HOLISEUM

Les mots de passe sont-ils obsolètes ?

Les alternatives pour un avenir sécurisé

Lundi de la cybersécurité , 11 décembre 2023

Renaud Lifchitz, Directeur Scientifique

Version	1.0	Classification	Public

Présentation de l'intervenant

- Expert en sécurité informatique,
  Directeur scientifique chez Holiseum

- Principales activités:
  - Tests d'intrusion & audits de sécurité
  - Recherche
  - Formations & sensibilisations
- Centres d'intérêt :
  - Sécurité des protocoles (authentification, cryptographie, fuites d'information, preuves à divulgation nulle de connaissance...)
  - Théorie des nombres (factorisation, tests de primalité, courbes elliptiques...)

HOLISEUM
Pure Player de la Cybersécurité des infrastructures critiques et industrielles

NOTRE ADN

- Innovation & disruption
- Excellence & expertise
- Vision & approche à 360° de la sécurité
- Légitimité issue des expériences terrain
- Scalabilité & efficience opérationnelle

3 PILIERS

- Conseil & services
- Éducation & formations
- Édition logicielle

RÉFÉRENCES

CHIFFRES-CLÉS

2018
Création de Holiseum

40
Collaborateurs

20%
De dépenses investies en R&D

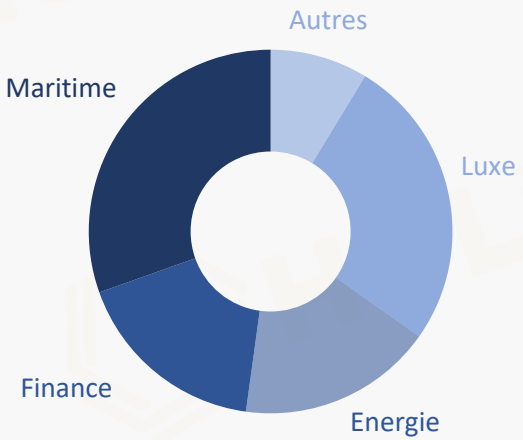
5
Continents couverts avec ¼ du CA réalisé à l'international

HOLISEUM
Pure Player de la Cybersécurité des infrastructures critiques et industrielles

QUALIFICATIONS & RÉFÉRENCEMENTS

- Qualification PASSI* sur les 5 portées
- Sélection pour la phase expérimentale PACS**
- Référencement par France Relance (audits & remédiation)
- Statut de Jeune Entreprise Innovante

SECTEURS D'ACTIVITÉ



HOLISEUM EST MEMBRE DE

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

GICAN

CHIFFRES-CLÉS

1er
Tir à Blanc de Ransomware® du marché

3
Distinctions remportées pour nos solutions innovantes

+150
Audits 360 réalisés

+250
Pentests / an effectués

**PASSI : Prestataire d'Audit de Sécurité des Systèmes d'Information*
***PACS : Prestataire d'Accompagnement et de Conseil en Sécurité des systèmes d'information*

Les mots de passe sont-ils obsolètes ?
Sommaire

1. Hier

2. Aujourd'hui

3. Demain

01 Hier : Identification et confiance par défaut

HOLISEUM

01. Hier…

- Réseaux de confiance : collègues, utilisateurs avertis, …
- Accès basé sur la connaissance du système
- Accès à un périmètre physique/logique suffisant (comme le « shadow IT » aujourd'hui)
- « Sécurité par l'obscurité »
- Identification plutôt qu'authentification
  - Déclarer plutôt que prouver : principe de la photo du porteur sur un badge porté
  - Toujours le cas de pas mal de systèmes :
    - Cartes RFID LF (« Low Frequency ») très souvent utilisées pour leur identifiant censé être u
    - ou certaines cartes RFID HF/NFC avec une authentification utilisant une cryptographie faible (= faciles à dupliquer) :
      - Clés par défaut
      - Rétrocompatibilité : downgrade de la sécurité
      - Mauvaise utilisation des fonctions de sécurité
- Déclaratif ≠ « Zero Trust »

