Model Context Protocol

URL MODE ELICITATION

Designing Secure Confirmation Screens for CLI/TUI Applications based on SEP-1036

THE CONTEXT OF SEP-1036

Evolving the Elicitation Mechanism

ELICITATION MODES COMPARED

FORM MODE

In-band interaction where the client renders a structured form. Best for non-sensitive data like preferences or simple text inputs.

URL MODE

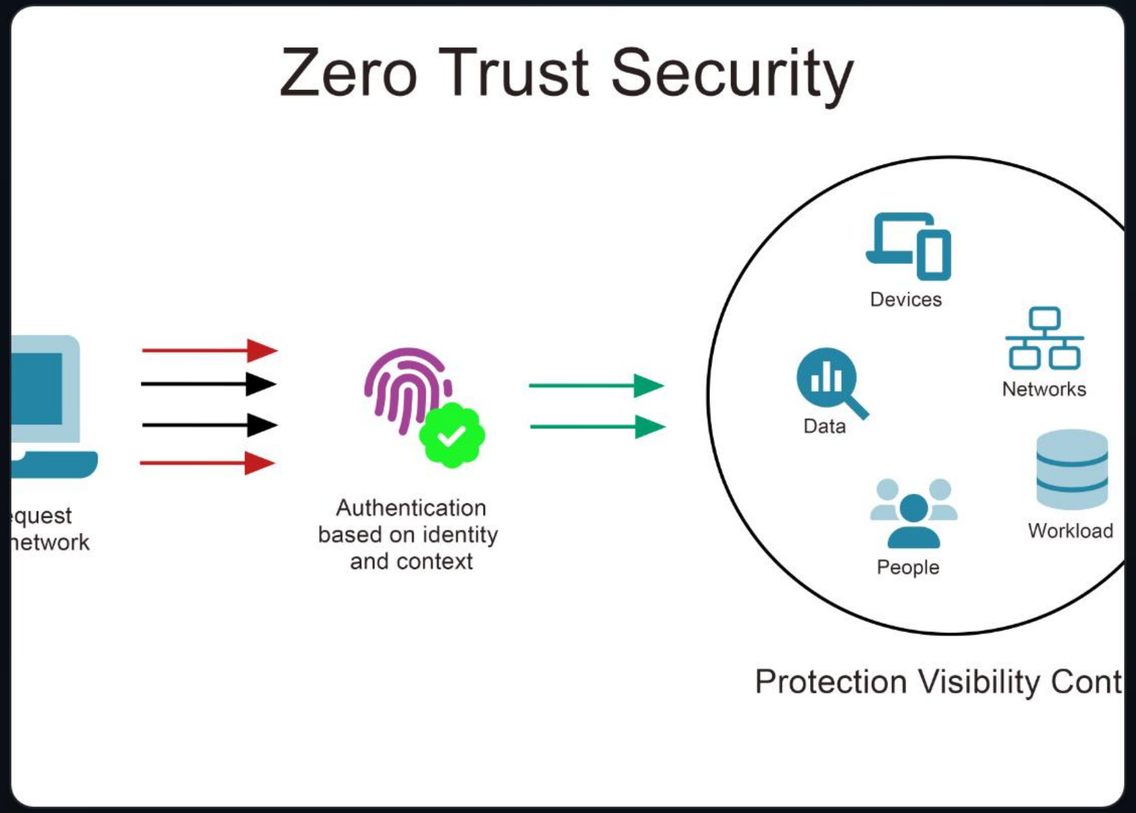
Out-of-band interaction. The server provides a URL for sensitive tasks like OAuth, payments, or credential entry in a secure browser.

ESTABLISHING TRUST BOUNDARIES

Zero-Secret Architecture

By using URL mode, the MCP Client acts only as a gateway, never observing the sensitive data itself.

- Client bypass for secrets
- Hardened browser contexts
- Server-to-Server completion



TUI CONFIRMATION STANDARDS

- **Domain Transparency:** Always display the target domain and host clearly to prevent SSRF and phishing attacks.
- **Explicit User Consent:** Do not auto-open URLs. Require a deliberate user action (e.g., "Press Y to open").
- **System Browser:** Launch the default system browser rather than internal webviews that could inspect traffic.
- **Contextual Awareness:** Display the server's human-readable message to explain the interaction is needed.

