6th INTERNATIONAL CONFERENCE ON

PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS

(PKIA 2025)

SEPTEMBER 3-4th, 2025

A Usable and Secure Authentication for Multi-server Environments to Enhance Digital Trust

Dr. Mohammad Misbahuddin (CDAC), Dr. S D Sudarsan(CDAC), Ankur Sanda(Acharya Institutes), Adilkhan H Kulkarni(Acharya Institutes)

Motivation: The Problem of Trust in Multi-Server Environments

- **Foundational Paradigms (Kerberos, SAML, FIDO):** Provide strong authentication models centralized (Kerberos), federated (SAML), and device-bound (FIDO).
- **The Shared Technical Gap:** Despite their strengths, these protocols lack a standardized mechanism for state augmentation and verifiable chained authentication for multi-server environments.
- **Our Objective:** To introduce a framework that increases trust, is stateful, and cryptographically verifiable across independent services.

Challenges in Multi-Server Authentication

- **General Authentication Weaknesses:**
  - Persistent risk of stored password hashes on server-side.
  - Vulnerabilities in biometric factors, which can be spoofed.
- **Limitations of Single-Server Paradigms:**
  - FIDO2 provides strong authentication but is scoped to individual Relying Parties.
- **Key Research Challenges for Multi-Server Environments:**
  - Maintaining secure sessions across independent SPs.
  - Securely transferring an authentication assertion.
  - The lack of robust state management in existing protocols.

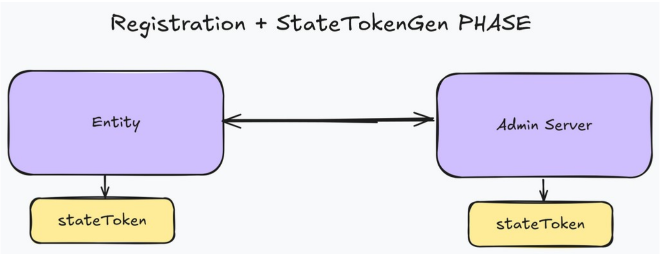
Proposed Solution: The State Token Relay Protocol (STRP)

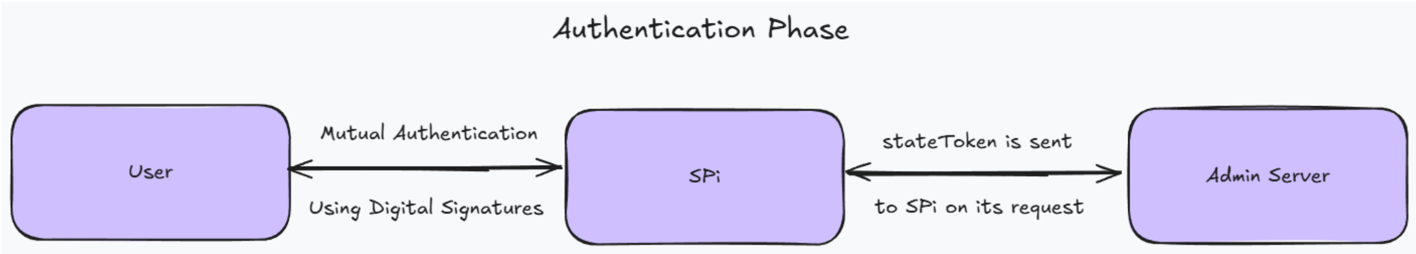
A comprehensive framework for **stateful** and **chained** authentication.

- **Protocol Entities:**
  - **Admin Server (AS):** Central trust anchor and state manager.
  - **User (U):** The entity being authenticated.
  - **Service Providers (SPs):** Mutually trusting but independent services.
- **Core Principle:** STRP's core principle is to combine dynamic state token management with a secure, multi-party chained authentication process to enable robust authentication in multi-server environments.

STRP Protocol Lifecycle

- **Register:** One-time identity establishment with the Admin Server.
- **StateTokenGen:** A collaborative sub-protocol used during Registration and Recovery to create the dynamic state token.
- **Auth:** Establishes the initial, primary authentication with a Service Provider.
- **Validate:** Enables seamless, repeated access to subsequent SPs in the trust domain.
- **Recovery:** A secure way to re-establish credentials in case of loss of device or account compromise.





