Security of mobile health

MOBILE HEALTH CONGRESS
30.11.2016

Pablo d'Alcantara, Abrumet's Director

Smart phones are considered attractive platforms for healthcare

1) pervasiveness
2) computational capabilities
3) user-friendly interface
4) built-in sensors
5) availability
6) mobility
7) connectivity

Security threats

- Research shows that smart phones are vulnerable to security threats
- Target of malware
- Security attacks due to weakness in design
- Applications can have full access to the data
- Apps can communicate with other apps

mHealth Security Requirements

CIA :

- **Confidentiality** : assurance information is not made available or disclosed
- **Integrity** : assurance information has not been modified or destroyed
- **Availability** : usability & accessibility of information by an authorized party at anytime from anywhere

More mHealth Security

- **Audit Control**: record and examine the activities of the system
- **Effective User Authentication**: patient or physician identity check to access information
- **Access Control**: restricted access to some users (patient, physicians, nurses, pharmacist…)
- **Freshness of Health Data**: recent and accurate data
- **Patient Consent**: patient's permission

Traditional methods and concepts

- Encryption algorithm & standard
- Using public key
- Multi-level authentication system

mHealth Security Threats

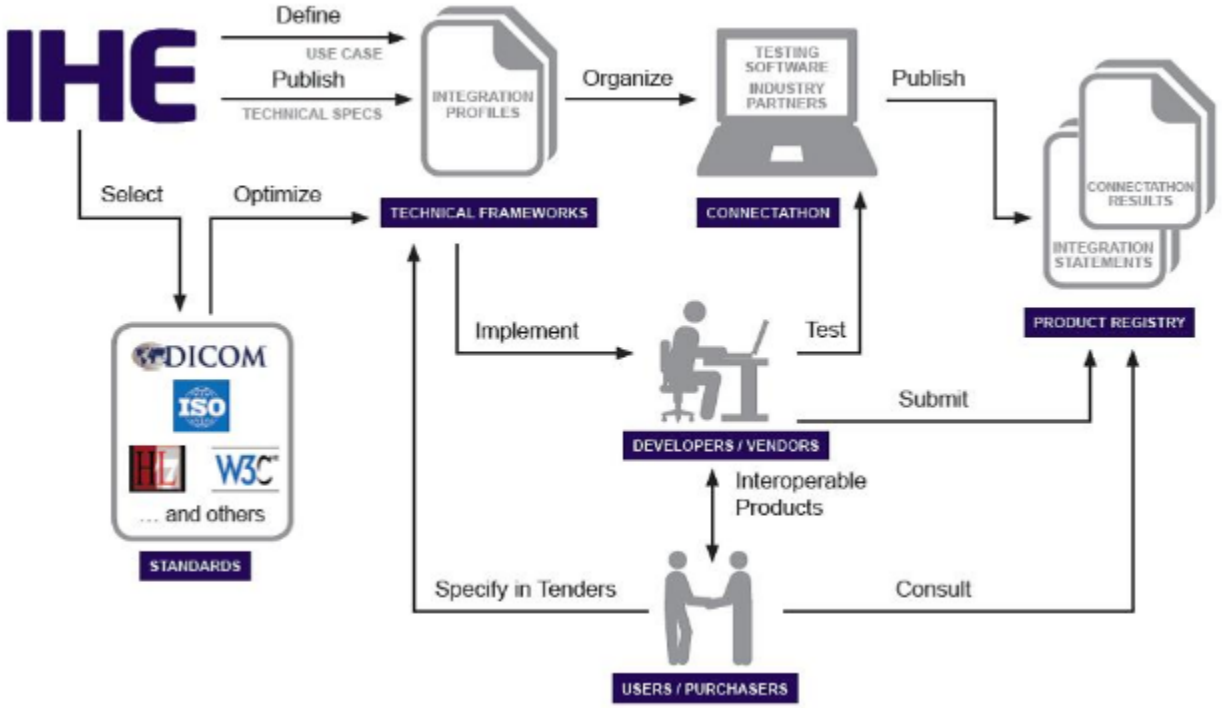
- **Malware Infections**:
  - use of social engineering techniques to install itself on a mobile device
  - can damage, alter or transfer the information
- **Application Developers**: poor implemented are open doors for hackers
- **Mobile Devices**: unauthorized usage after robbery

mHealth Security Threats (2)

