Contexte

Rappel des Mécanismes d'authentification

Wiuz Agri et Wiuz Web disposent de mécanismes d'authentification qui leur son propre.

Coté Wiuz Agri, trois mécanismes existent :

- « external login » : formulaire d'authentification interne au site web ➔ En production pour 7 coopératives

- « extranet » : SSO avec le jeton d'authentification au format custom d'Atol ➔ Uniquement pour les agriculteurs, en production pour 3 coopératives (dont TERRENA)

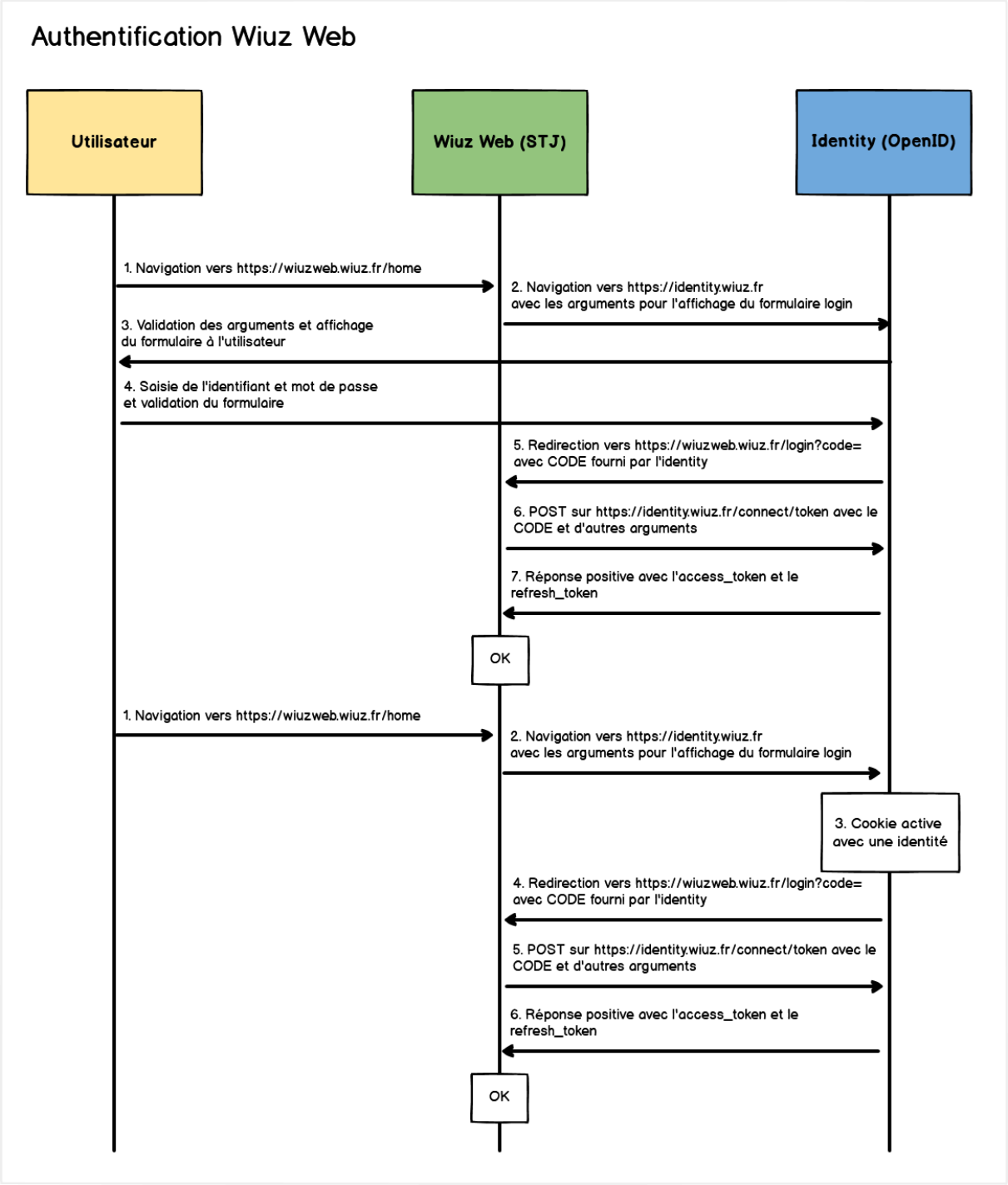
- « annuaire » : challenge d'un gestionnaire de compte externe, au format OpenId ➔ En phase de développement, pour TERRENA uniquement, nécessitera à priori une campagne de recréation de compte