Contribution 1: The Dynamic State Token

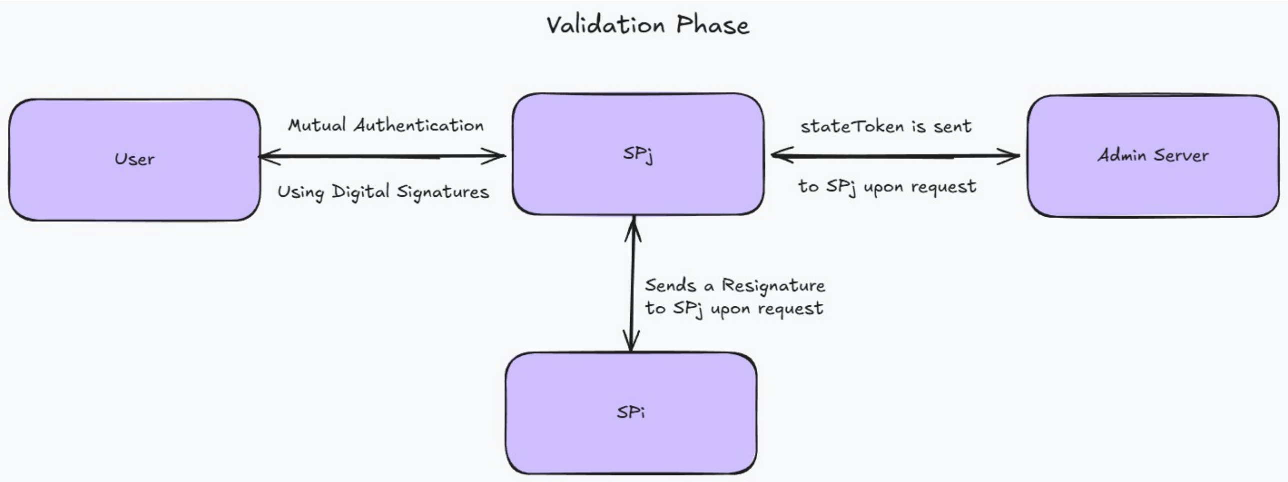
A novel cryptographic anchor for stateful authentication, distinct from static credentials.

- **Collaborative Generation:** Interactively derived by an Entity (U/SP) and the Admin Server.
- **Dynamic Properties:**
  - **stateEntropy:** A unique secret derived via HKDF.
  - **counter:** Monotonically increasing counter for replay protection.
  - **lifecycle:** Explicit creation and expiry timestamps.
- **Function:** Serves a short-lived, stateful and verifiable proof of an protocol session.

1) State id: $state\_id$
2) State Entropy: $stateEntropy$
3) Entity id: e_{id}
4) Counter: $count$
5) Creation time: $issued\_at$
6) Expiry time: $expires\_at$

State token fields

Contribution 2: Validation Phase



- SP_j trusts SP_i's assertion about U, which is cryptographically bound to U's original challenge-response.
- SP_i sends a resignature to SPj that it can use to Authenticate both U and SP_i, thus performing chained Authentication.
- The Admin Server (AS) acts as the trusted mediator, providing the necessary state tokens to SP_j to perform the final verification.

Contribution 3: Formalized Trust Domain Management

A mechanism for establishing and managing a bounded trust environment.

- **Privilege Group (PG):**
  - A formally defined set of mutually trusting Admin Servers and Service Providers.
  - Establishes a clear operational boundary for chained validation.
- **Trusted Server List (TSL):**
  - An authoritative directory for verifying an SP's membership in the Privilege Group.
  - Provides a trusted distribution medium for SP public keys.

Security Analysis: Formal Verification with ProVerif

The protocol's security guarantees were formally analyzed and verified.

- **Tool:** ProVerif, for automated cryptographic protocol verification.
- **Adversary Model:** The Dolev-yao model.
- **Verified Properties:**
- **Secrecy:** Long term and short term secrets of the protocol remain confidential.
- **Authentication:** Correct entity authentication is guaranteed through correspondence properties, mitigating impersonation and replay attacks.

Conclusion and Key Contributions

- **A Novel Framework (STRP):**
  - For stateful and chained authentication in multi-server environments.
  - Delivers an SSO-like experience for user convenience with explicit, verifiable trust.
- **Dynamic State Tokens:** A robust mechanism for secure, replay-protected session management using HKDF-derived entropy.
- **Formalized Trust Boundaries:** Established via Privilege Groups and TSLs.
- **Rigorous Security Guarantees:** Claims are validated through formal verification with ProVerif, proving secrecy and authentication properties.

STRP provides a foundational solution for enhancing security, usability, and explicit trust in interconnected digital services.

THANK YOU

References

- D. Dolev and A. Yao, "On the security of public key protocols," IEEE Transactions on Information Theory, 1983.
- Web Authentication Working Group, "Web Authentication: An API for accessing Public Key Credentials Level 2," W3C Recommendation, 2021.
- H. Xiong, et al., "A novel multiserver authentication scheme using proxy resignature with scalability and strong user anonymity," IEEE Systems Journal, 2020.B. Blanchet,
- "Modeling and verifying security protocols with the applied pi calculus and proverif," Foundations and Trends in Privacy and Security, 2016.