DOSSIER DE SECURISATION DES WEB SERVICES

ANNEXE 1 : ANALYSE DE SECURITE PREALABLE

TABLE DES MATIERES

1.AVANT PROPOS

Ce document constitue une annexe du « Dossier de sécurisation des Web Services » publié par l'AMUE. Il a pour objectif de présenter l'analyse de sécurité préalable dans un objectif de sécurisation des Web Services. Par conséquent, afin d'appréhender correctement le contexte et le contenu de ce document, il est conseillé de lire au préalable le dossier de sécurisation des Web Services [DOSSIERSECWS].

Ce document est mis à la disposition des établissements pour illustrer une approche d'analyse de sécurité sur un domaine donné.

2.OBJECTIFS DE L'ANALYSE SECURITE PREALABLE

L'analyse sécurité préalable a pour objectif principal de prendre connaissance du contexte métier et technique dans lequel se trouvent les web services à sécuriser ainsi que des éventuelles contraintes pesant sur l'architecture qui supportent ces derniers.

De ces informations, on déduit non seulement les risques les plus importants mais également la sensibilité des données manipulées. Cela permet donc d'établir le contexte « sécurité ».

L'objectif ultime est de fixer le bon niveau de sécurité à adopter sur l'ensemble des thèmes de sécurité abordés dans l'étude pour ne pas faire de sur-sécurité ni de sous-sécurité.

Par ailleurs, certains éléments reportés dans ce document dépassent le cadre de l'analyse sécurité et seront des points d'entrée pour l'étude proprement dite.

3.METHODOLOGIE

3.1. LA METHODOLOGIE

L'analyse sécurité préalable s'appuie sur des entretiens avec les différents experts de l'AMUE. Les questions posées ont pour objectif d'identifier le plus précisément possible les risques généraux, les scénarios de risques possibles.

Les questions ont porté sur les thèmes suivants :

- L'organisation,
- L'architecture SOA,
- Aspects métiers,
- Place des WS dans le workflow global,
- Estimation des risques.

3.2. QUESTIONNAIRE

3.2.1. L'ORGANISATION

ORG.Q1 : Quel est le rôle exact de l'AMUE ?

ORG.Q2 : Quelle relation existent avec les universités ?

ORG.Q3 : Existe-t-il des contraintes organisationnelles de nature à impacter les services publiés ? Attribution de droits…?

3.2.2. L'ARCHITECTURE SOA

SOA.Q1 : existe-t-il des documents décrivant techniquement l'architecture SOA ?

SOA.Q2 : existe-t-il une cartographie des services publiés ? Sous quelle forme ? Quel périmètre ?

SOA.Q3 : y a-t-il des évolutions technologiques majeures prévues à court et moyen terme ?

SOA.Q4 : existe-il un document précisant la place de l'architecture SOA dans le système d'information global ? Interaction avec les différentes briques du SI (référentiels, serveur d'authentification, passerelle d'accès, firewall, VPN, plus globalement tous les équipements traversés par le workflow web services…)

SOA.Q5 : existe-t-il des contraintes particulières liées à cette architecture SOA ?

SOA.Q6 : existe-t-il des mesures de sécurités existantes pour ces web services ?

3.2.3. ASPECTS METIERS

MET.Q1 : quelles sont les fonctions métiers des web services à sécuriser ?

MET.Q2 : y a-t-il des contraintes métiers particulières liées à ces web services ?

MET.Q3 : y a-t-il des données personnelles manipulées dans ces web services ?

MET.Q4 : y a-t-il des données confidentielles manipulées dans ces web services ?

MET.Q5 : y a-t-il des besoins forts en intégrité ?

3.2.4. PLACE DES WEB SERVICES DANS LE WORKFLOW GLOBAL

WORK.Q1 : les web services sont ils interrogés directement ou bien y a-t-il des enchaînements de web services (web services qui en appellent d'autres) ?

