



indico

Indico Workshop 2.0

**Enterprise Authentication
with Indico**

Michał Kołodziejcki
Indico Developer

A short glossary

Authentication

Authentication means verifying that someone is indeed who they claim to be.



Fig. 1 <https://andrewjprokop.files.wordpress.com/2015/01/authentication.jpg>

Authorization

Authorization means deciding which resources a certain user should be able to access, and what they should be allowed to do with those resources.



Fig. 2 <https://www.colourbox.com/preview/11986872-authorized.jpg>

Authentication and authorization

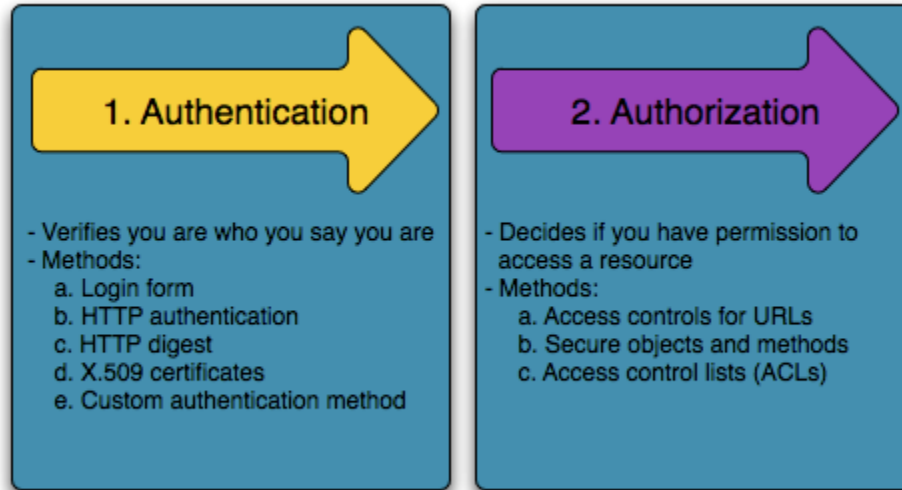
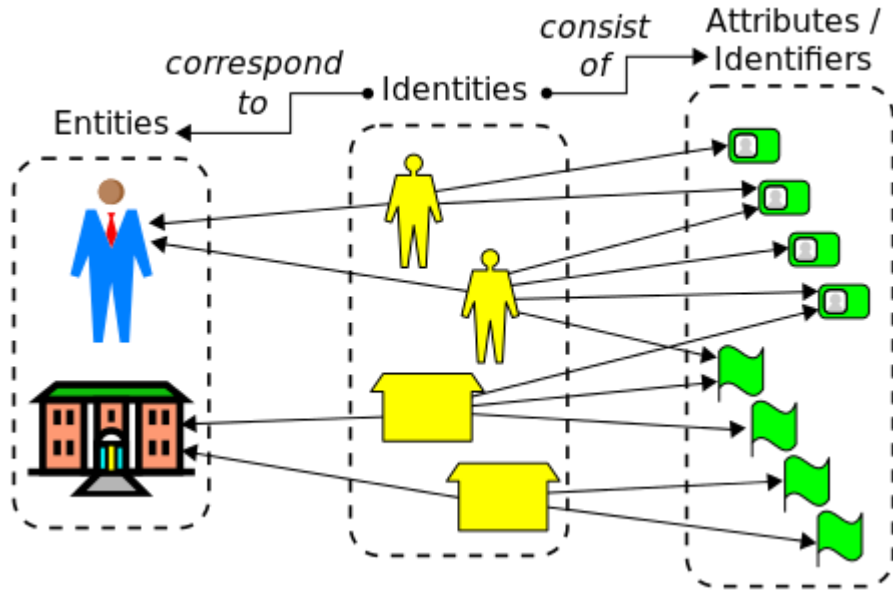


Fig. 3 http://mistaguy.com/wp-content/uploads/2014/08/security_authentication_authorization.png

