ADULLACT

Association des Développeurs et des Utilisateurs de Logiciels Libres pour les Administrations et les Collectivités Territoriales

GROUPE DE TRAVAIL COLLABORATIF AUTHENTIK

COMPTE RENDU DE LA SÉANCE DE TRAVAIL DU 12 MAI 2016 À PARIS BD DIDEROT

SUJET :	GTC AUTHENTIK	RÉDACTEUR : RELECTURE :	ADULLACT - Pascal KUCZYNSKI Pascal.Kuczynski@adullact.org ENTR'OUVERT - Mikael ATES mates@entrouvert.com
OBJET :	Compte rendu de réunion	STATUT :	Valide
DATE :	12 mai 2016	DATE DIFFUSION :	20 mai 2016

LISTE DES PARTICIPANTS :

COLLECTIVITÉS	PARTICIPANTS
Conseil Départemental de Seine Maritime	Mickael HERVIEUX
Communauté Urbaine de Dunkerque	Patrick LANVIN
Centre de Gestion des Côtes d'Armor	Jérôme LE NOUVEL
Conseil Départemental de la Drôme	Catherine LEPOUTRE
Ville de Paris	Pierre LEVY
Ville de Paris	François MERLIN
Conseil Départemental de la Gironde	Yvon NGARBOUI
Conseil Départemental des Côtes d'Armor	Delphine ROUXEL
CA Valence Roman Sud Rhône Alpes	Xavier VEVE
ADULLACT	Pascal KUCZYNSKI
Entr'ouvert	Mikael ATES
Entr'ouvert	Brice MALLET

LISTE DES CONTRIBUTEURS EXCUSÉS :

COLLECTIVITÉS	PARTICIPANTS
Ville de Villenave d'Ornon	Jean-Paul ARAMBURU
Ville d'Orvault	Françoise CANEVET
Ville de Limoges	Olivier CARLES
Ville de Porto-Novo	Abdou Kadiri KITOYI
Ville d'Albi	Jean-François MARTEL

SUJET :	GTC AUTHENTIK	RÉDACTEUR :	ADULLACT - Pascal KUCZYNSKI Pascal.Kuczynski@adullact.org
OBJET :	Compte rendu de réunion	STATUT :	Valide
DATE :	12 mai 2016	DATE DIFFUSION :	20 mai 2016

SOMMAIRE

SUJET :	GTC AUTHENTIK	RÉDACTEUR :	ADULLACT - Pascal KUCZYNSKI Pascal.Kuczynski@adullact.org
OBJET :	Compte rendu de réunion	STATUT :	Valide
DATE :	12 mai 2016	DATE DIFFUSION :	20 mai 2016

1. ORDRE DU JOUR

11H00 - 11H10	Accueil des participants
11H10 - 11H30	Tour de table - Témoignages
11H30 - 13H15	Présentation de AUTHENTIK
13H15 - 14H00	Pause déjeuner
14H00 - 15H00	Évolutions enregistrées - Discussions
15H00 - 15H30	Planning et conclusion

Pièce jointe : le fichier de présentation présenté en séance.

2. INTRODUCTION

ADULLACT ouvre le GTC et en rappelle le principe. Les participants sont invités à se présenter et décrire leur degré d'implication sur la Gestion d'Identité.

2.1. TOUR DE TABLE

- **Communauté Urbaine de Dunkerque** (CUD) : avait lancé un appel d'offre emporté par Entr'ouvert – Les premières expérimentations en cours montrent que le problème de Gestion d'Identité (GI) est plus un problème d'organisation que technique et génère beaucoup de questions. La CUD mutualise son service informatique avec la ville de Dunkerque.

- **Conseil Départemental de Seine Maritime** (CD76) : le besoin de GI en interne commence à se faire sentir. Le CD76 participe à ce GTC pour découvrir la GI et AUTHENTIK. Le CD76 utilise également les outils libres i-parapheur et as@lae.