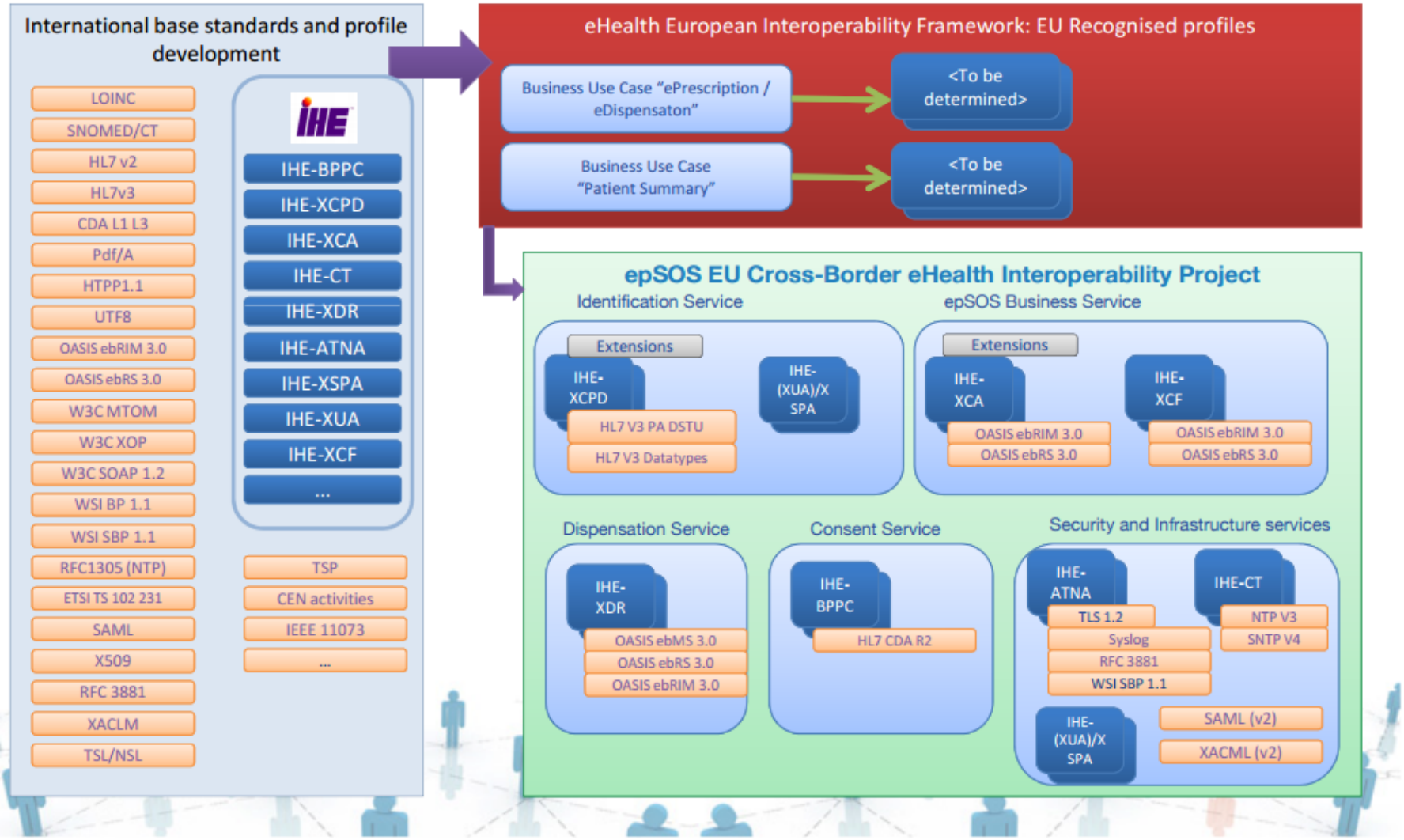
- **Human Users**:
  - share passwords with others
  - no password protection on phones
  - used of unknown networks
- **Health Insurance Companies**: advantage with access to health information
- **Data Intelligence Companies**: accumulate information to sell it