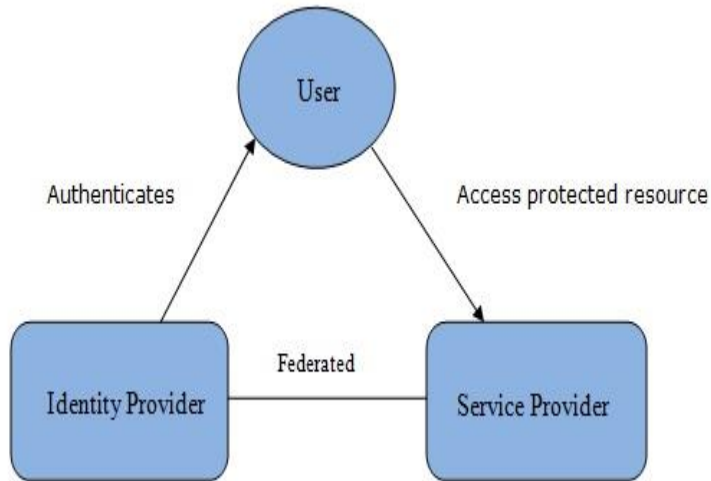
Identity management



To control information about users on computers. Such information includes information that authenticates the identity of a user, and information that describes information and actions they are authorized to access and/or perform

Fig. 4 <https://upload.wikimedia.org/wikipedia/commons/thumb/3/38/Identity-concept.svg/450px-Identity-concept.svg.png>

Identity Provider



An identity provider offers user authentication as a service.

Fig. 5 <https://blog.imaginea.com/wp-content/uploads/2013/05/saml1.jpg>

**How can we authenticate users?
(Indico as an example)**

Logon Passwords

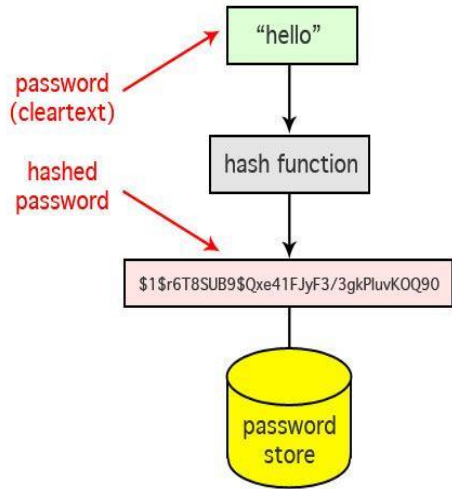
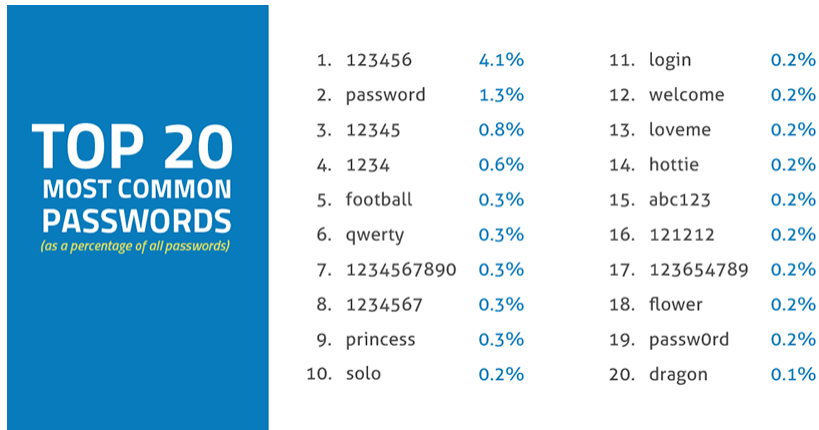


Fig. 6 <https://www.miracl.com/hs-fs/hub/230906/file-598871743-jpg/images/history-auth-2.jpg>

In this case Indico is the Identity Provider

Problems with passwords



- **Unique passwords for every account**
- **Users have to change passwords frequently**
- **Passwords can't be easy to guess (avoiding dictionary attacks)**

Fig. 7 <https://uploads.skyhighnetworks.com/2015/07/09195038/blog-image-top-passwords-850.png>

Flask-Multipass

Flask-Multipass is an extension that provides a user authentication system for Flask which can use multiple backends (such as local users, LDAP and OAuth) simultaneously.

