🛡️ Decentralized Identification with Press ID Badge

By: Patrick O. Ingle, July 16, 2025

Empowering Secure, Passwordless Authentication Through Local Cryptographic Signing

📌 Abstract

This whitepaper presents the Press ID Badge browser extension, a decentralized identification tool designed to eliminate reliance on passwords and centralized credential stores. By leveraging local cryptographic signing—where private keys never leave the user's device—Press ID Badge offers a secure, auditable, and user-respecting alternative to traditional login and verification systems. We explore its implementation, benefits, and implications for digital trust, especially in high-sensitivity environments such as journalism, decentralized governance, and credential-backed interactions.

🧩 Introduction

Digital identity remains fraught with compromise, complexity, and centralization. The dominant user-password model breeds weak credentials, dependency on trust intermediaries, and vulnerability to phishing, leaks, and social engineering. Press ID Badge tackles this problem head-on, enabling:

- Service message signing via locally stored private keys
- Auth workflows based on verifiable credentials and DID documents
- Passwordless authentication fortified with cryptographic assurance
- Seamless integration into content-script-secured browsers via modular architecture

🔐 Core Features & Safety Guarantees

1. ✅ Local Private Key Signing

- Press ID Badge generates and stores the user's signing key **locally**.
- All cryptographic operations—RSA, ECDSA, etc.—happen **in-browser**, using Web Crypto or WASM-backed modules.
- No external transmission or exposure of the private key.

2. 📜 Signed Service Messages

- Requests, attestations, and credential presentations are **digitally signed**.
- Services verify these signatures using publicly shared keys or DID documents.
- Reduces attack surface for MITM and replay attacks.

3. 🔑 Passwordless Logins via Credential Exchange

- Users authenticate by presenting signed, verifiable credentials.
- No passwords to forget, reuse, or reset.
- Compatible with W3C Verifiable Credentials and DID Auth flows.

4. 🧠 2FA Without the Fuss

- Built-in support for hardware key challenge signing (e.g., WebAuthn fallback).
- Optional biometric prompts via browser APIs.

🌐 Decentralized Architecture Overview

```
graph TD;
  User["User (Browser)"]
  DID["Decentralized Identifier (DID)"]
  VC["Verifiable Credential"]
  Service["Service (Verifier)"]

  User -->|Signs Message| Service
  Service -->|Requests Proof| User
  User -->|Presents VC| Service
  User --> DID
  Service --> DID
```

- **No centralized authority** governs credential issuance or user identity.
- Credentials are **portable**, **revocable**, and **selectively disclosable**.

⚙️ Technical Design

- Modular architecture with separation of **content scripts**, **background logic**, and **signature engine**
- CSP-compliant script injection workflows
- Enforced origin trust boundaries for messaging and credential presentation
- JSON-based JWK support with RSA/ECDSA encoding utilities
- Compatibility across Chrome, Brave, and Firefox

🧪 Security Benefits

Feature	Traditional Auth Model	Press ID Badge
Password Resets	Frequent, brittle	Eliminated
Phishing Risk	High	Cryptographically mitigated
Credential Storage	Server-side, breach-prone	Local-only, user-owned
Key Rotation	Manual, error-prone	Built-in with DID updates
2FA Bypass	Possible via phishing	Challenge-response signed locally

📣 Use Cases

- Newsroom access control via Press ID Badge verification
- Independent journalists presenting verified credentials to secure interviews or sensitive locations
- DAO members authenticating cryptographically without revealing personal data
- Enterprise users reducing IT overhead by using decentralized IDs for internal tooling

🛠️ Future Directions

- zk-proof-backed disclosures for pseudonymous participation
- Integration with reputation systems and selective transparency layers
- Open-source tooling for cross-language validators (PHP, Node.js, etc.)

🔚 Conclusion

Press ID Badge represents a paradigm shift in how we verify identity and trust online. By empowering users with tools to sign and authenticate locally, the extension moves us closer to a world where credentials are **secure**, **self-sovereign**, and **independent of centralized control**.
