M2 Miage

Gestion des Identités et des Accès

Damien Ploix
Université d'Evry Val d'Essonne

Plan

- Introduction
- Autorisation
- Authentification / Identification
  - Automatisés (Certificats)
  - Modèles de SSO

Authentification / Identification exigences

Authentification de l'utilisateur ou de l'entité demandant un accès (à un réseau local ou à une application)		***libelle cours***
Y a-t-il un mécanisme d'authentification de chaque utilisateur avant tout accès à une ressource du réseau local ou une application ?		authentification systématique
Le processus de définition ou de modification de l'authentifiant supportant le contrôle d'accès pour les accès internes vérifie-t-il le respect d'un ensemble de règles permettant d'avoir confiance dans sa solidité intrinsèque ? *Dans le cas de mots de passe : longueur suffisante (8 caractères ou +), mélange obligatoire de types de caractères, changement fréquent (<1 mois), impossibilité de réemployer un mot de passe ancien, test de non trivialité fait en relation avec un dictionnaire, interdiction des "standards systèmes", des prénoms, de l'anagramme de l'identifiant, de dates, etc.* *Dans le cas de certificats ou d'authentification reposant sur des mécanismes cryptologiques, processus de génération évalué ou reconnu publiquement, clés de chiffrement de longueur suffisante, etc.*		authentifiant fonctionnel unique, mot de passe fort certificat fort
Tout identifiant reconnu par les applications correspond-il à une personne physique unique et identifiable, directement ou indirectement ? *Nota : Dans le cas où une application en appelle une autre ou déclenche un appel système, il se peut que l'application ne transfère pas au système cible l'identifiant ayant initialisé la demande. Le lien entre cet appel et l'identifiant et la personne d'origine doit cependant rester possible a posteriori.*		tout identifiant correspond à une personne physique

Authentification / Identification exigences

Authentification de l'utilisateur ou de l'entité demandant un accès (à un réseau local ou à une application)		***libelle cours***
Le processus de présentation par l'utilisateur de son authentifiant garantit-il son inviolabilité ? *La frappe d'un mot de passe sera toujours un point faible notable. Les seuls processus qui soient observables sans divulguer d'information consistent soit à introduire un objet contenant un secret (carte à puce), soit à frapper un code qui change à chaque instant (jeton d'authentification), soit à présenter un caractère biométrique.*		saisie mot de passe
La conservation et l'utilisation par les équipements de sécurité d'éléments de référence supportant l'authentification (mots de passe, numéro d'appelant, etc.) font-elles appel à des mécanismes qui en garantissent l'inviolabilité et l'authenticité ? *Dans le cas de mots de passe, ils doivent être stockés chiffrés et un contrôle d'accès préliminaire à l'utilisation de ces éléments par l'utilisateur doit être effectué.* *Dans le cas d'authentification faisant appel à des procédés cryptologiques, le mécanisme doit présenter des garanties de solidité validées par un organisme de référence*		protection mot de passe
La transmission entre le poste appelant et les équipements de sécurité d'éléments de référence supportant l'authentification (mots de passe, numéro d'appelant, etc.) fait-elle appel à des mécanismes qui en garantissent l'inviolabilité et l'authenticité ? *La transmission d'un mot de passe doit être chiffrée ou utiliser un algorithme qui introduise un aléa à chaque transmission.* *Dans le cas d'authentification faisant appel à des procédés cryptologiques, le mécanisme doit présenter des garanties de solidité validées par un organisme de référence.*		transport mot de passe

Authentification / Identification exigences

Authentification de l'utilisateur ou de l'entité demandant un accès (à un réseau local ou à une application)		***libelle cours***
A-t-on mis en place une dévalidation automatique de l'utilisateur appelant, en cas de tentatives multiples infructueuses, avec nécessité d'intervention de l'administrateur pour revalider le poste ou l'utilisateur ?		dévalidation mot de passe
La procédure permettant de redonner un authentifiant à un utilisateur qui a perdu le sien (mot de passe, jeton d'authentification, etc.) permet-elle de neutraliser instantanément l'ancien authentifiant ?		neutralisation du mot de passe changé
La procédure permettant de redonner un authentifiant à un utilisateur qui a perdu le sien (mot de passe, jeton d'authentification, etc.) permet-elle un contrôle effectif de l'identité du demandeur ?		contrôle identité lors du changement mdp
Les processus qui assurent l'authentification sont-ils sous contrôle strict ? *Un contrôle strict requiert que le logiciel correspondant ait été validé et subisse régulièrement un test d'intégrité (sceau) et qu'il existe un audit au moins annuel des procédures et processus de l'authentification.*		audit des procédures et processus d'authentification

Authentification / Identification exigences

Authentification de l'utilisateur ou de l'entité demandant un accès (à un réseau local ou à une application)		***libelle cours***
Les paramètres de l'authentification sont-ils sous contrôle strict ? *Un contrôle strict requiert que la liste des personnes habilitées à changer les règles de définition des authentifiants, les authentifiants eux-mêmes, les règles de surveillance des tentatives de connexion, etc. soit très limitée, qu'il existe un contrôle d'accès renforcé pour procéder à ces modifications, que les modifications soient journalisées et auditées et qu'il existe un audit général au moins annuel de l'ensemble des paramètres de l'authentification.*		contrôle des authentifications (log)
Tous les comptes génériques ou par défaut ont-ils été supprimés ?		comptes génériques supprimés
L'acceptation de l'identifiant par le système est-elle systématiquement sujette à une authentification ? *L'authentification systématique requiert que ce processus soit effectivement mis en oeuvre pour l'ensemble des sous-systèmes (moniteur de télétraitement, SGBD, traitements par lots, etc.) et pour toutes les demandes d'accès en provenance des applications ainsi que pour toutes les voies et ports d'accès, y compris depuis des ports réservés tels que la télémaintenance éventuelle.*		contrôle des accès techniques

Authentification / Identification exigences

Authentification de l'utilisateur ou de l'entité demandant un accès (à un réseau local ou à une application)		***libelle cours***
Y a-t-il une répétition de la procédure d'authentification en cours de session pour les transactions jugées sensibles ?		contrôles multiples
Y a-t-il une dévalidation automatique de la session de l'utilisateur, en cas d'absence d'échange pendant un délai défini, nécessitant une nouvelle identification - authentification ?		timeout de session
Utilise-t-on des contrôles d'accès applicatifs permettant de limiter la visibilité et l'accès aux informations les plus sensibles ?		contrôles renforcés pour les données sensibles
Y a-t-il un contrôle systématique du profil du demandeur, de son contexte et de l'adéquation de ce profil et du contexte avec l'accès demandé, en fonction de règles de contrôle d'accès formalisées ?		contrôle du profile correspondant à l'accès
Les paramètres de définition et de gestion des règles de filtrage des accès sont-ils sous contrôle strict ? *Un contrôle strict requiert que la liste des personnes habilitées à changer les paramètres de sécurité du filtrage des accès soit très limitée, qu'il existe un contrôle d'accès renforcé pour pouvoir les modifier, et que les modifications soient journalisées et auditées.*		contrôle et audit des actions de sécurité

(reprise du) Fil conducteur

libelle cours	***Type d'action***
authentification systématique	P/T
authentifiant fonctionnel unique	P/T
mot de passe fort	P/T
certificat fort	P/T
tout identifiant correspond à une personne physique	P/T
saisie mot de passe	T
protection mot de passe	T
transport mot de passe	T
dévalidation mot de passe	P/T
neutralisation du mot de passe changé	P/T
contrôle identité lors du changement mdp	P
audit des procédures et processus d'authentification	P
contrôle des authentifications (log)	P/T
comptes génériques supprimés	P/T
contrôle des accès techniques	P/T
contrôles multiples	P
timeout de session	T
contrôles renforcés pour les données sensibles	P
contrôle du profile correspondant à l'accès	P
contrôle et audit des actions de sécurité	P/T

Plan

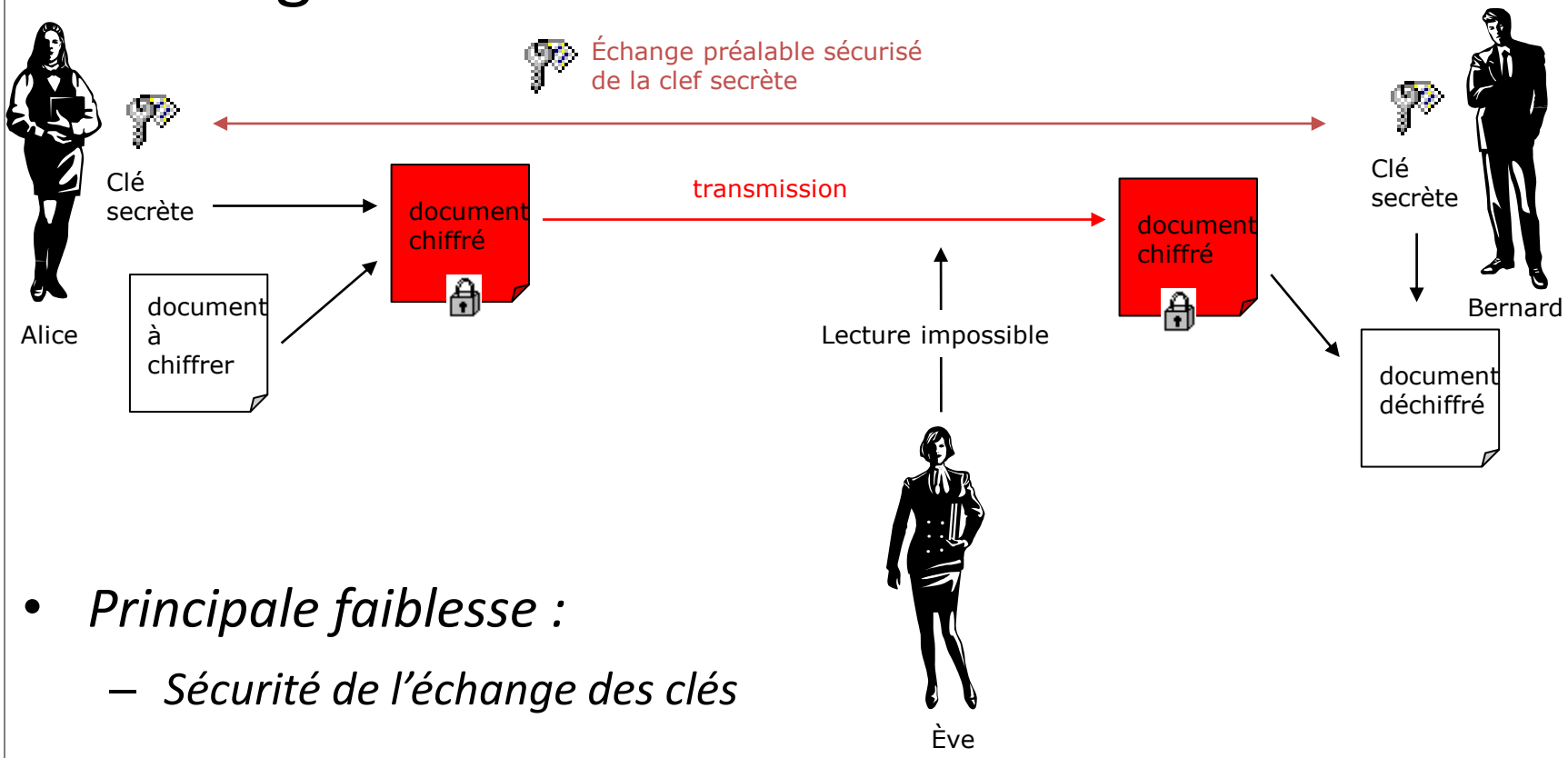
- Introduction
- Autorisation
- Authentification / Identification
  - Certificats
    - Identification des composants / personnes
    - Protection des communications
    - Échanges de données Informatiques (EDI)
  - Modèles de SSO

Authentification
Le chiffrement

- Problématique :
  - transmission de message secret entre deux partenaires dans un milieu ouvert (public) : avoir la certitude que seul le destinataire voulu est en capacité de lire le message.
  - Longue histoire…
- À la base de la confiance dans les échanges numériques.
  - Basé sur le principe de la cryptographie via une clef qui seule permet de comprendre le message;
  - Les types d'échanges de clés :
    - Clefs secrète partagées
    - Clefs privées / publiques