Coté Wiuz Web, un seul mécanisme existe :

- « identity » : challenge du gestionnaire de compte(*) Wiuz, au format OAuth2 (compatible OpenId) ➔ En production pour les comptes mobiles (4219 comptes / Agriculteur : 3264 / Technicien : 882 / Superviseur : 73)

(*)Un gestionnaire de compte est un site web dédié à l'authentification. Une fois qu'un utilisateur s'est authentifié, le siteweb génère un cookie avec une durée de vie définie, permettant à l'utilisateur qui le désire (en fonction des politiques de sécurité) de ne saisir son mot de passe qu'une seul fois.

Ce mécanisme est en PRODUCTION pour Wiuz Web. Vous trouverez ci-dessous un schéma explicatif :



Parcours utilisateur

Le parcours utilisateur est l'élément primordial pour la réflexion de la stratégie de développement.

Pour la majorité des utilisateurs, il est souhaité le **parcours n°1** suivant :

1. Authentification sur Wiuz Web **uniquement**

2. Clic sur un bouton/lien de Wiuz Web pour naviguer vers Wiuz Agri avec une **authentification transparente** pour l'utilisateur ➔ A développer
3. Possibilité de revenir sur Wiuz Web avec une **authentification transparente**, grâce au cookie actif

Pour les utilisateurs TERRENA, il est souhaité le **parcours n°2** suivant :

1. Authentification sur Wiuz Agri **uniquement**

2. Clic sur un bouton/lien de Wiuz Agri pour naviguer vers Wiuz Web avec une **authentification transparente** pour l'utilisateur ➔ A développer

3. Possibilité de revenir sur Wiuz Agri avec une **authentification transparente**, grâce à la session toujours active

En complément, nous avons identifié un **parcours n°3**, ne nécessitant aucun développement :

1. Authentification sur Wiuz Agri

2. Clic sur un bouton/lien de Wiuz Agri ou un lien externe pour naviguer vers Wiuz Web

3. Authentification **semi-transparente** :
    a. récupération du cookie actif pour une **authentification transparente**
    b. ou authentification sur Wiuz Web à défaut

4. Possibilité de revenir sur Wiuz Agri avec une **authentification transparente**, grâce à la session toujours active

Enfin, nous avons identifié un **parcours hybride n°4**, correspondant au parcours n°3 avec le développement identifié pour à l'étape 2 du parcours n°1, dans le cas où la session ne serait plus active coté Wiuz Agri.

Mise en place d'un SSO entre Wiuz Agri ⇔ Wiuz Web

En croisant les mécanismes d'authentification, les parcours utilisateurs, et la transparence pour l'utilisateur, 3 solutions sont envisagées :

Solution n°1 – Wiuz Agri ➔ Wiuz Web avec 100% authentification transparente – Parcours n°2

Mise en place d'un certificat privé pour signer les demandes d'accès de Wiuz Agri vers Wiuz Web + Mécanisme custom sur « identité » pour obtenir un compte uniquement sur la base des éléments fournis par Wiuz Agri.

Développement coté TERRENA :

- Ajout de la génération du lien sécurisé vers Wiuz Web :
    - Récupération des arguments attendus
    - Signature avec le certificat partagé
    - Génération du lien final sur Wiuz Web

