

ANNEXE - LinkedIn (PERSONA Verification)

PROOF OF HUMANITY (PHILOSOPHIE).....	2
L'IMPACT ALGORITHMIQUE (THE BADGE).....	2
SOUS LE CAPOT (STANDARD ICAO 9303).....	3
Le Handshake.....	3
PROCÉDURE D'ENRÔLEMENT (CLEAN INSTALL).....	3
Initialisation.....	4
Acquisition de la Preuve (NFC Handshake).....	5
Preuve de Vie (Liveness Check).....	6
Commit & Push.....	7
ALERTE DE SÉCURITÉ - "REUSABLE PERSONA".....	7
ANALYSE DES RISQUES & RÉVOCATION.....	8
Risque : Le Tiers de Confiance (Persona).....	8
Protocole de Révocation (Kill Switch).....	8
TROUBLESHOOTING & DEBUG (CAS D'ÉCHEC).....	8

PROOF OF HUMANITY (PHILOSOPHIE)

Dans un écosystème saturé par l'IA générative et les bots de scraping, l'identité numérique devient une commodité instable. La certification d'identité LinkedIn (via Persona) n'est pas une simple "coche bleue", c'est une preuve cryptographique d'existence biologique.

Selon le principe de l'Échange Équivalent :

- **Gain (Asset)** : Augmentation massive de la confiance (Trust Score) auprès des recruteurs et de l'algorithme. Accès prioritaire aux offres.
- **Coût (Liability)** : Cession de données biométriques (géométrie faciale) et régaliennes (Passeport) à un tiers de confiance américain (Persona).

Pour une infrastructure Souveraine, c'est une hérésie. Pour une stratégie de carrière (Marketability), c'est un impératif tactique. Nous classons cette opération comme une **"Exposition Contrôlée Temporaire"**.

Note : C'est un peu comme donner ses empreintes digitales pour entrer en boîte de nuit. C'est idiot, mais si c'est la seule façon de parler au DJ (le recruteur), on le fait. On se lave juste les mains après.

L'IMPACT ALGORITHMIQUE (THE BADGE)

Visuel (Frontend) Un bouclier gris avec une coche apparaît à côté du nom ou dans la section "Infos".

- *Mention* : "Identité vérifiée par Persona".

SEO & Algorithme (Backend) C'est le véritable ROI (Retour sur Investissement) de l'opération.

- **Priorité de tri** : Dans LinkedIn Recruter, les profils vérifiés apparaissent souvent avant les autres à compétences égales.
- **Anti-Spam** : Votre compte sort de la "Sandbox" des suspects. Vous pouvez envoyer plus de demandes de connexion sans déclencher les captchas ou les blocages temporaires.
- **Crédibilité** : Pour un rôle lié à la Sécurité ou l'IT (comme Architecte), cela prouve une maîtrise des outils numériques modernes.

Note : Félicitations, vous êtes officiellement "Certifié Humain". C'est triste d'en arriver là, mais dans un monde de Deepfakes, votre visage est devenu votre clé PGP publique.

SOUS LE CAPOT (STANDARD ICAO 9303)

