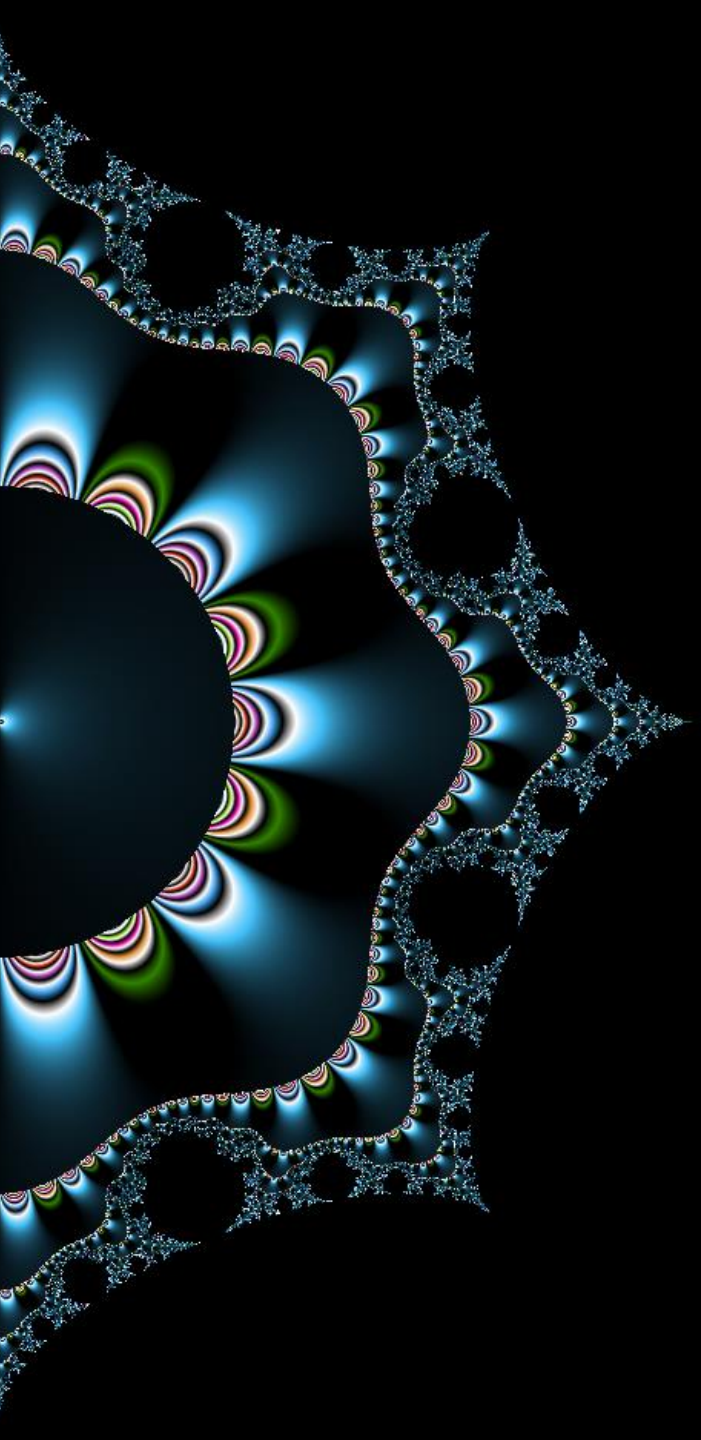


Annuaires
Et contrôle d'accès

Thibaut HENIN

tbowan@arsouyes.org

Annuaire

Fournisseurs d’identités

(oauth, openid, kerberos, ldap, ...)

IAM

Identity and Account Management

(gestion des identités et des comptes)

Principes

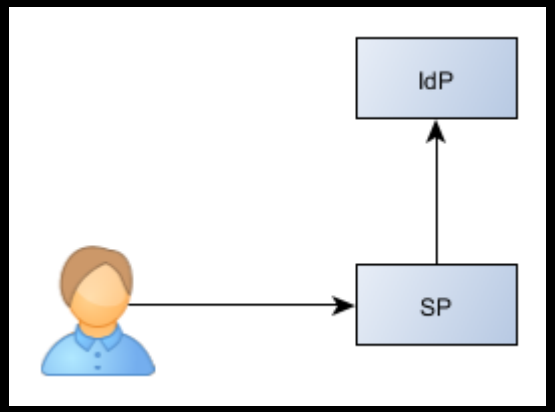
Fournisseur de Service

SP « Service Provider »