LDAP as Identity Provider

```
cern_ldap_config = {  
    ... 'uri': 'ldaps://cerndc.cern.ch',  
    ... 'bind_dn': 'cn=indicodew,OU=Users,OU=Organic Units,DC=cern,DC=ch',  
    ... 'bind_password': '__password__',  
    ... 'timeout': 30,  
    ... 'verify_cert': False,  
    ... 'page_size': 1500,  
  
    ... 'uid': 'cn',  
    ... 'user_base': 'DC=cern,DC=ch',  
    ... 'user_filter': '(objectCategory=user)',  
  
    ... 'gid': 'cn',  
    ... 'group_base': 'OU=Workgroups, DC=cern, DC=ch',  
    ... 'group_filter': '(objectCategory=group)',  
    ... 'member_of_attr': 'memberOf',  
    ... 'ad_group_style': True,  
}
```

LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet.

OAuth in Indico

```
DEBUG = True

_cern_oauth_config = {
    ... 'consumer_key': '__key__',
    ... 'consumer_secret': '__secret__',
    ... 'request_token_url': None,
    ... 'access_token_method': 'POST',
    ... 'access_token_url': 'https://oauth.web.cern.ch/OAuth/Token',
    ... 'authorize_url': 'https://oauth.web.cern.ch/OAuth/Authorize'
}
```

OAuth 2 is an authorization framework that enables applications to obtain limited access to user accounts on an HTTP service, such as Facebook, GitHub, and DigitalOcean. It works by delegating user authentication to the service that hosts the user account, and authorizing third-party applications to access the user account.

Authentication Providers

```
    }  
    AUTH_PROVIDERS = {  
        'cern-ldap': {  
            'type': 'ldap_cern',  
            'title': 'CERN LDAP',  
            'ldap': _cern_ldap_config,  
            'default': True  
        },  
        'cern-oauth': {  
            'type': 'oauth_cern',  
            'title': 'CERN OAuth',  
            'oauth': _cern_oauth_config,  
            'callback_uri': '/oauth/cern',  
            'user_info_endpoint': 'https://oauthresource.web.cern.ch/api/Me'  
        }  
    }  
}
```

```
IDENTITY_PROVIDERS = {
```




Fig. 8 <https://www.wpmayor.com/wp-content/uploads/wordpress-plugins2.jpg>

Easy to extend!
You can also use Github, Shibboleth and much,
much more!



Login with CERN LDAP

or change authentication provider

Static

Indico

or connect with

CERN OAuth

CERN OAuth (new)

GitHub

If you do not have an Indico account yet, you can [create one here](#).

[← Back](#)

```
class LocalAuthProvider(SQLAlchemyAuthProviderBase):
    ... identity_model = Identity
    ... provider_column = Identity.provider
    ... identifier_column = Identity.identifier

    ... def check_password(self, identity, password):
    ...     ... return identity.password == password

class LocalIdentityProvider(SQLAlchemyIdentityProviderBase):
    ... user_model = User
    ... identity_user_relationship = Identity.user
```

```
32
33 app.config.from_pyfile('example.cfg')
34 multipass.register_provider(LocalAuthProvider, 'example_local')
35 multipass.register_provider(LocalIdentityProvider, 'example_local')
36 multipass.init_app(app)
37 db.init_app(app)
38 with app.app_context():
39     ... db.create_all()
40     ... if not User.query.filter_by(name='Local Guinea Pig').count():
```

Thanks for your attention!

Questions?