FAIRE ENTRER L'ÉCOLE
DANS L'ÈRE DU NUMÉRIQUE

#EcoleNumerique

Interconnexion des fédérations Education Nationale et Education Recherche

02/07/2015

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'ÉDUCATION
NATIONALE, DE
L'ENSEIGNEMENT
SUPÉRIEUR ET DE
LA RECHERCHE

Pole Orléans-Tours

Présentation

Pôle de compétences national IH2M

Resp. : Alexandre Guyot

Piloté par le Ministère (DNE B)

Identité (resp. : *Nicolas Romero*)

- **Expertise technique**
  - habilitations, authentifications, fédérations, annuaires
- **AMOA, AMOE**
- **Assistance aux académies**
- **Implémentation des politiques d'habilitation nationales**
- **Qualification, intégration, diffusion des briques techniques**

Hub / Hébergement / Messagerie (resp. : Luc Veillon)

- **Mise en œuvre et exploitation du Hub**
- **Hébergement d'applications nationales**
- **Expertise messagerie**

La fédération Education Nationale (1/2)

Objectif initial : rationaliser les accès aux applications nationales centralisées

Permettre de fédérer les académies (IdP) vers

- **Des centres de production nationaux du MEN**
- **Des fournisseurs de services externes (CNDP, Onisep, ...)**

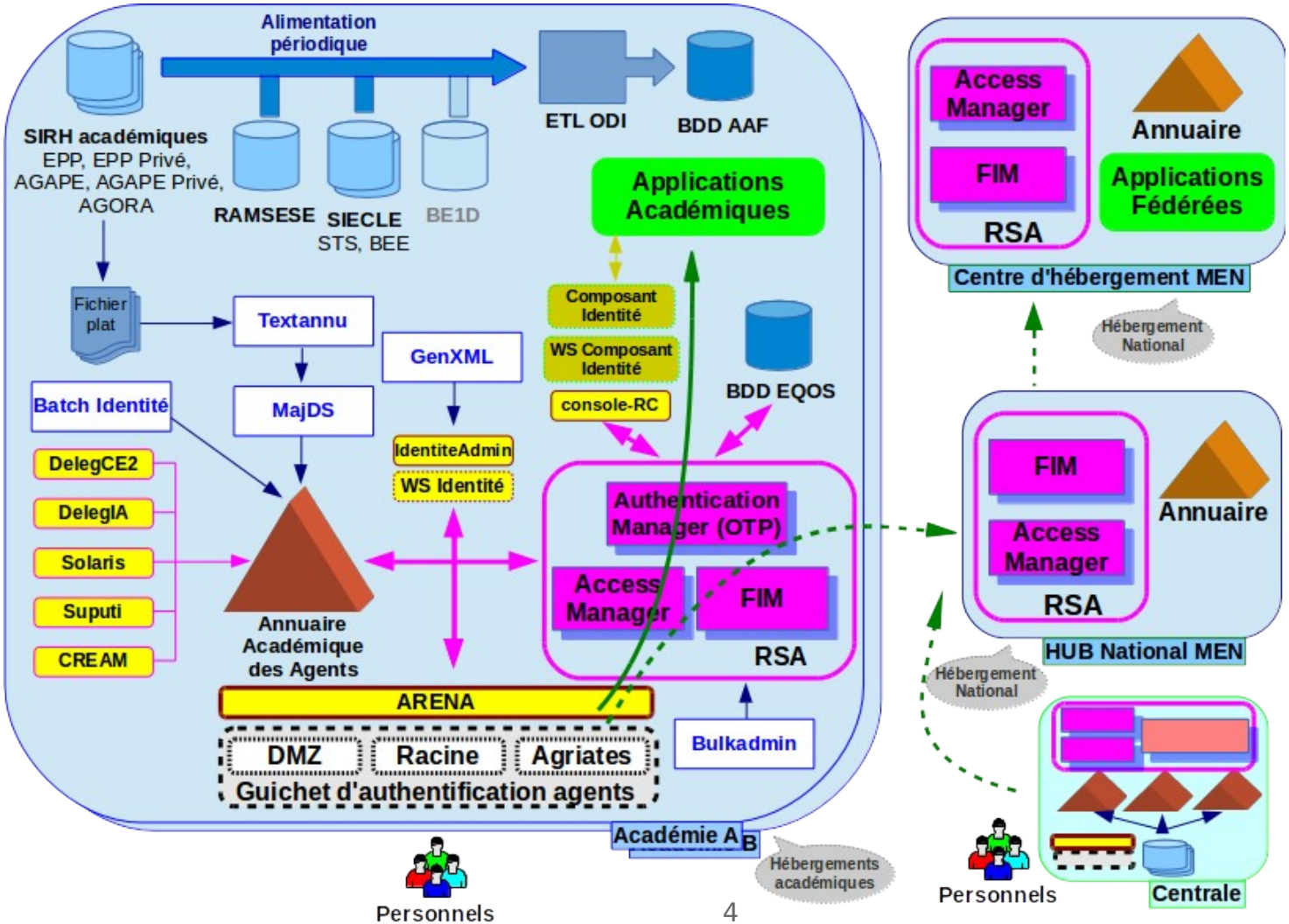
Fédérations internes à l'Education Nationale