COUNTERMEASURES

- Use of IHE profiles

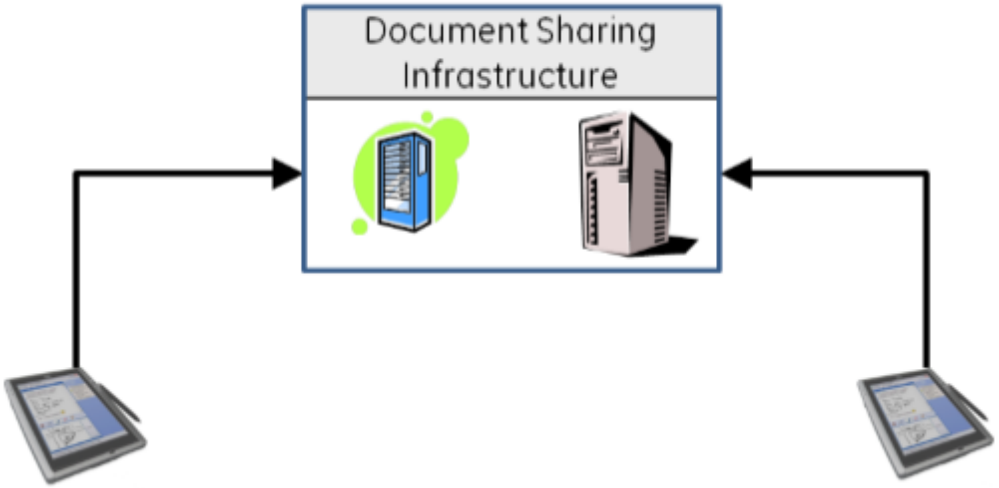


EU eHealth project:
Cross Border Patient Summary in Belgium



Mobile access to Health Documents (MHD)

- profile defines a simple HTTP interface to an XDS like environment
- simplified HTTP RESTful technology rather than the more robust technology used in XDS

