`Présents :`

- Frédérick Bigrat - UNPIdF
- Sabin Galuscan - Université de Versailles Saint-Quentin-en-Yvelines
- Cyrille Ghesquiere - Université Paris VIII
- Jean Marc Liger - Université de la Sorbonne / SIRIS
- Philippe Werle - Université Paris XIII
- Mikaël Ates - Entr'ouvert
- Thomas Noël - Entr'ouvert
- Fédéric Péters - Entr'ouvert

Rappel du principe du portail captif

`Présentation rapide des logiciels principaux employés :`

- pfSense 2.0, basé sur FreeBSD 8.1
- AuthSAML2, module de Authentic2 (python)
- Bibliothèque SAML 2.0 Lasso, et les dépendances OpenSSL, libXML2, libxmlsec

`Discussion sur les certificats nécessaires pour le portail captif et l'impact sur les métadonnées de fédération::`

La discussion a porté sur l'utilisation d'un **certificat commun** à plusieurs portails captifs, au niveau des échanges de la fédération et au niveau de la connexion HTTPS (page de connexion au portail).

Il existe une PKI avec une AC racine universitaire/CNRS : chaque université dispose de ses propres certificats qui seront bien validés par les navigateurs du marché. Dans ce cas, le déploiement d'un portail eduspot nécessitera d'acquérir les certificats, de les configurer au sein du portail (partie HTTPS et SAML 2.0) puis de déclarer les métadonnées de son portail au sein de la fédération.

Entr'ouvert indique que si chaque portail est déclaré indépendamment au niveau de la fédération (i.e. un certificat par portail), cela permettra de mettre en oeuvre des profils SAML 2.0 (qui ne sont pas déployés à ce jour), notamment le ***Single Logout IdP initiated via SOAP*** -- à la condition que le portail soit directement accessible en SOAP (http/https) par les IdPs.

Entr'ouvert indique qu'en cas de certificat commun à plusieurs portails (utilisé pour la fédération), il serait possible de ne faire qu'une déclaration de métadonnées pour de multiples portails. Cela empêcherait, pour ces portails, le déploiement de profils SAML où l'IdP adresse directement les SP et les IdP n'auraient pas connaissance du portail faisant une requête d'authentification au travers des échanges (mais pourrait relever l'adresse IP). Cependant, ce mode de déploiement pourrait être intéressant pour des organismes souhaitant déployer un portail captif et n'étant pas familiers avec l'obtention de certificats et l'enregistrement de services auprès de la fédération. Il serait alors nécessaire qu'un organisme prennent en charge la distribution de la clé privée et du certificat aux organismes souhaitant déployer un portail dans cette configuration.

À l'issue de cette discussion, penchant vers l'usage de multiples certificats seulement, Phillipe Werle a proposé de discuter de cette question avec le groupe RSSI. Cette discussion sera ensuite portée sur les listes EDUSPOT et Univnautes.

Discussion sur les attributs d'identités

Les attributs d'identités sont envoyés de l'IdP au portail au sein de l'assertion d'authentification.

Il avait été discuté lors de la précédente réunion les points suivants :

- Faire redescendre un attribut d'autorisation de l'université d'appartenance à l'université d'accueil. Entr'ouvert avait signalé que l'usage de cet attribut pourrait être couplé avec une liste noire des utilisateurs maintenue par les universités d'appartenance
- Faire redescendre l'attribut ***eduPersonAffiliation***

Cela a fait l'objet d'une discussion avec Olivier Salaün :

- La notion de contrôle d'accès basé sur un attribut n'a pas été abordée au sein du groupe de travail EDUSPOT mais ce serait intéressant ;
- Olivier émet cependant la recommandation suivante : moins d'attributs sont envoyés plus la solution est simple et robuste, donc ***a minima*** seul le NameID serait envoyé ;
- Il indique enfin qu'il est nécessaire de discuter de l'usage de l'attribut ***eduPersonAffiliation***.

Entr'ouvert précise les points suivants :

- Pas de difficulté à traiter un attribut d'autorisation une fois celui-ci défini.
- Les autres attributs pourront servir
  - soit à enrichir les logs
  - soit à affiner la décision de contrôle d'accès

La décision de contrôle d'accès peut notamment avoir une portée qui dépasse la simple autorisation d'accès au réseau. Elle pourrait notamment porter sur la limitation de la bande passante ou les services autorisés.

Il est donc nécessaire dans un premier temps de **définir ces décisions (les usages) et les attributs entrant dans ces décisions (noms/valeurs)**. Une discussion conjointe Unvinautes et EDUSPOT à ce sujet est nécessaire.

