Politique d'habilitation nationale

Fiche projet détaillée

App académique exemple

Gestion des données de l'app académique exemple

Historique du document

Version	Date	Auteur	Nature de la modification
1.0	30/08/2016	LM	Création du document
1.01	06/09/2016	LM	Correction suite retours pôle identité
1.02	09/09/2016	LM	Correction suite retours pôle identité
1.03	26/09/2016	LM	Revue en séance réunion politique d'habitation
1.04	07/11/2016	LM	- Correctifs sur la sélection du CE dans le périmètre d'expérimentation. - Redéfinition des profils accessibles dans le périmètre d'expérimentation - Mise à jour de la liste des établissements expérimentateurs - Ajout du contact Intégration
1.05	07/09/2017	LM	Revu du périmètre établissement en expérimentation

Validation

Le tableau ci-dessous doit obligatoirement être renseigné lors de la réunion de validation de la politique d'habilitation.

Service	Représentant	Date
MOE (CPN)	CPN scolarité 2nd degré – GG	
MOE (CPND)	CPND – APP ACADEMIQUE EXEMPLE – LM	26/09/2016

DNE B2-1	CPN Identité - Farida AZEGGAGH	26/09/2016

Table des matières

Table des matières 3
1 Introduction 4
2 Présentation de l'application 4
2.1 Nom de l'application 4
2.2 Documents de référence 4
2.2.1 Fiche préparatoire 4
2.2.2 Autres documents 4
2.3 Contacts projet 4
3 Politique d'habilitation 5
3.1 Présentation fonctionnelle de la politique d'habilitation 5
3.2 Informations et remarques complémentaires 5
3.3 Définition de la politique d'habilitation 5
3.3.1 Points d'entrée dans l'application 6
3.3.2 Autres ressources protégées 6
3.3.3 Exclusion de la politique d'habilitation 6
3.3.4 Utilisateurs de l'application 7
3.3.5 Accès à l'application 7
3.3.6 Authentification 8
3.3.7 Délégation et assistance 8
3.3.8 Contrôles internes à l'application (optionnel) 9
3.4 Pré-requis techniques 9
3.4.1 Composant de gestion d'identité 9
3.4.2 Type de version du composant de sécurité 9
3.4.3 Méthodes utilisées 9
3.4.4 Paramétrage applicatif 10
4 Fédération 10
4.1 Fournisseurs d'identité 10
4.1.1 Paramétrage technique 10
4.2 Fournisseur de services 11
4.2.1 Paramétrage technique 11
4.3 Vecteur d'identité 11
5 Planning 12
6 Annexe 13

1 Introduction

La politique d'habilitations d'une application est l'ensemble des dispositifs à mettre en œuvre en académie et en administration centrale pour permettre l'accès à l'application. Elle contient notamment

- les règles d'habilitation qui sont mises en œuvre pour gérer l'authentification et les droits d'accès,
- les attributs utilisateurs sur lesquelles se base l'application pour déterminer le profil et le périmètre de responsabilité de chaque utilisateur,
- les niveaux d'authentifications requis selon les ressources et les zones d'accès

La politique d'habilitation est décrite dans deux documents complémentaires :

1. la fiche préparatoire, renseignée par la MOA et le CPN MOE
2. la fiche projet détaillée (ce document), renseignée par le CPN MOE et le CPN Identité.

2 Présentation de l'application

2.1 Nom de l'application

Nom de l'application	APP ACADEMIQUE EXEMPLE

2.2 Documents de référence

2.2.1 Fiche préparatoire

La fiche préparatoire est obligatoire et sert de base de travail à la définition de la politique d'habilitation de l'application.

Référence	Version	Date
Fiche_préparatoire_APPACAEXEMEPLE_1.03	1.03	26/09/2016
liste_etablissements_experimentateurs_1.00.xlsx	1.00	08/11/2016

2.2.2 Autres documents

Voir la fiche préparatoire référencée au §2.2.1

2.3 Contacts projet

Contact	Email	Téléphone
MOA *Voir la fiche préparatoire référencée au §2.2.1* MOE *Voir la fiche préparatoire référencée au §2.2.1* Équipe de développement		
LM	LM@ac-grenoble.Fr	xx xx xx xx xx
Équipe de qualification		
XG	XG@ac-clermont.fr	xx xx xx xx xx
Équipe de diffusion		
TL	LT@ac-nancy-metz.fr	xx xx xx xx xx
Autre		

Intégration SCOLARITE Aïcha GUELLIL	pole-integration@ac-orleans-tours.fr	02 38 79 45 48

3 Politique d'habilitation

3.1 Présentation fonctionnelle de la politique d'habilitation

Décrivez en quelques lignes les différents types d'utilisateurs et leurs droits d'accès à l'application.