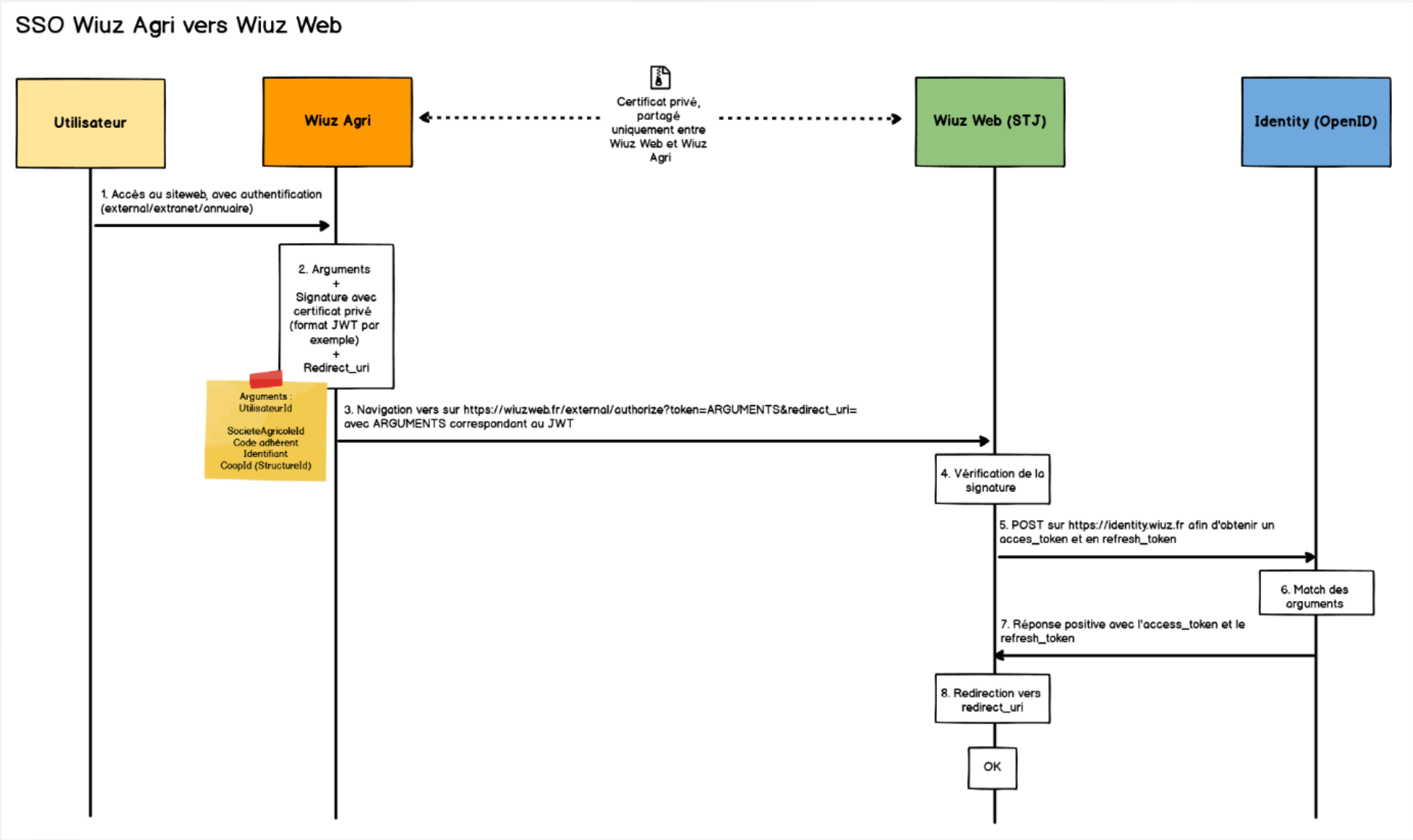
Développement coté WIUZ :

- Ajout de l'url sécurisé :
    - Vérification de la signature
    - Récupération arguments

- Flow custom sur « identité » :
    - Mise en place d'une exception de sécurité sur la base d'un flow custom
    - Match avec une identité active

La mise en place du flow custom sur « identité » est couteux et réduit le niveau de sécurité des identités.

Schéma explicatif :



Solution n°2 – Wiuz Web ➔ Wiuz Agri avec 100% authentification transparente – Parcours n°1 / parcours n°4

Mise en place d'un certificat privé pour signer les demandes d'accès de Wiuz Web vers Wiuz Agri.

Développement coté WIUZ :