02

Aujourd’hui :
Transition entre complexité et interopérabilité

HOLISEUM

02. Les fameux mots de passe

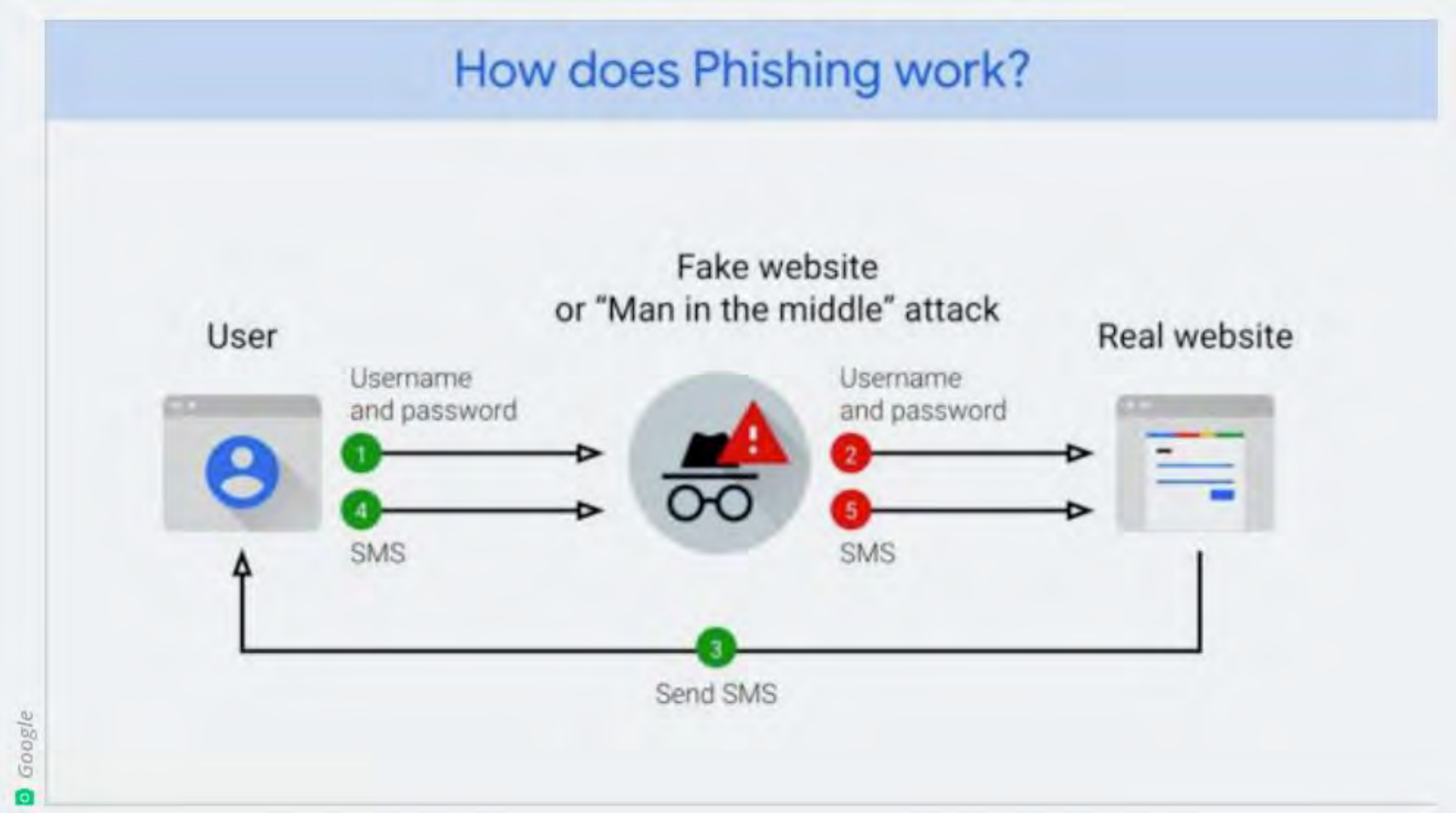
- Avantages :
  - Compatibilité universelle sur la plupart des périphériques
- Inconvénients :
  - Trop nombreux
  - Nécessité d'être **suffisamment complexes** sinon faciles à bruteforcer en ligne ou hors ligne
  - Nécessité d'être **différents** par service, souvent réutilisés en pratique :
    « password reuse » / « password spraying » / « credential stuffing »
  - Nécessité de se souvenir et/ou **centraliser ses mots de passe** utilisés
  - Nécessité de **restauration** de temps en temps des mots de passe oubliés avec les risques associés (**phishing**, sécurité du compte **mail**, …)
  - **Partiellement nominatif** à cause du login (pseudo, adresse mail)
  - **Croisements possibles** de données utilisateurs par les fournisseurs de service par login/mail
  - Utiliser des mots de passe est donc non sécurisé pour beaucoup de raisons et coûteux en temps

