

## OFFRE DE STAGE 2014 - 2015 INGENIEURS SECURITE des SI

ref : 35CSD-2014-SEC-3

### Intitulé du stage

**Gestion des identités « IAM » : Etat de l'art, Etude des solutions « One premises et dans le Cloud Computing » et proposition d'implémentation**

### Contexte du stage

Au sein d'une équipe Capgemini spécialisée en sécurité des systèmes d'informations, et dans le cadre du développement des offres « **Architecture de Sécurité** » et « **Gestion des Identités des Accès : IAM** » portées par Capgemini, le stagiaire aura pour mission d'effectuer une étude approfondie des aspects fonctionnels de l'IAM, de produire une modélisation de la gestion de l'IAM, d'étudier les différents systèmes de gestion et de fédération des identités et des accès (SSO, Annuaire, SAML, etc.) et de proposer des implémentations logicielles utilisant des frameworks de sécurité (Spring Security, Apache Shiro, OAUTH, JAAS, ESAPI, OpenID Connect etc.).

Cette étude a pour objectif de définir les différents cas d'usages et l'état de l'art de l'utilisation des différents Systèmes de gestion des identités. En complément de quoi, sera identifié un cadre d'utilisation des différentes solutions/Frameworks afin, de simplifier le choix de la solution par les équipes sécurité de Capgemini selon les besoins et les cas d'usages proposés.

### Descriptif de la mission

Au sein d'une équipe Capgemini dédiée aux problématiques de sécurité et constituée, d'architectes, de consultants et d'experts spécialisés en sécurité des systèmes d'information et en management de risques, le stagiaire aura pour mission l'étude et la contribution à la mise en place de l'offre Gestion des identités et des accès.

Le stagiaire participera à la vie de la communauté « Sécurité » de Capgemini et pourra s'y appuyer pour sa montée en compétence et pour mener à bien son stage de fin d'étude.

### Objets du stage et activités attendues :

Ce stage est constitué des étapes suivantes :

#### **Etape1 : Etude et Etat de l'art fonctionnel de l'IAM**

1. Etat de l'art et tour d'horizon de l'IAM
2. Etude de la problématique de gestion de l'identité de bout-en-bout à travers le SI : création, modification, suppression, provisionning amont et aval, etc.
3. Etude de la problématique de l'authentification : modélisation de l'authentification selon les différents critères
4. Etude de la problématique d'autorisation et de la gestion de l'habilitation : Modélisation des différents niveaux d'habilitation (Coarse Grained, Middle Grained, Fine Grained)
5. Etude des aspects liés à la fédération de l'identité : Etude protocolaire (SAML, etc.)
6. IAM dans le Cloud : Etat de l'art

#### **Etape2 : Etude des solutions IAM « On Premises »**

1. Etude de solutions technique IAM : Authentification, Autorisation, Provisionning, SSO, etc.
2. Etude des solutions de fédération IAM :
  - a. Etude des standards : SAML V2, WS-Federation, etc.
  - b. Implémentation des standards
3. Etude comparative des solutions technique « on premises » :
  - a. Référentiel d'identité : OpenLDAP, Active Directory, ADFS, etc.
  - b. Open Identity Stack (OpenAM, OpenDJ, Open IDM)
  - c. CAS + Shibboleth
  - d. IBM : TAMEB + ITIM + TFIM
  - e. Etc.

4. Implémentation technique.

### **Etape3 : Etude des solutions IAM « Cloud IDaaS »**

1. Etude de l'état de l'art de l'IAM dans le Cloud
2. Définition des critères de choix d'une solution IAM dans le Cloud
3. Etude comparative des solutions dans le Cloud
4. Etude technique de 2 solutions Cloud IAM.

### **Etape4 : Etude et Intégration des systèmes IAM dans les architectures logicielles**

1. Etude des différents styles d'architectures logicielles de type N-Tier : SOA, REST, Mobile, etc.
2. Identification de Pattern d'architecture de sécurité pour l'IAM
3. Etude des solutions techniques existantes IAM dans les frameworks de sécurité : Spring, Apache, etc.
4. Etude des solutions de fédération des identités dans les frameworks : SAML, Liberty, WS-Federation, etc.
5. Intégration et maquetage des différentes solutions IAM en utilisant des frameworks de sécurité

### **Etape5 : Rapport de stage**

1. Rédaction du rapport de stage.

Vous utiliserez l'environnement technologique suivant :

**Sécurité** : Architecture Sécurité, Gestion d'identités et des accès (IAM), SSO, Annuaire, Provisionning, Fédération (SAML), Sécurité dans le Cloud (IDaaS)

**Langages** : JAVA/JEE.

**Frameworks**: Spring Security, Apache Shiro, JAAS, ESAPI, OpenID Connect

## **Compétences acquises à la fin du stage**

1. Compétences en sécurité des systèmes d'information :
  - a. Bonnes pratiques sécurité
  - b. Architecture Sécurité
  - c. IAM : Gestion des identités et des accès
  - d. Sécurité dans le Cloud Computing
  - e. Sécurité dans les frameworks de développements
2. Une méthodologie de suivi de projet et la capacité à travailler en équipe
3. Une vision des différentes phases d'un projet
4. Une mise en œuvre sur le terrain de connaissances techniques
5. Intégration dans des équipes de conseil, d'architecture et d'expertise en sécurité des SI

Vous serez accompagné tout au long de votre stage par un maître de stage (Consultant Sénior) et un Manager qui vous guideront au sein de la société.

**Il s'agit d'un stage de pré-embauche.**

## **Profils**

De formation Bac+5, école d'ingénieur ou formation universitaire avec une composante **Sécurité de SI**, vous recherchez un stage de fin d'études et vous possédez des bases solides en sécurité des systèmes d'informations.

Vous disposez d'une bonne faculté d'adaptation et possédez un esprit de synthèse développé.

Esprit d'équipe, rigueur, autonomie, et empathie sont des aptitudes les plus essentielles que nous souhaitons retrouver chez nos futurs chefs de projets, architectes ou consultants.

### **Lieu du stage**

Rennes ou Nantes

### **Indemnités de stage**

Selon le profil

### **Durée du stage**

6 mois.

### **Contact**

Merci de nous faire parvenir votre CV, en précisant la référence de l'offre « **ref : 35CSD-2014-SEC-3** » à :

[ali.bekkali@capgemini.com](mailto:ali.bekkali@capgemini.com)

[Tel : +33 6 88 63 83 45](tel:+33688638345)