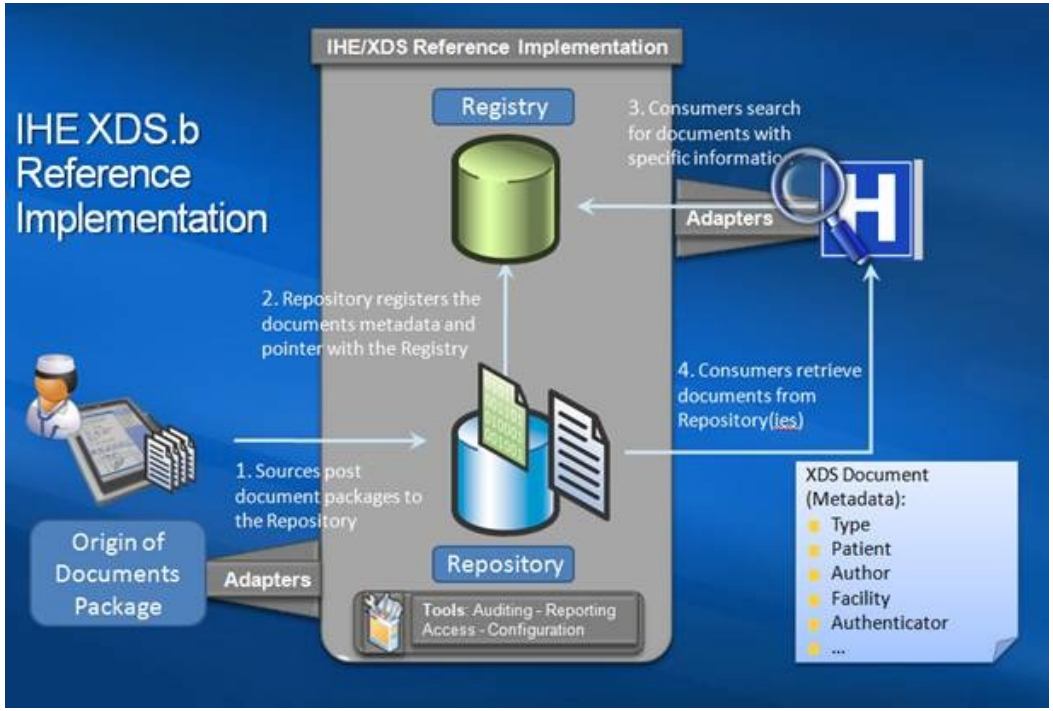


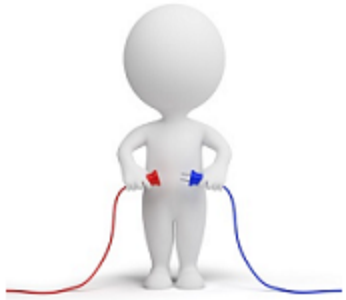
MHD defines transactions to

- submit a set of documents and metadata from the mobile device to a document receiver
- find the document submission set metadata based on query parameters
- find document entries containing metadata based on query parameters
- retrieve a copy of a specific document

MHD

- The MHD profile does not replace XDS
- Used to access an XDS health information exchange





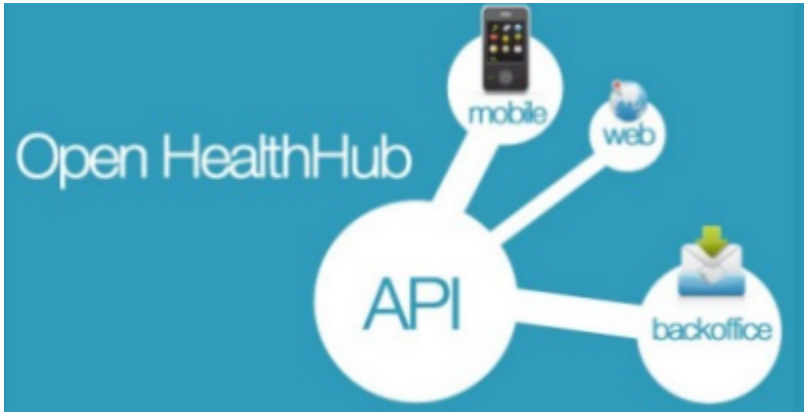
MHD

The MHD profile defines one standardized interface (API) to health documents for use by mobile devices so that deployment of mobile applications is more consistent and reusable