02. Authentification forte « traditionnelle » (1/2)

- Avantages :
  - En principe plus **difficile** à attaquer

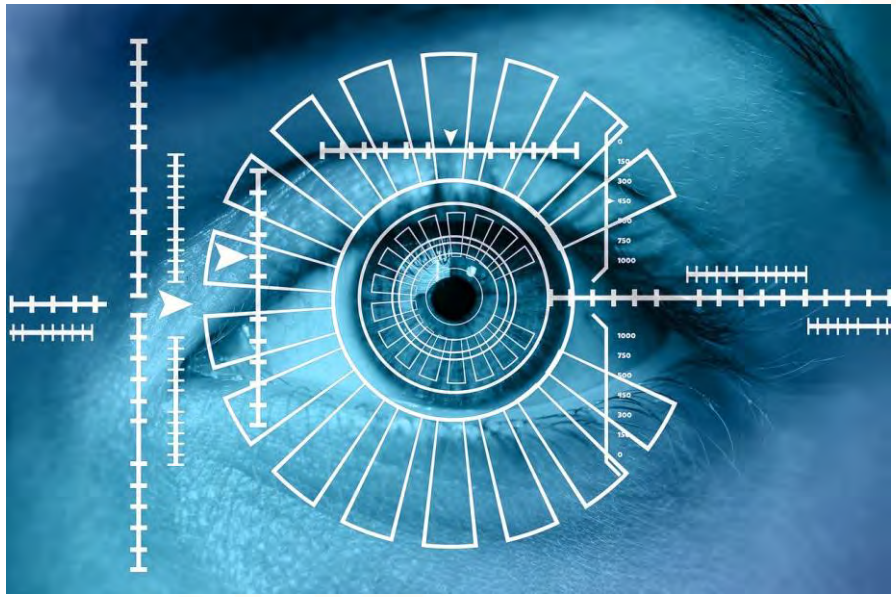
- Inconvénients :
  - Certaine lourdeur pour l'utilisateur
  - Les **SMS utilisés sont assez facilement piratables** (peu ou pas chiffrés « on air », « SIM swapping »)
  - La **boîte mail utilisée** peut avoir été piratée
  - Contournement presque tout autant facile pour l'attaquant par **vol de session** (cookies notamment)
  - **Vulnérabilité au phishing**
  - « **MFA fatigue** »
  - Nombreux **outils de vols existants** : OTP-Bot, telbot-otp, SMSBotBypass, SMSBypass, …

02. Authentification forte « traditionnelle » (2/2)



02. Biométrie (1/2)

- Avantages :
  - On l'a toujours sur soi, **impossible à oublier**
  - **Plutôt unique et fiable** : une empreinte digitale a moins d'une chance sur 1 milliard d'être identique, y compris pour de vrais jumeaux (*National Forensic Science Technology Center*)
- Inconvénients :
  - Inchangeable : **compromission à vie**
  - La plupart du temps **rejouable**
  - Implémentations parfois mauvaises (notamment car traces partielles)
  - **Règlementé** en Europe
  - Sensible aux **accidents de la vie** :
    - Que se passe-t-il si on perd des doigts, la main, un bras ?
    - Reconnaissance vocale : un rhume suffit à la rendre inopérante, **les outils d'IA**
    - Reconnaissance faciale : **les outils d'IA** permettent de générer autant de photos et vidéos que souhaité
  - **L'intelligence artificielle rend quasi-inopérants les procédures de KYC** (« Know Your Customer »)



02. Biométrie (2/2)

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STOR

HELLO AND GOODBYE —

Researchers figure out how to bypass the fingerprint readers in most Windows PCs

Microsoft's Surface didn't even use the Microsoft-developed security protocol.