le chiffrement à clé partagée

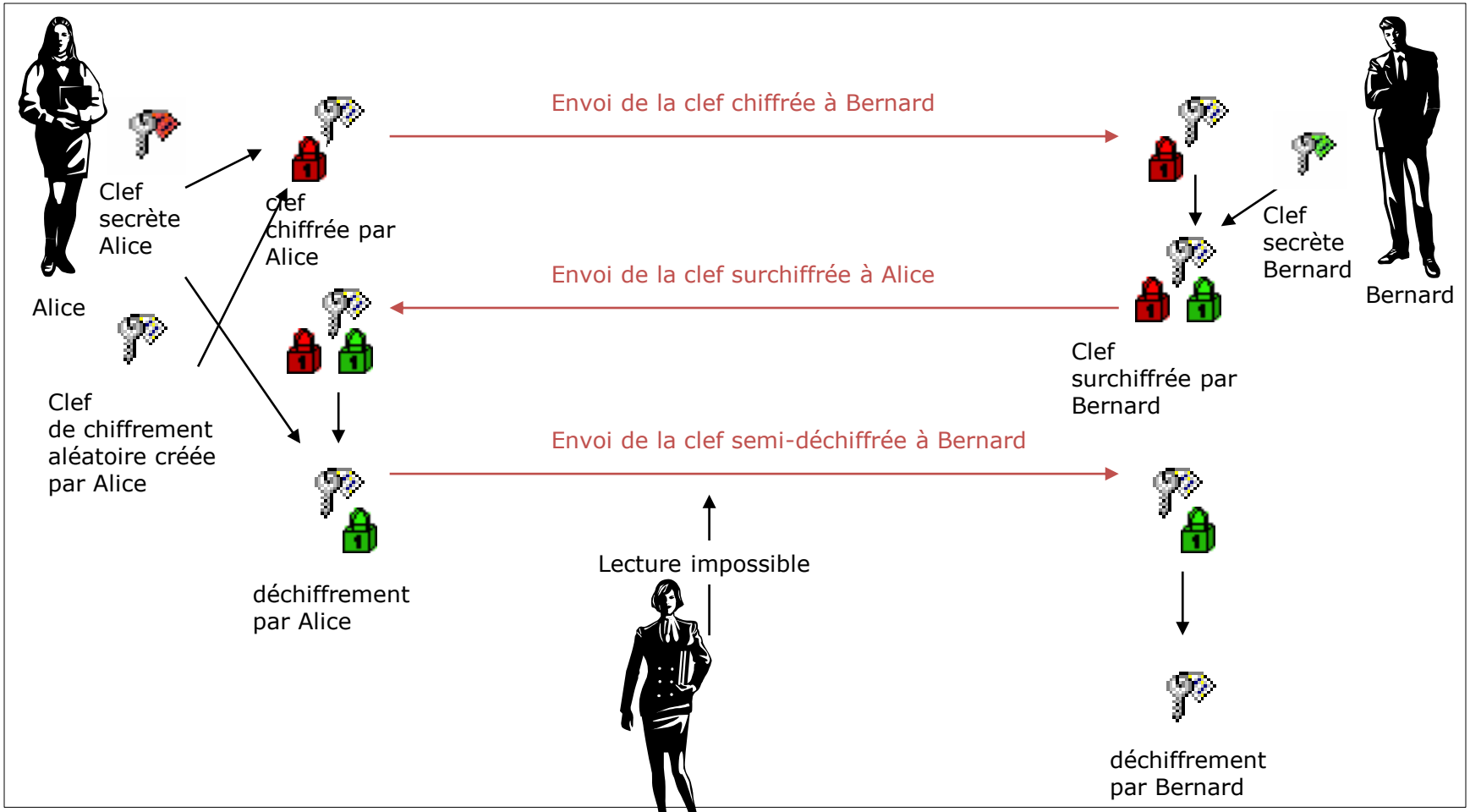
- Échanges à base de clé secrète



- *Principale faiblesse :*
  - *Sécurité de l'échange des clés*

Chiffrement à clés partagées

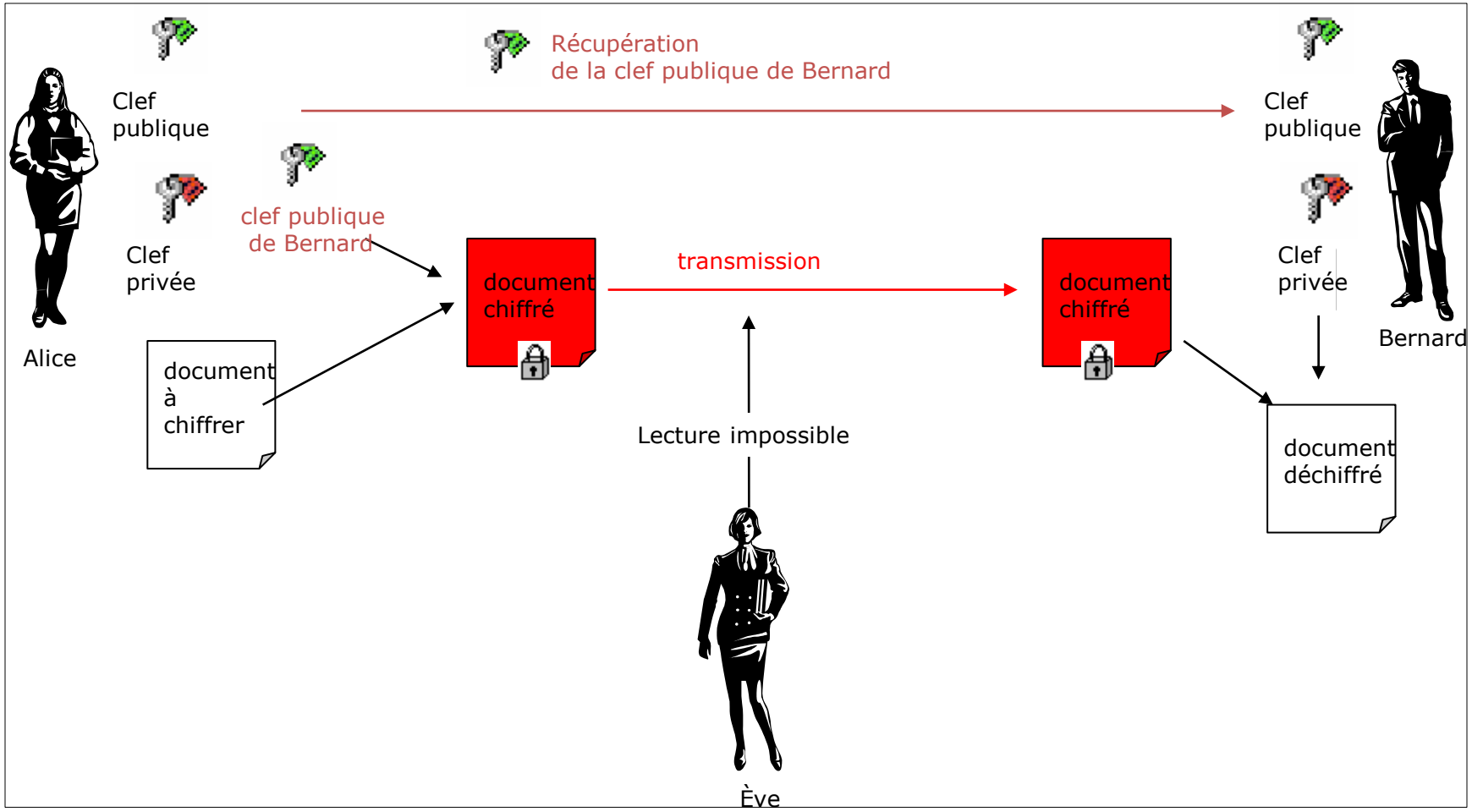
Diffie Hellman : échange d'une clé secrète



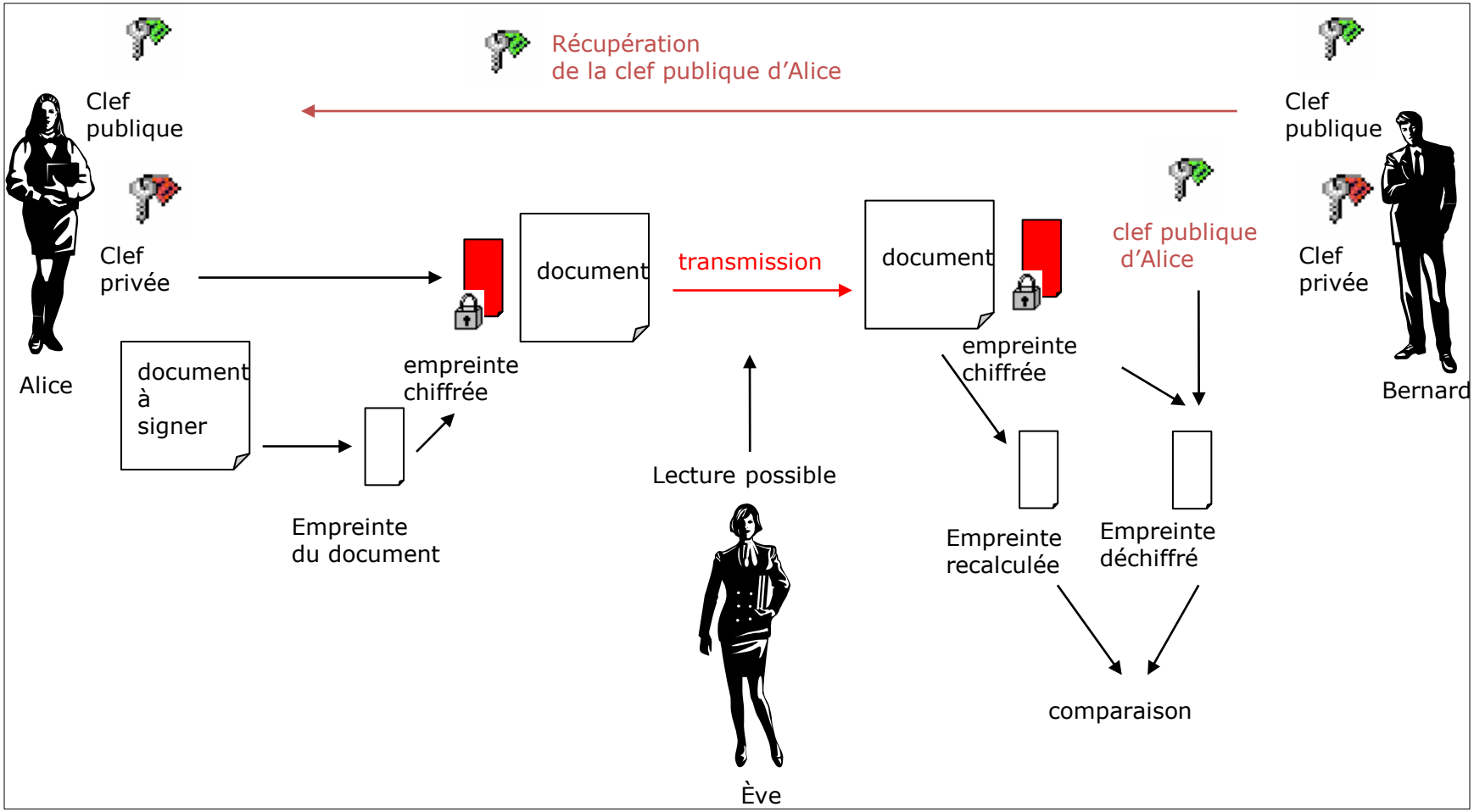
Le chiffrement à clés asymétriques

- Principe général :
  - Une clef publique, une clef privée.
  - Un message chiffre avec l'une des clefs ne peut être déchiffré qu'avec l'autre clef.
- Deux utilisations possibles :
  - Confidentialité (chiffrement avec la clef publique, déchiffrement avec la clef privée)
  - Signature (chiffrement avec la clef privée, déchiffrement avec la clef publique)

Le chiffrement à clés asymétriques

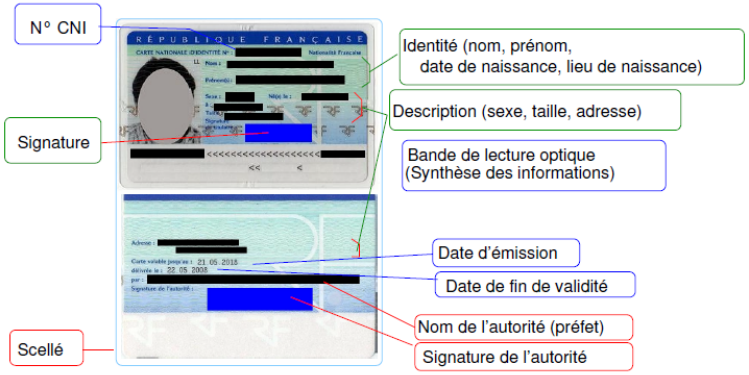


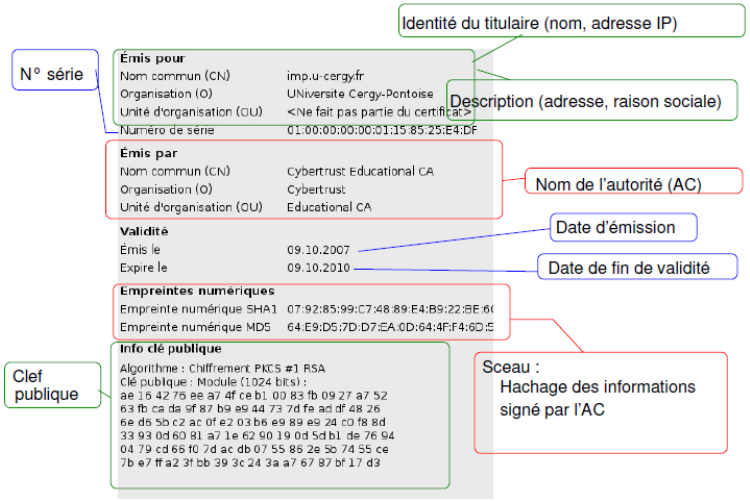
Le chiffrement à clés asymétriques
signature de documents



Certificat

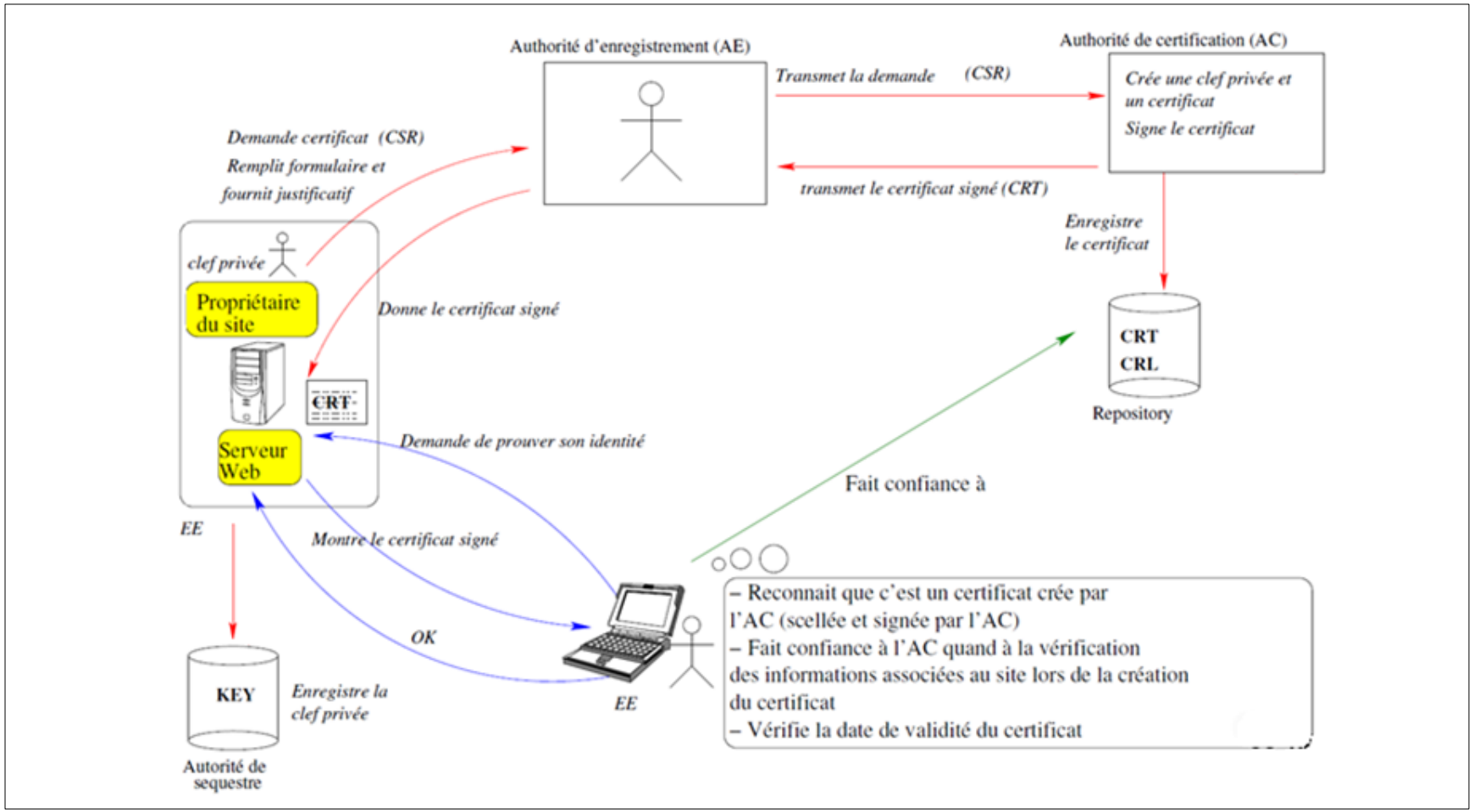
- Analogie CNI / X509





- Les systèmes à clés publiques certifiées ont pour but de délivrer des certificats numériques via des AC qui offrent les garanties suivantes lors des transactions électroniques :
  - **confidentialité** : seul le destinataire légitime du message pourra le lire
  - **authentification** : l'identité de l'émetteur est garantie (par l'AC)
  - **intégrité** : Garantie qu'un message expédie n'a pas été altéré, accidentellement ou intentionnellement ;
  - **non-répudiation** : l'auteur du message ne peut pas renier son message.

PKI (Public Key Infrastructure) / IGC (Infrastructure de Gestion de Clef)



PKI (Public Key Infrastructure) / IGC (Infrastructure de Gestion de Clef)

- **L'entité finale** (EE : End Entity) : L'utilisateur ou le système fait la demande d'un certificat
- **L'autorité d'enregistrement** (AE/RA) : effectue les vérifications d'usage sur l'identité de l'utilisateur. Fait la demande de certificat et donne le certificat signé à l'utilisateur.
- **L'autorité de certification** (AC/CA) : signe les demandes de certificat (CSR) et les listes de révocation (CRL)
- **L'autorité de dépôt** (Repository) : stocke les certificats numériques et les listes de révocation (CRL).
- **L'autorité de séquestre** (Key Escrow) : stocke de façon sécurisée les clés de chiffrement qui ont été générées par l'IGC, pour pouvoir les restaurer le cas échéant.

Autorité d'enregistrement (AE) et Classe de certificat

1. L'AE verie l'identite de l'utilisateur : 4 classes de certificats en fonction des verifications effectuées auprès de l'autorité d'enregistrement :
   - classe 1 : adresse e-mail du demandeur requise ;
   - classe 2 : preuve de l'identité requise (photocopie de carte d'identité par exemple) ;
   - classe 3 : présentation physique du demandeur obligatoire.
   - classe 3+ : identique a la classe 3, mais le certificat est stocké sur un support physique (clé USB a puce, ou carte a puce)
2. l'AE génère le certificat et demande à l'AC de le signer (Certificate Signing Request - CSR).
3. l'AE donne le certificat signé (Certificate - CRT) à l'utilisateur.

