

# SPECIFICATION DE RECONSTRUCTION SIGL

Ce texte est l'autorité de reconstruction ; le texte masqué ci-dessus est historique. Le projet contient web, ios, esp, and et mac. Seuls web et ios sont implémentés. Il n'y a ni cookie, ni polling, ni DID dans une URL GET. Les versions Web et iOS sont indépendantes et augmentent à chaque changement de leur code.

## Serveurs et stockage

aiohttp, derrière Caddy HTTPS, sert `pico1.sigl.ai` (Soleil & Montagne, ☀, #b45309), `pico2.sigl.ai` (Box Énergie, ⚡, #0e7490) et `pico3.sigl.ai` (Autoconsommation Collective, ♻, #15803d). Chaque serveur a une clé P-256 publique compressée de 33 octets ; ses 6 derniers octets sont son SID. Un unique fichier JSON de persistance, lu et écrit directement par `app.py`, conserve les collections `sites(hôte, titre, icône, SID, clé)`, `users(target, UID, number, admin, pseudo, avatar)`, `sessions(DID, privé, UID, target, début, total)`, `tickets(ticket, target, UID, expiration, consommé)`, `counters(target, UID, total, début)` et `backgrounds(target, UID, MIME, image)`. SQLite est interdit ; JSON est réservé à ce fichier local et interdit dans les messages réseau.

## Web

### IHM

Sans h, GET / crée un DID aléatoire de 5 octets et rend la page publique. Elle est sombre, liquid glass, couvre les zones sûres et définit `theme-color` RGB. La version est en haut à gauche. À 8 px des coins du viewport : menu en haut à droite, deux accès fixes vers les autres serveurs en bas à gauche, domino en bas à droite. Chaque accès serveur mesure 58×58 et affiche favicon et nom blanc. En page personnelle uniquement, une croix de retrait discrète de 10×10 apparaît en haut à droite de l'accès ; le bouton +, transparent à contour pointillé, ouvre à chaque ouverture une matrice recalculée uniquement composée des serveurs absents, à l'exclusion du serveur courant ; si aucun serveur ne manque, le bouton + est masqué. Cette sélection locale est persistante. Les accès personnels sont des SigLinks navigate.

Le menu Web contient Photo de fond, Spécification PDF vers `/spec.pdf` et une entrée Contact. Cette dernière ouvre une fenêtre superposée avec `laurent.fourniercalmet@gmail.com` et 06 19 29 14 85, liés respectivement par `mailto:laurent.fourniercalmet@gmail.com` et `tel:+33619291485`.

### Comportement

Le fond public est stocké sur son serveur avec UID nul. Le fond personnel est stocké par `(target, UID)`. Une photo est envoyée par POST `/background` sous `UID(4)|mime(1)|image`, MIME 1 JPEG, 2 PNG, 3 HEIC, maximum 20 Mo. UID 00000000 est public. À la sélection ou au chargement, un calque de fond apparaît par opacité linéaire en 3 secondes.

### IHM : domino et identité

Le domino mesure 100×100. Le QR SVG est 21×21, 100 px, modules de 4 px, quiet zone de 8 px et code strictement `gatewaySID(6)|DID(5)`. Le toucher du QR bascule le plein écran natif de l'élément main, en public comme en personnel, sans traitement graphique particulier du QR ni modification de sa taille ; il ne provoque jamais de logout. Pendant ce plein écran, le calque photo est rattaché à main afin que le fond reste visible, puis revient à la page à la sortie. La page ouvre `/ws` sans paramètre et envoie DID(5) comme premier message WebSocket. Une page personnelle ajoute à gauche une bande noire translucide de 60×100 en 3 secondes. Le QR garde ses coins droits arrondis et rend ses coins

gauches carrés. La bande est une grille fixe 20/60/20 px : pseudo 20 px, avatar centré dans un cadre blanc 50×50, puis compteur jaune HH:MM:SS 20 px.