Fournisseur d’identité

IdP « Identity Provider »

Délégation



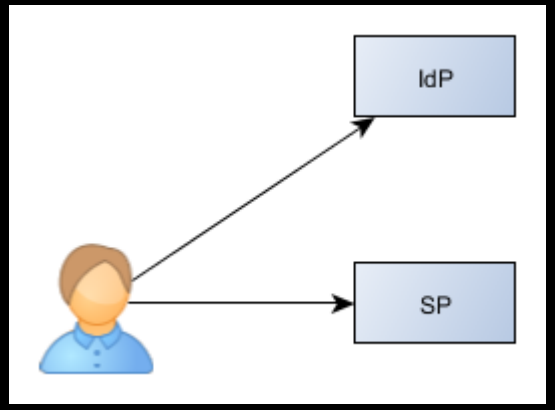
Base de donnée

.htpasswd, PHP + mySQL

Annuaires

LDAP, Active Directory

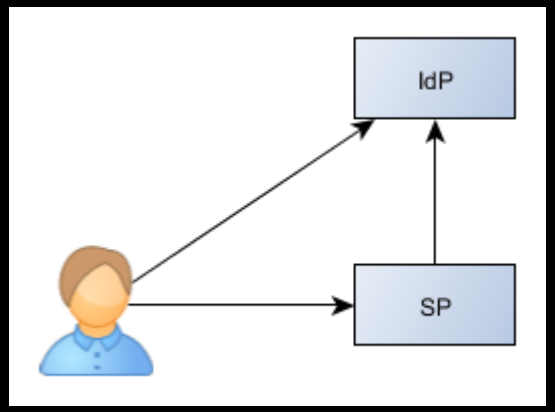
Jeton et assertions



Kerberos

SAML

Principe