- **Conseil Départemental de Côte d'Armor** (CD22) : une réflexion est engagée autour de France Connect et de la GI en général. Le CD22 participe à ce GTC pour découvrir la GI et AUTHENTIK.

- **Conseil Départemental de la Drôme** (CD26) : une réflexion est engagée autour de France Connect et de la GI en particulier à l'occasion de la refonte des sites internet et des outils RH.

- **Ville de Paris** : C'est à l'occasion du développement de la gestion des relations usagers dans LUTECE que la ville de Paris s'est sérieusement intéressée à la GI. De nombreux problèmes autour de la GI ont été identifiés du fait de la diversité des outils (*novell, cas, openam*). Paris vient chercher de l'expertise sur la GI avec Entr'ouvert qui reste une référence sur le sujet. Remarque : la ville de Paris est déjà opérationnelle sur France Connect, dont 2 projets avec la DINSIC (cartes de stationnement & quotient familial).

- **Centre de Gestion des Côtes d'Armor** (CDG22) : exprime le besoin de GI pour ses propres collectivités adhérentes et leurs agents (~15000 agents au total). Besoin de sécurité : ouverture à la GED ainsi qu'aux données confidentielles des agents.

- **Communauté d'Agglomération de Valence** : quelques applications fonctionnent avec un SSO (Single Sign One) mais il n'y a pas de solution globale. La CA vient chercher des informations et participe à ce GTC pour découvrir la GI et AUTHENTIK.

- **Entr'ouvert** : éditeur des offres PUBLIK et **AUTHENTIK** sous licences libres. Mikaël ATES est un expert GI. Il en a fait sa thèse de doctorat. Mikaël ATES a été élu gérant de Entr'ouvert en juin 2015. Entr'ouvert est une SCOP née en 2002 dédiée aux logiciels libres. Il y a 9 salariés et elle intègre le réseau "libre-entreprise". 5 personnes travaillent sur AUTHENTIK.