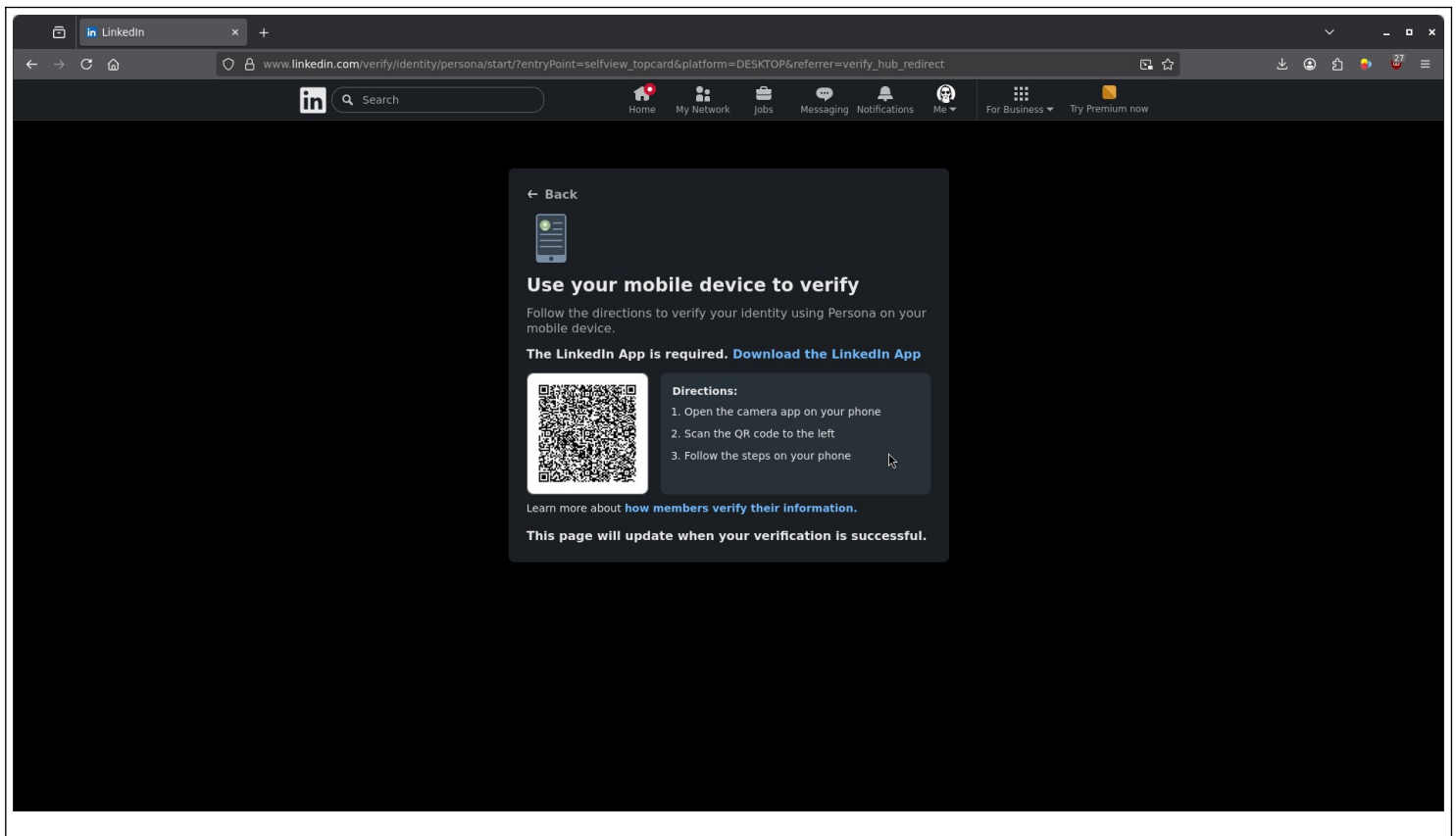
Le Mécanisme : La vérification repose sur la cryptographie asymétrique. La puce RFID de votre passeport ne contient pas juste une photo, mais une signature numérique de l'État émetteur (Country Signing Certification Authority - CSCA).

Le Handshake

- **BAC (Basic Access Control)** : L'app lit la zone MRZ (les lignes de code en bas du passeport ou de la carte d'identité) par caméra pour dériver la clé de déchiffrement de la puce.
- **Passive Authentication** : Le téléphone lit la puce NFC, extrait la photo HD signée et vérifie que le hash correspond à la signature de l'État. Impossible à falsifier sans la clé privée du gouvernement.

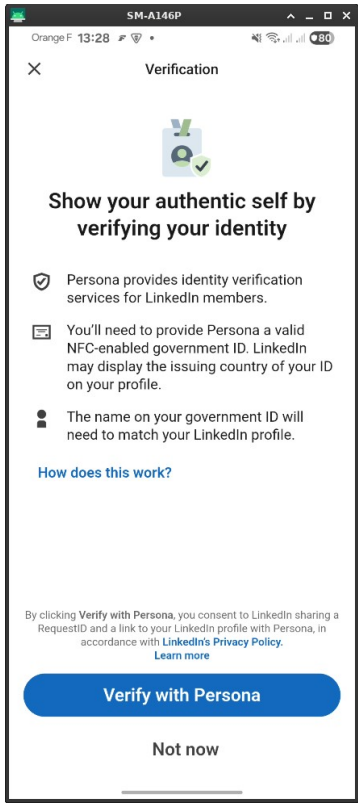
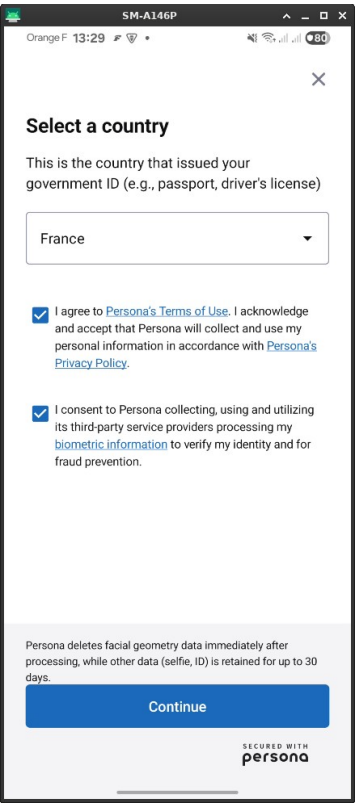
Note : En gros, c'est du SSL/TLS mais version papier. Si la puce ne répond pas, c'est soit qu'elle est morte, soit que vous essayez de vérifier un passeport diplomatique acheté sur le Darknet.

