HELXSYNC

Mutual Visual Authentication Protocol

Protocole d'Authentification Visuelle Mutuelle

Auteur / Author: Frederic St-Laurent	**Organisation:** iCounter Inc., Québec, Canada
Version: v1.0	**Date:** 22 février / February 22, 2026
DOI: 10.5281/zenodo.XXXXXXXX	**Licence:** CC BY 4.0 — helxsync.com

ABSTRACT / RÉSUMÉ

ENGLISH

HELXSYNC introduces the Mutual Visual Authentication Protocol (MVAP), a novel network-level authentication mechanism providing real-time, cross-domain, visually verifiable proof of site legitimacy. Unlike existing standards (TLS, FIDO2, TOTP) which authenticate the user toward the server but leave the server-side unauthenticated to the user, HELXSYNC deploys a cryptographic network token — identical across all official domains of a network — synchronized in real time from an isolated compute environment. The token is bounded by a strict temporal validity window, making replay and cloning attacks detectable by visual inspection alone, without any application, hardware, or user training. Five formal security properties are defined: temporal freshness, temporal integrity, secret isolation, network coherence, and infrastructure opacity.

FRANÇAIS

HELXSYNC introduit le Protocole d'Authentification Visuelle Mutuelle (MVAP), un mécanisme d'authentification réseau inédit permettant une vérification en temps réel de la légitimité d'un site, à l'échelle multi-domaines, vérifiable visuellement. Contrairement aux standards existants (TLS, FIDO2, TOTP), HELXSYNC déploie un token cryptographique réseau — identique sur tous les domaines officiels — synchronisé en temps réel depuis un environnement isolé. La validité temporelle stricte rend toute attaque par rejeu ou clonage détectable par simple observation visuelle, sans application, sans matériel ni formation. Cinq propriétés de sécurité formelles sont définies : fraîcheur temporelle, intégrité temporelle, isolation du secret, cohérence réseau et opacité de l'infrastructure.

Keywords / Mots-clés : *mutual authentication, visual authentication, network token, cross-domain, anti-phishing, MVAP, authentification mutuelle, protocole visuel, sécurité réseau*

01 — PROBLEM / PROBLÈME

Authentication is One-Directional.

L'authentification est à sens unique.

For over 30 years, network authentication protocols have focused exclusively on proving the user's identity to the server. The inverse relationship — the server proving its legitimacy to the user — remains an unsolved problem in production environments.

Depuis plus de 30 ans, les protocoles d'authentification réseau se sont exclusivement concentrés sur la preuve de l'identité de l'utilisateur vers le serveur. La relation inverse — le serveur prouvant sa légitimité à l'utilisateur — reste un problème non résolu dans les environnements de production.

- **Fundamental Asymmetry / Asymétrie fondamentale**
  The user authenticates to the server. The server bears no reciprocal obligation. TLS proves domain registration — not operational legitimacy. | L'utilisateur s'authentifie vers le serveur. Le serveur n'est soumis à aucune obligation réciproque. TLS prouve l'enregistrement d'un domaine — pas sa légitimité opérationnelle.
- **2FA Does Not Solve This / La 2FA ne résout pas ce problème**
  TOTP, FIDO2, and Passkeys strengthen user→server proof. They do not address the inverse. Credentials remain at risk if the site is not authentic. | TOTP, FIDO2 et Passkeys renforcent la preuve utilisateur→serveur. Ils ne traitent pas le problème inverse.
- **Invisible to Users / Invisible pour les utilisateurs**
  No visual signal distinguishes an official site from a fraudulent clone. SSL padlocks are ubiquitous. Design, URL, and branding can be reproduced identically. | Aucun signal visuel ne distingue un site officiel d'un clone frauduleux.
- **No Existing Standard / Aucun standard existant**
  No current standard provides multi-domain, real-time, visually verifiable network proof without a third-party application, dedicated hardware, or required expertise. | Aucun standard actuel ne fournit de preuve réseau multi-domaines, temps réel, vérifiable visuellement, sans application tierce ni expertise.

---

02 — PROTOCOL / PROTOCOLE

One Identical Token Across the Entire Network.

Un token identique sur tout le réseau.

HELXSYNC deploys a cryptographically derived network token — computed in an isolated server environment — displayed identically and simultaneously across all official domains of a network. The token is bounded by a strict temporal validity window. Any divergence between two simultaneous displays is immediately detectable by direct visual comparison.

HELXSYNC déploie un token réseau cryptographiquement dérivé — calculé dans un environnement serveur isolé — affiché de manière identique et simultanée sur tous les domaines officiels d'un réseau. Toute divergence entre deux affichages simultanés est immédiatement détectable par comparaison visuelle directe.

- **Network Membership Proof / Preuve d'appartenance réseau**
  All official domains display a cryptographically identical indicator. Irreproducible without the network secret — never exposed, never transmitted to the client. | Tous les domaines officiels affichent un indicateur cryptographiquement identique.
- **Temporal Freshness Proof / Preuve de fraîcheur temporelle**
  Synchronized timestamp with a bounded validity window. Any divergence between two simultaneous displays is observable. | Horodatage synchronisé et fenêtre de validité bornée.
- **Mutual Authentication / Authentification mutuelle**
  Site and user authenticate simultaneously. Zero password. Zero SMS. Zero dedicated device required. | Site et utilisateur s'authentifient simultanément — zéro mot de passe, zéro SMS, zéro appareil dédié.