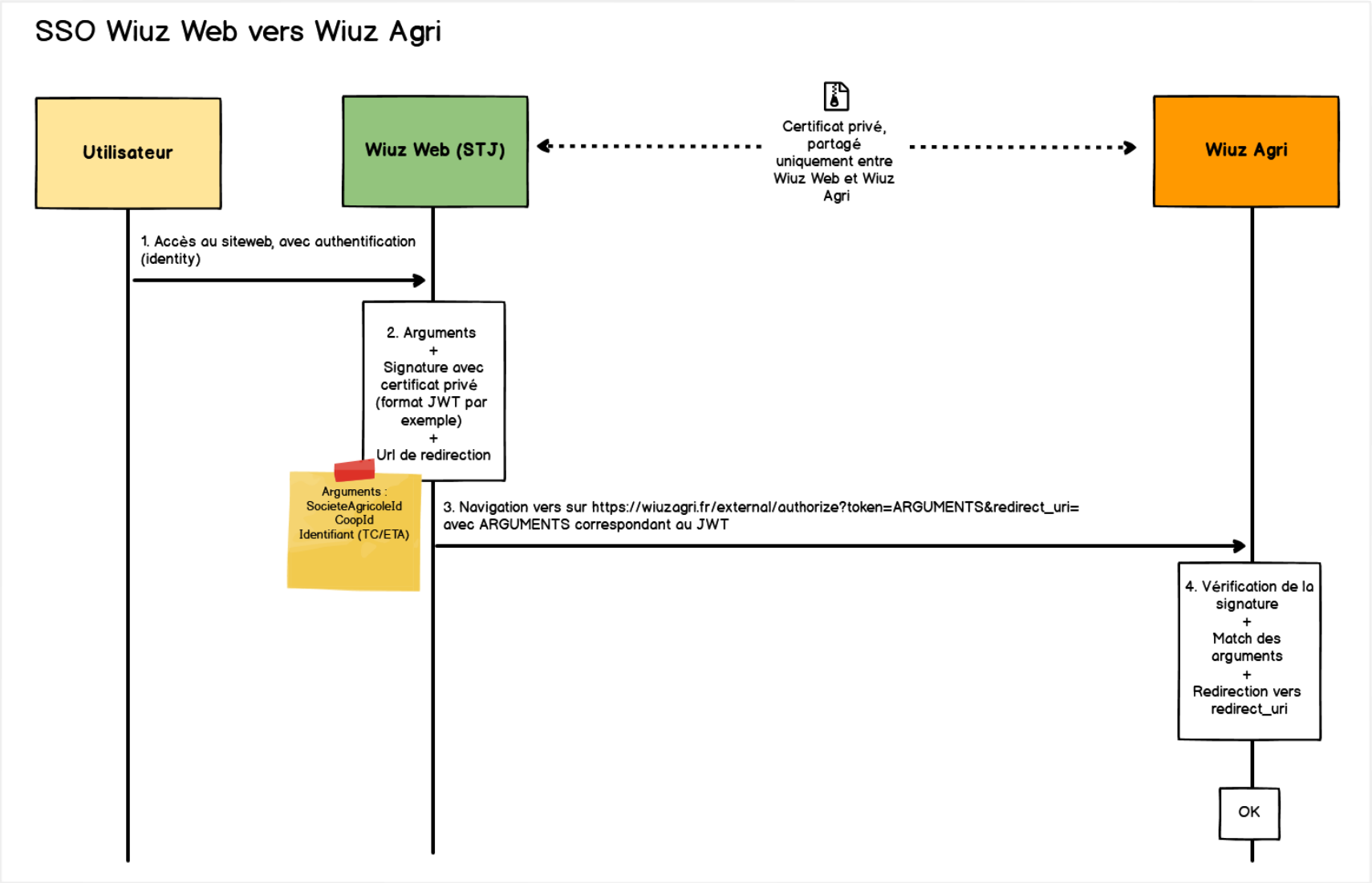
- Ajout de la génération du lien sécurisé vers Wiuz Agri :
  - Récupération des arguments attendus
  - Signature avec le certificat partagé
  - Génération du lien final sur Wiuz Agri

Développement coté TERRENA :

- Ajout de l'url sécurisé :
  - Vérification de la signature
  - Récupération arguments
  - Match avec une identité active

Cette solution est moins couteuse que la solution n°1 car Wiuz Agri dispose déjà d'un process d'authentification (cf. « external login ») en interne.

Schéma explicatif :



Solution n°3 – Wiuz Web ⇔ Wiuz Agri avec authentification semi-transparente – Parcours n°3

Wiuz Agri et Wiuz Web disposent de mécanisme d'authentification permettant à l'utilisateur de rester connecté, dès lors qu'il s'est connecté une fois. En acceptant qu'un utilisateur se connecte une fois sur chaque site web, aucun développement supplémentaire n'est à faire (ni WIUZ ni TERRENA), hormis les liens entre sites.

Solution n°4 – Wiuz Web ⇔ Wiuz Agri avec authentification transparente entre « identité » et « annuaire »

Les gestionnaires de compte « identité » et « annuaire » sont tous les deux compatibles avec le format OpenId. Ce format permet de mettre en place des challenges entre les gestionnaires de compte.

Cette solution technique reste à analyser/vérifier car nous n'avons jamais mis en place ce type de lien.