Présentation fonctionnelle de la politique d'habilitation	App académique exemple est une application à destination des établissements du second degré pour la gestion des données de l'établissement. Au niveau du portail ARENA, l'application sera accédée en utilisant un et un seul accès intitulé " Vie de l'établissement ". L'application est accessible de plein droit en consultation aux catégories de population CE, CPE, AED, ENS,DOC. ***Le chef d'établissement*** a tous les droits dont les droits d'administration. Il peut par ailleurs déléguer ses droits à toute personne de son établissement. ***Les enseignants*** peuvent accéder aux fonctionnalités de consultation uniquement pour les élèves dont ils ont la charge. . L'application propose un bouton de sortie de l'application : Libellé du bouton : Quitter Description de l'action : Suppression de la session applicative et retour au portail Arena

3.2 Informations et remarques complémentaires

Vous pouvez indiquer ici les informations ou les remarques que vous n'avez pas pu faire figurer ailleurs dans la fiche.

Informations et remarques complémentaires	Le profil PAD est utilisé pour identifier les utilisateurs n'accédant à l'application qu'en délégation

3.3 Définition de la politique d'habilitation

La politique d'habilitation distingue 3 types de ressources :

- les ressources à protéger et à afficher dans Arena : ce sont les liens qui s'afficheront dans Arena qui sont des points d'entrée dans l'application
- les ressources à protéger mais à ne pas afficher dans Arena : ce sont des ressources internes à usage interne à l'application, ou par ex des URL "de délégation" à n'afficher que dans DELEGCE2

- les ressources à exclure de la protection et à ne pas afficher non plus dans Arena : par ex, la page racvision.

3.3.1 Points d'entrée dans l'application

La liste des domaines et sous-domaines Arena est référencée en annexe. Si le domaine ou sous-domaine souhaité n'apparaît pas, il faut contacter le CPN Identité.
L'affichage dans Pléiade n'est à définir que pour les applications concernées.
Vous devez définir autant de ressources que de liens d'accès dans la fiche préparatoire référencée au §2.2.1.

Nom de la ressource		vieetab
Description		Ressource proposée aux personnes du second degré ayant accès de plein droit à l'application. Elle englobe toutes les fonctionnalités de l'application. **Cette ressource est délégable via KIALEDROUAT.**
Affichage ARENA	Domaines	Domaine xxx
	Sous-domaine	sous domaine yyy
	Libellé	Accès à app acad exemple
	Numéro d'ordre	…
URL	Lien d'accès	/appae/index.html
	Arborescence	/appae/*

3.3.2 Autres ressources protégées

Nom de la ressource		vieetab_secure
Description		Ressource permettant de sécuriser les accès aux fonctions d'administration depuis la DMZ dont l'authentification par OTP est obligatoire. Cette ressource sera appelée systématiquement avant l'accès aux fonctionnalités d'administration.
URL	Lien d'accès	S.O
	Arborescence	/vieetab/secure/*

3.3.3 Exclusion de la politique d'habilitation

Précisez si certaines pages de l'application ne doivent pas être protégées, par exemple, les pages Racvision.

Ressource	**Description**
/appae/racvision	**Page de supervision applicative**

3.3.4 Utilisateurs de l'application

*Pour chacun des types d'utilisateurs définis dans la fiche préparatoire 2.2*référencée au §2.2.1, *précisez les règles techniques de sélection. Il peut s'agit de règles basées sur les attributs LDAP ou sur des groupes LDAP de l'annuaire.*
Par exemple, pour les chefs d'établissement : « l'attribut FrEduFonctAdm est égal à DIR » ou pour un groupe : « membre du groupe GRP_GEST».

La liste des attributs LDAP est référencée en annexe.

Règles spécifiques pour l'expérimentation

Utilisateurs	Règle de sélection
CE	FrEduFonctAdm=DIR
PAD	possède une entrée dans l'attribut délégation

Prendre en compte la liste des codes RNE des établissements expérimentateurs – L'expérimentation est limitée sur l'académie de Grenoble

Cf liste_etablissements_experimentateurs_1.00.xlsx

Règles à appliquer pour la généralisation

Utilisateurs	Règle de sélection
AED	title=AED
CPE	title=EDU
CE	FrEduFonctAdm=DIR
DOC	title=DOC
ENS	Title=ENS et l'établissement contient $T3$
PAD	dispose d'une délégation

3.3.5 Accès à l'application

Précisez quels utilisateurs (cf §3.3.24) accèdent aux différentes ressources (cf §3.3.1).
Cochez avec un X les zones d'accès concernées pour chaque type d'utilisateur.