Après consommation d'un ticket, la target affiche Page personnelle de <pseudo>, relit son fond, son identité et son compteur. À la création, le pseudo est tiré parmi Pierre, Paul, Jacques ; l'avatar parmi 🐱 🦉 🐝 🐹 🦋. Ils persistent par (target, UID). Toucher le pseudo le remplace dans la bande par un champ mono-ligne de 50 px, limité à 20 caractères et sans débordement. Toucher l'avatar ouvre la table : 🐱 🦉 🐝 🐹 🦋 🐱 🐶 🦊 🐼 ☀️ ⚡ 🌿 🚀 💡 ★. La sauvegarde est POST /profile, binaire : UID(4)|pseudoLength(1)|pseudo\_UTF8|avatar\_UTF8.

### Comportement : identité et compteurs

Le serveur est la référence du compteur : il reprend (target, UID), avance tant qu'il est actif, et le fige au logout ou navigare. Le Web initialise son affichage avec cette valeur et l'incrémente chaque seconde. Dans le domino, le compteur est jaune vif, monospace 10 px, centré dans sa bande fixe de 20 px ; le toucher du compteur personnel déclenche le logout. Les compteurs bleus restent figés et ne sont jamais remis à zéro.

### Protocole de communication

Le Web ouvre GET /ws et envoie DID(5), reçoit targetSID|ticket ou L, ouvre ensuite GET /?h=tickethex, et émet POST /logout, /background, /profile et /sigl/open. Les contenus et séquences sont définis dans les tableaux communs ci-dessous.

## iOS

### IHM

SiglPro est SwiftUI plein écran, fond sombre avec photo locale persistante AppStorage. Version en haut à gauche. Le bouton menu blanc est toujours visible au premier plan, en haut à droite ; il ouvre un panneau tactile en anglais contenant choix/suppression de photo, spécification PDF <https://pico1.sigl.ai/spec.pdf>, Contact e-mail et téléphone ci-dessus. Version, menu et journal déroulant sont ajoutés par les zones sûres haute et basse, autour des boutons : ils restent visibles, ne recouvrent pas les boutons et le journal ne passe jamais sous l'indicateur d'accueil. Le journal est en anglais, très petit, chaque ligne commence par la date complète YYYY-MM-DD HH:MM:SS, affiche le plus récent en haut et permet de faire défiler les événements anciens vers le bas. Les trois boutons 120×120 sont alignés et espacés pour iPhone XS : titre sur deux lignes au plus, favicon centré, compteur HH:MM:SS bas. Ils sont triés par compteur synchronisé décroissant, le plus élevé en premier ; l'horloge du bouton jaune reste indépendante et avance chaque seconde.

### Comportement

États : bleu public ; orange entre la capture et la réponse HTTP 201 de /present, avec preview caméra strictement dans les 120×120. Jaune seulement dès cet ACK, texte noir et compteur en marche ; T synchronise ensuite sa valeur serveur ; bleu après L, compteur figé. Un seul jaune est autorisé et un seul WebSocket iPhone est actif par UID ; il est réutilisé tant qu'il est vivant et ses callbacks d'un socket obsolète sont ignorés. Les messages tardifs d'une autre target sont ignorés. Les fondus d'image sont strictement décoratifs : ils ne retardent ni trame, ni ACK, ni couleur de bouton.

### Protocole de communication

Chaque iPhone garde un secret P-256 Keychain. Pour targetSID : H=hash\_to\_curve(targetSID), N=xH, UID=SHA-256("SIGL-MINI-UID-1"|targetSID|N)[0..3]. L'UID est clair dans les messages mais n'est pas une clé publique.

## Séquences de communication Web ↔ iOS

Routes : GET /ws, GET /phone, GET /api/sites, POST /present, /callback, /logout, /background, /profile, /sigl/open, et GET /spec.pdf. Toutes les trames de protocole sont binaires et commencent par un opcode. GET /api/sites répond la forme compacte S(1)|count(1)|siteIndex(1)|SID(6) répétée count fois ; l'index référence les trois serveurs fixes de l'iPhone. Aucun échange de protocole n'utilise JSON.

P[113]=gatewaySID(6)|DID(5)|UID(4)|N(33)|R(33)|z(32). C'est Schnorr P-256 sur H(targetSID), hash-to-curve RFC9380 XMD SHA-256 SSWU, domaine SIGL-ZKP-V00-CS01-P256\_XMD:SHA-256\_SSWU\_RO\_, challenge SIGL-ZKP-V00-CS01-P256-SCALAR, transcript SIGL-ZKP-0-AUTH|targetSID|DID|N|R avec longueur u32 big-endian de chaque champ. La target vérifie UID, N, R et z.

