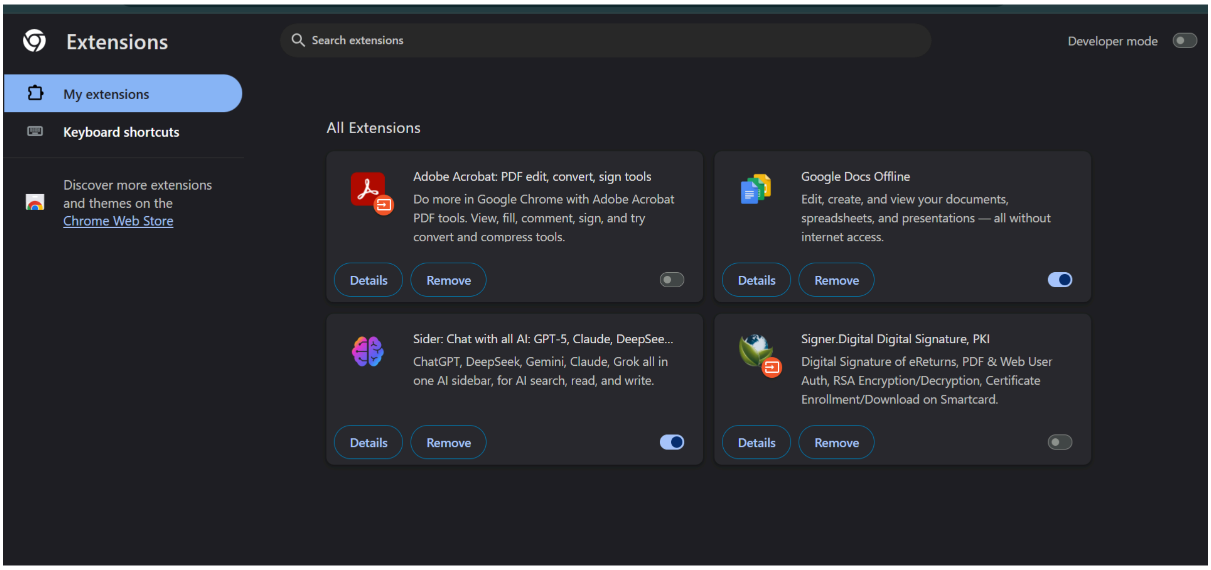
Task 7: Identify and Remove Suspicious Browser Extensions

Objective

To identify, analyze, and remove potentially harmful browser extensions and understand how malicious extensions can pose security risks to users.

Tools Used

- **Browser:** Google Chrome
- **Extension Manager:** `chrome://extensions/`



Discover more extensions and themes on the Chrome Web Store

All Extensions

Adobe Acrobat: PDF edit, convert, sign tools
Do more in Google Chrome with Adobe Acrobat PDF tools. View, fill, comment, sign, and try convert and compress tools.

Google Docs Offline
Edit, create, and view your documents, spreadsheets, and presentations — all without internet access.

Sider: Chat with all AI: GPT-5, Claude, DeepSee...
ChatGPT, DeepSeek, Gemini, Claude, Grok all in one AI sidebar, for AI search, read, and write.

Signer.Digital Digital Signature, PKI
Digital Signature of eReturns, PDF & Web User Auth, RSA Encryption/Decryption, Certificate Enrollment/Download on Smartcard.

Installed Browser Extensions (Observed)

Based on the provided screenshot, the following extensions were installed:

1. **Adobe Acrobat: PDF edit, convert, sign tools**
2. **Google Docs Offline**
3. **Sider: Chat with all AI (GPT-5, Claude, DeepSeek, Gemini, etc.)**
4. **Signer.Digital – Digital Signature, PKI**

Extension-wise Security Review

1. Adobe Acrobat: PDF edit, convert, sign tools

- **Developer:** Adobe (Trusted vendor)
- **Purpose:** PDF viewing, editing, signing
- **Permissions:** Required for PDF handling
- **Risk Level:** Low
- **Remarks:** Legitimate and widely used extension. No suspicious behavior detected.

2. Google Docs Offline

- **Developer:** Google LLC
- **Purpose:** Offline document editing
- **Permissions:** Access to Google Docs files
- **Risk Level:** Low
- **Remarks:** Official Google extension. Safe and necessary for productivity.

3. Sider: Chat with all AI (GPT, Claude, Gemini, etc.)

- **Purpose:** AI-powered sidebar for search, reading, and writing
- **Permissions:** Reads webpage content to provide AI responses
- **Risk Level:** Medium (Permission-based risk)
- **Remarks:**
    - Not malicious
    - Requires **webpage access**, which could be risky if misused
    - Safe **only if installed from official Chrome Web Store and kept updated**

4. Signer.Digital – Digital Signature, PKI

- **Purpose:** Digital signatures, certificate-based authentication
- **Use Case:** Government & enterprise-level document signing
- **Permissions:** Cryptographic operations
- **Risk Level:** Medium
- **Remarks:**
    - Legitimate but **security-sensitive**
    - Should be used only when required
    - Must be kept updated to avoid certificate misuse

Suspicious Extensions Found

None

Extensions Removed

None

All installed extensions were found to be **legitimate, relevant, and purpose-driven**.

Research: How Malicious Browser Extensions Can Harm Users

Even though no malicious extensions were found, harmful extensions may:

- Steal login credentials and passwords
- Track browsing activity and personal data
- Inject ads or redirect traffic

- Perform phishing attacks
- Execute malicious scripts silently
- Abuse permissions like “Read and change all website data”

Outcome

This task improved awareness about:

- Browser security risks
- Importance of reviewing extension permissions
- Safe extension management practices

Conclusion

Based on the review of installed browser extensions, no suspicious or malicious extensions were found. All extensions were verified to be legitimate and necessary. Regular auditing of browser extensions is recommended to maintain browser security.