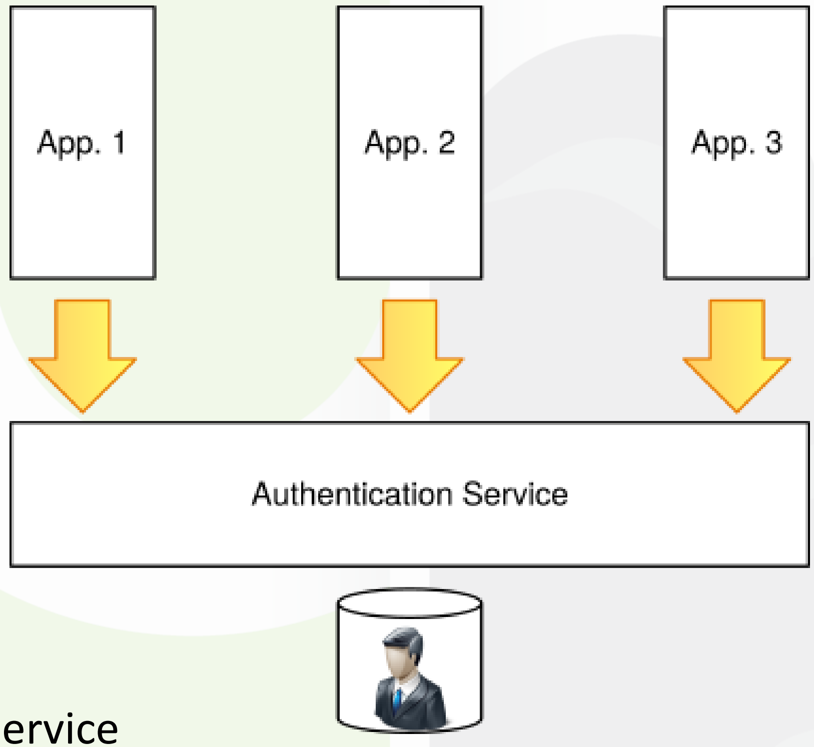
Various identity sources?



<u>Shared sources</u>

- One single identity
- Application specific ?
- No isolation

Various identity sources?



<u>External authentications service</u>

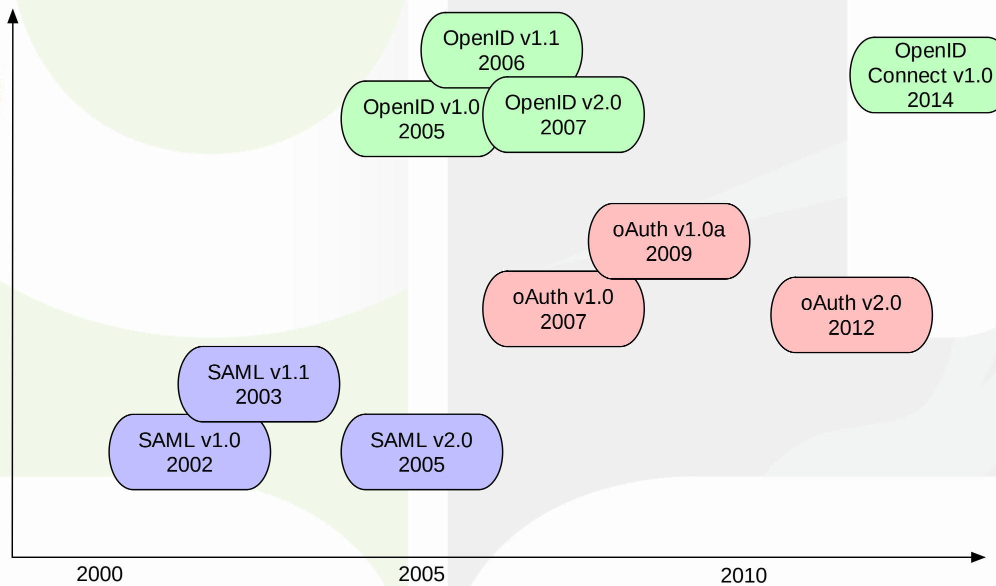
- Frees the application from the management of identities and authentication process
- Requires a secure protocol
- Requires trust between parties, possibly cross-organization

Distributed identity management

- Motivations
  - One authoritative source of information
  - Better control over privacy
  - Reduced management overhead
  - Better user experience
  - Better structured software architecture
  - Security: credentials never shared
  - Cross-body integration and cooperation

Distributed identity management

- Major protocols
  - OpenIDv1, v2, OpenID Connect
  - oAuthv1, oAuthv2
  - SAML – Security Assertion Markup Language



CAS

Conclusion

- Authentication is the key to your system
- Different approaches are available, with various scopes and levels of complexity and cost
- Make sure you adopt secure yet usable authentication mechanism
- When going for distributed approach, choose for interoperability: adopt a standard
- Implementation can (will) be costly and lengthy
- Re-assess mechanisms regularly