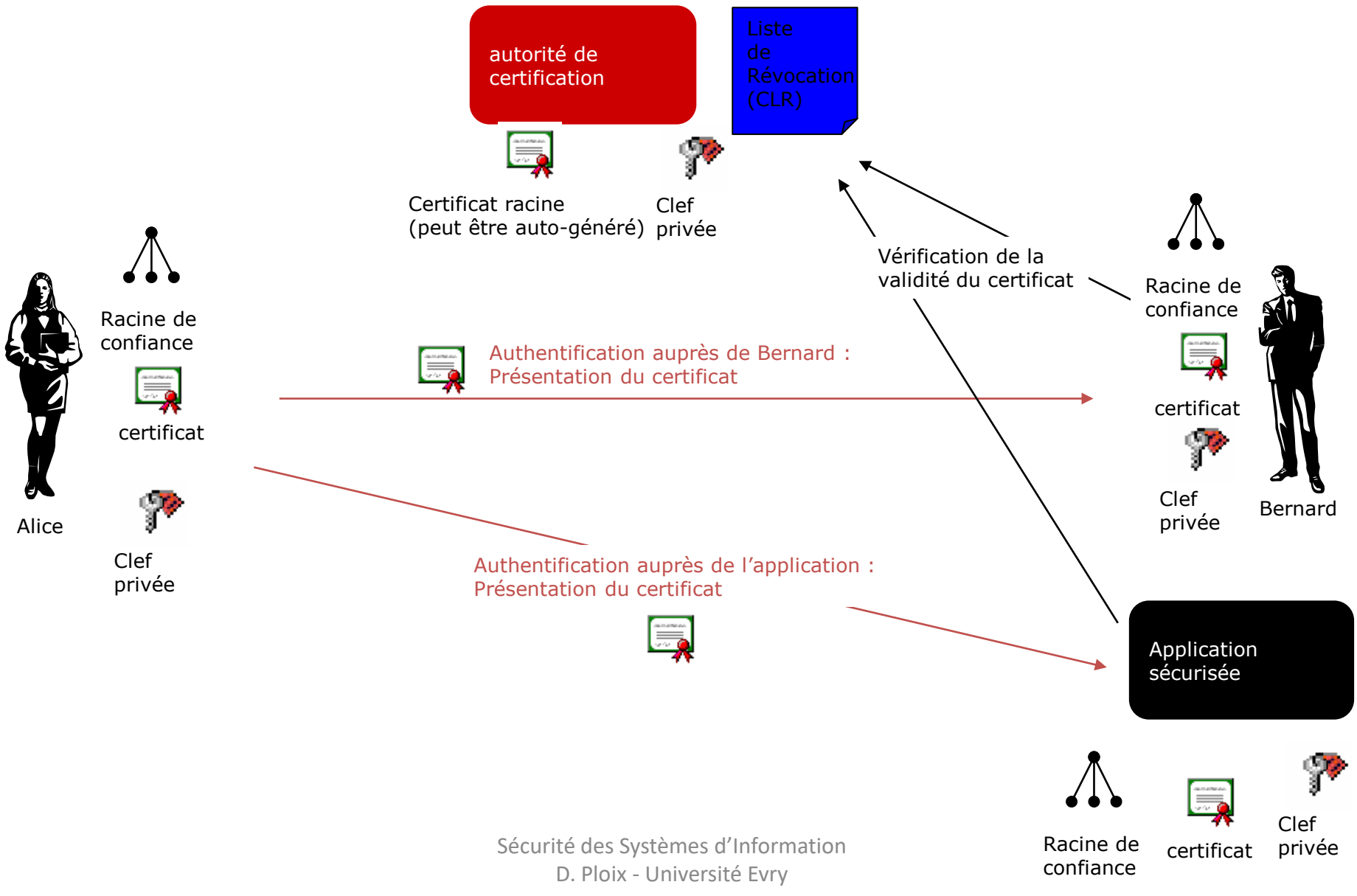
Infrastructures PKI

- AC publique :
  - Sont inscrites dans tous les navigateurs,
  - Gèrent les listes de révocation via des CLR publiques,
  - Nécessitent une connexion (internet) entre le serveur/client et la CLR,
  - Ne peuvent pas certifier des certificats serveurs pour des IP/noms de domaines privés.
- AC privées :
  - Destinées aux certificats utilisés en situation de réseaux privés d'entreprise.
    - Accès à un serveur d'application.
    - Identification des composants privés (OT)
  - Demande la mise en place d'une organisation dédiée à la gestion de l'AC et la mise en place de « cérémonie des clés » visant à en garantir la probité.
  - Structurée en fonction des usages / situations
    - Clé PKI utilisateur,
    - Réseaux spécifiques (industriel, confidentiel, …),
    - Sécurisation de l'administration des serveurs
- Certificats autosignés
  - Permet aux infrastructures de fonctionner de manière sécurisée sans avoir besoin d'ouvrir le réseau vers d'autres composants (fermes vmWare par exemple).

Plan

- Introduction
- Autorisation
- Authentification / Identification
  - Certificats
    - Identification des composants / personnes
    - Protection des communications
    - Échanges de données Informatiques (EDI)
  - Modèles de SSO

Utilisation des certificats



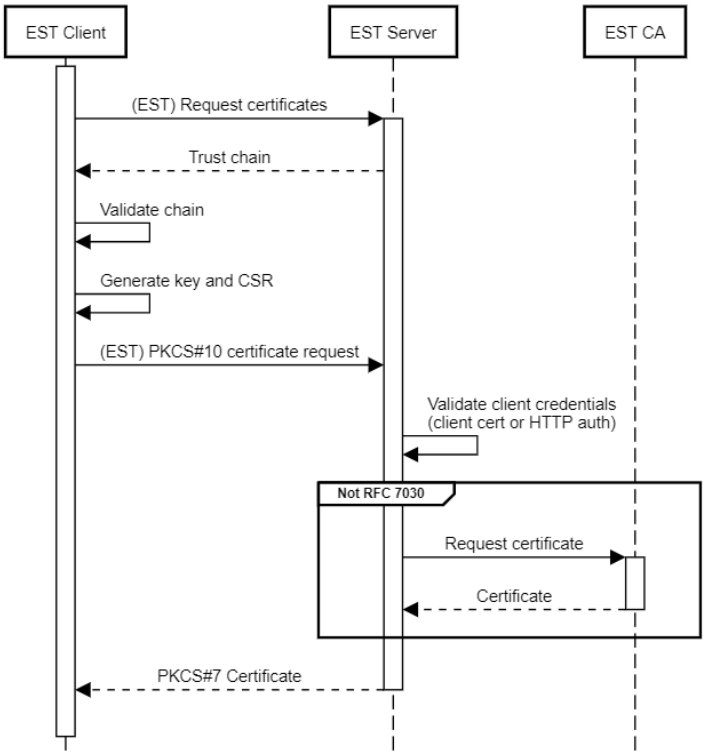
Enrôlement de composants

- Problématique :
  - sécurisation des composants autonomes : OT, IOT, appliance, terminaux mobiles, …
- Définition de protocoles d'enrôlement sécurisés :
  - Doivent garantir l'identité du composant dans ses usages futur.
- Principe de base :
  - Attribution sécurisée d'un certificat (X.509) propre à chaque composant.

Protocole EST
(Enrollment over Secure Transport)

- Serveur EST :
  - a le rôle d'autorité d'enregistrement (X.509),
  - utilise HTTPS (API / IHM)
- Client EST :
  - le composant
- La CA EST :
  - l'autorité de certification

- Les « credentials » permettent l'identification formelle du client EST vis-à-vis du serveur EST via :
  - Authentification HTTP (user / mdp) via TLS-SRP ou autres
  - Présentation d'un certificat « usine » propre à chaque composant,

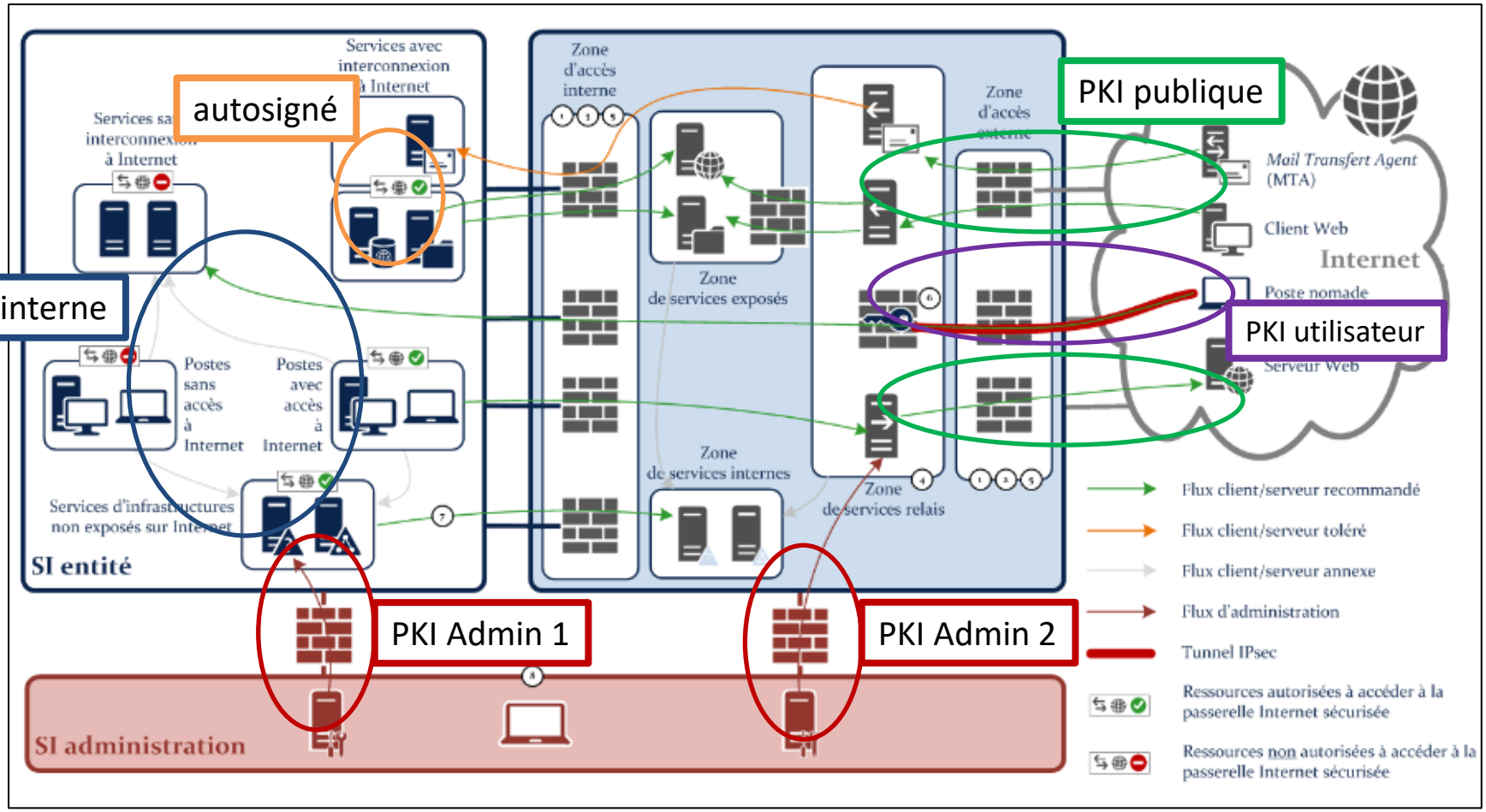


Plan

- Introduction
- Autorisation
- Authentification / Identification
  - Certificats
    - Identification des composants / personnes
    - Protection des communications
    - Échanges de données Informatiques (EDI)
  - Modèles de SSO

Architecture Internet sécurisée

https://www.ssi.gouv.fr/uploads/2012/01/anssi-guide-passerelle_internet_securisee-v2.pdf



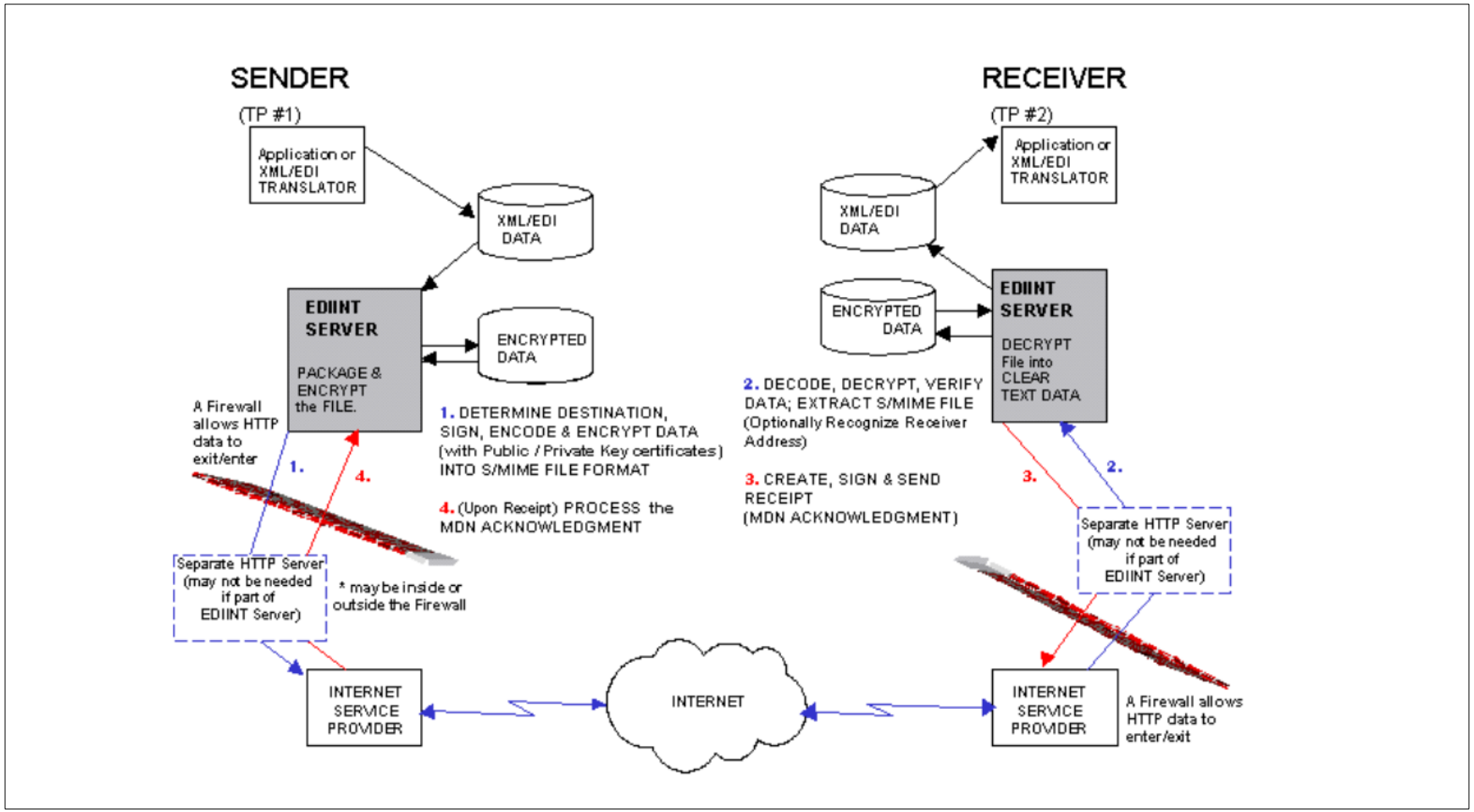
Plan

- Introduction
- Autorisation
- Authentification / Identification
  - Certificats
    - Identification des composants / personnes
    - Protection des communications
    - Échanges de données Informatiques (EDI)
  - Mécanismes d'authentification