WORK.Q2 : existe-t-il une description même partielle du workflow global dans lequel s'inscrivent les appels et les réponses des web services ?

3.2.5. RISQUES

RISK.Q1 : les environnements susceptibles d'appeler les web services présentent il des risques particuliers ?

RISK.Q2 : si, pour une raison quelconque, un ou plusieurs deviennent indisponibles, quels sont les impacts ?

3.3. SYNTHESE DES REPONSES FOURNIES

3.3.1. L'ORGANISATION

L'AMUE, est un groupement d'intérêt public à vocations multiples, dont :

- une vocation d'éditeur,
- une vocation d'intégrateur,
- une vocation de partenaire.

La présente étude se déroulera dans un contexte de partenariat avec les établissements membres de l'AMUE.

Les différents établissements membres constituent autant de systèmes d'informations différents sur lesquels les web services de l'AMUE sont susceptibles d'être utilisés.

3.3.2. L'ARCHITECTURE SOA

Il existe un document présentant les principes généraux de l'architecture SOA et les principales briques utilisées. Il n'existe pas de document d'architecture détaillée car potentiellement, cette architecture peut être instanciée dans l'ensemble des systèmes d'informations des établissements membres (une centaine environ).

Néanmoins une cartographie précise des web services et des connecteurs proposées existe. La description fonctionnelle de ces web services sera explicitée dans la partie métier.

Actuellement, les seules évolutions technologiques prévues sur l'architecture SOA sont des évolutions de versions pour :

- L'environnement JAVA : une étude est prévue en 2008 ou en 2009 pour un éventuel passage de la version JDK 1.4 à la version JDK 1.5
- La Framework SOAP AXIS : il est envisagé de passer à la version 2 à l'horizon 2009 ou 2010 mais dans le cadre de la présente étude de sécurisation, la version à considérer est la 1.3 (version actuellement en cours d'utilisation).

Par ailleurs, il existe naturellement des interactions possibles de l'architecture SOA avec les différentes briques SI. L'AMUE a soulevé l'utilisation d'annuaires LDAP type OpenLDAP ou Active Directory ainsi que des fonctionnalités de SSO autour des produits CAS et SHIBBOLETH.

Enfin, il existe actuellement une seule mesure de sécurisation des web services préconisée par l'AMUE qui consiste en une préconisation de filtrage réseau.

3.3.3. ASPECTS METIERS

Il existe une cartographie précise des web services et des connecteurs proposés. Fonctionnellement, on peut répartir les web services de la façon suivante :

- Consultation du dossier des agents (professeur,…)
- Consultation du dossier des étudiants,
- Modification de certaines informations sur les agents (pour l'instant, uniquement les adresses),
- Modification de certaines informations sur les étudiants (pour l'instant, uniquement les adresses et des tables temporaires),
- Récupération des informations de type référentiel (code pays, code établissement,…)

La grande majorité des données manipulées (consultation et/ou modification) sont des données à caractère personnel.

3.3.4. PLACE DES WEB SERVICES DANS LE WORKFLOW GLOBAL

L'utilisation des web services est effectuée de manière unitaire. Plus précisément, il n'existe pas de web services « chapeau » appelant des web services, ou des enchaînements de web services (web services en appelant un autre)

L'interrogation de ces web services doit être effectuée par une application. Ces web services ont une visibilité majoritairement interne au SI de l'établissement et ont éventuellement vocation à être invoqués de l'extérieur du SI des établissements.

3.3.5. RISQUES

Comme cela a été mentionné dans la partie organisationnelle l'AMUE n'a pas nécessairement la vision complète et la maîtrise totale du système d'information de ses membres. La gestion des risques appartient donc aux établissements. Néanmoins, l'AMUE possède une vision des risques encourus et se positionne

comme force de proposition sur le sujet, notamment en proposant aux établissements les mesures de sécurité adaptées pour réduire les risques identifiés. Les résultats de l'étude de sécurisation de ces web services constituent naturellement l'un de ces outils.