ANDREW CUNNINGHAM - 11/27/2023, 7:52 PM

Enlarge / The fingerprint sensor on a Lenovo ThinkPad X1 Carbon.

02. Les SSO

- « Single Sign On »
- Bouton « Se connecter avec » …
- Propriétaires : Google, Apple, Facebook, …
- Open source : OpenID

- Inconvénients :
  - **Disponibilité** : complexe car service très centralisé
  - Donne un **privilège incroyable** à ces services
  - Rend encore plus « **valuable** » les comptes

02. Les Passkeys (1/3)

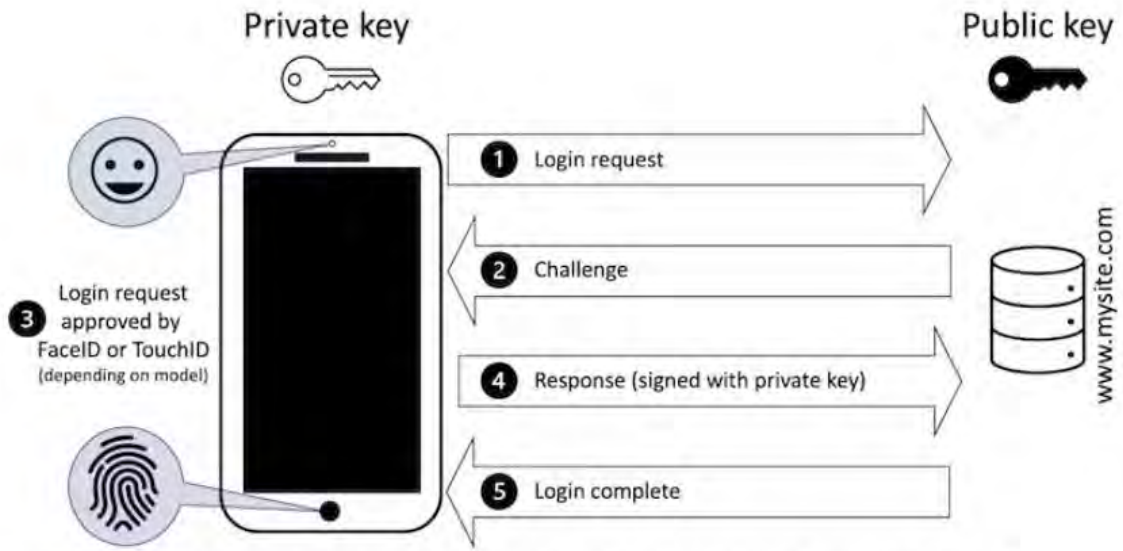
- En français : « clés d'accès » ?
- Développés par l'Alliance FIDO : Google, Apple, Microsoft, Samsung, Amazon, Meta, …
- 2 principes (authentification forte) :
  - Reconnaissance de l'appareil :
    - A l'enrôlement : clé privée générée dans l'appareil, clé publique complémentaire dans le service ou l'application
  - Reconnaissance de l'utilisateur :
    - Déverrouillage biométrique, code PIN, schéma, …
- Avantages :
  - Authentification forte
  - Simplicité pour l'utilisateur
  - Protège contre la plupart des attaques par phishing (dépend de l'implémentation)

Passkeys

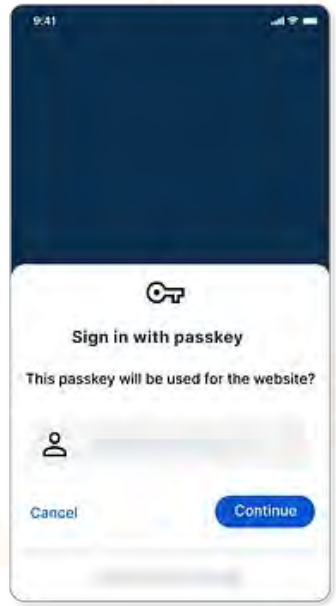
02. Les Passkeys (2/3)