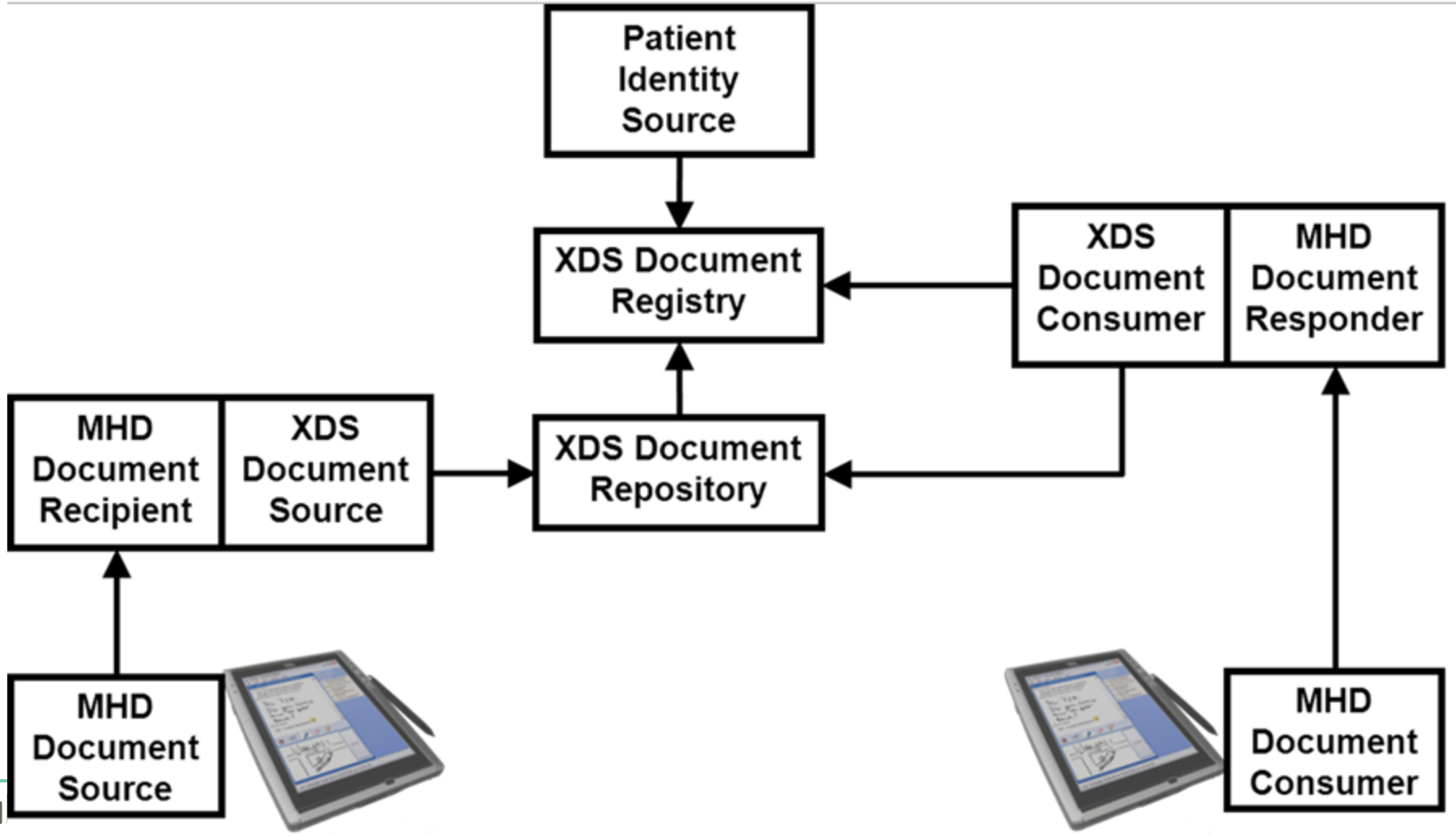
- mobile resources are constrained :
  - has a simple programming environment (e.g., JSON, javascript)
  - simple network stack (e.g., HTTP)
  - simple display functionality (e.g., HTML browser).

MHD

- Goal is to limit the additional libraries that are necessary to process
  - SOAP
  - WSSE
  - MIME-Multipart
  - MTOM/XOP
  - ebRIM
  - multi-depth XML



