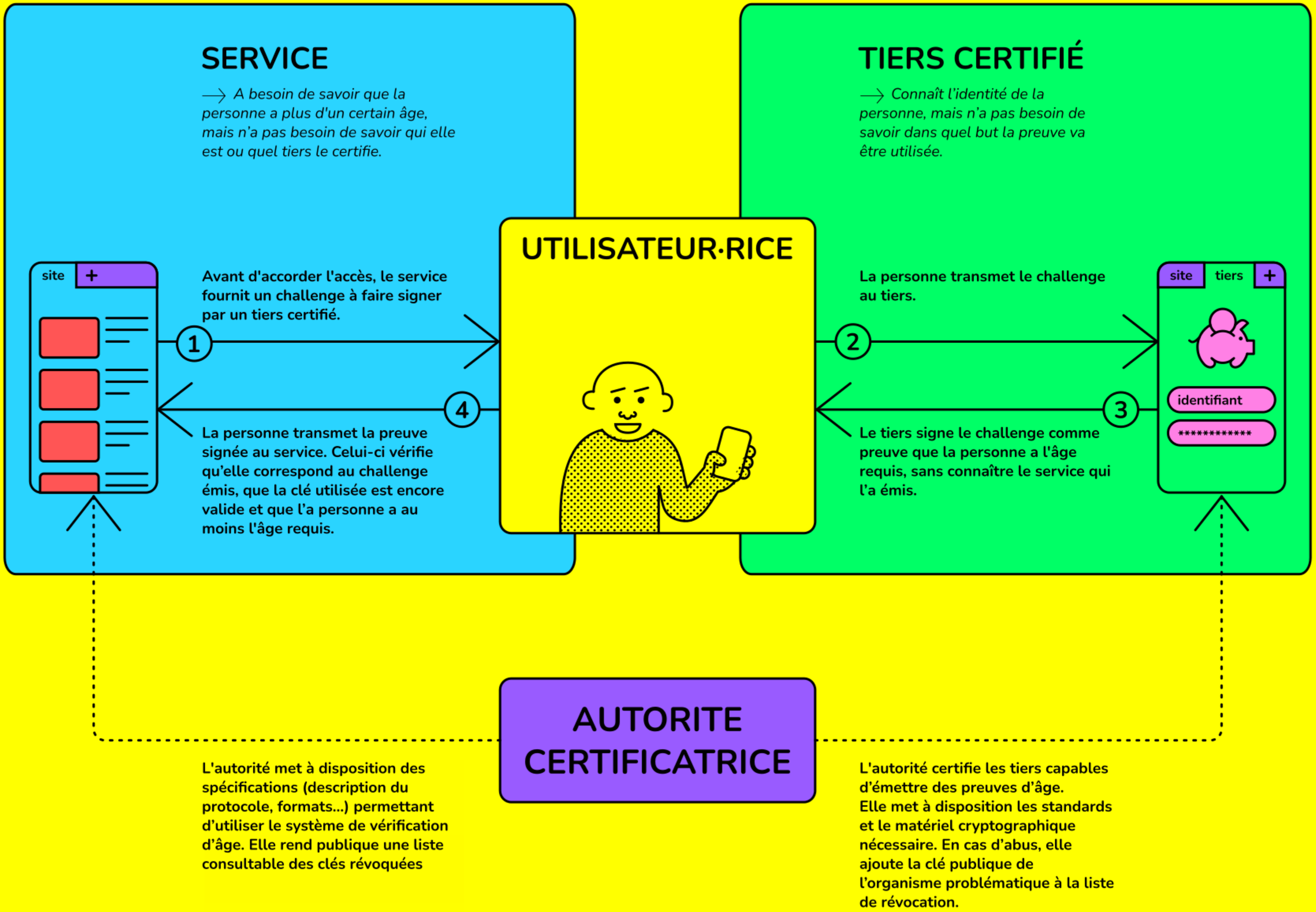
SERVICE
→ A besoin de savoir que la personne a plus d'un certain âge, mais n'a pas besoin de savoir qui elle est ou quel tiers le certifie.
TIERS CERTIFIÉ
→ Connaît l'identité de la personne, mais n'a pas besoin de savoir dans quel but la preuve va être utilisée.
UTILISATEUR·RICE
site
+
site
tiers
+
identifiant
****
1
Avant d'accorder l'accès, le service fournit un challenge à faire signer par un tiers certifié.
2
La personne transmet le challenge au tiers.
3
Le tiers signe le challenge comme preuve que la personne a l'âge requis, sans connaître le service qui l'a émis.
4
La personne transmet la preuve signée au service. Celui-ci vérifie qu'elle correspond au challenge émis, que la clé utilisée est encore valide et que l'a personne a au moins l'âge requis.
AUTORITE CERTIFICATRICE
L'autorité met à disposition des spécifications (description du protocole, formats...) permettant d'utiliser le système de vérification d'âge. Elle rend publique une liste consultable des clés révoquées
L'autorité certifie les tiers capables d'émettre des preuves d'âge.
Elle met à disposition les standards et le matériel cryptographique nécessaire. En cas d'abus, elle ajoute la clé publique de l'organisme problématique à la liste de révocation.