- **Partenaires fixés a priori**
  - 32 fournisseurs d'identité (académies + Centrale)
  - 9 fournisseurs de service (centres d'hébergement nationaux)
- **Organisation centralisée et descendante** : articulation MOA / STSI / académies
  - Cadre formel de la GID
  - Périmètre défini : les applications nationales identifiées
  - Contrôles d'accès identiques au niveau des IdP et des SP
- **Des portails d'applications nationales homogènes dans chaque académie**
  - Fédération en mode IdP-initiated
  - Du point de vue de l'utilisateur, pas de différence d'accès que l'application soit fédérée ou non
- **Des infrastructures identiques et un modèle de données partagé**
  - Briques RSA, SAML v2, schéma LDAP « Education Nationale »

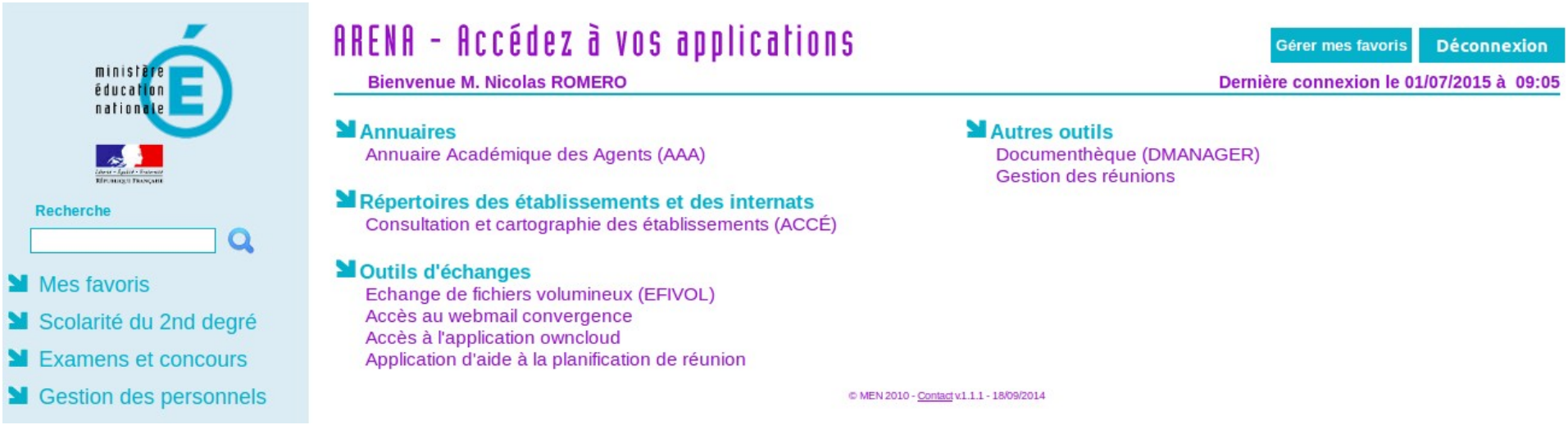
Publics

- **Historiquement les personnels du MEN**
- **Avec les Téleservices / ENT / « numérique pour l'éducation » → élèves et parents**