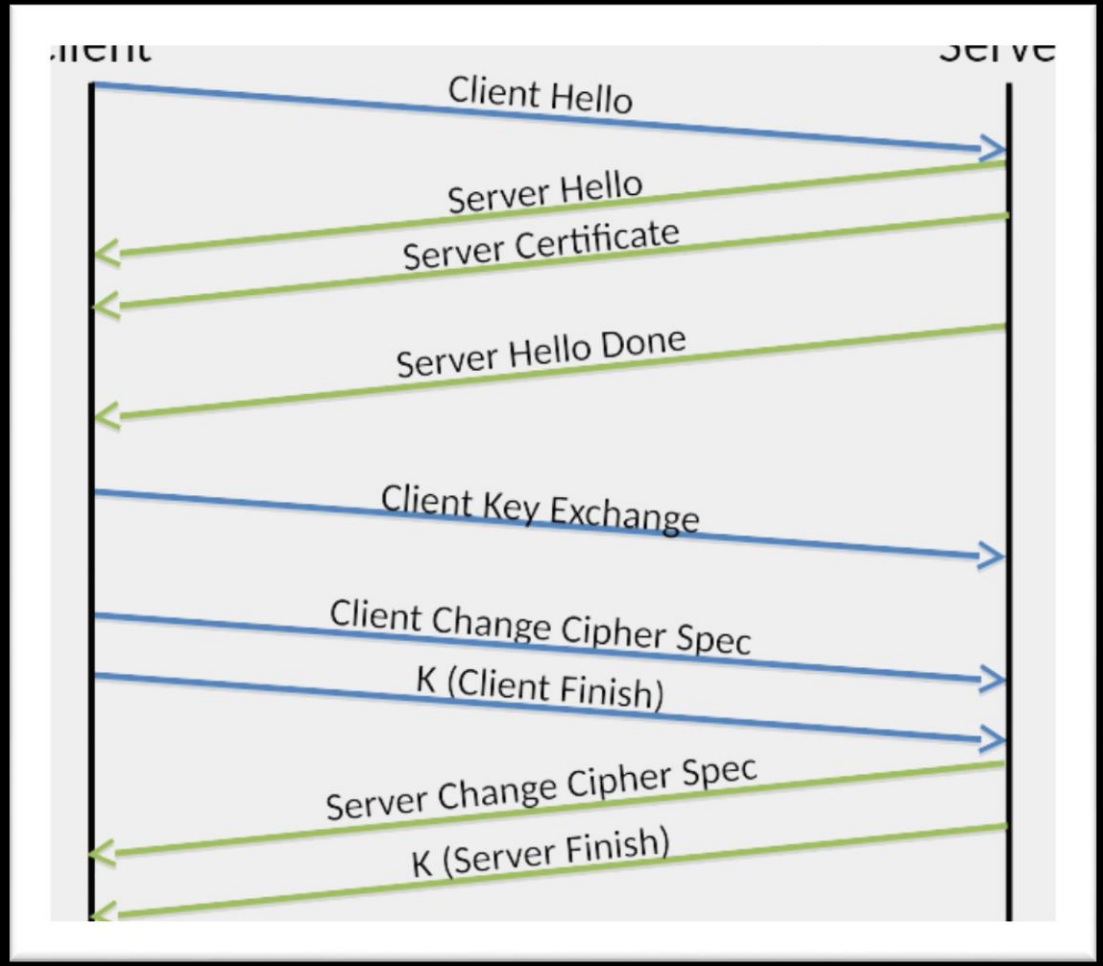


- Oauth
- OpenID
- Tiers de paiement en ligne

Authentification cryptographique

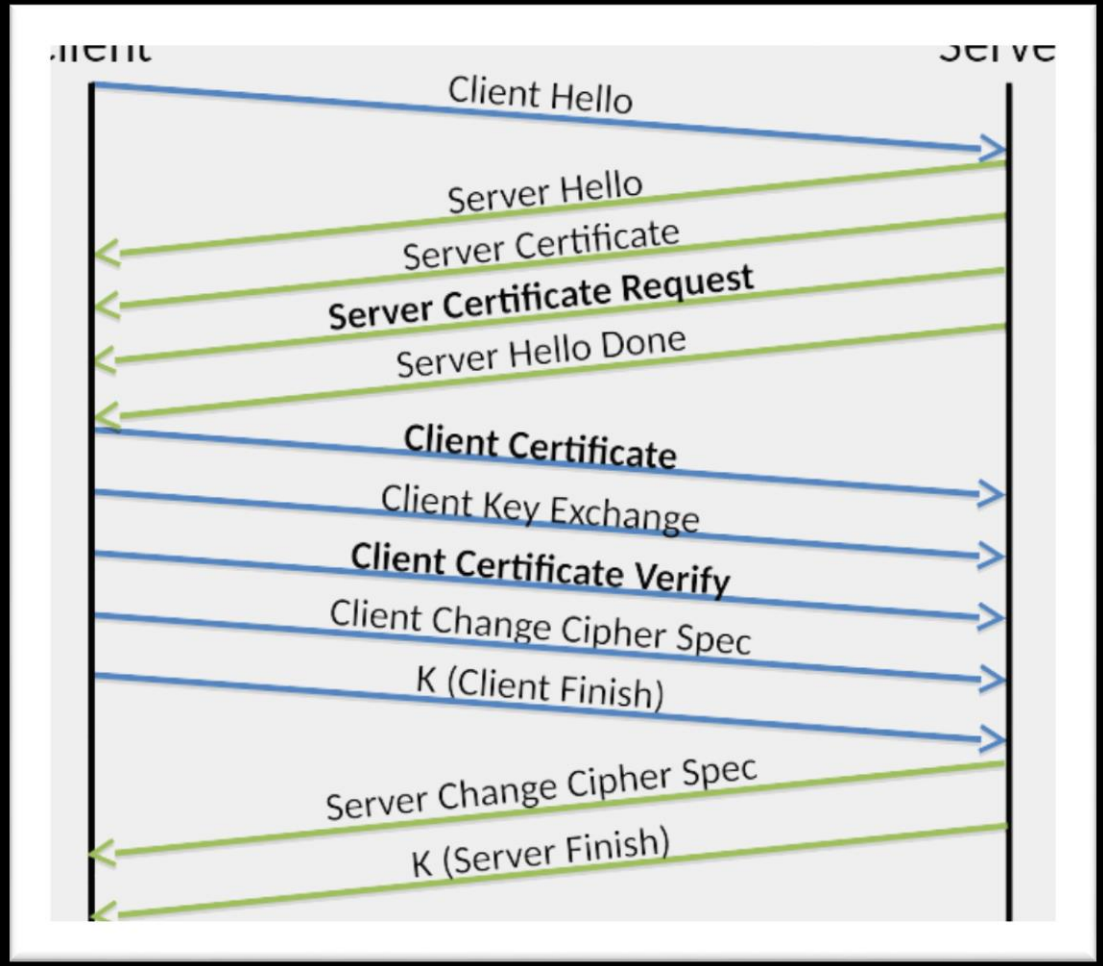
SSL/TLS, SAML, JWT

SSL/TLS : serveur



Source : http://www.allanbank.com/blog/security/tls/x.509/2014/10/13/tls-x509-and-mongodb/