### Login

| Étape | De      | Vers              | Message / effet                                                                   |
|-------|---------|-------------------|-----------------------------------------------------------------------------------|
| 1     | Web     | iPhone            | QR binaire : gatewaySID(6) DID(5)                                                 |
| 2     | iPhone  | gateway /phone    | UID(4), à l'ouverture du WebSocket                                                |
| 3     | iPhone  | target /present   | P[113]                                                                            |
| 4     | target  | gateway /callback | targetSID(6) DID(5) ticket(16), ticket unique TTL 5 s                             |
| 5     | gateway | WebSocket DID     | targetSID(6) ticket(16), 22 octets                                                |
| 6     | Web     | target            | GET /?h=tickethex, consommation du ticket                                         |
| 7     | target  | iPhone            | T UID(4) elapsed(8) number(2), ACK, synchronisation du compteur et de la pastille |

### Logout

| Étape | De     | Vers            | Message / effet                       |
|-------|--------|-----------------|---------------------------------------|
| 1     | Web    | target /logout  | UID(4), toucher du compteur personnel |
| 2     | target | iPhone          | L UID(4) elapsed(8), compteur figé    |
| 3     | target | WebSocket écran | L, retour page publique               |

### Navigate

Le scanner est interdit tant qu'un bouton est jaune. Les boutons n'ont aucun effet d'appui ni animation implicite : toute couleur est une affectation d'état instantanée. Au toucher d'un bouton bleu pendant Navigate, qu'il provienne de l'iPhone ou d'un SigLink Web, l'ancien jaune bascule en bleu et la cible en orange par affectation immédiate, avant tout envoi réseau ou animation ; l'ACK de présentation bascule ensuite la cible en jaune. Il n'existe donc jamais de clignotement bleu de la cible ni d'instant où tous les boutons sont bleus. Un SigLink personnel envoie DID(5)|targetSID(6) à POST /sigl/open de la source, puis suit les mêmes étapes.

| Étape | De              | Vers                     | Message / effet                                                                           |
|-------|-----------------|--------------------------|-------------------------------------------------------------------------------------------|
| 1     | iPhone          | source /phone            | 01 targetSID(6), aucun scan                                                               |
| 2     | source          | iPhone                   | L UID(4) elapsed(8), ancien bouton bleu et compteur figé                                  |
| 3     | source          | iPhone                   | O targetSID(6) gatewaySID(6) DID(5)                                                       |
| 4     | iPhone          | nouvelle target /present | P[113] reconstruit                                                                        |
| 5     | nouvelle target | iPhone                   | T UID(4) elapsed(8) number(2), ACK, synchronisation du nouveau compteur et de la pastille |

ESP, Android et macOS sont hors périmètre.

Le calque de fond iOS est un arrière-plan plein écran, non interactif et exclu du calcul de mise en page : son chargement ne déplace jamais les icônes ni les boutons. La version iOS est affichée en très petit dans un cadre transparent à bord discret.

Lorsqu'un nouveau téléphone présente une preuve pour prendre un serveur déjà personnel, la target ferme immédiatement toutes les sessions personnelles existantes de ce serveur et envoie L aux anciens iPhone avant l'acceptation du nouveau ticket.

Sur les iPhone étroits, l'espacement horizontal entre les trois boutons est recalculé selon la largeur disponible, jusqu'à zéro, afin d'éviter tout débordement tout en conservant les boutons centrés.

Pendant scanning, un second appui sur le même bouton arrête la caméra, annule le scan et remet immédiatement le bouton à l'état bleu public. Pendant waitingAck, l'appui reste sans effet.

Lorsqu'un nouveau téléphone ouvre une page personnelle sur un serveur, toute session personnelle précédente de ce serveur reçoit L proprement, son compteur est figé et son écran revient public avant l'ouverture de la nouvelle page.