Utilisateur	Ressource	Accès depuis le réseau administratif de l'établissement scolaire	Accès pour les agents des services déconcentrés		Accès pour les agents de l'administration centrale		Accès depuis la fédération Education-Recherche
		Agriates	Racine	DMZ	Racine	DMZ	DMZ
CE	/appae/index.html	**X**		**X**			
CPE	/appae/index.html	**X**		**X**			
ENS	/appae/index.html	**X**		**X**			
AED	/appae/index.html	**X**		**X**			
DOC	/appae/index.html	**X**		**X**			
PAD	/appae/index.html	**X**		**X**			
CE	/appae/secure	**X**		**X**			
PAD	/appae/secure	**X**		**X**			

3.3.6 Authentification

*Cochez avec **X** les cases correspondant aux niveaux d'authentification pour chaque ressource définie au §3.3.1.*

Ressource	Accès depuis un établissement	Accès pour les agents des services déconcentrés		Accès pour les agents de l'administration centrale		Accès depuis la fédération Education-Recherche	
	Agriates	Racine	DMZ	Racine	DMZ	DMZ	
/appae/index.html	**X**		**X**				Mot de passe
	X		**X**				OTP
/appae/secure	**X**						Mot de passe
	X		**X**				OTP

3.3.7 Délégation et assistance

Cocher la case correspondante avec X pour préciser les informations de la fiche préparatoire référencée au §2.2.12.2.

Délégation	Assistance	Sans objet
X	**X**	

3.3.8 Contrôles internes à l'application (optionnel)

Précisez si possible les tests internes à l'application.

<table>
<tr><td>Contrôles internes à l’application</td><td>On vérifie pour tous les utilisateurs que le périmètre récupéré par le vecteur identité contient des établissements actifs.

Ce périmètre est ensuite réduit pour les enseignants :
- aux divisions pour lesquelles une responsabilité existe
- aux divisions pour lesquelles l’enseignant est le professeur principal (Echange avec l’application APP)

Une fois l’utilisateur connecté, un rôle lui est associé :

<table>
<tr><td>Rôle</td><td>Description</td><td>Utilisateur</td></tr>
<tr><td>ADMIN</td><td>Accès à toutes les fonctionnalités

Elles sont restreintes aux élèves de leurs établissements.</td><td>CE, PAD</td></tr>
<tr><td>CONSULTATION</td><td>Accès aux fonctionnalités de consultation.</td><td>ENS, DOC, CPE,AED</td></tr>
</table>

Certaines fonctionnalités de l’application nécessitent une authentification OTP depuis la DMZ, dans ce cas l’application déclenche un appel vers /vieetab/secure pour s’assurer que l’utilisateur bénéficie d’une authentification forte.</td></tr>
</table>

3.4 Pré-requis techniques

3.4.1 Composant de gestion d'identité

La liste des versions du composant de gestion d’identité est référencée en annexe.

Version du composant identité utilisée dans l'application	4.8.4

3.4.2 Type de version du composant de sécurité

Cocher la case correspondante avec X pour précise si le composant sécurité est utilisé dans sa version WebService ou Java.

Version Webservice	**Version Java**
	X

3.4.3 Méthodes utilisées

Précisez ci-dessous :

La ou les méthode(s) du composant de gestion d'identité qui seront utilisées pour récupérer les attributs LDAP nécessaires

- *à la politique d'habilitation (cf §3.3.2),*
- *à la gestion interne à l'application (cf §3.3.8),*
- *aux divers besoins de l'application (par exemple, l'email) ;*

Vérifiez que les méthodes nécessaires existent bien dans la version du composant souhaitée.

La liste des méthodes du composant de gestion d'identité est référencée en annexe.

Méthode du composant de gestion d'identité	Utilisation	Attribut(s)
getEtablissements()	Récupérer le périmètre en responsabilité d'un profil CE	RespExtractEnum.ETAB_N_UAJ
getEtablissements()	Récupérer l'affectation des profils ENS, CPE, AED, DOC	RespExtractEnum.ETAB_ENS
getEtablissements()	Récupérer le périmètre de délégation pour les ressources délégués	DelegExtractEnum.ETAB_N_UAJ, /vieetab/index.html
getUtilisateur()	Récupération des informations utilisateur	

3.4.4 Paramétrage applicatif

Précisez le nom technique de l'application, tel qu'il sera connu à la fois dans RSA Access Manager, au niveau du serveur d'application et des appels au composant identité.

Nom technique de l'application	appae

4 Fédération

Ce paragraphe ne concerne que les applications fédérées.

4.1 Fournisseurs d'identité

Précisez si l'application fédérée sera accessible depuis la centrale, pour toutes les académies, ou pour certaines académies.
Dans le cas d'un accès par certaines académies, renseignez la liste exhaustive des académies concernées.

Académies		Toutes
		Aucune
	Liste	
Administration Centrale		Oui
		Non
Fédération Recherche (FER)		Oui
		Non

4.1.1 Paramétrage technique

Ce paragraphe sera complété avec le Pôle IH2M.