Architecture type



Portail utilisateur



Portail utilisateur

La fédération Education Nationale (2/2)

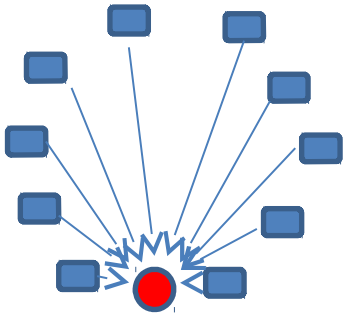
FAIRE ENTRER L'ÉCOLE DANS L'ÈRE DU NUMÉRIQUE
#EcoleNumerique

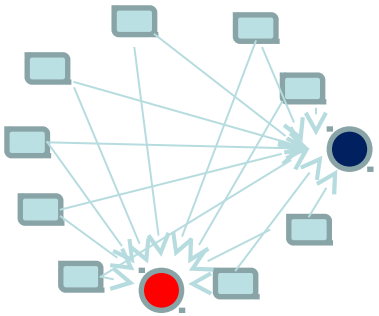
Le Hub de fédération du MEN

Couche d'abstraction technique, fonctionnelle, organisationnelle

Avant le Hub : fédérations « parallèles »

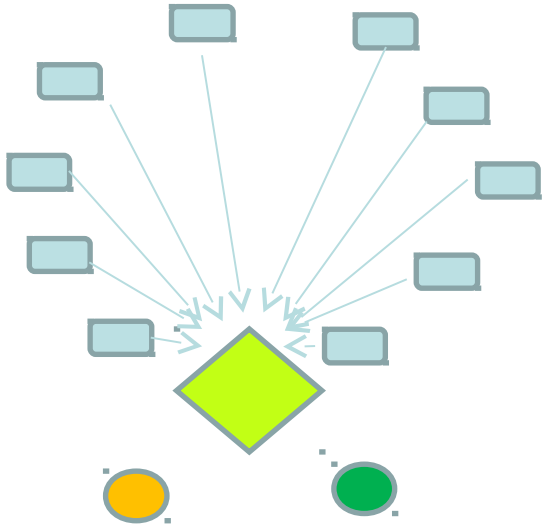
- 32 fournisseurs d'identités
- 9 fournisseurs de service (centres d'hébergement nationaux)
- Fédérations point à point
- Combinatoire : 9 x (32 → 1)





Avec le hub : modèle centralisé « hub-and-spoke »

- Du point de vue des IdP : **un seul** fournisseur de service
- Du point de vus des SP : **un seul** fournisseur d'identité
- 1 x (32 → 1) + n x (1 → 1)



La fédération Education Recherche

Objectif : partager des services

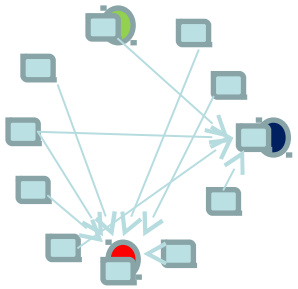
Fédérations dans la sphère Supérieur/Recherche

- **Organisation décentralisée et de gré à gré**
- **Des infrastructures standardisés et un modèle de données partagé**
  - Shibboleth, SAML v2, schéma LDAP « SupAnn »
- Pas d'homogénéité imposée
  - Pas de portail utilisateur « unique » : fédération en mode « SP initiated »
  - Contrôle d'accès porté par le SP

Publics : les personnels, les chercheurs, les étudiants, les externes

Modèle décentralisé « mesh »

- **p x (n → m)**



Les deux approches sont-elles compatibles ?

Oui… mais !