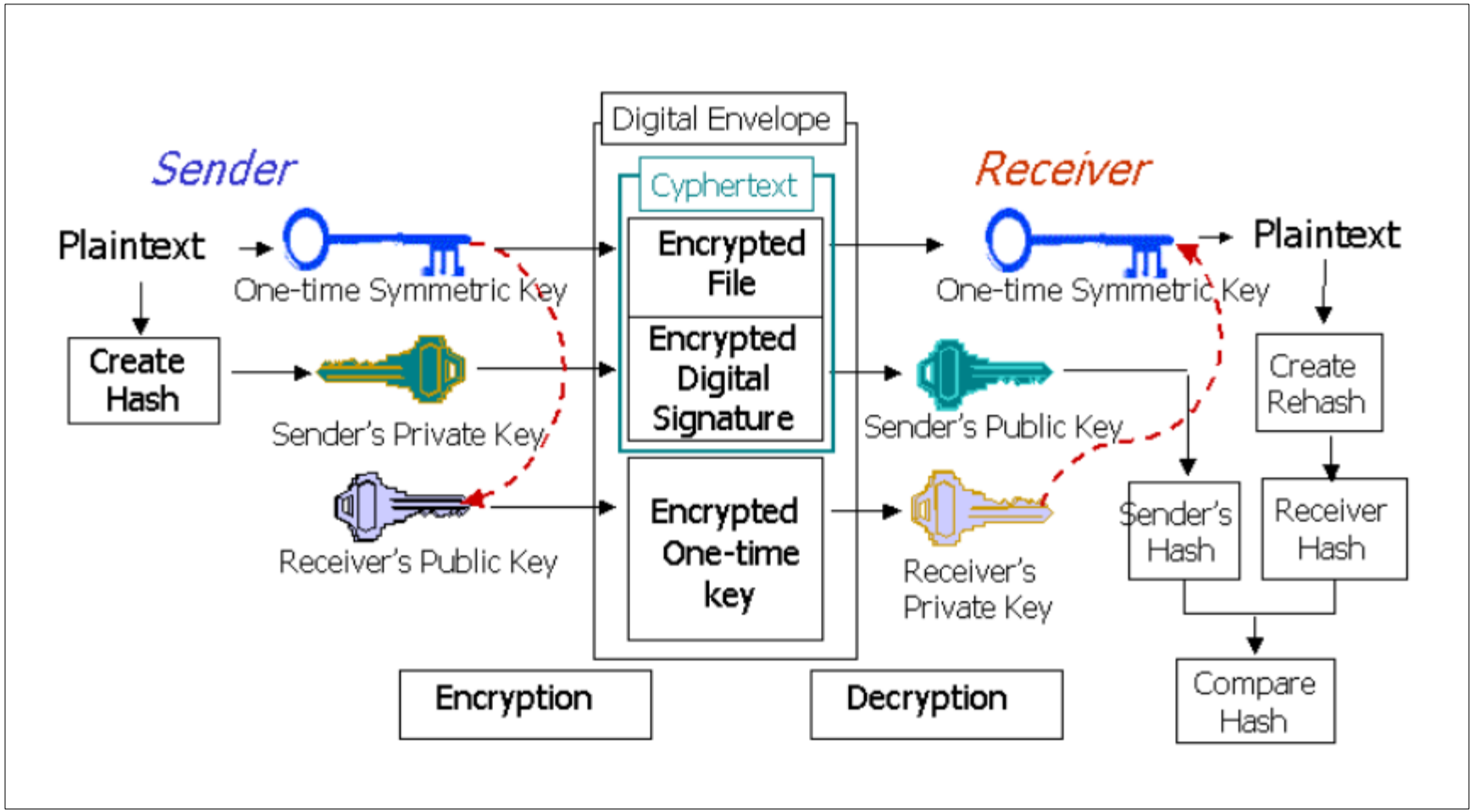
Sécurisation des échanges de données EDI

- But : établir des standard d'échange de données sécurisées B2B sur Internet de même niveau que ceux en place sur les réseaux inter-entreprises privés permettant de garantir la confidentialité, l'authentification des partenaires, l'integrité des échanges et la non répudiation des messages.
- Base du protocole :
  - Un protocole d'échange (AS1 = SMTP, AS2 = HTTP, AS3 = FTP, AS4 = WebService)
  - Une signature chiffré garantissant l'identité des partenaires,
  - Des mécanismes de MDN (Message Delivery Notification) à trois niveaux :
    - Technique : acquittement de la réception d'un message
      - Transmit « rapidement » après réception du message pour acquitter de sa réception
    - Fonctionnel : le message reçu est compréhensible
      - En asynchrone (minutes/heures) après validation par le système du respect des règles métier de constitution du message.
    - Métier : les données véhiculées dans le message sont bonnes
      - En asynchrone selon un timing déterminé par le processus de consolidation des données

Sécurisation des échanges de données EDI : protocoles ASx



Sécurisation des échanges de données EDI : protocoles AS1/AS2



Sécurisation des échanges de données EDI

Functionality	AS2	AS4
Core Messaging	HTTP 1.1 and MIME	Web Services
Internet Transport	HTTP 1.1	HTTP 1.1
Transport Layer Integrity, Sender Authentication, Receiver Authentication and Message Confidentiality (Non-Persistent)	Transport Layer (SSL / TLS) Security (Optional)	Transport Layer (SSL / TLS) Security (Optional)
Message and Payload Packaging	MIME	SOAP 1.2 with attachments (MIME)
Message Identification	AS2 “Message-Id”	ebMS 3.0 “MessageId”
Message Timestamp	MIME “Date” header	ebMS 3.0 “Timestamp”
Party Identification	AS2 “From” and “To” system identifiers	ebMS 3.0 “From” and “To” party identifiers.
Non-Repudiation of Origin	MIME Multipart/Signed (optional)	WS-Security 1.1 using XML Security (optional)
Message Confidentiality	MIME Multipart/Encrypted (optional)	WS-Security 1.1 using XML Encryption (optional)
Non-Repudiation of Receipt	Signed Message Disposition Notification	Signed Receipt Signal Message

Sécurisation des échanges de données EDI

- Liens : le site http://www.gs1.org/ du groupe qui organise les échanges sur les protocoles d'échanges…

Plan

- Introduction
- Autorisation
- Authentification / Identification
  - Certificats
  - Modèles de SSO

Authentification / Identification (S)SO

- SignOn : pour un système est d'établir l'*identité* du sujet qui s'y connecte via un mécanisme d'*authentification*.
  - En interne
  - Via un annuaire externe
  - Via un partenaire externe
    - Pour vérifier son identité (ID)
    - Pour lui déléguer son authentification
- En couplant l'authentification et l'autorisation
- *Fil conducteur* : implémentation PHP

Plan

- Introduction
- Autorisation
- Authentification / Identification
  - Certificats
  - Modèles de SSO
    - Interne
    - LDAP
    - Externe Kerberos
    - Externe OpenID
    - Externe OAuth
    - Externe SAML
    - Fédération d'identité

Authentification / Identification (S)SO : interne à l'application

- Gestion des authentification en interne à une application.
  - Use case : ne dépendre que de soi même (souvent en complément d'autres solutions)
  - Faiblesse : le mot de passe est saisie dans l'application qui le stocke
  - Bonne pratique de protection des mots de passes :
    - Technique de « salage » :
      - passwordHash = **MD5**(login + "zo5pro$1pvkhj6*cz4a8ùtvb#ui4oeuio" + **motdepasse**)
    - Nécessite le contrôle du changement des mots de passe
    - Permet la défense contre :
      - La force brute : ajoute N caractères au mot de passe,
      - Dictionnaire : garantie que le mot de passe stocké n'appartient à aucun dictionnaire,
      - Tables « arc en ciel » : évite que les empreintes soient identiques
        - » Demande à ce que le « sel » soit fonction de l'utilisateur

(reprise du) Fil conducteur

libelle cours	***Type d'action***
authentification systématique	P/T
authentifiant fonctionnel unique	P/T
mot de passe fort	P/T
certificat fort	P/T
tout identifiant correspond à une personne physique	P/T
saisie mot de passe	T
protection mot de passe	T
transport mot de passe	T
dévalidation mot de passe	P/T
neutralisation du mot de passe changé	P/T
contrôle identité lors du changement mdp	P
audit des procédures et processus d'authentification	P
contrôle des authentifications (log)	P/T
comptes génériques supprimés	P/T
contrôle des accès techniques	P/T
contrôles multiples	P
timeout de session	T
contrôles renforcés pour les données sensibles	P
contrôle du profile correspondant à l'accès	P
contrôle et audit des actions de sécurité	P/T

Plan

- Introduction
- Autorisation
- Authentification / Identification
  - Certificats
  - Modèles de SSO
    - Interne
    - LDAP
    - Externe Kerberos
    - Externe OpenID
    - Externe OAuth
    - Externe SAML
    - Fédération d'identité

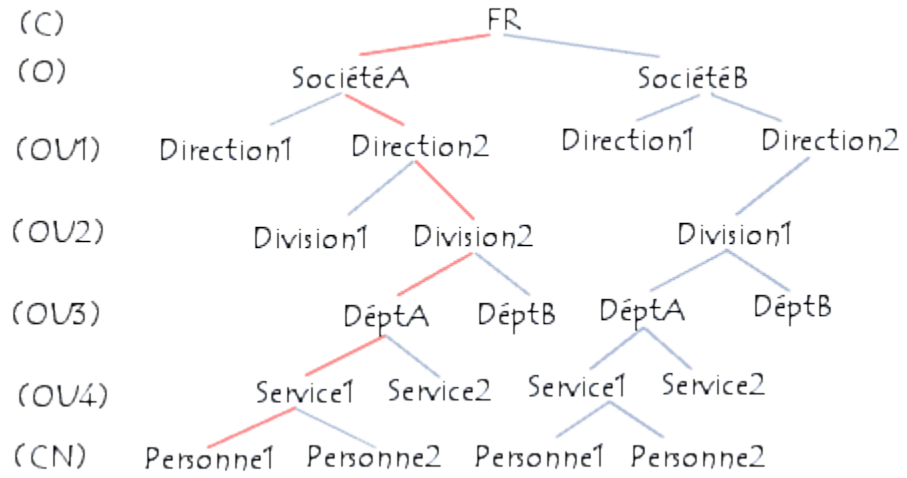
Authentification / Identification (S)SO : annuaire

- Modèles LDAP (Lightweigth Directory Access Protocol) :
  - Requière un serveur LDAP
    - Plusieurs annuaires répondent au protocole LDAP.
    - Les plus utilisés sont
      - OpenLDAP
      - AD Microsoft
      - Annuaire Notes
      - …
    - Problème :
      - la migration de l'un vers l'autre est complexe / impossible du fait d'une non compatibilité dans la gestion interne des mots de passe.

Authentification / Identification (S)SO : LDAP

- Mise en œuvre LDAP :
  - définition de la DIT (Directory Information Tree) selon un modèle « organisationnel » structuré (également à la base du modèle d'organisation des AD).

C = country
O = organisation
OU = organisation unit
CN = common name



Authentification / Identification (S)SO : LDAP

- Attributs des nœuds/feuilles :
  - **uid** (*userid*), il s'agit d'un identifiant unique obligatoire
  - **cn** (*common name*), il s'agit du nom de la personne
  - **givenname**, il s'agit du prénom de la personne
  - **sn** (*surname*), il s'agit du surnom de la personne
  - **o** (*organization*), il s'agit de l'entreprise de la personne
  - **ou** (*organization*), il s'agit du service de l'entreprise dans laquelle la personne travaille
  - **mail**, il s'agit de l'adresse de courrier électronique de la personne
  - **rdn** : nom unique dans la branche (uid)
  - **dn** : nom unique absolue : composition d'attributs (uid=xx1080,cn=ploix,givenname=damien)
- Seront utilisé pour les requêtes d'interrogation / de consultation

Authentification / Identification (S)SO : LDAP

- Intégration dans un site en PHP

1. Connexion au serveur

```
<?
// Fichier de configuration pour l'interface PHP
// de notre annuaire LDAP
$server = "ldaps://localhost/";
$port = "389";
$racine = "o=universite-evry, c=fr";
$rootdn = "cn=ldap_admin, o=universite-evry, c=fr";
$rootpw = "secret";
echo "Connexion...<br>";
$ds=ldap_connect($server);
          if ($ds==1) {
                    // on s'authentifie en tant que super-utilisateur, ici,
                    ldap_admin $r=ldap_bind($ds,$rootdn,$rootpw);
                    // Ici les opérations à effectuer
                    echo "Déconnexion...<br>";
                    ldap_close($ds);
          }
          else { echo "Impossible de se connecter au serveur LDAP"; }
?>
```

Authentification / Identification (S)SO : LDAP

- Administration des utilisateurs (requière le droit de le faire ☺)
  - int ldap_add (int identifiant, string dn, array entry) : ajout d'une « entrée »
  - int ldap_delete (int identifiant, string dn) : effacement d'une « entrée »
- Contraintes de sécurité sur l'administration (critique dans des contextes d'annuaire partagé). Fonctionne sur la délégation de responsabilité (exemple AD) :
  - Lecture du contenu de l'OU
  - Création d'OU
  - Réinitialisation de mots de passe utilisateurs
  - Modification de X attributs de comptes utilisateurs
  - Création et suppression de comptes utilisateurs
  - Création et suppression de groupes
  - Création et suppression de compte ordinateurs type postes de travail
  - Création et suppression de comptes ordinateurs type serveurs
  - connexion à un serveur Terminal Serveur
  - Création de GPO
  - Liaison de GPO à une OU
  - …

Authentification / Identification (S)SO : LDAP

- Interrogation de l'annuaire (authentification d'un utilisateur)
  - Comparaison de valeur

Le mot de passe est saisi dans l'application et va circuler sur le réseau (ldaps)

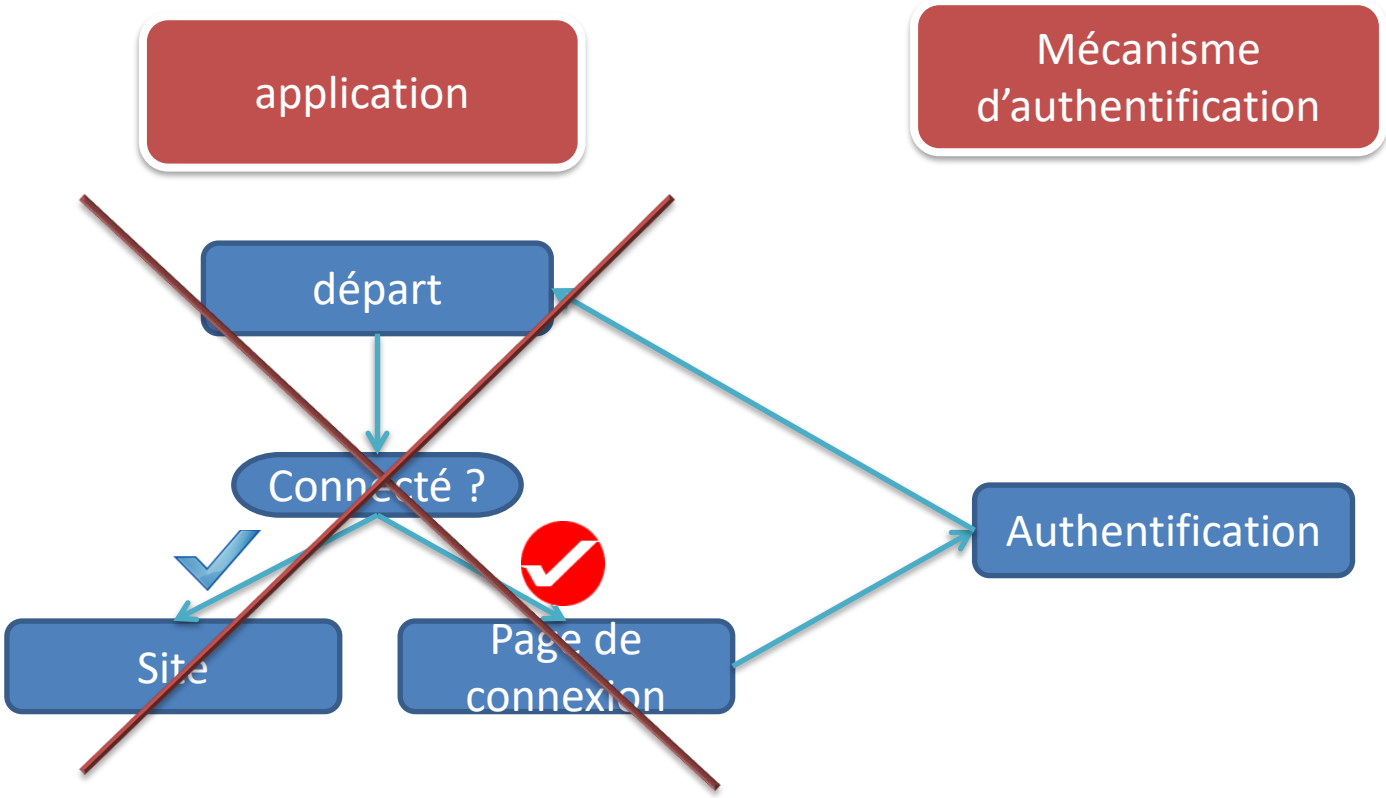
```
<?php
$ds=ldap_connect($server);
if ($ds) {
     $r=ldap_bind($ds,$rootdn,$rootpw);
    // preparation des données
    $dn="cn=Ploix Damien, o=universite-evry,c=fr";
    $valeur="MonMot2Passe";
    $attribut="password";
    // Comparaison du mot de passe à celui dans l'annuaire
    $resultat=ldap_compare($ds, $dn, $attribut, $valeur);
    if ($resultat == -1) { echo "Erreur:".ldap_error($ds); }
    elseif ($resultat == TRUE) { echo "Le mot de passe est correct"; }
    else ($resultat == FALSE) { echo "Le mot de passe est erronné..."; }
    ldap_close($ds);
} else { echo "Connexion au serveur LDAP impossible"; }
```