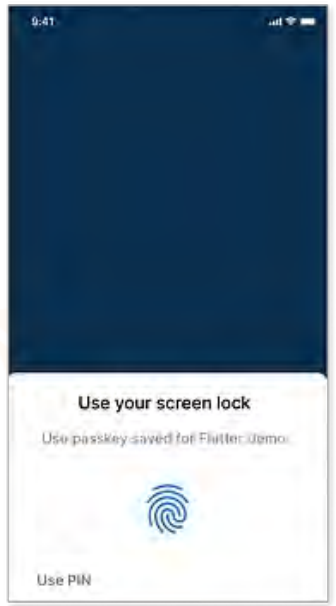
- Inconvénients :
  - Compatibilité faible : peu d'applications compatibles (lesquelles ?)
  - Interopérabilité : quasi nulle à l'heure actuelle (migration difficile, parfois par QR code)
    - Frictions pour des utilisateurs sur plusieurs écosystèmes : Android/iOS/Microsoft
    - Travail en cours sur des normes d'interopérabilité
  - Difficulté/impossibilité à sauvegarder, complexité en cas de perte/dommage du périphérique
    - Forte liaison au service cloud du provider/périphérique pour ce qui est de la sauvegarde
  - Disponibilité : importante dépendance au périphérique d'authentification

02. Les Passkeys (3/3)



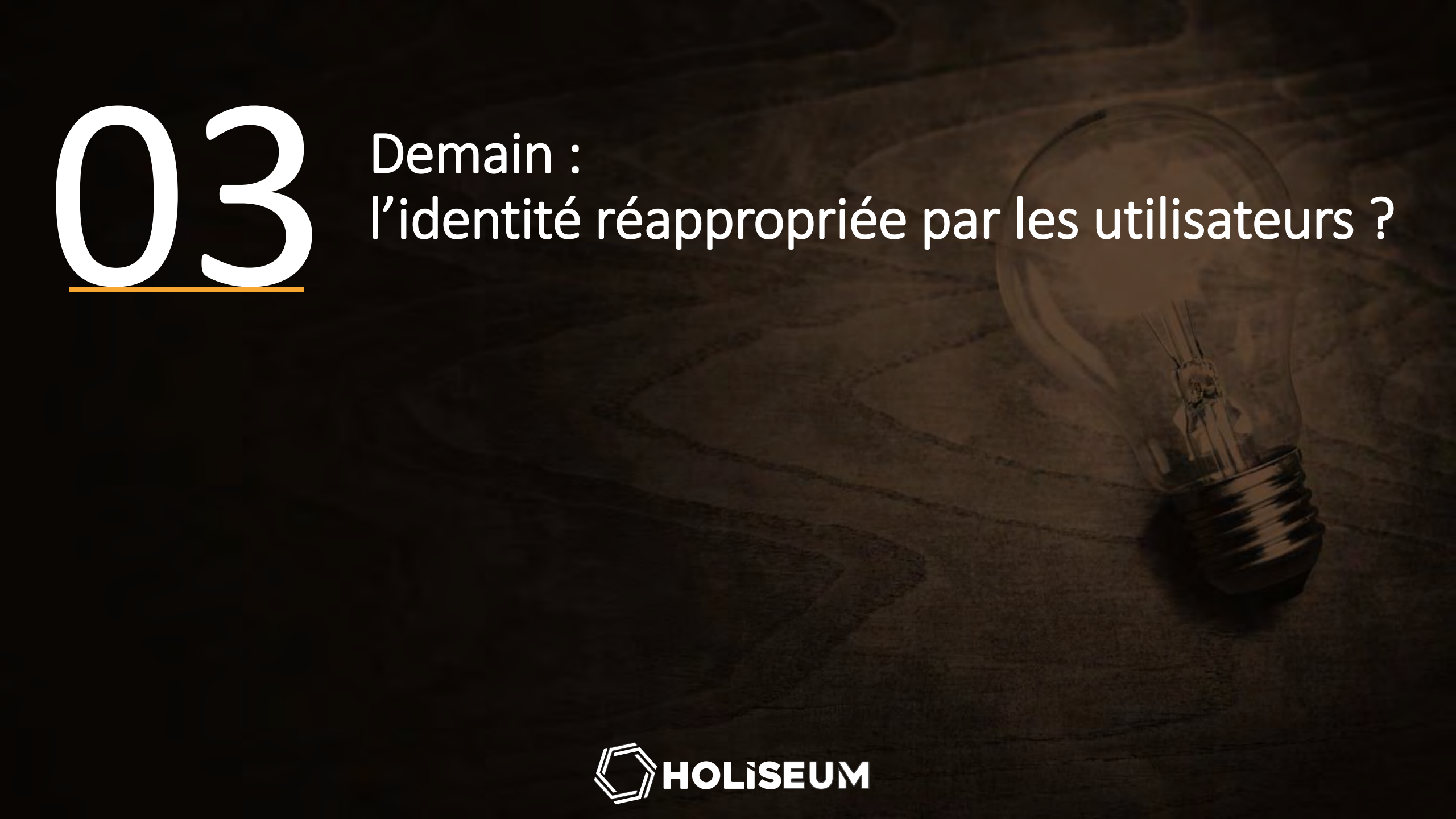
Passwordless web authentication uses a combination of two keys, one public and one private. Paul Haskell-Dowland