The MHD Profile enables many deployment models



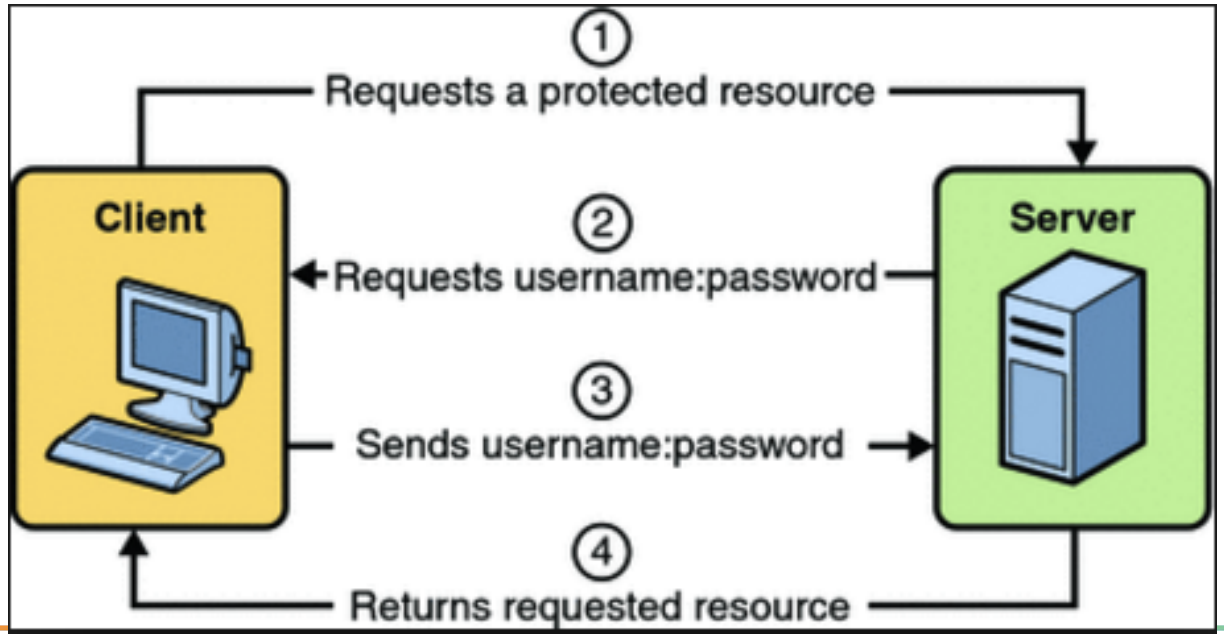
MHD Security Considerations

Many reasonable methods of securing interoperability transactions:

- use of TLS is encouraged
- use of the Audit Trail and Node Authentication (ATNA) profile (Security Audit logging)
- OAuth2 with OpenID Connect

Traditional client-server authentication

- Apps store resource owner's credentials, typically a password
- Servers have to support password authentication, despite the security weaknesses



Traditional client-server authentication

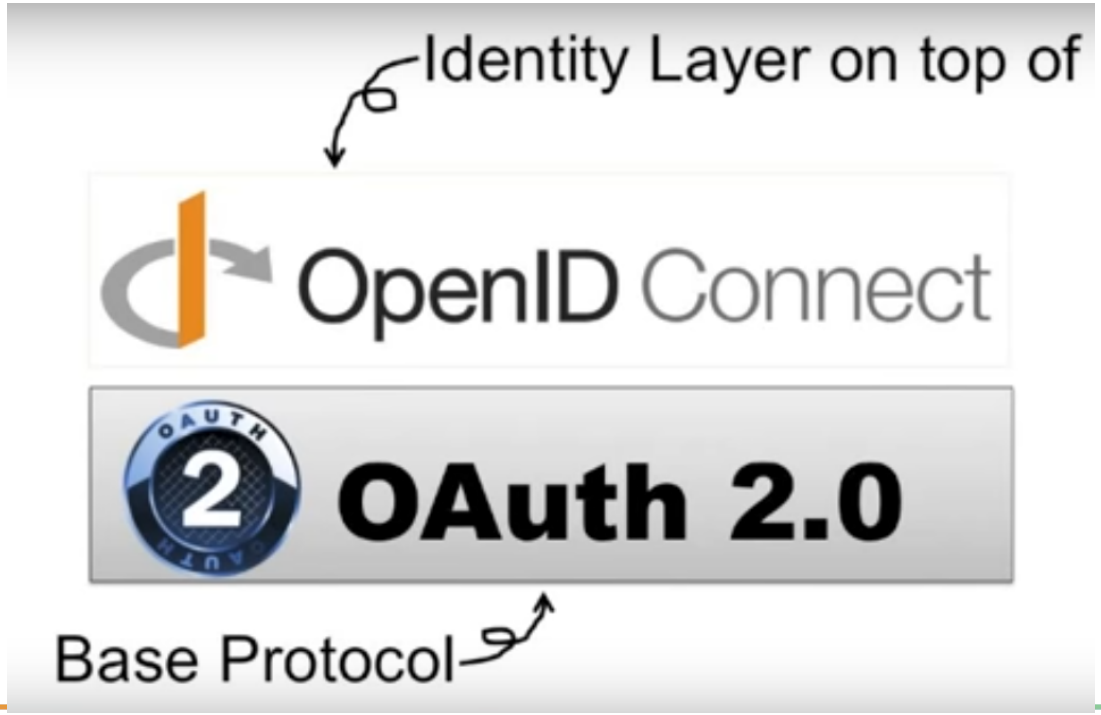
- No ability to restrict duration or access to a limited subset of resources
- Cannot revoke access to an individual apps without revoking access to all apps, and must change the apps password