PROCÉDURE D'ENRÔLEMENT (CLEAN INSTALL)



Initialisation

- Sur le mobile, ouvrir l'application LinkedIn (MàJ requise).
- Aller sur le profil > Bouton "Plus" > "À propos de ce profil" > "Vérifier maintenant".
- Redirection vers le sous-traitant **Persona**. Accepter les CGU (après lecture en diagonale, comme tout le monde).

		
---	--	--

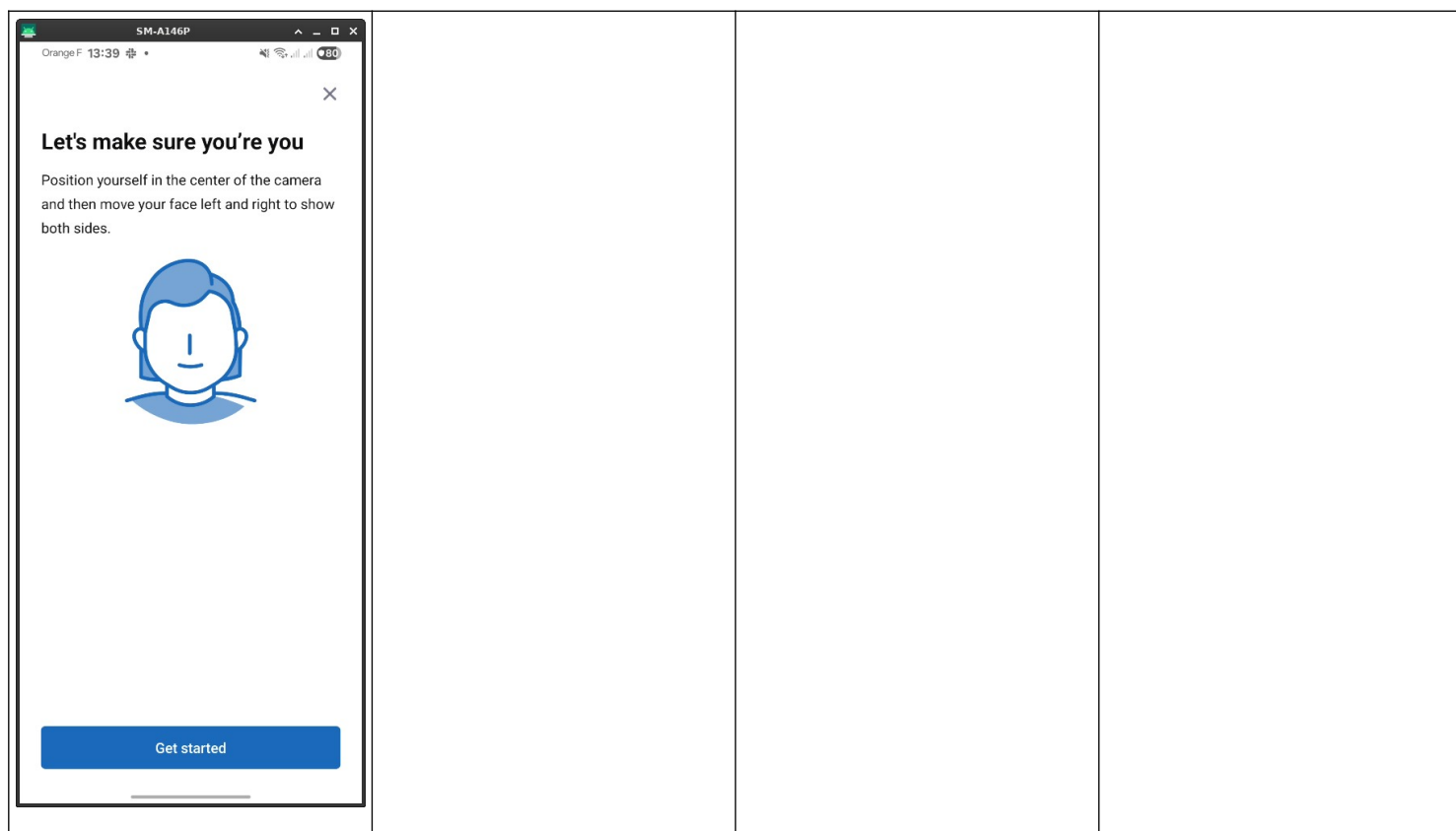
Acquisition de la Preuve (NFC Handshake)

- Prendre en photo la page d'identité du passeport ou de la carte d'identité (netteté absolue requise).
- **L'étape critique (NFC)** : L'app demande de scanner la puce.
 - Poser le téléphone **sur** le passeport fermé ou sur la carte d'identité.