Par ailleurs, les différents risques identifiés sont décrits un peu plus loin dans ce document (cf. 4)

4. ETUDE DES RISQUES

Cette partie est consacrée à l'étude des risques généraux dans le contexte de la mise en place et de l'utilisation des web services.

Nous fournissons par ailleurs des exemples de scénarii de risques. L'objectif est de mettre en exergue des éléments concrets autour des risques, notamment sur les impacts et les conséquences de ces impacts. Ce sont autant d'éléments d'appréciation permettant de définir les différents niveaux de sensibilits des informations manipulées dans le cadre de l'offre web service de l'AMUE.

4.1. LES ECHELLES UTILISEES

4.1.1. ECHELLE DE POTENTIALITE D'OCCURRENCE

Une échelle de potentialité d'occurrence de la menace est proposée.

Niveau 1 : **PEU PROBABLE**

Techniquement ou fonctionnellement, ce risque est à envisager, en revanche, sa complexité ou le coût de sa mise en œuvre font qu'il ne surviendra probablement jamais. Par exemple, la manipulation de données pendant une transmission est peu probable : en effet, elle nécessite des droits d'accès spécifiques, une connexion physique sur le LAN d'échange, et des connaissances pointues sur les protocoles utilisés.

Niveau 2 : **PROBABLE**

Ce risque devrait arriver un jour. Par exemple, l'accès à des données non autorisées proposés par l'intermédiaire des web services est probable.

Niveau 3 : **FORT PROBABLE**

Ce risque devrait survenir à court terme.

4.1.2. ECHELLE DES IMPACTS

Une échelle d'impact selon trois niveaux de gravité est retenue.

Niveau 1 : **IMPACTS NON SIGNIFICATIFS**

Le risque n'aura pas ou peu d'impacts.

Niveau 2 : **IMPACTS SIGNIFICATIFS**

Le risque peut avoir des impacts sur l'image de l'AMUE ou des établissements. Par exemple, l'absence de contrôle d'accès permettant de lire ou d'écrire dans la base contenant les informations relatives aux étudiants.

Niveau 3 : **IMPACTS GRAVES**

Le risque peut avoir des impacts forts qui dépassent très significativement la perte d'image. Par exemples, on peut citer les fraudes sur les notes des étudiants (notamment pour les concours), ou encore la récupération d'informations à caractère personnel à des fins malveillantes passibles de sanctions judiciaires lourdes.

4.1.3. GRAVITE DU RISQUE

Compte tenu des impacts et des potentialités définies précédemment, nous construisons le tableau de gravité du risque suivant :

		POTENTIALITE		
		Niv . 1 PEU PROBABLE	**Niv . 2 PROBABLE**	**Niv . 3 FORT PROBABLE**
IMPACT	**Niv . 3 IMPACTS GRAVES**	**Moyen**	**Fort**	**Fort**
	Niv . 2 IMPACTS SIGNIFICATIFS	**Faible**	**Moyen**	**Fort**
	Niv . 1 IMPACTS NON SIGNIFICATIFS	**Faible**	**Faible**	**Moyen**

4.2. LES RISQUES GENERAUX

Au regard des différentes informations recueillies sur les aspects techniques et métiers, les principaux risques identifiés des web services de l'architecture SOA AMUE sont:

- Le vol d'informations,
- La modification d'informations accidentelles ou non,
- L'indisponibilité d'une partie ou de la totalité des web services.

4.3. EXEMPLES DE SCENARII DE RISQUE

Sur la base des risques généraux identifiés plus haut, nous pouvons établir quelques scénarii de risques à titre d'illustration.