Plan

- Introduction
- Autorisation
- Authentification / Identification
  - Certificats
  - Modèles de SSO
    - Interne
    - LDAP
    - Externe Kerberos
    - Externe OpenID
    - Externe OAuth
    - Externe SAML
    - Fédération d'identité

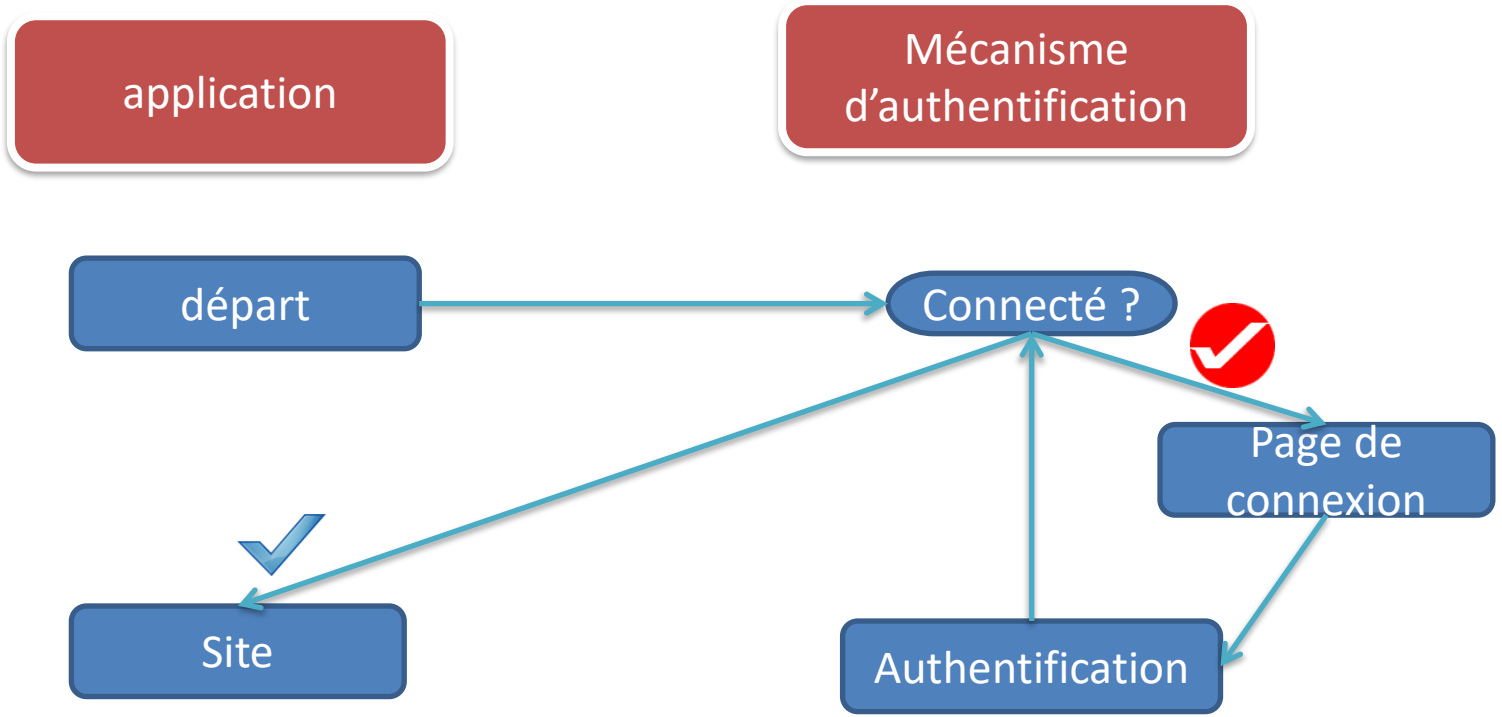
Authentification / Identification
(S)SO : passage à l'externe

- Application « autonome »



Authentification / Identification
(S)SO : passage à l'externe

- Application *SSO* compatible



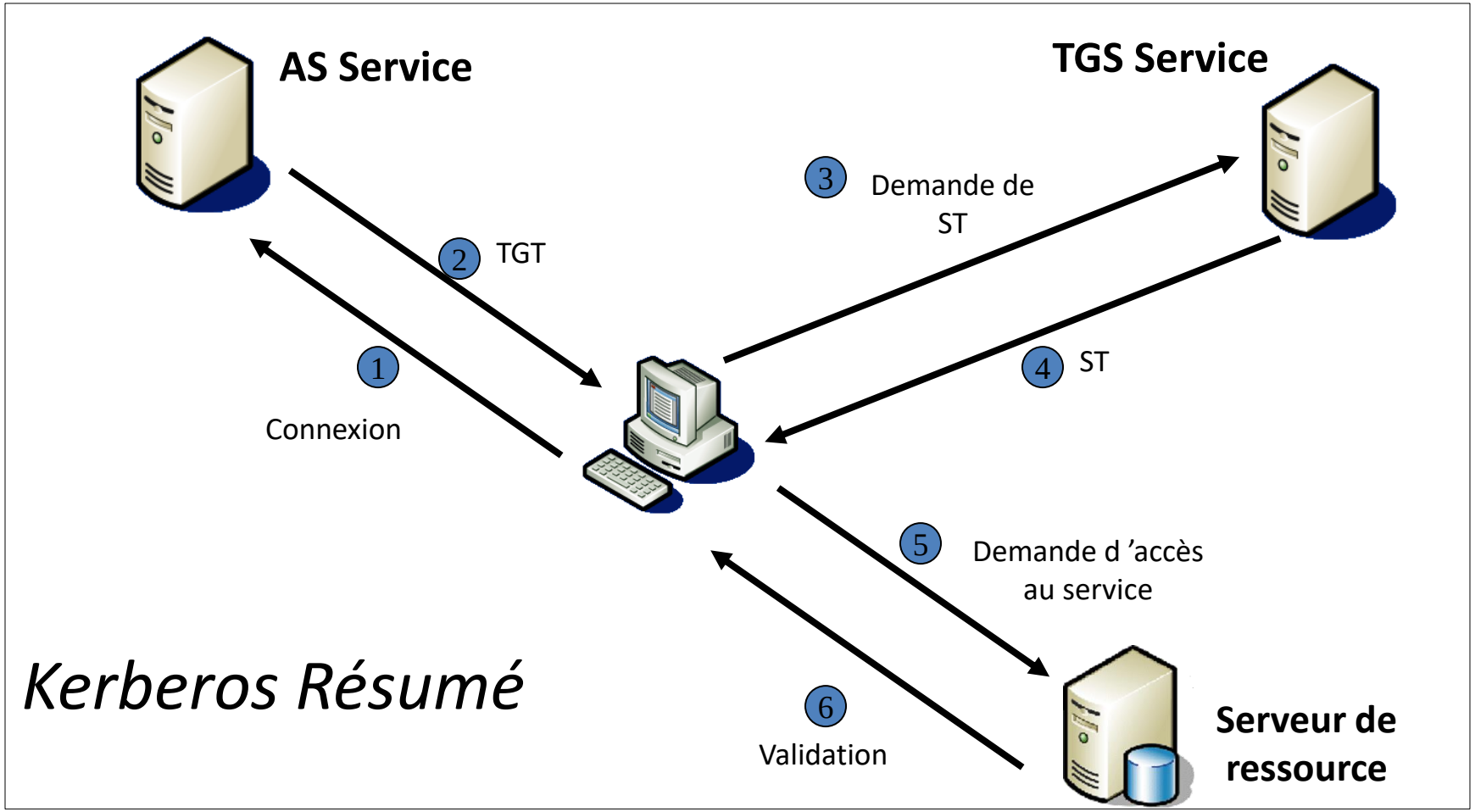
Plan

- Introduction
- Autorisation
- Authentification / Identification
  - Certificats
  - Modèles de SSO
    - Interne
    - LDAP
    - Externe Kerberos
    - Externe OpenID
    - Externe OAuth
    - Externe SAML
    - Fédération d'identité

Authentification / Identification (S)SO : Kerberos

- Les principes de Kerberos sont :
  - Basé sur la notion de « Ticket », limités dans le temps, servent à authentifier les requêtes des clients :
    - Tickets d'authentification : Ticket Granting Ticket
    - Tickets d'accès aux services : Service Tickets
  - Cryptographie à Clefs secrètes
  - Authentification mutuelle et mécanismes anti-rejeux
- L'architecture de Kerberos constitue une architecture 3 tiers :
  - un client
    - aussi appelés les « principaux »
  - une autorité approuvée (AA, comparables aux AC)
    - stocke les info. relatives aux principaux, génère et gères le clés de session (GT)
  - un serveur de ressources
    - Gère les tickets permettant d'accéder aux ressources (ST)

Authentification / Identification (S)SO : Kerberos

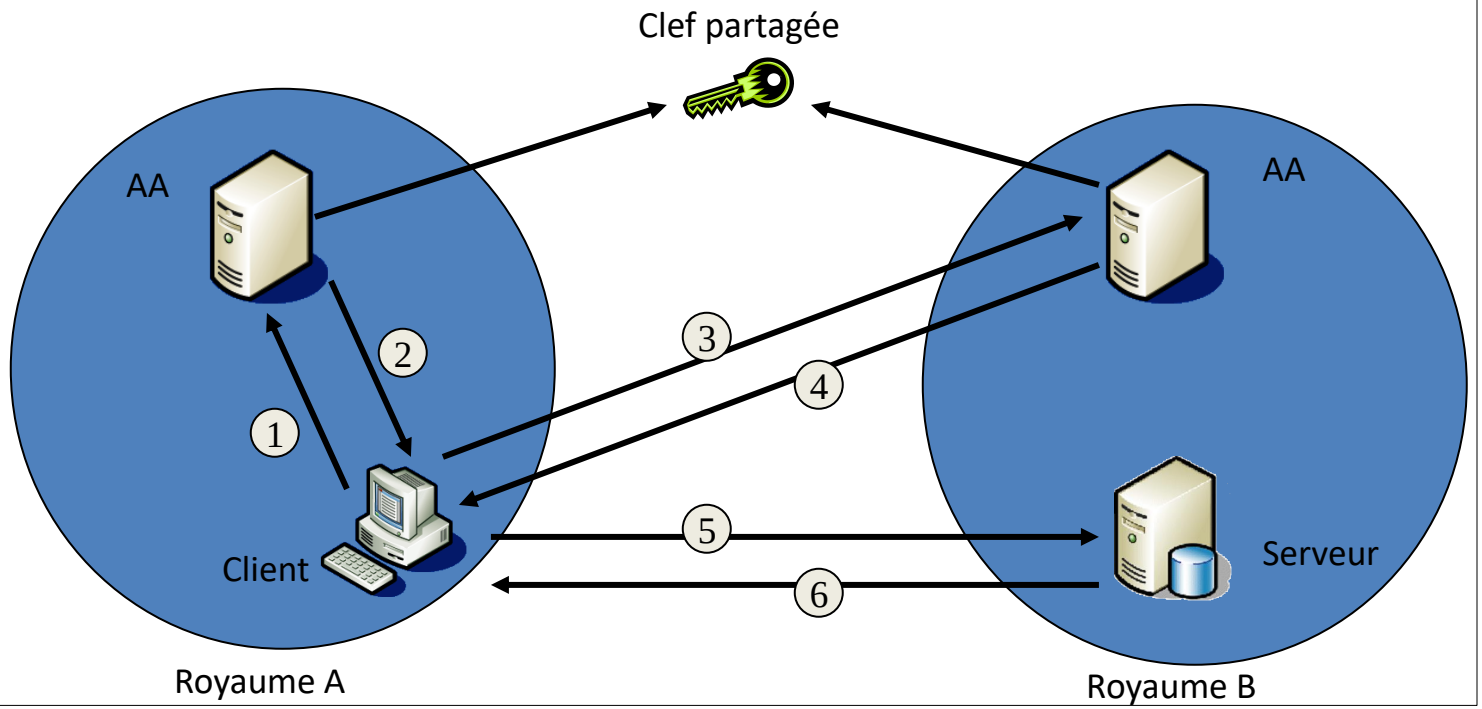


Authentification / Identification (S)SO : Kerberos

- Un ensemble un AA + n serveur(s) de ressource(s) constituent un « royaume » Kerberos (une forêt AD Windows).
- Quand un utilisateur d'un royaume A souhaite atteindre un serveur d'un royaume B :
  - il contacte sa propre AA,
  - qui lui transmet un Refferal Ticket (TGT chiffré avec une clef partagée inter-royaume)
  - qui servira à obtenir auprès de l'AA de B un ST pour le serveur souhaité.

Authentification / Identification (S)SO : Kerberos

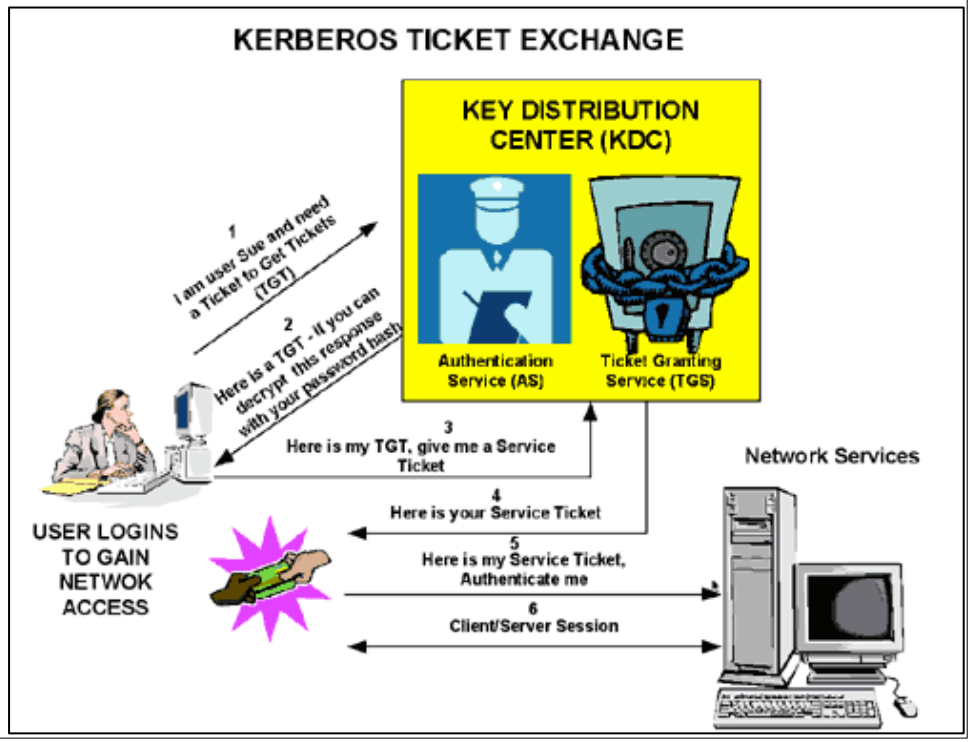
1 : demande d'accès	**4** : renvoi d'un ticket pour le serveur
2 : renvoi d'un ticket pour B	**5** : demande d'accès
3 : demande d'accès	**6** : accès autorisé



Authentification / Identification (S)SO : Kerberos

- Modèle Microsoft : Le contrôleur de domaine Windows combine les deux fonction AS et TGS au sein d'un KDC.

- À l'accès d'une ressource (service), un TGS est échangé avec le DC qui permet à l'utilisateur d'y accéder.
- Le liens entre plusieurs forêts d'AD (de DC) permet l'échange de confiance (TGS) et l'accès aux ressources.