Les noms des serveurs sont centrés sur une ou deux lignes au maximum, avec ellipse et sans débordement, dans les accès de page et dans la matrice d'ajout. Le cadre de la matrice adopte exactement le nombre de colonnes correspondant aux boutons ajoutables, sans colonne vide. En page personnelle, une petite pastille sombre affiche le numéro séquentiel de l'utilisateur sur le coin de l'avatar sans modifier l'avatar sauvegardé ; le premier utilisateur du serveur est le numéro 1 et l'administrateur. Ce numéro appartient à l'identité (serveur, UID), pas à une session : le même utilisateur conserve le même numéro sur plusieurs écrans.

À l'initialisation de l'app iOS, un fond de couleur aléatoire est choisi une seule fois pour cette instance. Il couvre tout l'écran sous les contrôles ; une photo de fond sélectionnée ultérieurement le masque entièrement sans déplacer les contrôles.

La version, le menu et le journal iOS sont des superpositions explicites alignées respectivement en haut et en bas de la vue racine ; ils restent donc visibles au-dessus du fond coloré ou photographique et des boutons.

Un T iOS est T|UID(4)|elapsed(8)|number(2)|pseudoLength(1)|pseudo ; il n'est accepté que pour un bouton orange ou déjà jaune. Tout T retardé après un L est ignoré. Le L reçu pour le bouton personnel ou en transition le repasse immédiatement au bleu et fige son compteur.

Le traitement de L ferme toutes les sessions personnelles locales de l'iPhone, quel que soit le callback du WebSocket qui le porte ; lors d'un changement de serveur, l'ancienne liaison est fermée avant l'ouverture de l'unique nouvelle liaison.

Le changement de serveur fige d'abord la liste de liaisons à fermer, puis les ferme avant d'enregistrer la nouvelle : aucune collection de WebSockets n'est modifiée pendant son parcours.

Chaque bouton iPhone affiche, à côté du favicon, la pastille du numéro number reçu pour ce serveur ; cette valeur est celle de l'identité persistante (serveur, UID), jamais l'UID lui-même. Les numéros exposés sont strictement limités à 1, 2 et 3 ; les anciennes lignes historiques au-delà de 3 sont ignorées et aucune nouvelle ligne 4 ou 5 n'est attribuée.

Le pseudo reçu dans ce même ACK est affiché en très petit sous la pastille du bouton iPhone, tronqué sur une ligne si nécessaire ; aucun pseudo n'est affiché avant la première visite du serveur.

Le chrono des boutons iOS utilise une police monospace de 14 px ; le journal déroulant occupe toute la largeur de l'écran, sans marge horizontale.

Sur iOS, ce pseudo est noir lorsque le bouton est jaune. Sur le Web, la page personnelle de l'administrateur (numéro 1) affiche en plus un tableau incluant la ligne 1 – Admin, puis les autres utilisateurs du serveur avec numéro, avatar et pseudo.

La barre supérieure iOS reste alignée en haut mais est décalée de 22 px vers l'intérieur de l'écran afin de ne pas toucher l'encoche.

Le catalogue comprend aussi `pico4.sigl.ai` (Vigie Baignade,  #2563eb). Les quatre boutons iOS sont remplis en ordre de lecture : rangées de trois, gauche à droite dans chaque rangée puis rangée suivante.

La grille iOS conserve un espacement unique entre les boutons et entre les boutons et les bords de l'écran. Cet espacement est calculé selon la largeur disponible ; les cartes rétrécissent ensemble sur les écrans étroits.

Pour Navigate, l'iPhone réutilise uniquement une liaison `/phone` dont l'état est actif. Si cette liaison n'est plus active ou si l'envoi échoue, la trame `01|targetSID(6)` est mise en attente et une seule reconnexion événementielle la transmet ; aucun polling ni doublon n'est généré.

Lorsqu'une nouvelle liaison `/phone` reprend le même UID sur une target, le serveur sélectionne uniquement les sessions privées de cette target, fige leurs compteurs, envoie une seule trame `L|UID(4)|elapsed(8)` directement aux anciennes liaisons, puis ferme celles-ci. Les sessions du même utilisateur sur d'autres targets restent inchangées.

Lorsqu'une nouvelle liaison `/phone` reprend un UID déjà connecté, chaque session privée de cet UID est d'abord figée et reçoit `L|UID|elapsed`, puis l'ancienne liaison est fermée.