Précisez le paramètre technique applicationname pour chaque ressource ***associée à un point d'entrée*** *dans l'application.(§3.3.1)*

Ressource	Paramètre applicationname	
	Agriates	
	Racine	
	DMZ	
	Agriates	
	Racine	
	DMZ	

4.2 Fournisseur de services

Ce paragraphe sera complété avec le Pôle IH2M.

*Définissez le centre d'hébergement de l'application et les url du fournisseur de services pour chaque ressource (****points d'entrée §3.3.1 et autres ressources §3.3.2****).*

La liste des centres d'hébergement est référencée en annexe. Si le centre d'hébergement souhaité n'apparaît pas, il faut contacter le CPN Identité.

Ressource	Centre d'hébergement	Url du FS	
		Agriates	
		Racine	
		DMZ	
		FER	
		Agriates	
		Racine	
		DMZ	
		FER	

4.2.1 Paramétrage technique

Ce paragraphe sera complété avec le Pôle IH2M.

Précisez si l'application utilisera un Hub de fédération national, en cochant avec un X les cases concernées.

Non	
HN01	
HN02	

4.3 Vecteur d'identité

Définissez la liste des attributs contenus dans le vecteur d'identité, en prenant soin de sélectionner au moins un attribut « clé de jointure », en cochant avec un ***X*** *les cases concernées.*

La liste des attributs est référencée en annexe. Si un attribut souhaité n'apparaît pas, il faut contacter le CPN Identité.

Accès Académies/Centrale	
Clé de Jointure	**Attribut**

Accès FER	
Clé de Jointure	**Attribut**

5 Planning

La politique d'habilitation doit être initiée dès la phase d'avant-projet, car elle peut avoir un impact sur le développement de l'application.

La diffusion des éléments relatifs à la mise en place de la politique d'habilitation décrite dans ce document est soumise à :

- la validation de la fiche par toutes les parties prenantes matérialisées dans le tableau de validation,
- la réception par le CPN Identité d'un GO/NO GO explicite (Jalon J6) envoyé par le CPN en charge de l'application concernée.

La phase d'expérimentation est optionnelle. Si elle a lieu, la diffusion des éléments relatifs à la mise en place de la politique d'habilitation pour l'expérimentation est soumise à l'envoi par le CPN en charge de l'application concernée au CPN Identité :

- d'un GO/NO GO explicite (Jalon J3),
- de la liste des académies participant à l'expérimentation (Jalon J3).

Les dates des jalons J2, J3, J4, J6, J7 seront renseignées lors de la réunion de validation.

	Jalon	Etape	Délai	Acteurs	Date
Réalisation	**J1**	Validation de la fiche de politique d'habilitation		*MOA, CPN MOE* *CPN Identité, Pôle Identité, Diffusion Identité*	
	J2	Diffusion des éléments identité pour la qualification	*Au **minimum** J1 + 15 jours*	*Pôle Identité* *Equipe de qualification*	10/10/2016
Expérimentation	**J3**	GO/NO GO de mise en expérimentation de l'application et envoi de la liste des établissements et des académies concernées		*CPN MOE* *CPN Identité*	28/11/2016

	J4	Diffusion des éléments identité pour l'expérimentation	*Au **minimum** J3 + 7 jours*	*Pôle Identité*	05/12/2016
	J5	Mise en expérimentation de l'application	*Au **minimum** J4 + 7 jours*	*CPN MOE*	12/12/2016
Généralisation	**J6**	GO/NO GO de mise en production de l'application		*CPN MOE* *CPN Identité*	
	J7	Diffusion des éléments identité	*Au **minimum** J6 + 7 jours*	*Pôle Identité, Diffusion Identité*	
	J8	Mise en production de l'application	*Au **minimum** J7 + 7 jours*	*CPN MOE*	

6 Annexe

Référence	Document
Liste des domaines Arena	Sur le site du pôle rubrique Pôle IH2M - Identité > Gestion des accès > Politiques d'habilitations > Chaîne Agents
Liste des sous-domaines Arena	Sur le site du pôle rubrique Pôle IH2M - Identité > Gestion des accès > Politiques d'habilitations > Chaîne Agents
Liste des attributs LDAP	Sur le site de la diff rubrique Annuaire AAA/LDAP > LDAP > Alimentation Annuaire LDAP
Liste des versions et méthodes du composant de gestion d'identité	La documentation : sur la forge La dernière version : su la forge
Liste des centres d'hébergement	Sur le site du pole rubrique Pôle IH2M - Identité > Fédération > Chaîne Agents
Liste des attributs pour le Vecteur d'Identité	Sur le site du pole rubrique Pôle IH2M - Identité > Fédération > Documents