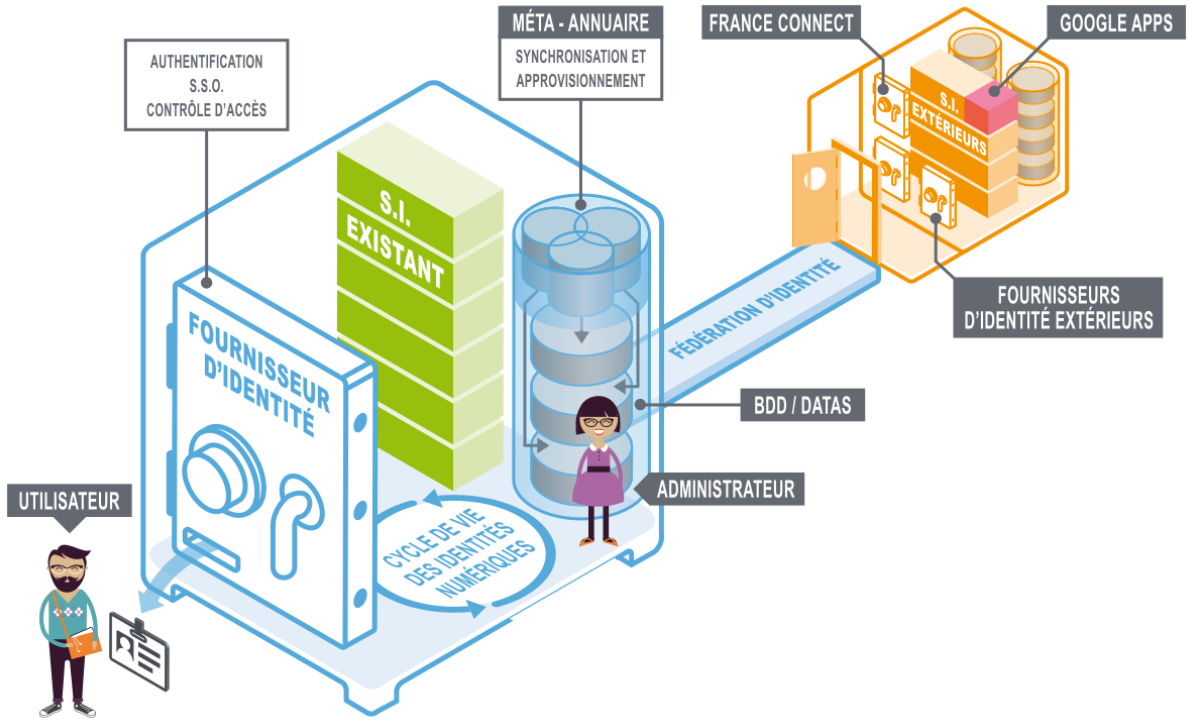
2.2. PRÉSENTATION ENTR'OUVERT

En 2004, Entr'ouvert avait travaillé sur "Mon service public" avec la DGME, ce qui a donné naissance à la librairie LASSO conforme SAML2. Les travaux ont continué. Lasso intègre aujourd'hui l'offre AUTHENTIK. C'est une boite à outils qui permet de gérer les identités numériques que ce soit en interne (agents) ou en externe (gestion relation usagers).

Entr'ouvert a ainsi acquis une réputation d'expert en gestion d'identité reconnue par de nombreuses collectivités (Paris, CDG59, ...)

3. PRÉSENTATION AUTHENTIK

AUTHENTIK a déjà été déployé dans plusieurs structures publiques parmi lesquelles on peut compter : la DGME, la Gendarmerie Nationale, des universités, le CD14, le Ministère de l'Intérieur, Alfortville, la Métropole de Montpellier, Nancy, Orléans, Vincennes…



Il convient de préciser quelques définitions:

- authentification = preuve de possession d'identité (mot de passe, certificat…).
- ouvrir une session = identification (IBAC) + rôles (RBAC) et attributs (ABAC).
- Annuaire = répertoire d'informations souvent liées à l'identité (login, mot de passe, service...). Standard : LDAPv3.

3.1. DESCRIPTION AUTHENTIK

AUTHENTIK est une boite à outils comprenant l'outil "authentic2" dont les sources sont déposées sur la forge Entr'ouvert[1].

Mikaël ATES réalise une démonstration AUTHENTIK en ligne, ce qui permet de mieux comprendre l'importance des interactions entre les notions d'identification, gestion des utilisateurs, des rôles, et du cas particulier de l'administrateur.

Présentation du *back-end* qui offre une gestion des référentiels d'identités, et du *front-end* qui permet l'interface avec l'utilisateur. Il y a 2 possibilités pour la création de compte : création de compte par l'utilisateur (avec ou sans modération) ou par l'administrateur.

Description de la gestion des rôles. Il y a 2 rôles institués par défaut : administrateur des utilisateurs et administrateur des rôles (create/delete/modify).

Par définition, l'objectif d'un SSO est de simplifier la vie de l'utilisateur.

Il est intéressant d'offrir à l'utilisateur la possibilité de supprimer un lien de fédération d'identité, surtout s'il s'agit d'utilisateurs externes (ex : un usager d'une collectivité). Dans ce cas l'idéal est que l'usager continue à pouvoir exploiter les services via un compte local. C'est ce que permet AUTHENTIK en demandant par exemple un mot de passe lors de la suppression d'un lien avec un compte France Connect si l'utilisateur n'a pas de mot de passe. On peut aussi vouloir imposer l'utilisation de la fédération d'identité (et donc ne pas permettre de supprimer le lien) par exemple pour les utilisateurs internes tels que les agents de la collectivité.

AUTHENTIK s'interface naturellement avec des fournisseurs de service SAML2 et CAS. L'intégration est donc simplifiée pour les applications supportant ces protocoles.