Authentification / Identification (S)SO externe : Kerberos

- Exemple : SSO Windows vers un serveur PHP.
- Le token Kerberos d'identification peut être intercepté par le serveur Apache (configuration navigateur).
- Pour cela, il faut au préalable :
  - Enregistrer le serveur (du serveur PHP) et (pour un contrôle supplémentaire) le service dans le DC.
  - Configurer Apache pour qui intercepte les données Kerberos dans le flux http via le mod_auth_kerb

Authentification / Identification (S)SO externe : Kerberos

auth_kerb.conf

```
<Location /logon>
  AuthType Kerberos
  AuthName "Kerberos Login"
  KrbMethodNegotiate On
  KrbMethodK5Passwd On
  # domaine (royaume) Kerberos
  KrbAuthRealms DOM1.MABOITE.FR DOM2.MABOITE.FR
  # localisation locale des clés services inscrits dans le domaine
  Krb5KeyTab /etc/krb5.keytab
  KrbSaveCredentials On
  # nom du service
  KrbServiceName HTTP
  # on peut aussi spécifier une liste restreinte d'utilisateurs…
  require valid-user
</Location>
```

Authentification / Identification (S)SO externe : Kerberos

index.php

```
<?php
if(isset($_SERVER['REMOTE_USER']) && !empty($_SERVER['REMOTE_USER'])) {
?>
        <p>Connecté en tant que : <?php echo $_SERVER['REMOTE_USER']; ?>
        ...
<?php
} else {
?>
        <p>merci de vous connecter avant de venir sur le site…
<?php
}
?>
```

Authentification / Identification (S)SO externe : Kerberos

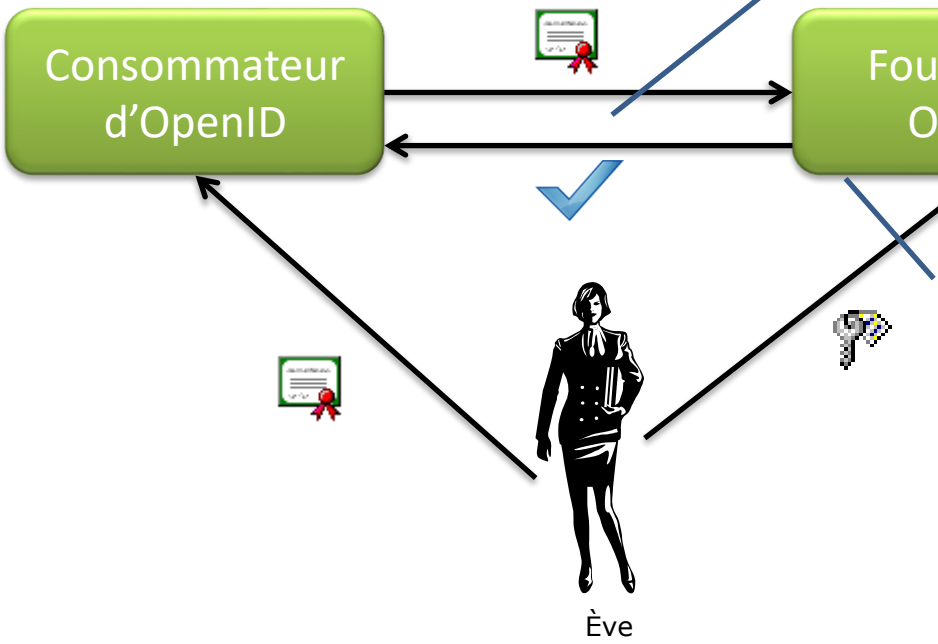
- Pour aller plus loin … :
  - Le retour d'expérience de l'INRIA sur la mise en place de Kerberos dans un contexte hétérogène Unix / Windows :
    - https://2011.jres.org/archives/75/paper75_article.pdf

Plan

- Introduction
- Autorisation
- Authentification / Identification
  - Certificats
  - Modèles de SSO
    - Interne
    - LDAP
    - Externe Kerberos
    - Externe OpenID
    - Externe OAuth
    - Externe SAML
    - Fédération d'identité

Authentification / Identification (S)SO externe : OpenID

- Utilisation d'un référentiel **externe** pour la gestion des **identités**.



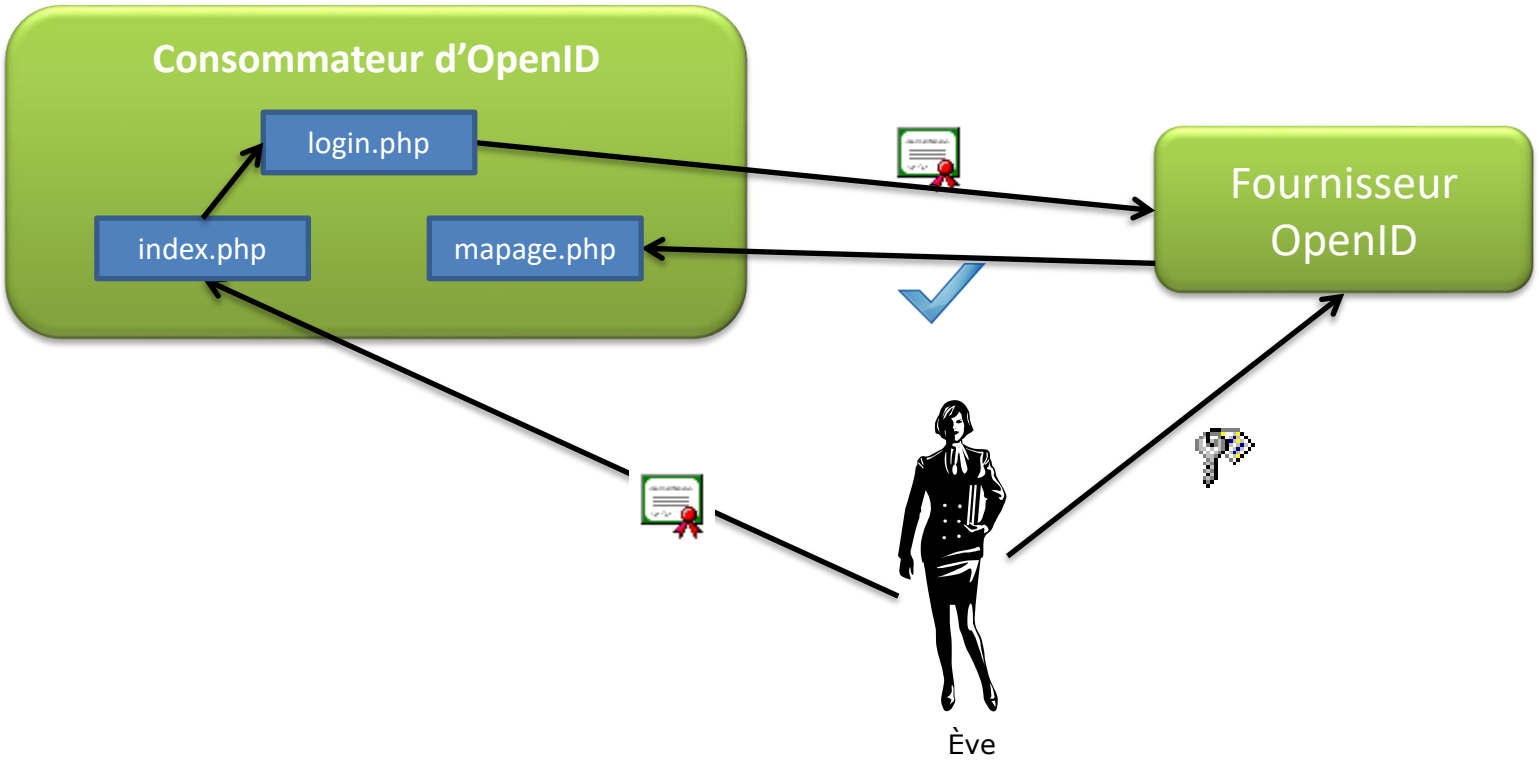
La force/faiblesse réside dans le lien de confiance entre les partenaires :

Le mot de passe est géré par le fournisseur qui fonctionne comme un annuaire (non structuré).

La *fédération* vient avec le partage de fournisseurs openID *de confiance* entre différents partenaires

Authentification / Identification (S)SO externe : OpenID

- Exemple PHP avec Zend



Authentification / Identification (S)SO externe : OpenID

index.php

```
<?php
if(isset($_SESSION[‘identity’]) && !empty($_SESSION['identity'])) {
?>
        <p>Connecté en tant que : <?php echo $_SESSION['identity']; ?>
        ...
<?php
} else {
?>
        <p>merci de vous connecter avec votre openID
        <p><form method="post" action="login.php">
                <input type="text" name="openid_identifier" size="100"/>
                <input type="submit" name="openid_action" value="login"/>
        </form>
        <p>
<?php
}
?>
```

Authentification / Identification (S)SO externe : OpenID

login.php

```
<?php
require_once('zfinit.php');
$status = 'failed';

if (!isset($_POST['openid_identifier']) ||
empty($_POST['openid_identifier'])) {
   $status='parametremanquant';
} else {
   try {
     $cons = new Zend_OpenId_Consumer();
     if ($cons->login($_POST['openid_identifier'], 'mapage.php', NULL)) {
         // jamais ateind !
   } catch (Exception $ignore) {
   }
}
header('Location:index.php?status='.$status);
```

Authentification / Identification (S)SO externe : OpenID

mapage.php

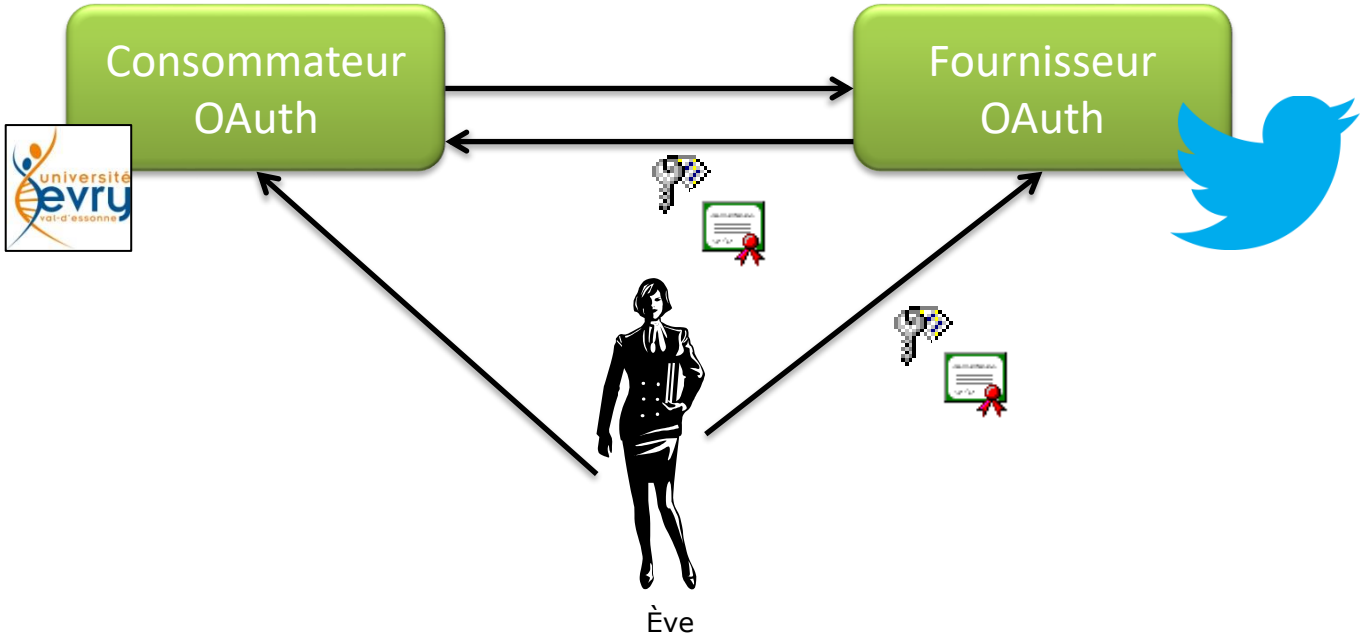
```
<?php
require_once('zfinit.php');
$status = 'failed';

if (isset($_REQUEST['openid_mode']) {
   if($_REQUEST['openid_mode'] == 'id_res') {
        $cons = new Zend_OpenId_Consumer();

        $id = NULL;
        if($cons->verify($_REQUEST, $id)) {
                $status = 'succes';
                $_SESSION['identity'] = $id;
        }
    } else if ($_REQUEST['openid_mode'] == 'cancel') {
        $status = 'annule';
    }
}
header('Location:index.php?status='.$status);
```

Plan

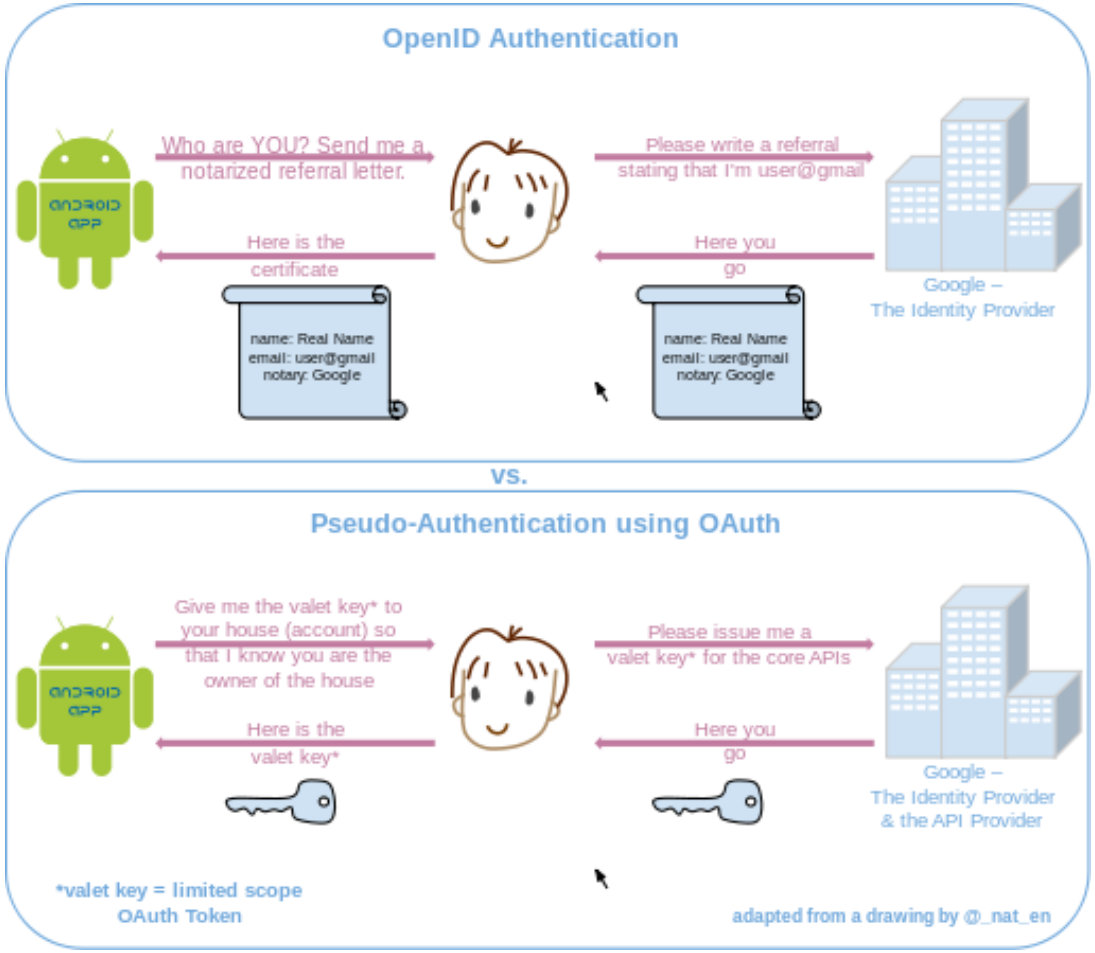
- Introduction
- Autorisation
- Authentification / Identification
  - Certificats
  - Modèles de SSO
    - Interne
    - LDAP
    - Externe Kerberos
    - Externe OpenID
    - Externe OAuth
    - Externe SAML
    - Fédération d'identité

Authentification / Identification (S)SO externe : OAuth

- Partage d'information entre fournisseurs via un protocole d'échanges de **données**.

