Université de Lorraine **XML et Sécurité**
2022-2023

TP – XML sécurisée et BDs relationnelles
(délai ferme pour l'envoi 21/04/2023)

L'objectif de ce TP est d'implanter une application java permettant à deux agents (threads) de lire des bases de données distribuées (stockée sur sgbd Oracle ou MySQL) par l'intermédiaire de requêtes échangées dans un format XML sécurisé (voir Figure 1).

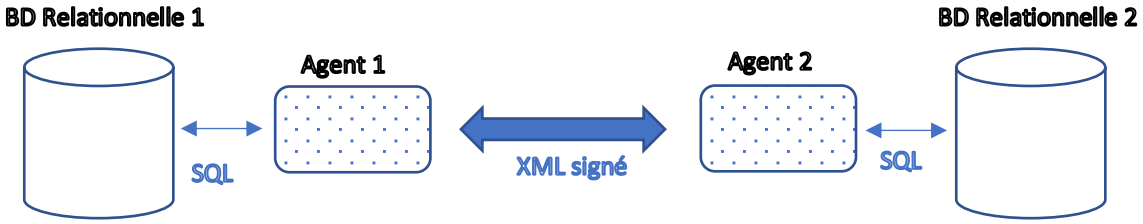

Figure 1 : Applications Java échangeant des documents XML signés

Les agents possèdent des BD différentes mais chacun connait la structure de l'autre. Chaque agent exécute les actions suivantes :

- Charger des documents xml contenant des requêtes sql ;
- Signer un document xml selon le standard XML Digital Signature W3C ;
- Envoyer un document xml signé vers l'autre agent ;
- Recevoir et valider des documents xml signés ;
- Extraire du contenu (la requête sql ou ses résultats) à partir d'un document xml valide ;
- Appliquer la requête sur sa BD ;
- Mettre les résultats de la requête dans un document xml signé et l'envoyer à l'autre agent.

L'application possède les caractéristiques suivantes :

1. Au démarrage, une paire de clés (chiffrement asymétrique) est générée pour chaque agent. Chaque agent partage sa clé publique avec l'autre.
2. La connexion de l'application à la BD se fait via l'API JDBC.
3. Les requêtes SELECT seront décrites en XML :

Requête	***XML***
SELECT Listes des champs **FROM** Tables **WHERE** Condition	<SELECT> <CHAMPS> <CHAMP> … </CHAMP> <CHAMP> … </CHAMP> … </CHAMPS> <TABLES> <TABLE> … </TABLE> <TABLE> … </TABLE> … </TABLES> <CONDITION> … </CONDITION> </SELECT>

3. Le résultat d'un SELECT sera produit en XML :

```
<RESULTAT>
  <TUPLES>
      <TUPLE>
          <CHAMP>     Value</CHAMP>
          <CHAMP> Value</CHAMP>
            ...
      </TUPLE>
      <TUPLE>
          <CHAMP> Value</CHAMP>
          <CHAMP> Value</CHAMP>
            ...
      </TUPLE>
       ...
  </TUPLES>
</RESULTAT>
```

4. Chaque agent doit charger un ou plusieurs documents xml pour les signer et l'envoyer vers l'autre agent.
5. Chaque agent doit afficher les résultats reçues de ses requêtes.

Le choix des tables dans les deux BD est laissé libre.

Les fonctionnalités à prévoir sont les suivantes :

- Une programmation à deux threads.
- Le chargement de documents XML.
- La génération de paires de clés pour une cryptographie asymétrique.
- La signature des documents XML.
- La validation des documents signés.

Travail à rendre :

1. Le script sql pour créer les tables dans les deux BDs.
2. Les fichiers code source bien documents (à la javadoc).
3. Des exemples de fichiers XML pour les deux agents.

Mettre tous les fichiers dans un répertoire portant votre nom, et compresser ce répertoire au format **ZIP** dont le nom de fichier doit suivre le format suivant : **NomEtudiant.zip**