03

Demain :
l’identité réappropriée par les utilisateurs ?



HOLISEUM

03. Une tendance qui s'esquisse ?

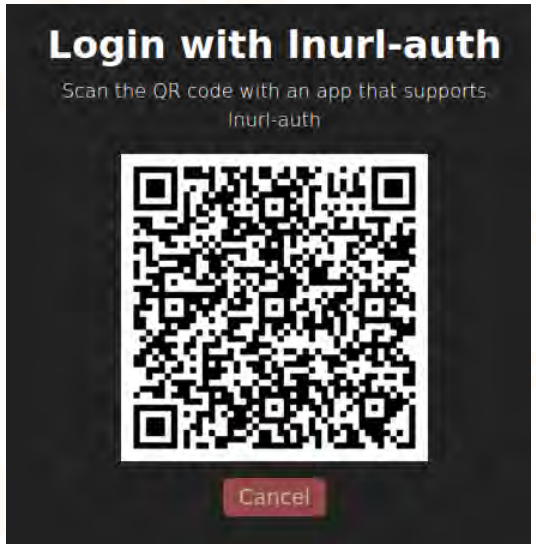
- Dé-GAFA-isation des accès ?
- Réappropriation par l'utilisateur de son identité :
  l'idée est de conserver tous les secrets côté utilisateur

- Avantages :
  - Choix des données personnelles partagées ? (chiffrement par attributs)
  - Décentralisation des secrets d'authentification :
    - Meilleur pour la disponibilité
    - Évite les fuites de données massives d'authentification

- Inconvénients :
  - C'est à l'utilisateur de faire des sauvegardes ou d'utiliser des solutions de restauration…