Do you see this symbol on the front or back of your ID? If you see this symbol, your government ID contains a chip that can be scanned using your mobile device. Yes, continue I'm unable to do this now	persona Select ID type We require a photo of your government ID to verify your identity. Choose 1 of the following options Identity card (Issued in Aug 2021 or later) Passport Residency Permit	Front of Government ID Take a clear photo of the front of your government ID. Camera capture with a mobile device will improve photo quality. Upload	Back of Government ID Take a clear photo of the back of your government ID. Camera capture with a mobile device will improve photo quality. Upload
Review national ID details Make sure the information below is exactly as it appears on your national ID. Your verification may fail if details don't match. First name: [Redacted] Last name: [Redacted] Document Number: [Redacted] Birthdate: [Redacted] Day: [Redacted] Year: [Redacted] Expiration date: [Redacted] Day: [Redacted] Year: [Redacted] Accept and Continue Retake Photo of ID	Not sure where the chip is located? If you can't locate the chip, don't worry - it's embedded inside the ID and may not be visible. Continue Not now	Scan the NFC chip that's in your national ID - Place your ID card on a flat, level surface, so that the area where the chip is embedded is facing up and hold your phone above it. - Slowly move the phone around until you get an indication the scanning has started (via a progress indicator screen, a sound, or a vibration) - Keep your phone steady until you get an indication that the scan is complete (this may take up to 10 seconds) Please do not move your phone till you see "document processed successfully" screen Start scanning Not now	

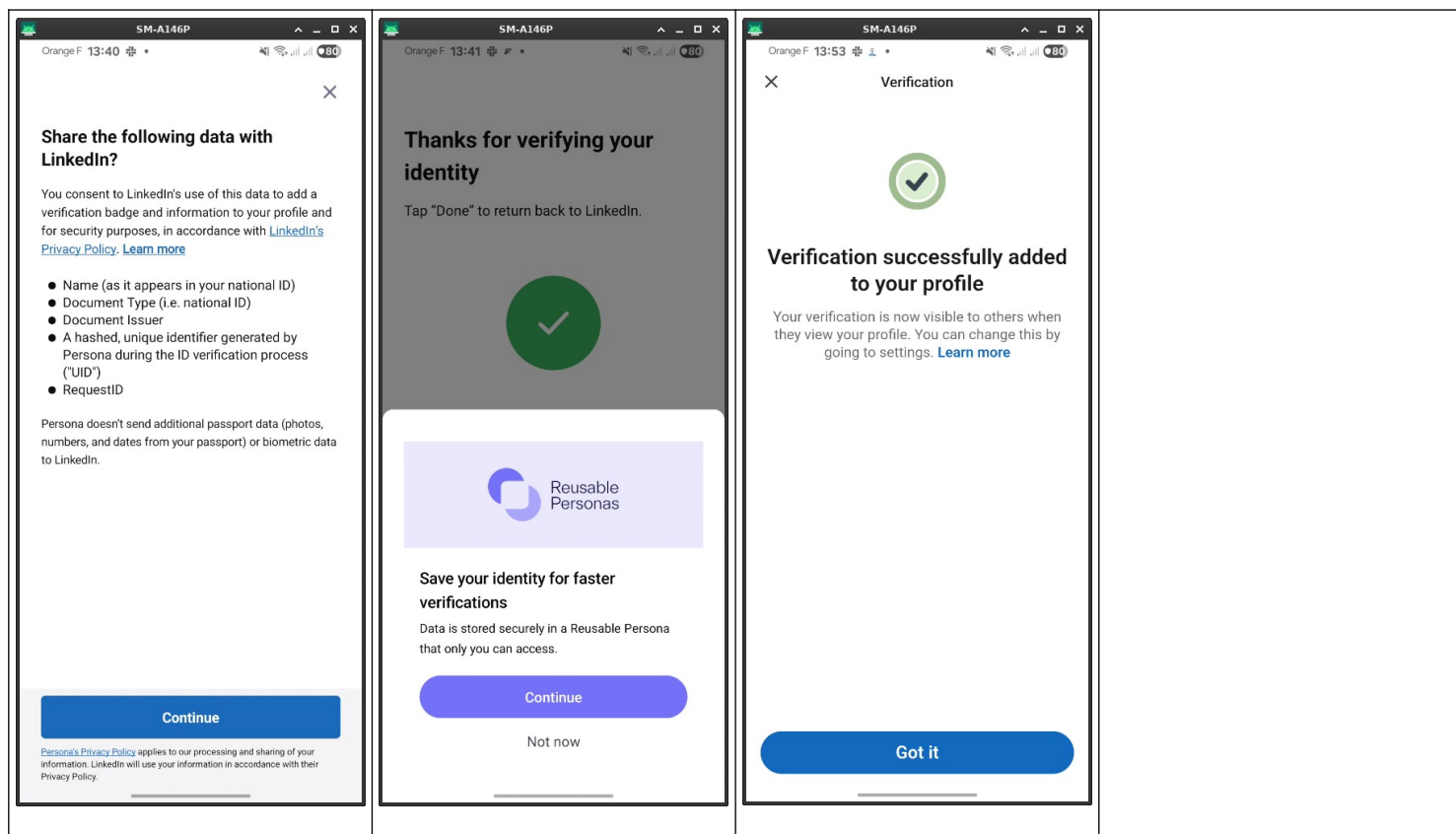
Preuve de Vie (Liveness Check)