Traçabilité, logs, législation

Entr'ouvert rappelle que le ***nameID*** permet d'obtenir l'identité réelle (nom, prénom, établissement, etc.) auprès de l'IdP. L'IdP doit gérer l'enregistrement des assertions d'authentification délivrées. Le ***nameID***, même ***transient***, est un identifiant unique délivré par l'IdP et associé au compte informatique d'un usager. Il n'existe pas de meilleur identifiant délivré par l'IdP tel que pourrait l'être un uid ou une adresse mail. (Le nameID est une valeur aléatoire prise dans un espace grand.)

Philippe Werle, souligne le fait qu'il est nécessaire pour des questions de législation sur les opérateurs que le portail puisse enregistrer les informations suivantes : nom, prénom, organisation, identifiant, adresse IP, adresse MAC le cas échéant, date et heure de connexion, et cela dès l'ouverture du service et non pas au travers d'une opération ***a posteriori***.

Il est donc nécessaire de **valider le prérequis légal de traçabilité** et les attributs requis (nom, prénom, organisation...) et notamment ceux à faire redescendre dans l'assertion. Une discussion conjointe Unvinautes et EDUSPOT à ce sujet est nécessaire.

```
Démonstration de l'exploitation du portail, présentation des interfaces::
```

Supervision

Les efforts vont être concentrés sur l'extension du serveur SNMP déjà intégré à pfSense. Ainsi le portail fournira un maximum d'information sur son état via ce protocole. Le portail intègre par ailleurs de nombreux outils qui permettent de le superviser (notamment des graphes de suivi type ***rrd***) et de faire des diagnostics.

Interfaces de connexion

Philippe Werle indique que la page de connexion doit préciser que « se connecter implique acceptation des CGU (disponibles en ligne) » .

Une discussion conjointe Unvinautes et EDUSPOT sur les textes apparaissant par défaut sur les interfaces est nécessaire.

```
Interfaces d'accueil (après succès de la connexion)::
```

Frédérick Bigrat demande que le clic sur l'URL demandée au départ s'ouvre dans un nouvel onglet.

Virtualisation

La solution est testée chez Entr'ouvert sur des machines en KVM (base Linux Debian). FreeBSD est connu pour fonctionner sur VMWare et VirtualBox, qui seront les solutions utilisées par les sites de test / pré-déploiement.

En terme de performance, il est possible que FreeBSD ne puisse pas proposer dès maintenant les mêmes qualités que d'autres OS, notamment pour tout ce qui est I/O. Mais cela ne gênera pas les tests.

IPv6

Entr'ouvert souligne les soucis que pose IPv6, liés principalement au fait que le portail captif de pfSense est fortement lié à IPv4, mais aussi que les machines IPv6 sont en général dual IPv4/IPv6 et enfin que le protocole IPv6 a été conçu dans une optique «une IP publique par machine» qui peut encore poser des soucis de changement de pratique de sécurité.

Entr'ouvert émet à ce jour des réserves sur l'intégration d'IPv6 dans la solution, notamment au regard d'un déploiement en pratique d'IPv6.

Redondance

Le protocole CARP intégré à FreeBSD est géré par pfSense : il sera la solution technologique pour gérer la redondance (***fail-over***)

Performances

Frederick interroge Entr'ouvert sur les performances du portail. Entr'ouvert n'a pas encore mené de tests de charge (***NB : ils seront fait prochainement***). Cependant, les briques logicielles impliquées sont performantes : FreeBSD est un excellent noyau réseau, Lasso est une des implémentation les plus performantes dans le traitement des flux SAML 2.0, la partie Python/Django est gérée via lighttpd en FastCGI.

Logs

Entr'ouvert indique que les logs seront stockés localement et/ou exportés (***syslog***).

Ergononomie & infographie

Entr'ouvert demande à être mis en contact le plus tôt possible avec le(s) prestataire(s) en charge des recommendations sur l'ergonomie, le design, l'infographie, etc.

Entr'ouvert évoque une version pour mobile (i.e. petits écrans type iPhone/Android) : sera étudiée dans un autre projet.

Démonstration de l'installation depuis une clé USB

Livraison

EO explique qu'un soucis technique dans la production d'une image ISO est survenu récemment (le 4 janvier matin) et remettra les livrables au plus tard en fin de semaine.

- Un ISO téléchargeable (régulièrement mis à jour) : http://isos.univnautes.entrouvert.com/
- Une documentation consultable en ligne (régulièrement mise à jour): http://wiki.entrouvert.org/Univnautes/DocumentationLivrable