03. LNURL-AUTH (1/4)

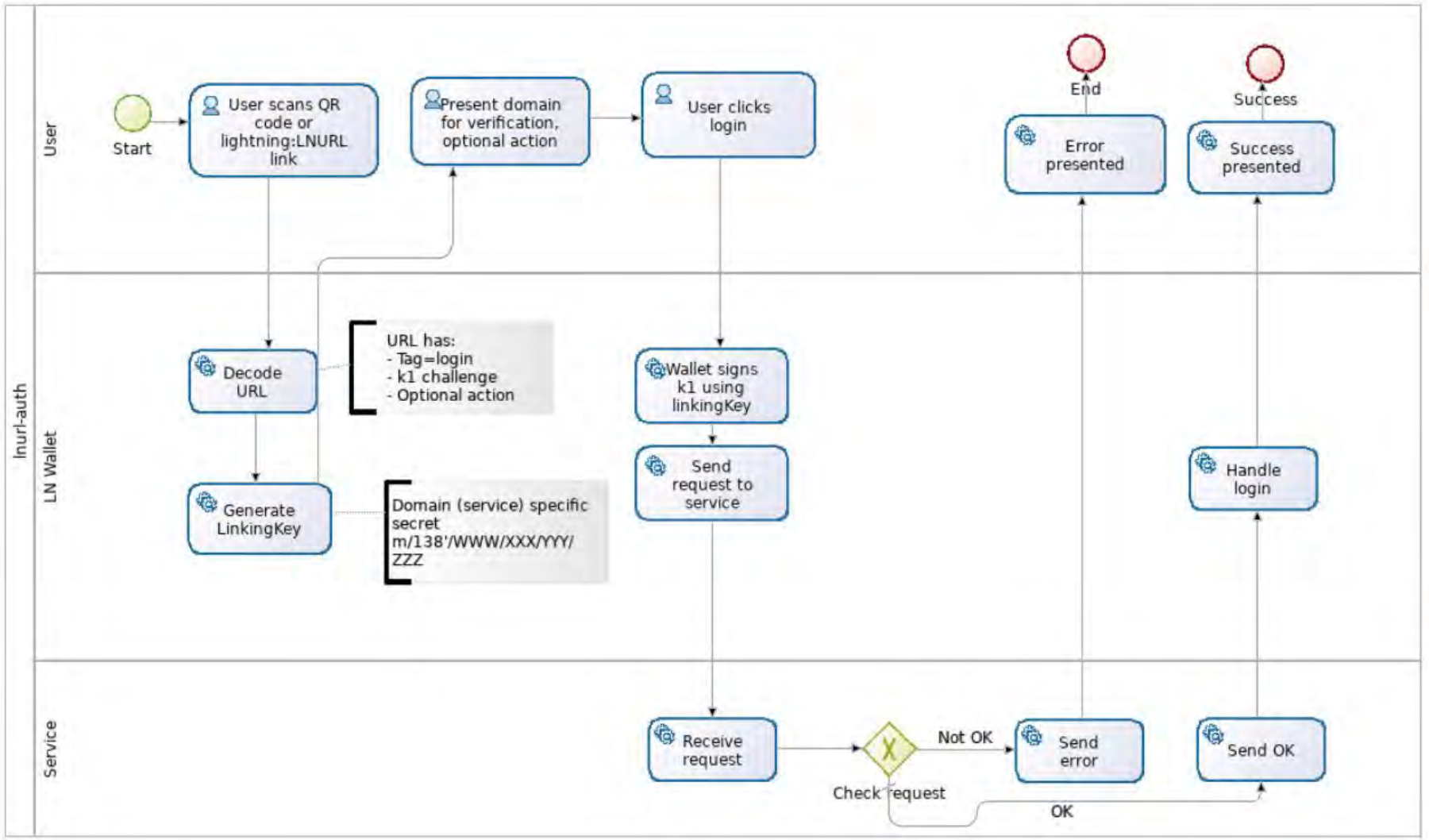
- Protocole ouvert et inviolé
- Protocole hors chaîne, utilisé avec Bitcoin Lightning
- Spécifications LNURL-AUTH ouvertes et simples : https://github.com/fiatjaf/lnurl-rfc/blob/legacy/lnurl-auth.md
- Aucune confiance à accorder à un tiers
- Secrets résident sur le périphérique client
- Exemple : https://lightninglogin.live/