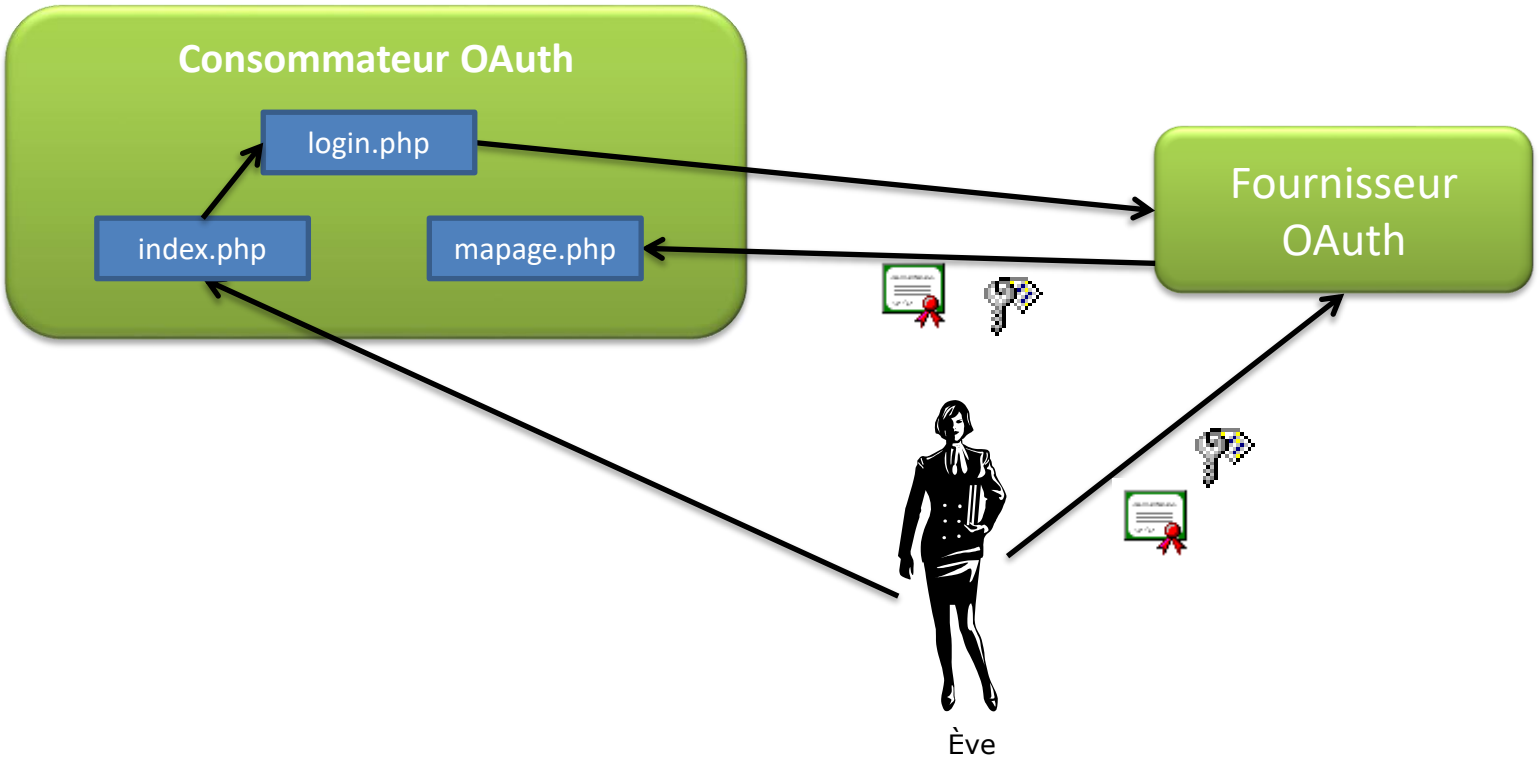


Authentification / Identification (S)SO externe : OAuth



Authentification / Identification (S)SO externe : OAuth

- Exemple PHP avec Zend



Authentification / Identification (S)SO externe : OAuth

index.php

```
<?php
if (isset($_SESSION['twitter_access_token']) &&
          !empty($_SESSION['twiteer_access_token'])) {
?>
          <p>connecté en tant que : <?php echo $_SESSION['identity']; ?>

          ...

          <p><a href="logout.php">déconnexion</a>
<?php
} else {
?>
          <p>vous devez être connecté pour la suite.
          Vous pouvez utiliser pour cela votre compte <a herf="login.php">Twitter</a>.
<?php
}
?>
```

Authentification / Identification (S)SO externe : OAuth

Configuration OAuth dans config.php

```
<?php

$configOAuth = array(
          'siteUrl' => 'https://twiter.com/oauth',
          'callbackUrl => 'http://monsite.fr/mapage.php',
          'consumerKey' => '[macleenregistreecheztwiter.com]',
          'consumerSecret' => '[monsecretconvenuavectwiter.com]',
);
```

Authentification / Identification (S)SO externe : OAuth

login.php

```
<?php

require_once('zfinit.php');
include('config.php');

try {
  $cons = new Zend_Oauth_Consumer($configOAuth);

  $token = $cons->getRequestToken();
  $_SESSION['twitter_request_token'] = serialize($token),

  $cons->redirect();
}
```

Authentification / Identification (S)SO externe : OAuth

mapage.php

```
$cons = new Zend_Oauth_Consumer($confOAuth);

if(!empty($_GET) && isser($_SESSION['twitter_request_token'])) {
   if (isset($_GET['denied'])) {
          $status = 'annule';
   } else {
          try {
             $requestToken = unserialize($_SESSION['tiwtter_request_token']);

             $accessToken = $cons->getAccessToken($_GET, $requestToken);

             $_SESSION['twitter_access_token'] = serialize($accessToken);
             $_SESSION['tiwtter_request_token'] = null;

             $_SESSION['identity'] = $accessToken->getParam('screen_name');
             $status = 'success';
          }
          catch(Exception $ignore) { }
   }
}
header('Location:index.php?status='.$status);
```

Plan

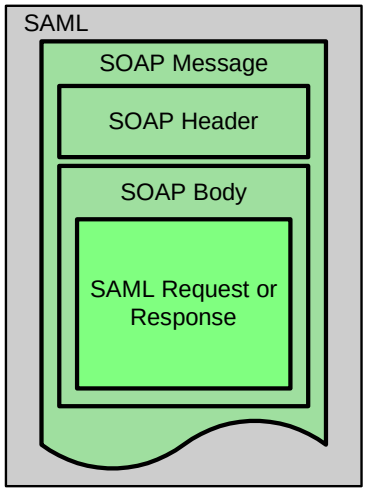
- Introduction
- Autorisation
- Authentification / Identification
  - Certificats
  - Modèles de SSO
    - Interne
    - LDAP
    - Externe Kerberos
    - Externe OpenID
    - Externe OAuth
    - Externe SAML
    - Fédération d'identité

Authentification / Identification (S)SO externe : SAML

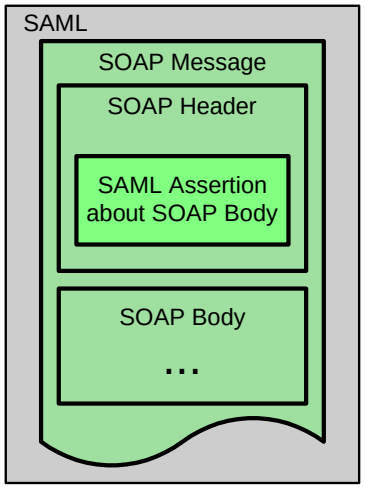
- SAML est un *protocole* qui définit l'échange « d'assertions » de type
  - Authentification
    - Une autorité *compétente* (fournisseur d'identification) valide qu'un sujet S a été identifié par des moyens M à une heure T
    - SAML ne garanti pas la sécurité de l'autorité compétente…
  - Attributs
    - Un fournisseur *compétent* indique qu'un sujet S est associé avec les attributs A, B, C, … ayant pour valeurs respective a, b, c, …
    - Exemple type d'utilisation : attributs LDAP d'un utilisateur
  - Décision d'autorisation
    - Un fournisseur *compétent* (fournisseur de service) décide d'autoriser le sujet S d'un accès de type A à une ressource R sur la base de la preuve P

Authentification / Identification (S)SO externe : SAML

- Sécurisation de SAML
  - Protocole d'échange (de transport) des mesages : Bindings (SOAP-over-HTTP)
  - Profiles (scénarios) d'échange sur les autres assertions (profil SOAP)



SOAP-over-HTTP



SOAP Profile

Profiles
Combinaison d'assertions, de protocoles et de bindings définit pour un cas d'usage particulier

Bindings
Implémentation du protocole SAML sur des protocoles de messages et de communication standards

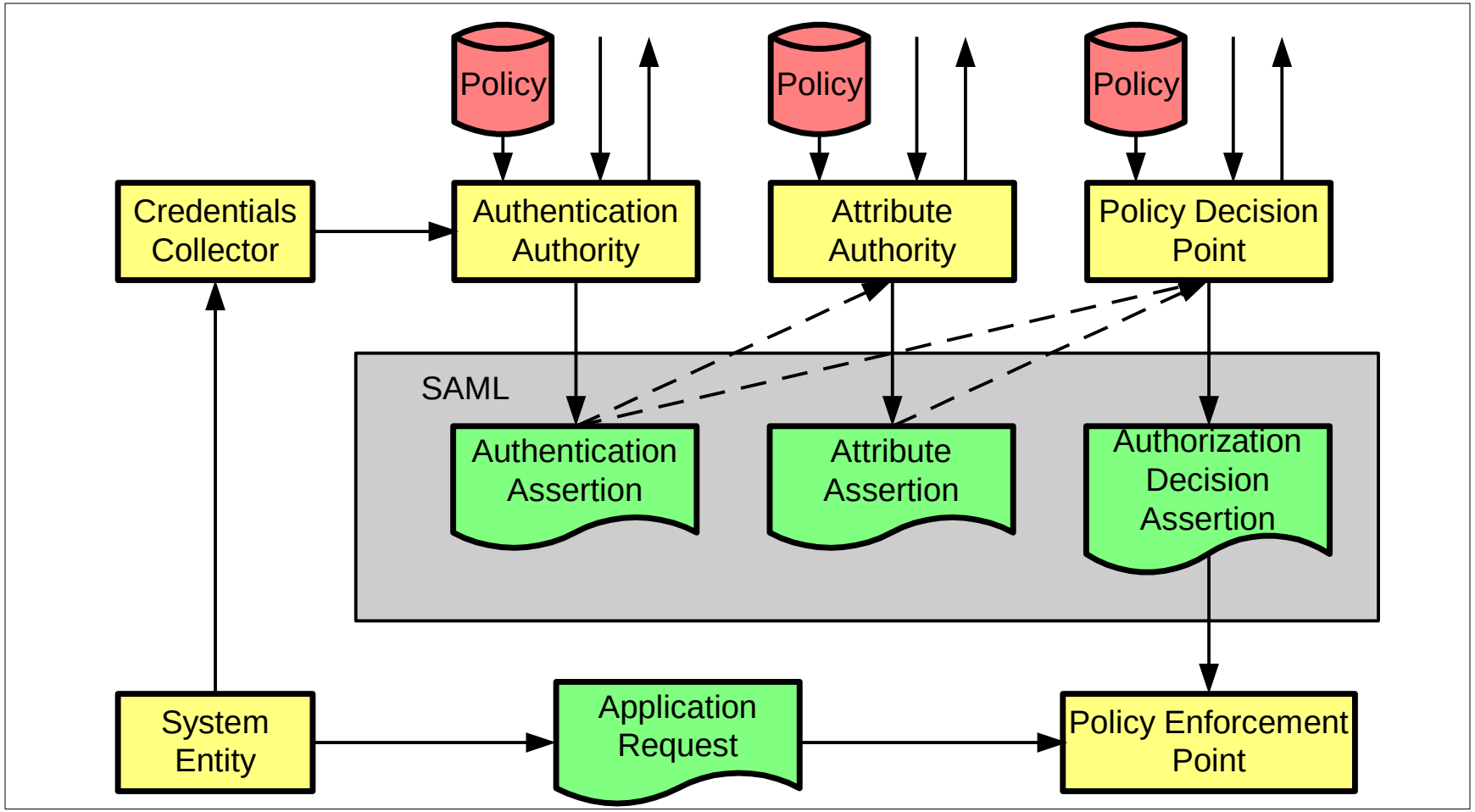
Protocoles
Requête et réponse pour obtenir les assertions et réaliser le management des identités

Assertions
Authentification, attributs, décision

Authentification / Identification (S)SO externe : SAML

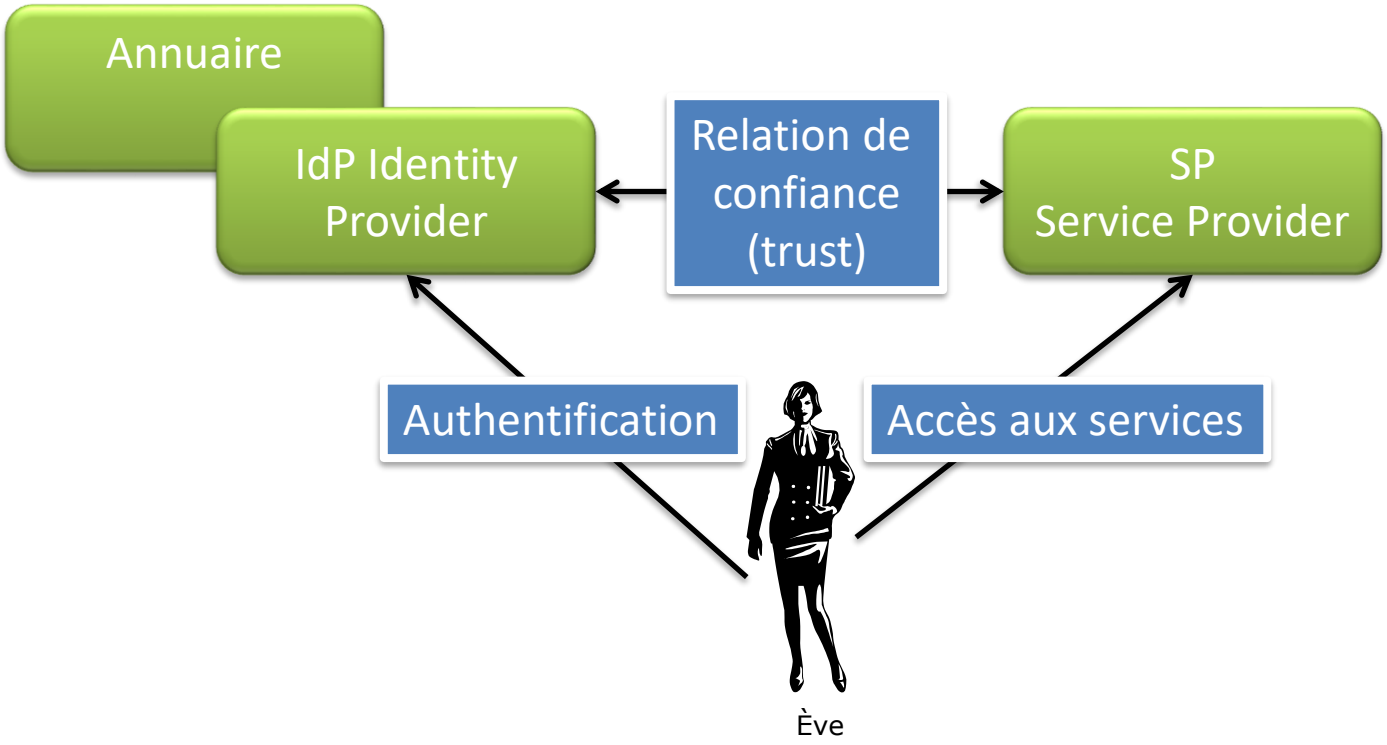
- Protocoles de
  - Demande d'authentification
  - Demande d'assertion
  - De résolution d'artefacts
  - De gestion des identifiant
  - De correspondance d'identifiant
  - De déconnexion globale (Single Log Out)
- Bindings
  - Redirection HTTP
  - HTTP Post
  - SAML SOAP
  - SOAP inversé (PAOS)
  - SAML URI
- Profiles
  - SSO Navigateur Web
  - Single Logout
  - Recherche d'IdP
  - ECP (Enhanced client proxy)
  - Assertion, Artefacts, identifiants…