PROTOCOL REQUEST PARAMETERS

PARAMETER	TYPE	DESCRIPTION	REQUIRED
`mode`	string	Must be set to `"url"`	✓
`url`	string	Target URL for the out-of-band flow	✓
`elicitationId`	string	Unique identifier for tracking state	✓
`message`	string	Human-readable context for the user	✓

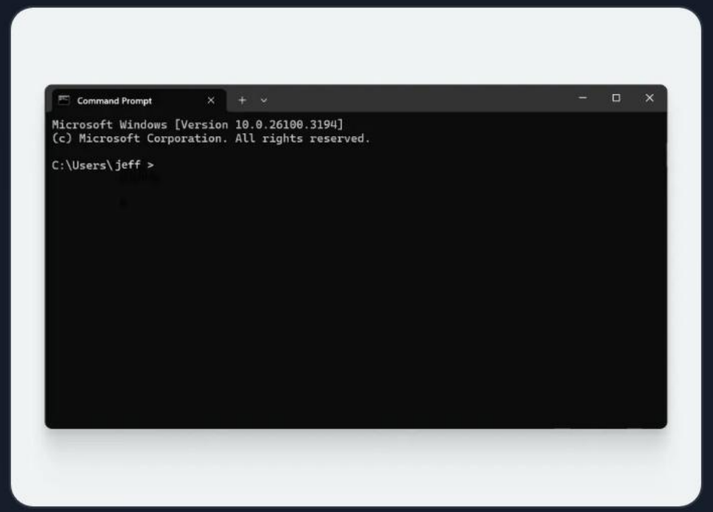
QUANTIFYING SECURITY BENEFITS

Risk analysis based on trust boundary analysis of the Model Context Protocol.

TUI IMPLEMENTATION DESIGN

Best Practices for Terminal Interfaces

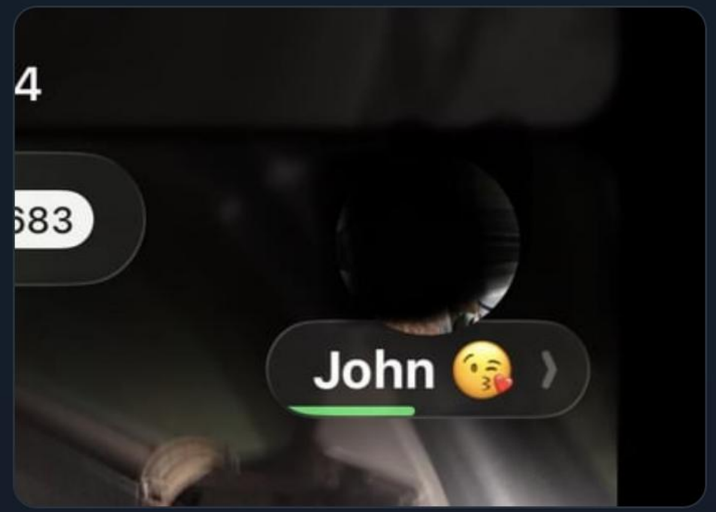
VISUAL UX BEST PRACTICES



Clear Prompts
Display URL and Message

```
[!] Domain Verification
Host: github.com
Verify this is correct.
```

Domain Focus
Highlight the Host



Completion
Server-side Auth feedback

IMPLEMENTATION ROADMAP

Q4 2025
SEP-1036 Proposal and Initial Draft

Q1 2026
Spec Revision and Capability Expansion

Q2 2026
Reference Implementation for Major Clients

Q3 2026
Secure-by-Default Standards Adoption

THE POWER OF SEP-1036

1036

Enhancement Proposal

A Critical Security Milestone

SEP-1036 introduces the `"url"` mode to the Model Context Protocol, enabling the gathering of sensitive credentials and payments without ever exposing them to the local LLM client.

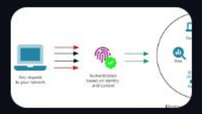
This is the definitive answer to the "Secret Leakage" problem in distributed AI protocol environments.

QUESTIONS?

Secure Your MCP Implementation Today

Read the full SEP: modelcontextprotocol.io/seps/1036

IMAGE SOURCES



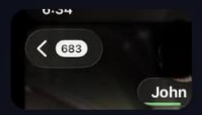
https://appcheck-ng.com/wp-content/uploads/Trust-Boundary-Pic-5.png

Source: appcheck-ng.com

---

https://images-www.contentful.com/fo9twyrwpveg/1CtED3zwrMQoV4X3QiEAMX/4721d48b8243e2a25f8464e599c35d89/image10.png?w=1320&q=60&fm=webp

Source: www.contentful.com



https://preview.redd.it/green-bar-under-contact-sms-photo-v0-5d6yq0wu3hgg1.jpeg?width=640&crop=smart&auto=webp&s=c43dde28947d9308cd589dd3ffa79901d9e8ca70

Source: www.reddit.com