Différences à prendre en compte

- **Modèle organisationnel :** centralisé / décentralisé
- **Infrastructures**
  - « Standards » identiques : SAML2, LDAP
  - Utilisation des spécificités des briques techniques : RSA / Shibboleth
  - Modèles de données à réconcilier : schémas LDAP « Educ Nat » / SupAnn
- **Niveau d'authentification**
  - La fédération MEN prend en compte plusieurs niveaux d'authentification : mot de passe, OTP (, certificats)
    - Avec « surauthentification » possible
  - Pas la FER
- **Expérience utilisateur**
  - Cela doit rester transparent pour l'utilisateur
  - Contrôle d'accès porté par le SP

Pourtant : les besoins existent !

- **Applications nationales de gestion communes**
  - SIRHEN, Galaxie
- **ESPE**
- **Services RENATER**

Planning

Hier

Au niveau national

- Discussions régulières DNE-B / CRU (RENATER) depuis ~2010
- JRES 2011 : Intérêt du monde du Supérieur pour l'approche MEN et réciproquement
- Mais : nécessité d'un cas d'implémentation concret pour avancer

Localement

- Les académies sont conventionnées avec RENATER pour le réseau !
  - Quelques initiatives locales

Aujourd'hui

2014 : accès du Sup à SIRHEN (projet GUILEN)

T4 2014 : début des travaux en collaboration avec RENATER

T1 2015 : Hub MEN → IdP FER en test

Avril 2015 : Hub MEN devient officiellement IdP et ouverture aux académies

En cours : Hub MEN → SP FER et surauthentification

Mise en œuvre technique

Techniquement

En théorie : SAML2 ↔ SAML2

- **Ça devrait être simple**
  - Mais il y a des trous dans les specs, et des particularités de chaque côté

Volonté de s'appuyer sur les briques d'infrastructures existantes et maîtrisées

- **RSA FIM côté Hub, Shibboleth côté FER**
- Conversion des données
  - *Ça c'est simple : plugins spécifiques*
- Chargement des métadonnées
  - *Pas simple : FIM ne fonctionne pas comme Shibboleth → rafraîchissement dynamique pas possible, il faut intégrer les partenaires à la main (ou presque : scripts)*
- Il reste quelques problèmes techniques à régler pour que Hub SP fonctionne « à tous les coups »
  - Indexassertion commence à 1, FIM attend 0
  - Quelques ressources posent problème (MS@home)

Besoin d'une surauthentification au niveau du Hub pour SIRHEN

- **Comment alimenter le référentiel ?**

Organisation

Exigences du MEN

Ne pas perturber l'expérience utilisateur

Ne pas brider l'ouverture de services

S'appuyer sur les portails pour les services officiels

Comment permettre un accès simple et organisé à plusieurs centaines de services potentiels ?

Proposer une organisation simple et non contraignante

Maîtriser le SI et l'offre de services associée

Processus organisationnel pour l 'accès aux services FER

Service déjà dans la fédération → accès immédiat

Service non présent dans la fédération

- Page expliquant à l'utilisateur que l'accès n'est pas possible pour l'instant
  - Demande automatique de validation d'ouverture par l'académie d'origine de l'utilisateur
- Si validation, ouverture du service

Pas de déclaration officielle dans le portail → Commission d'homologation

Service officiel (homologué)

- Définition d'une politique d'habilitation commune
- **Intégration dans les portails**

Conclusion

Techniquement

Ca marche (presque)

- **Une quinzaine de services RENATER déjà ouverts**
- Reste quelques réglages pour la fonction SP

Beaucoup de travaux autour des ESPE

- Interconnexion académies/ESPE (ex : MUSES)
- m@gistère
- Et aussi : surauthentification SIRHEN (GUILEN), Galaxie

Perspectives d'évolution des briques de fédération et du Hub

- Rafraîchissement automatique des métadonnées
- « Scalabilité »
- Interopérabilité avec OpenID Connect / France Connect

Organisationnellement

Processus à affiner

Contacts

Nicolas.Romero@ac-orleans-tours.fr

pole-identite@ac-orleans-tours.fr

Luc.Veillon@ac-orleans-tours.fr