SSL/TLS : mutuelle



Source : http://www.allanbank.com/blog/security/tls/x.509/2014/10/13/tls-x509-and-mongodb/

Signature des requêtes

SAML

Security assertion markup language

JWT

Json Web Token

Exemple SAML

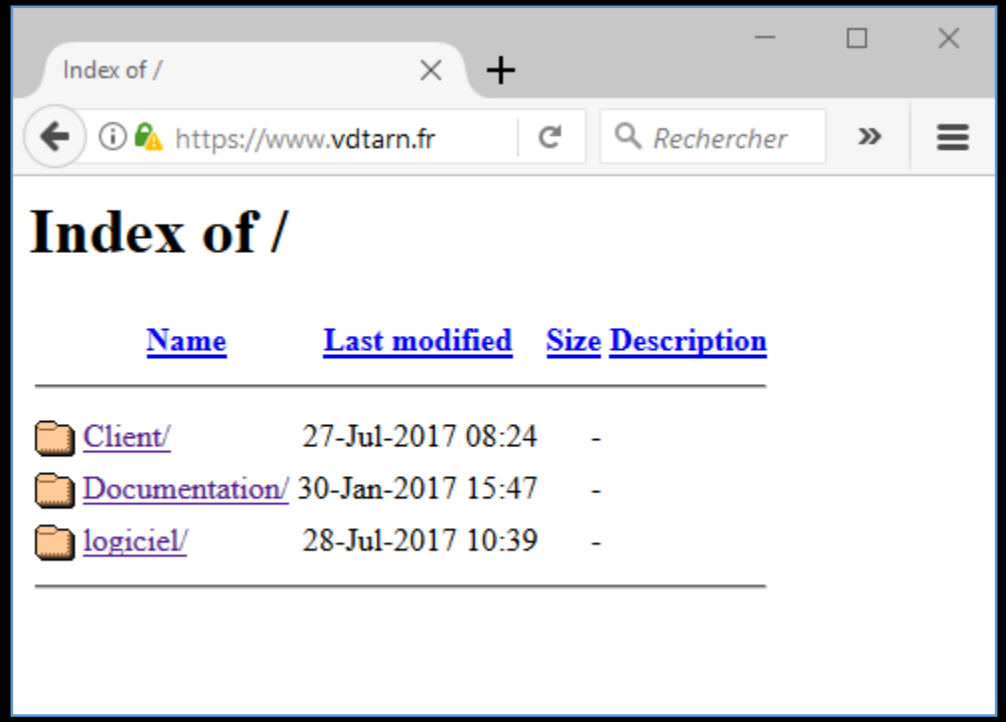
```
<samlp:Response ...>
  <saml:Issuer>http://idp.example.com/metadata.php</saml:Issuer>
  <samlp:Status>...</samlp:Status>
  <saml:Assertion ID="pfxcaa3deda-f4a7-863c-5d83-b714652c352c" ...>
    <saml:Issuer>http://idp.example.com/metadata.php</saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <ds:Reference URI="#pfxcaa3deda-f4a7-863c-5d83-b714652c352c">...</ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>TYGJ1Z8+jGNpQuRcNAWTbk2.........En8IYtAUjsrSVsr4=</ds:SignatureValue>
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>MIICajCCAdOgAwIBAgIBAD........Gyc4LzgD0CROMASTWNg==</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </ds:Signature>
    <saml:Subject>...</saml:Subject>
    <saml:AuthnStatement ...>...</saml:AuthnStatement>
    <saml:AttributeStatement>
      <saml:Attribute Name="uid" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">test</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="mail" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">test@example.com</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="eduPersonAffiliation" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">users</saml:AttributeValue>
        <saml:AttributeValue xsi:type="xs:string">examplerole1</saml:AttributeValue>
      </saml:Attribute>
    </saml:AttributeStatement>
  </saml:Assertion>
</samlp:Response>
```