A l'inverse, il peut être possible de passer par un outil tiers d'intégration (lasso, simplesamlphp, django-mellon, modmellon, etc.). Si ça n'est pas possible non plus, on passe par un **reverse proxy**.

Un « reverse proxy » permet de faire le "rejeu" du login/mdp auprès de l'application cible. Cela impose d'avoir un connecteur par application cible. L'idée consiste à intercepter la page de login de l'application, et d'enregistrer le lien entre le SSO et le login local lors de la 1ère connexion. Dès la 2eme connexion, le lien étant déjà fait, l'utilisateur n'aura pas à retaper son login/mdp local à l'application : son login SSO fonctionnera grâce au lien précédemment enregistré. Comme décrit plus haut, on peut éventuellement permettre à l'utilisateur de supprimer ce lien (cas des utilisateurs externes).

1 http://dev.entrouvert.org/

Une nouvelle démonstration de AUTHENTIK permet de comprendre comment ajouter un SSO dans AUTHENTIK, ou comment re-habiller un login d'application avec un « reverse proxy ».

3.2. PARENTHÈSE FRANCE CONNECT

France Connect est un proxy d'identité auprès de fournisseurs d'identités fiables et labellisés par l'État. (DGFiP, La Poste, …). AUTHENTIK sait se brancher sur France Connect.

Mikaël ATES nous montre une implémentation France Connect pour la métropole de Montpellier.

Remarque : dans l'implémentation AUTHENTIK, on peut voir que si un administré, après avoir créé son compte avec France Connect, décide de supprimer ce lien entre France Connect et le compte usager de la métropole, s'il n'a pas de mot de passe (cas d'un compte créé automatiquement après un SSO France Connect), alors un mot de passe lui est demandé pour que l'usager puisse conserver l'accès à son compte. Ainsi, le compte de l'administré continue d'être actif et opérationnel.

Remarque : AUTHENTIK permet également de relier plusieurs comptes France Connect avec un seul compte usager de la métropole de Montpellier.

Si besoin, AUTHENTIK sait se connecter à plusieurs annuaires LDAP. Attention : il n'est pas là pour administrer ces LDAP[2].

Les collectivités sont souvent confrontées à la multiplication des annuaire et des référentiels d'identité (ex : outil RH qui gère la base agents, LDAP pour l'annuaire interne, voire plusieurs LDAP selon les services…). Des outils de synchronisation pourront être utilisés pour rationaliser et automatiser certaines tâches d'administration.

3.3. PROCESSUS DE DÉVELOPPEMENT CHEZ ENTR'OUVERT

Mikaël ATES énumère plusieurs protocoles de développements opérationnels dans les équipes Entr'ouvert.

- Chaque développement est packagé sous la forme d'un paquet Debian 7 et 8. Il existe 3 dépôts dev/test/prod pour chaque distribution. Si l'outil est destiné à fonctionner sous une autre distribution Linux que Debian, il est possible de travailler directement à partir des sources disponibles sur la forge.

- Les versions déployées chez les utilisateurs d'AUTHENTIK sont suivies à l'aide de l'outil SCRUTINY.

- Tous les tickets sont publics et visibles (redmine).

- Le cycle d'un nouveau développement est le suivant : développement/patch sur redmine/revue de code/test/commit sur la forge puis recettage/mise en production.

- Tous les produits Entr'ouvert disposent d'un processus d'intégration continu et de tests automatiques.

2 cf la société EASTER EGGS qui a développer un outil libre pour cela

- Les produits Entr'ouvert sont respectueux du RGAA.

Mikaël ATES fait remarquer que les développements sur l'outil authentic2 doivent être et sont très réactifs. Le produit est donc versionné sur le n° de version + révision: ex 2.1.20-960, 2.1.20.988… Il n'y a pas de version formelle annoncées plusieurs mois à l'avance. La prochaine version importante : v2.2, intégrera les nouvelles "grosses" évolutions.

