EncryptedID et EncryptedAssertion

Étapes de l'implémentation

Toutes les étapes décrites sont maintenant terminées

- Ajouter un <m:KeyDescriptor use="encryption"> dans les metadata
  - pour les tests
  - dans Authentic
  - dans WCS
  - dans le SP de la conformance
- Charger cette clé publique de chiffrement dans Lasso
- Charger un fichier de clé privée de chiffrement dans Lasso
- Générer une clé symétrique et chiffrer l'EncryptedData avec
- Chiffrer la clé symétrique dans EncryptedKey, avec la clé asymétrique publique
- Ajouter le noeud dans son élément parent
  - EncryptedID dans un Subject
  - EncryptedAssertion
- Déchiffrer l'EncryptedKey, avec la clé asymétrique privée
- Déchiffrer l'EncryptedData, avec la clé symétrique qu'on vient de déchiffrer
- Introduire de l'aléatoire dans le chiffrement de l'EncryptedID (voir http://www.w3.org/TR/xmlenc-core/#sec-Nonce) (la clé DES est générée à chaque fois par xmlsec, je pense que ça suffira comme aléatoire)
- Vérifier l'ordre de chiffrement et de signature (voir saml-core : 6.2 Combining Signatures and Encryption)
- Support de différents algorithmes de chiffrement : TRIPLE DES, AES-128, AES-256
- Permettre le passage d'un paramètre à Lasso pour activer ou désactiver le chiffrement