4.3.1. SCENARIO 1

4.3.1.1. Description

Interrogation d'un web service donnant des informations personnelles sur les étudiants à des fins malveillantes:

- Consultation non autorisée des notes d'un ou plusieurs étudiants,
- Utilisation discriminantes de certaines informations comme le sexe,…
- Obtention d'informations comme l'adresse ou le numéro de téléphone des étudiants.

4.3.1.2. Evaluation de la gravité

Type d'impact		Disponibilité	Intégrité	**Confidentialité**	Fraude
Type de scénario		Erreur	Accident	**Malveillance**	

POTENTIALITE				IMPACT				NIVEAU DE RISQUE		
1	2	3	X	1	2	**3**	=	1 **Faible**	**2 Moyen**	3 **Fort**

4.3.2. SCENARIO 2

4.3.2.1. Description

Modification volontaire des notes de certains étudiants (concours de médecine,…). Ce scénario n'est pas possible avec les connecteurs actuels qui ne font pas des modifications sur les notes mais il pourrait éventuellement se produire avec de futurs connecteurs.

4.3.2.2. Evaluation de la gravité

Type d'impact		Disponibilité	**Intégrité**	**Confidentialité**	**Fraude**
Type de scénario		Erreur	Accident	**Malveillance**	

POTENTIALITE				IMPACT				NIVEAU DE RISQUE		
1	**2**	3	X	1	2	**3**	=	1 **Faible**	2 **Moyen**	3 **Fort**

4.4. CLASSIFICATION AU REGARD DES RISQUES

4.4.1. LES CATEGORIES

Au regard des informations recueillies lors des interviews, il apparaît clairement trois grandes catégories d'informations accédées (en lecture/modification) :

- Les données de référentiel
- Les données des dossiers étudiants
- Les données des dossiers agents.

4.4.2. EVALUATION DU NIVEAU DE SENSIBILITE DE CES DONNEES

Les risques et la nature des données manipulées font apparaître différents niveaux de sensibilité.

Niveau 1 : **PEU SENSIBLE**

Il s'agit d'information pour lesquelles la divulgation ou la modification n'a pas ou peu d'impacts. On peut inclure dans cette catégorie les informations de référentiel par exemple.

Niveau 2 : **SENSIBLE**

Il s'agit des informations pour lesquelles la divulgation ou la modification peut entraîner des impacts non négligeables (discrimination, atteinte à l'image,…).

On peut insérer dans cette catégorie les informations relatives aux étudiants, aux agents.

Remarque :

Le découpage proposé ne fait pas état d'un niveau « ultra sensible » ou « très sensible ». Un tel niveau supposerait par exemple un impact très fort comme l'atteinte à l'existence même d'un établissement ou de l'AMUE ce qui, dans les faits, s'avère peu probable dans ce contexte précis de sécurisation d'une « brique » au sein d'un système d'information.

5.SYNTHESE DE L'ANALYSE SECURITE PREALABLE

Il ressort plusieurs idées essentielles :

- La majorité des web services manipulent des données à caractère personnel en consultation ou en modification. Ces web services sont donc sensibles de part le caractère sensible des informations échangées. Il est donc nécessaire que l'étude propose un ensemble de solutions de sécurité adaptées à ce niveau de sensibilité.
- Les briques techniques utilisées dans le cadre de l'architecture SOA et les éventuelles évolutions prévues n'apportent pas de risques majeurs dont il conviendrait de tenir compte durant l'étude.
- La sécurisation des web services s'inscrit dans deux processus plus globaux :
    - la mise en sécurité des projets informatiques menés dans les établissements,
    - le niveau de sécurité de l'infrastructure du SI des établissements.

Par conséquent, les solutions de sécurité qui seront proposées dans l'étude ne seront pertinentes que si le contexte est déjà sécurisé à un niveau convenable au regard des risques. Il serait en effet peu efficace d'imposer un niveau de sécurité assez fort pour les web services si l'environnement d'utilisation présente un défaut de sécurité permettant par exemple d'accéder facilement aux données dans les bases.