Echec de Contrôle d’accès

Directory listing, Direct access (url, id, ...), Fopen

Directory listing

```
<VirtualHost *:80>

  ServerName  intranet.example.com

  Options +Indexes

</VirtualHost>
```



Insecure Direct Object Reference

```
$ wget http://intranet.example.com/upload/secret.pem

$ wget http://api.example.com/Keys/1f5d6s2d1
```

Fopen / Path traversal

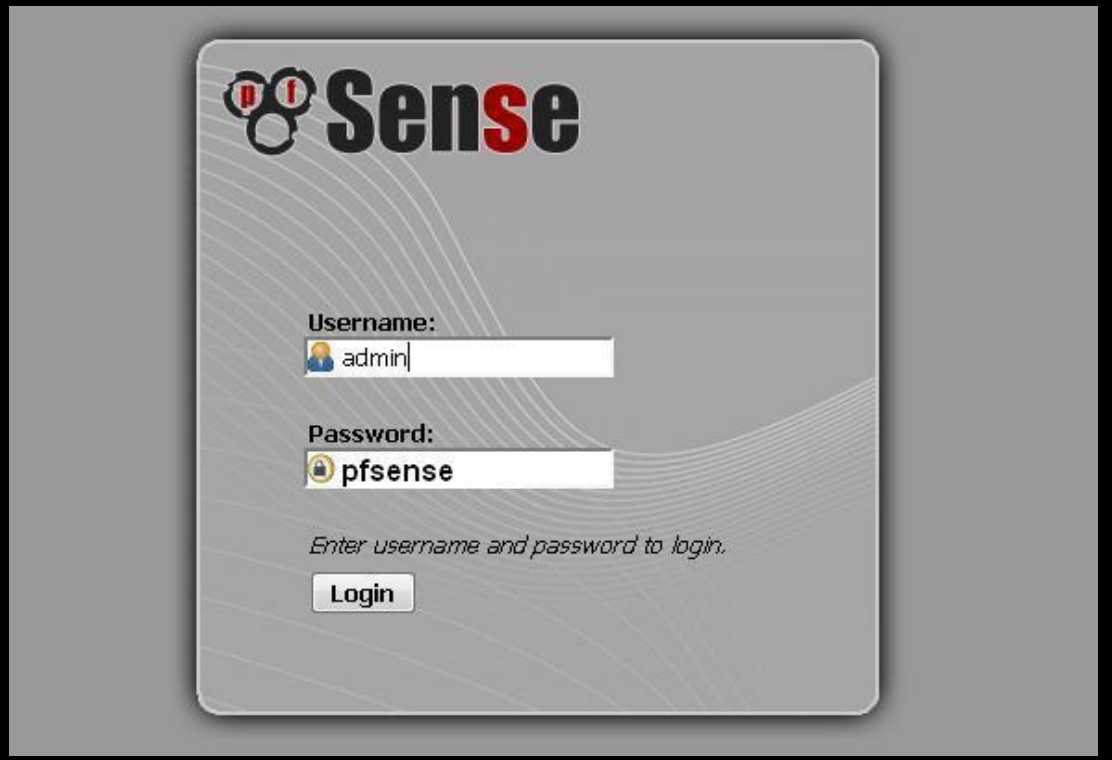
```php
<?php

$file = "./some/dir/to/" . $_GET["file"] ;
$fp   = fopen($file) ;
$data = fread($fp, filesize($file)) ;
fclose($data) ;
echo $data ;

// readfile, file, file_get_contents, …
```

Featured Backdoors

Mode debug

```php
<?php

$debug = isset($_GET["debug"]) ;
$user  = $_SESSION["user"] ;

if ($user->isAdmin() || $debug ) {

  do_admin_stuff($_GET, $_POST) ;

}
```

Compte admin



Role Based Access Control

Contrôle d’accès à base de rôles

Utilisateurs / Subjects

Qui est contrôlé

« thibaut HENIN »

Droits / Permissions

Ce qui est contrôlé

« ajouter un utilisateur »

Groupes / Roles

Ensemble de droits

« créer un utilisateur », …

Ensemble de personnes

« Thibaut HENIN », …

Variante Hiérarchique

Héritage entre les rôles

Administrateurs sont des utilisateurs

Variante Contrainte

Un seul rôle a la fois

Choix du rôle à la connexion

Principe du moindre privilège

Droits minimums

(pour chaque groupe)

Groupes minimums

(pour chaque utilisateur)