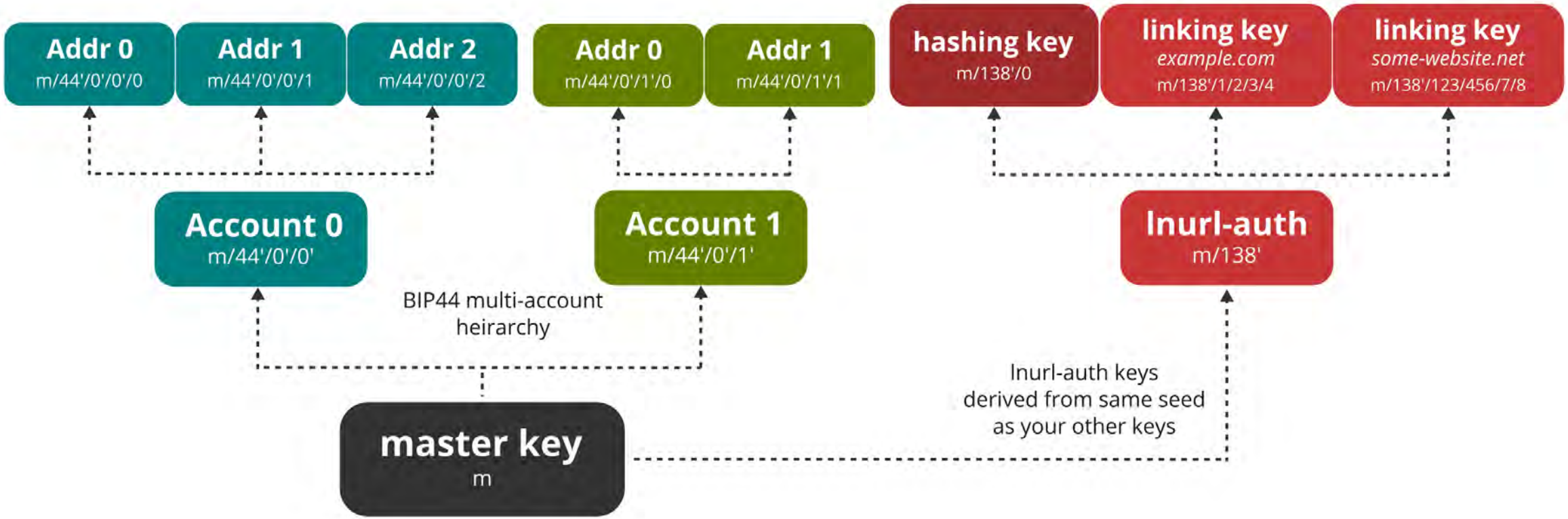
CINEMATIQUE

1. L'utilisateur se rend sur l'application souhaitée
2. L'utilisateur se voit présenter un QR code à l'écran
3. L'utilisateur lance l'application d'authentification sur son smartphone et scanne le QR code présenté avec son appareil photo
4. L'application mobile présente l'identité de l'application qui souhaite l'authentification
5. L'utilisateur tape sur « Confirmer » et est immédiatement authentifié

03. LNURL-AUTH (2/4)



03. LNURL-AUTH (3/4)

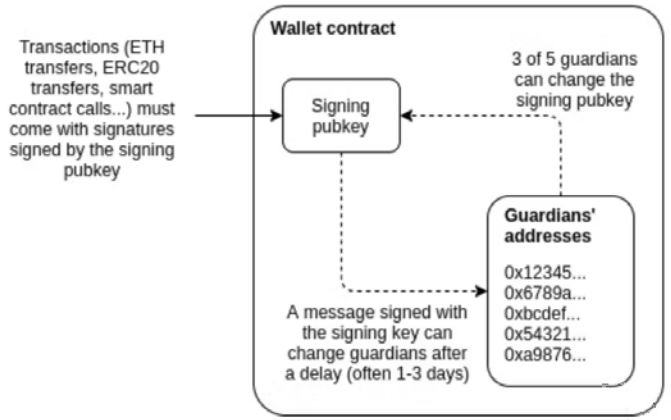


03. LNURL-AUTH (4/4)

- Avantages :
  - Sécurité :
    - **Authentification forte** tout en conservant une facilité et une fluidité d'usage
    - **Protection totale contre le phishing**
    - Le secret peut être enfoui dans une **enclave sécurisée** du téléphone, garantie par le constructeur
    - **Sans tierce partie de confiance** contrairement à de nombreuses solutions concurrentes (portes dérobées possibles)
  - Pérennité :
    - **Compatible** avec tous les smartphones avec appareil photo
    - **Standard ouvert** contrairement à de nombreuses solutions concurrentes
  - Vie privée et conformité :
    - **Aucune donnée personnelle** partagée implicitement entre l'utilisateur et l'application
    - **Une identité différente entre applications** utilisées, non recoupable par des moyens techniques
- Inconvénients :
  - Tous les secrets sont et restent côté client : sauvegarde à la charge de l'utilisateur

03. Social recovery

- Vient pallier les problème de sauvegardes de secrets côté client
- Plusieurs « gardiens » (>= 3) choisis par l'utilisateur
- Signature d'une majorité de gardiens pour changer la clé privée de signature de l'utilisateur
- Wallets : Argent wallet, Loopring wallet
- Principe d' « account abstraction » sur la blockchain Ethereum (EIP-4337)
- On attend la démocratisation de ce principe qui permettra une totale réappropriation de son identité par l'utilisateur



Questions & réponses !

renaud.lifchitz@holiseum.com

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

Holiseum est membre de Hexatrust, groupement français de la Cybersécurité et du Cloud de confiance

HOLISEUM

Faïz DJELLOULI
Président & Co-Fondateur
+33 6 69 72 29 64 | faiz.djellouli@holiseum.com

An NGUYEN
Directeur Général & Co-Fondateur
+33 6 98 84 39 97 | an.nguyen@holiseum.com