4. ÉVOLUTIONS

4.1. ÉVOLUTIONS PRÉVUES

- Contrôle d'accès au SSO (date : 3ème trimestre 2016).
- Fournisseur d'identité OpenID Connect (pas de date annoncée).
- Implémentation de la délégation de rôle - utile pour PUBLIK (pas de date annoncée). Remarque : plusieurs collectivités présentes autour de la table font état de leur intérêt pour cette évolution.
- Synchronisation des rôles entre authentic2 et LDAP (pas de date annoncée).

4.2. ÉVOLUTIONS SOUHAITÉES MAIS NON PROGRAMMÉES

- GUI pour déclarer les LDAP dans authentic2 plutôt que de simples fichiers de configuration (pas de date annoncée).
- Implémenter et rendre générique authentic2 en client pour les divers protocoles de SSO (SAML2, CAS, OIDC). ex: le logout SAML2 est différent du logout OIDC.
- Créer un SSO basé sur des cookies.
- Développement de nouveaux plugins authentic2.
- MandayeJS : nouveaux connecteurs sur divers produits du marché (ex: arpege, archimed, …).

4.3. QUESTIONS DES COLLECTIVITÉS PRÉSENTES

- Centre De Gestion 22
  - Q : AUTHENTIK peut-il traiter des authentifications fortes utilisant des SMS ?
  - Réponse Entr'Ouvert : Rien de tel n'est prévu.
  - Q : Par certificats ?

- Réponse Entr'Ouvert : C'est déjà le cas.

- Ville de Paris
  - Q : AUTHENTIK peut-il être serveur de fédération ?
  - Réponse Entr'Ouvert : Oui. Authentic2 peut être utilisé comme « IDP technique » en proxy vers un autre IdP.
  - Q : AUTHENTIK est-il interopérable ? Par exemple comment l'interfacer avec LUTECE ?
  - Réponse Entr'Ouvert : C'est tout à fait concevable et nous aimerions bien voir AUTHENTIK fonctionner avec LUTECE...

La discussion se termine avec une démonstration de la forge Entr'ouvert avec l'outil REDMINE.

5. MODÈLE ÉCONOMIQUE ET FINANCEMENTS

Entr'ouvert auto-finance un certain nombre d'évolutions (cf ci-dessus) et il y a aussi de nombreuses évolutions liées à des demandes récurrentes dans les CCTP. D'autres besoins liés à des besoins collatéraux de Entr'ouvert, tel que l'outil PUBLIK, sont auto-financés.

Globalement Entr'ouvert investit environ 150 000 € / an en recherche et développement dont une partie de traduit en développement de nouvelles fonctionnalités. Entr'ouvert reste aussi à l'écoute de ses clients et doit être en mesure de répondre à leurs besoins urgents si ces derniers sont prêts à les financer.

Les contrats de maintenance que propose Entr'ouvert à ses clients intègre un support et les évolutions correctives. Il est fait remarqué qu'il serait souhaitable de préciser dans le contrat de maintenance que les évolutions réglementaires y soient incluses.

6. CONCLUSION ET SUITES

Pascal KUCZYNSKI remercie tous les participants du GTC et conclut la journée en annonçant :

- la création d'une mailing list dédiée qui permettra de faire vivre la communauté AUTHENTIK composée des utilisateurs déjà actifs et des collectivités qui s'intéressent au sujet (sur le modèle d'autres mailing lists équivalentes relatives à d'autres GTC).
- L'organisation avant la fin de l'année d'une Web-conférence sur le thème générique de la gestion d'identités de type SAML2 (sous réserve de disponibilités des divers acteurs).
- L'organisation d'un nouveau GTC AUTHENTIK en 2017 (sous réserve de nouveautés à présenter et de l'activité de la communauté).