Authentification / Identification (S)SO externe : SAML



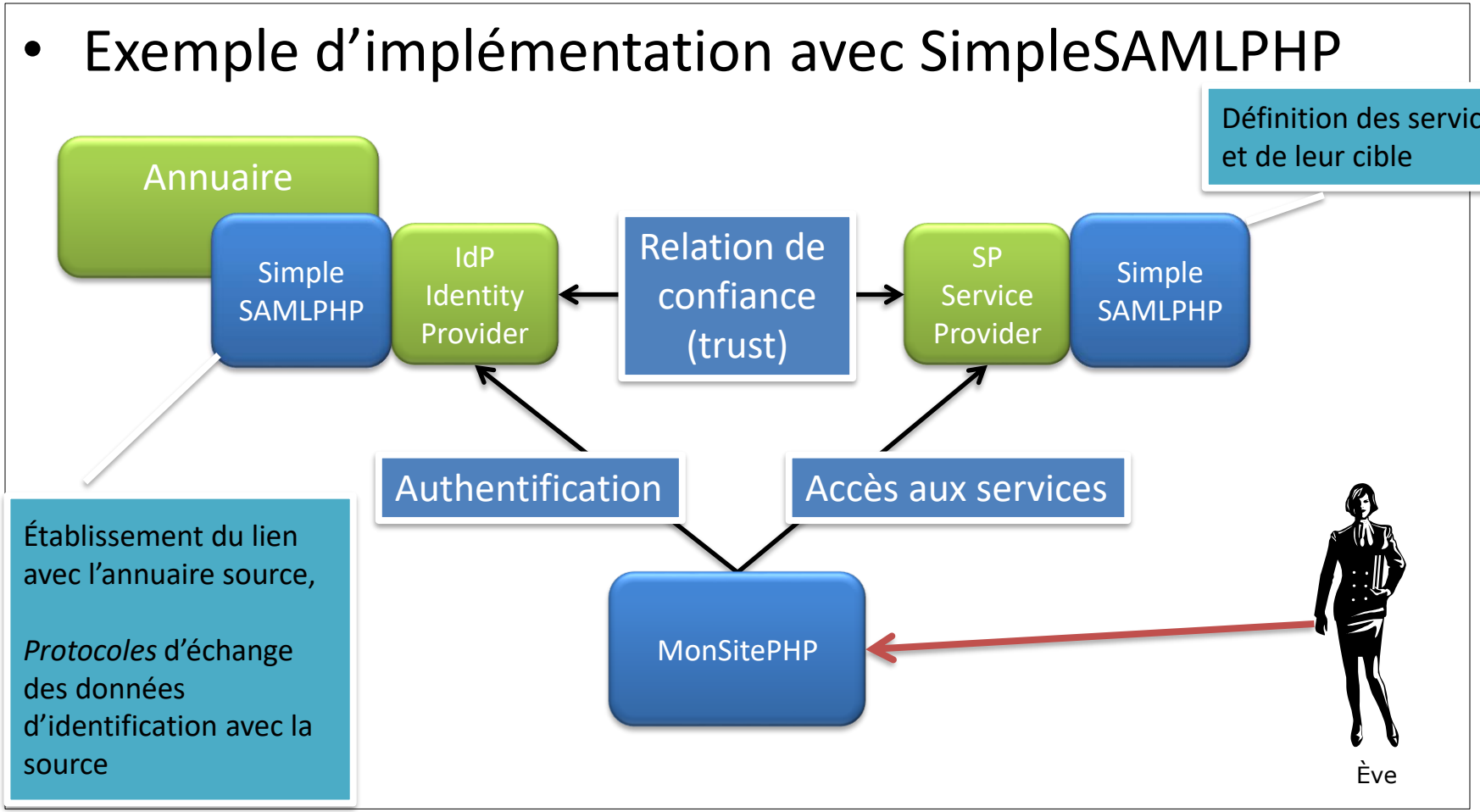
Authentification / Identification (S)SO externe : SAML

- En plus simple : rôles dans SAML



Authentification / Identification (S)SO externe : SAML

- Exemple d'implémentation avec SimpleSAMLPHP



Authentification / Identification (S)SO externe : SAML

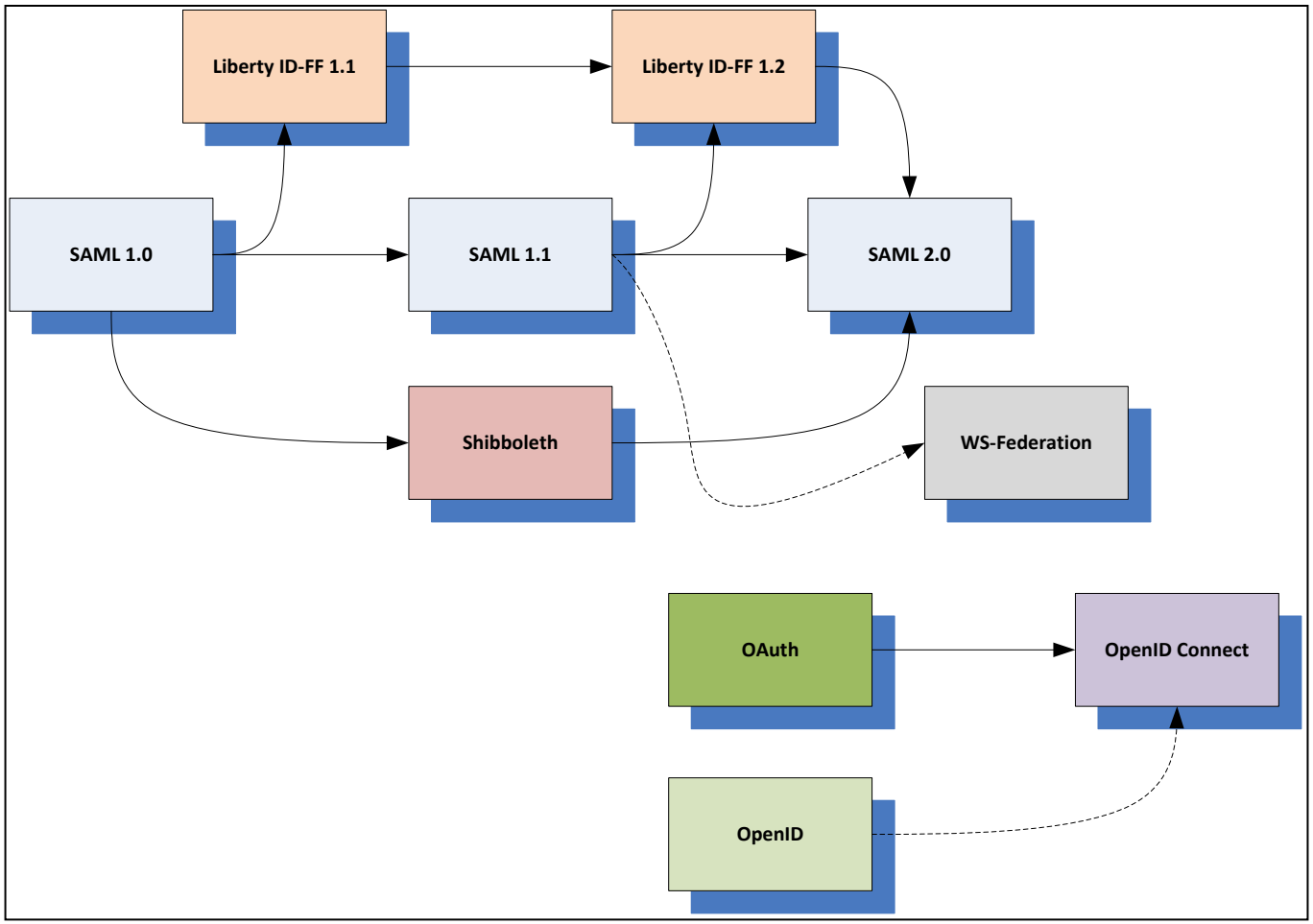
login.php

```
required_once('<SSP_URL_CONFIGURATION_FILE>');

$status = 'failed';
try {

  $as = new SimpleSAML_Auth_Simple('service_name');

  $as->requireAuth();

  $att = $as->getAttributes();

  $uid = $attributes['uid'][0];
  $_SESSION['identity'] = $uid;

  $_SESSION['logouturl'] = $as->getLogoutURL();

  $status = 'success';
}

catch(Exception $ignore) {
}
```

Plan

- Introduction
- Autorisation
- Authentification / Identification
  - Certificats
  - Modèles de SSO
    - Interne
    - LDAP
    - Externe Kerberos
    - Externe OpenID
    - Externe OAuth
    - Externe SAML
    - Fédération d'identité

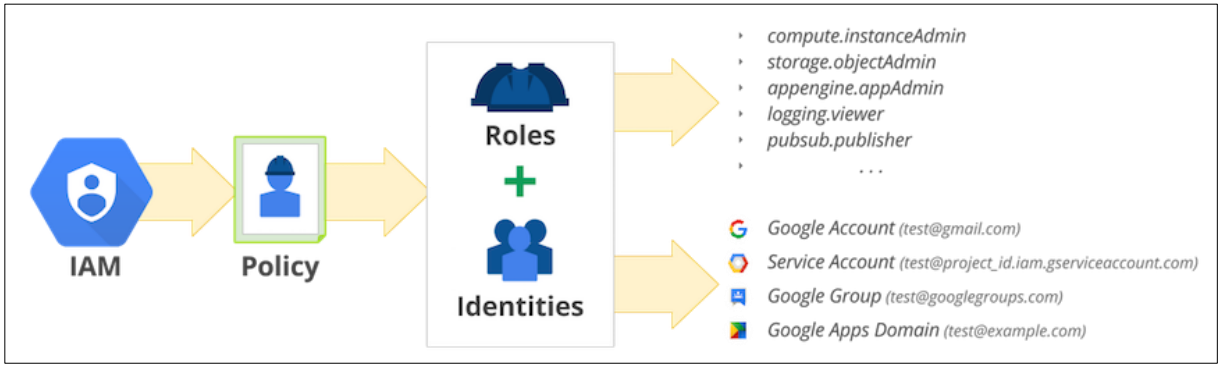
Fédération d'identité protocoles

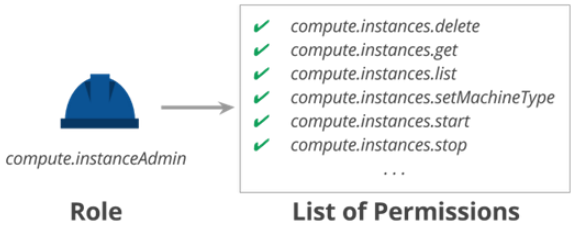


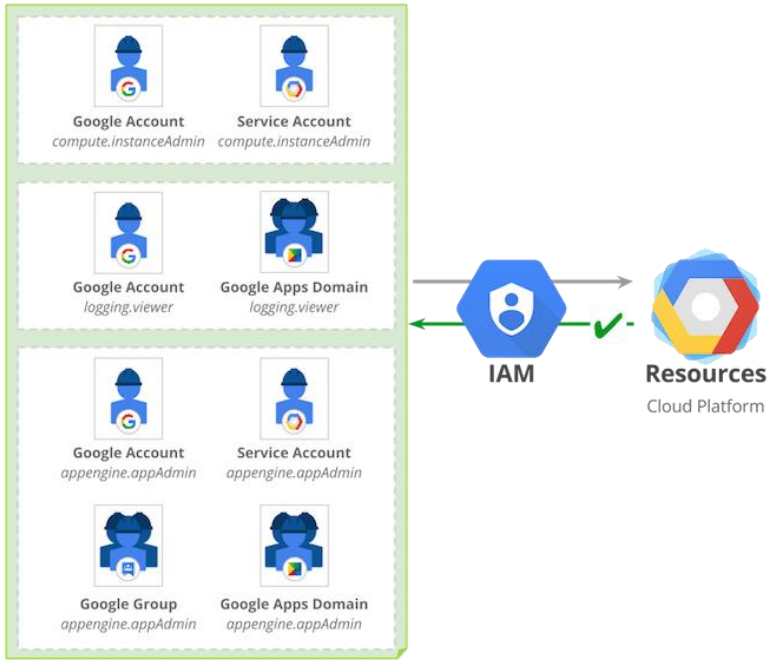
Fédération d'identité

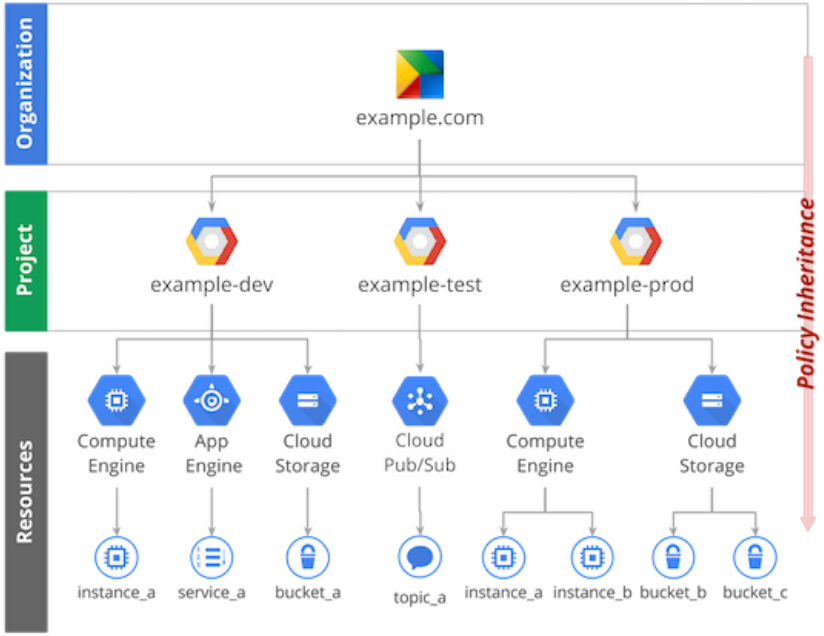
- La fédération d'identité à pour finalité le partage de l'identité (et du SSO) entre plusieurs partenaires.
  - Via du SAML
  - Via OpenID/OAuth
  - Via du ADFS (Microsoft)

IAM Cloud modèle Google

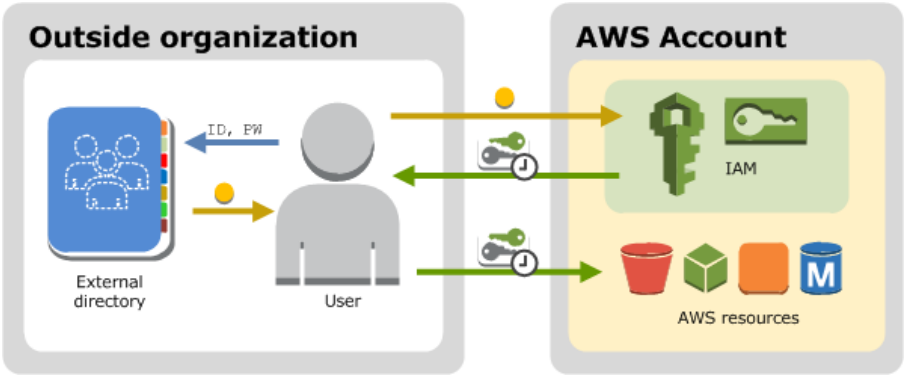


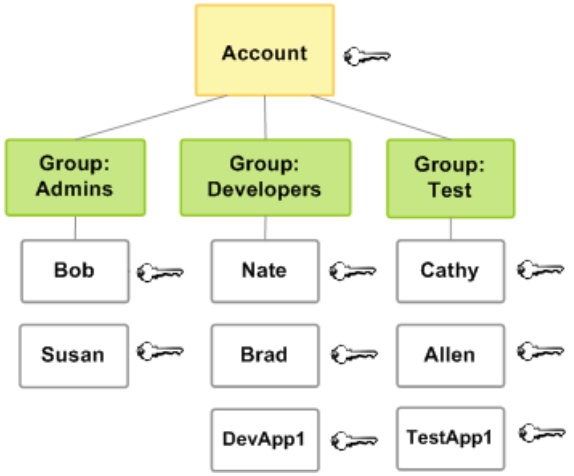






IAM Cloud modèle Amazone





Identité / authentification :

- OpenID Connect / SAML 2.0

Stratégies d'autorisations :

- Basée sur l'utilisateur :
  ➔ affectation de droits à un utilisateur sur une ressource
- Basée sur la ressource :
  ➔ affectation de droits sur une ressource à un ensemble d'utilisateurs/groupes

Exemple (WS-Fed)