---

03 — SECURITY PROPERTIES / PROPRIÉTÉS DE SÉCURITÉ

Five Formal Guarantees. Zero Exposed Details.

Cinq garanties formelles. Zéro détail exposé.

The five security properties below are described in terms of observable guarantees, independently of the specific cryptographic primitives employed. This formulation allows for future primitive substitution without loss of security model validity.

Les cinq propriétés de sécurité ci-dessous sont décrites en termes de garanties observables, indépendamment des primitives cryptographiques spécifiques employées.

P1	**Bounded Temporal Freshness / Fraîcheur temporelle bornée** Each indicator is valid for a strictly delimited temporal window. Any display outside the window is identifiable without tooling. | Chaque indicateur est valide pour une fenêtre temporelle strictement délimitée.
P2	**Verifiable Temporal Integrity / Intégrité temporelle vérifiable** Synchronized timestamp. Any deviation beyond the defined tolerance is detectable by direct observation. | Horodatage synchronisé — tout écart est détectable par observation directe.
P3	**Network Secret Isolation / Isolation du secret réseau** No secret in the client. No key in HTML/JS. Irrecoverable by observation or interception. | Aucun secret dans le client, aucune clé dans le HTML/JS. Irreconstituable par observation.
P4	**Network Coherence Guarantee / Cohérence de réseau garantie** All member domains display an identical indicator. The probability of coincidence is cryptographically negligible. | Tous les domaines membres affichent un indicateur identique.
P5	**Infrastructure Opacity / Opacité de l'infrastructure** The computation environment exposes no key. The client cannot derive the generation method. | L'environnement de calcul n'expose aucune clé — le client ne peut pas dériver la génération.

04 — COMPARATIVE ANALYSIS / ANALYSE COMPARATIVE

What Existing Standards Do Not Provide.

Ce que les standards existants ne fournissent pas.

Security Property	TOTP/2FA	FIDO2	TLS/SSL	HELXSYNC
Bidirectional Authentication / Authentification bidirectionnelle	—	~	—	✓
Visual Verification — No Tool / Vérification visuelle sans outil	—	—	—	✓
Multi-Domain Network Proof / Preuve réseau multi-domaines	—	—	—	✓
No Third-Party App / Sans application tierce	—	—	✓	✓
No Dedicated Hardware / Sans matériel dédié	✓	—	✓	✓
Sub-Second Temporal Freshness / Fraîcheur temporelle sub-seconde	—	—	—	✓
Cross-Domain Coherence Provable / Cohérence inter-domaines prouvable	—	—	—	✓
Zero User Training Required / Aucune formation utilisateur	—	—	✓	✓

05 — APPLICATIONS

Wherever Visual Trust Matters.

Partout où la confiance visuelle compte.

- **Finance & Banking / Finance & Bancaire**
  All domains display the same token. Customers recognize the official network instantly. | Tous les domaines affichent le même token — reconnaissance instantanée du réseau officiel.
- **Blockchain & DeFi**
  Passive trust layer across all domains (.com, .org, .io, app) without user action. | Couche de confiance passive sur tous vos domaines sans action utilisateur.
- **Government & Health / Gouvernement & Santé**
  Visual trust anchor for sensitive public services. No app, no training. | Ancre de confiance visuelle pour les services publics sensibles. Aucune app, aucune formation.
- **SaaS Enterprise**
  Prove legitimacy across all client subdomains. Protection against targeted impersonation. | Prouvez votre légitimité sur tous vos sous-domaines clients.
- **Authentication Standard / Standard de connexion**
  Site and user authenticate simultaneously. Replaces password without additional infrastructure. | Site et utilisateur s'authentifient simultanément — remplace le mot de passe.

06 — PRIORITY & CONCLUSION / ANTÉRIORITÉ & CONCLUSION

Originality Statement / Déclaration d'originalité

To the best of the author's knowledge, no prior art describes a network-level mutual visual authentication mechanism providing real-time, cross-domain, toolless, visually verifiable proof of site legitimacy as defined by the five formal properties enumerated above. This preprint is submitted to Zenodo to formally establish date of conception and public disclosure of the HELXSYNC — MVAP protocol.

À la connaissance de l'auteur, aucun art antérieur ne décrit un mécanisme d'authentification visuelle mutuelle au niveau réseau fournissant une preuve en temps réel, multi-domaines, sans outil, vérifiable visuellement, telle que définie par les cinq propriétés formelles énumérées ci-dessus. Ce preprint est soumis à Zenodo pour établir formellement la date de conception et de divulgation publique du protocole HELXSYNC — MVAP.

Frederic St-Laurent

Founder, iCounter Inc. — Québec, Canada

First public disclosure / Première divulgation publique : 22 février / February 22, 2026

helxsync.com · iCounter Inc. · CC BY 4.0 · DOI: 10.5281/zenodo.XXXXXXXX