- Tenir le téléphone face au visage.
- Suivre les instructions (tourner la tête à gauche, à droite, regarder en haut).
- C'est ici que l'IA vérifie la 3D de votre visage pour contrer les attaques par présentation (photos, masques).



Commit & Push

- Si succès : "Vérification réussie".
- Le badge apparaît sous 2 à 10 minutes sur le profil public.



ALERTE DE SÉCURITÉ - "REUSABLE PERSONA"

ATTENTION : À la fin du processus, Persona vous proposera souvent de *"Sauvegarder votre identité pour des vérifications plus rapides"* (Create a Reusable Persona).

Directive : **REFUSER IMPÉRATIVEMENT.**

- **Pourquoi ?** Si vous cochez cette case, Persona conserve vos données biométriques indéfiniment pour créer un compte utilisateur chez eux.

Objectif : Nous voulons une vérification "Stateless" (sans état). Une fois le token envoyé à LinkedIn, Persona ne doit rien garder (suppression après 30 jours). Ne créez pas de compte chez le sous-traitant.

Note : La flemme de refaire un scan de 30 secondes ne vaut pas le risque de laisser traîner son ADN numérique sur un serveur tiers. Cliquez sur "Not Now" ou "Decline".

ANALYSE DES RISQUES & RÉVOCATION

Risque : Le Tiers de Confiance (Persona)

Vos données ne sont pas chez Microsoft/LinkedIn, mais chez Persona. Bien que certifiés SOC2 et conformes RGPD, c'est un "Honey Pot" (Pot de miel) géant pour hackers.

- *Données exposées* : Numéro de passeport, Date de naissance exacte, Géométrie faciale.

Protocole de Révocation (Kill Switch)

Une fois le poste obtenu (Mission Accomplished), il est impératif de réduire la surface d'attaque.

- **Sur LinkedIn** : Profil > Editer > Vérifications > "Supprimer la vérification".
 - *Effet* : Le badge disparaît.
- **Droit à l'oubli (GDPR/CCPA)** :
 - Contacter le support **Persona** directement pour demander la purge des données associées à votre hash.
 - LinkedIn conserve un "token" de validation, mais la biométrie source doit être détruite.

Note : "Ce message s'autodétruit dans 5 secondes". Enfin, seulement si vous remplissez le formulaire de demande de suppression en trois exemplaires.

TROUBLESHOOTING & DEBUG (CAS D'ÉCHEC)

Si l'étape "NFC Handshake" échoue systématiquement (Erreur de lecture ou boucle infinie) :

- **L'Interférence Métallique** : Retirez impérativement la coque du smartphone, surtout si elle contient des aimants (Magsafe) ou une plaque de support voiture.

Le Positionnement de l'Antenne :

- Sur les Samsung, l'antenne NFC est souvent au milieu ou légèrement vers le haut.
- Ne faites pas des ronds. Posez, glissez lentement, figez.

Le Conflit Logiciel :

- Désactivez temporairement les paiements sans contact (Google Wallet) ou les apps de transport qui peuvent tenter de "voler" le focus NFC pendant le scan du passeport.