OAuth2 protocol

- OAuth2 is an open standard for authorization without password
- OAuth2 enables an application to obtain limited access to an HTTP service
- OAuth2 allows access tokens to be issued to apps by an authorization server
- The app then uses the access token to access the resource server
- OAuth 2.0 is not authentication (see TLS)

OpenID Connect (OIDC)

- OpenID Connect (OIDC) is an authentication layer on top of OAuth 2.0



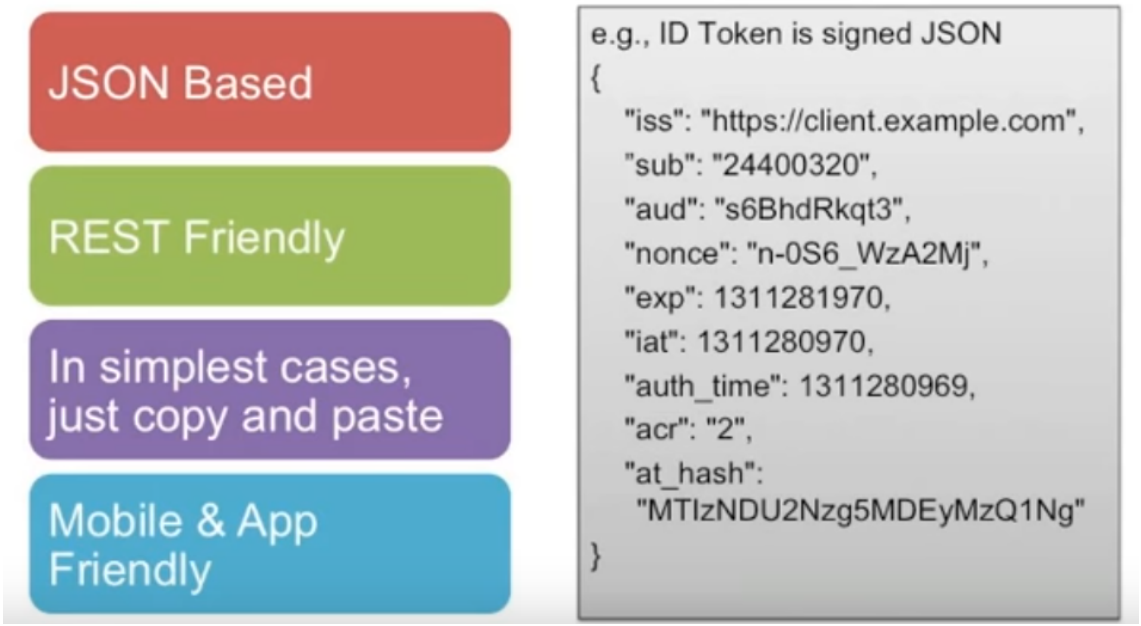
OpenID Connect (OIDC)

- Allows computing clients to verify the identity of an end-user

Identity = set of attributes related to an entity [iso 29115]

OpenID Connect (OIDC)

- OpenID Connect specifies a RESTful HTTP API, using JSON as a data format



OpenID Connect (OIDC)

- The OAuth2 vulnerability is phishing -> two-factor authentication

Two-factor authentication

- username / password
- SMS and/or email

Thank you for your attention

With the support of

GOUVERNEMENT DE LA RÉGION DE BRUXELLES-CAPITALE
BRUSSELSE HOOFDSTEDELIJKE REGERING
GOVERNMENT OF THE BRUSSELS CAPITAL-REGION

lifetech.brussels
by impulse.brussels