AI Security and Privacy (ai-snp) Working Group Charter

Name	AI Security and Privacy (ai-snp)
Initial Chairs	Andor Kesselman, Kim Hamilton Duffy
Status	Proposed
Repo	https://github.com/decentralized-identity/ai-snp

1. Overview

The **AI Security and Privacy Working Group (WG)** focuses on the intersection of **AI-driven systems** with **identity and authorization frameworks**. The group's goal is to identify, analyze, and address security and privacy challenges that arise when AI services interact with decentralized identity technologies and authorization layers. Through community collaboration, the WG aims to establish comprehensive guidelines, recommendations, and specifications that ensure **robust security** and **user-centric privacy** in AI-powered solutions.

2. Scope

1. **Threat Modeling & Risk Assessment**
   - Identify and assess threats specific to AI systems managing or processing identity data (e.g., adversarial usage of credentials, unauthorized credential access).

   - Evaluate how AI-based processes can be manipulated to bypass or undermine authorization controls.
2. **Security and Privacy Architecture & Design**
   - Define principles for integrating identity and authorization layers into AI workflows, ensuring **privacy-by-design** and **secure data flows**.

   - Explore patterns that support user sovereignty (e.g., minimal disclosure of identity data, privacy-preserving verification techniques).
3. **Operational Security for Identity & Authorization**
   - Outline best practices for continuous monitoring and incident response in AI systems that rely on decentralized identities or verifiable credentials.

   - Examine governance models that safeguard identity issuance, credential lifecycle management, and authorization revocation.
4. **Regulatory & Compliance Considerations**
   - Investigate regulatory requirements (e.g., GDPR, CCPA) as they pertain to AI-driven identity services, focusing on data protection

and consent.

- Provide guidance on aligning AI-based authorization practices with emerging privacy and security standards.

5. **Collaboration & Knowledge Sharing**
    - Encourage open dialogue around secure integrations between AI and identity/authorization layers.

    - Promote coordinated disclosure of vulnerabilities related to AI-driven identity services, fostering a shared understanding of risks and mitigations.

3. Deliverables

1. **Documentation & Best Practices**
    - Whitepapers and technical guidance that clarify how to securely integrate AI functionalities with identity and authorization frameworks.

    - Illustrative examples of threats and mitigations tied to AI-based decision-making around user credentials and access control.
2. **Reference Architectures & Conceptual Frameworks**
    - High-level architectural models showing **how AI systems can securely handle identity data** and authorization requests.

    - Recommendations for implementing privacy-preserving identity verification techniques within AI pipelines.
3. **Specifications & Standards Contributions**
    - Proposals or contributions to existing standards that address **AI security, privacy, identity, and authorization**.

    - Interoperability profiles ensuring alignment across different identity frameworks and AI services.
4. **Community Guidance & Outreach**
    - Educational materials (e.g., FAQs, explanatory briefs) on AI security and privacy topics related to user identification and authorization.

    - Public sessions or roundtables for sharing emerging insights and gathering feedback from the broader community.

4. Operating Procedure

1. **Leadership & Roles**
    - The Working Group is chaired or co-chaired by individuals with recognized expertise in AI, security, privacy, and identity/authorization.

   - Chairs coordinate discussions, keep the group aligned with objectives, and facilitate consensus-driven decisions.
2. **Decision-Making**
   - Major decisions (e.g., adoption of deliverables, publication of key guidelines) are made by group consensus.

   - In the absence of consensus, chairs may initiate a formal voting process to resolve outstanding issues.
3. **Collaboration Model**
   - Participants are encouraged to propose agenda items, contribute documents, and participate in focused subgroups (e.g., adversarial AI for identity, privacy-preserving AI methods).

   - Subgroups may produce specialized deliverables that align with the Working Group's overall scope.
4. **Meeting Cadence**
   - Regular virtual meetings (e.g., monthly) to track progress, discuss findings, and plan upcoming tasks.

   - Additional sessions or workshops may be organized as needed for deep dives into specific identity or authorization challenges in AI.

5. Membership

1. **Open Participation**
   - Membership is open to any individual or organization with an interest in AI security, privacy, identity, or authorization.

   - All participants must follow a code of conduct that promotes respectful, constructive collaboration.
2. **Contributions**
   - Contributions include research insights, proposals, and other materials relevant to AI security, privacy, identity, and authorization.

   - All participants are responsible for ensuring contributions are shared under licensing terms conducive to broad dissemination.

6. Intended Audience

- **AI Practitioners & Identity Specialists**
  Professionals who develop AI systems or manage identity solutions, seeking to integrate robust authorization mechanisms and privacy safeguards.

- **Security & Privacy Professionals**
  Experts who apply cybersecurity and data protection principles to AI technologies, particularly those involving user credentials and sensitive

attributes.

- **Organizations & Policymakers**
  Entities needing guidance on securely deploying AI that interacts with identity frameworks, ensuring compliance with relevant regulations.
- **Standards Bodies & Industry Consortia**
  Groups looking to define or refine norms and protocols for **AI, identity, and authorization** in decentralized or federated ecosystems.