ANP

Agent Network Protocol

Redefining Agent Connectivity and Collaboration

ANP Open Source Community
Gaowei Chang, James Waugh

2025-02

https://agent-network-protocol.com/

Outline

ANP

This presentation will cover the following topics:

- Core Assumptions of ANP Design
- ANP Authentication Scheme
- ANP Identity Verification Process
- ANP Agent Description Scheme
- How to Build an AI-Accessible Data Network Using Agent Descriptions
- Demo Demonstration

Agentic Web: The Impact of Agents on the Internet

ANP

Agents will replace existing software

- The personal assistant will replace humans in accessing the internet.
- Agents will replace software services for enterprises.
- Personal assistants will directly connect to agents.

A personal assistant is also an agent

Agentic Web: The Impact of Agents on the Internet

ANP

Agents must be interconnected

- AI must have access to complete contextual information.
- AI should be able to access all tool capabilities.
- The connectivity between agents will have a higher proportion.

The current data silos on the internet hinder the full potential of AI.

Agentic Web: The Impact of Agents on the Internet

ANP

Agents interact with each other through protocols

- The most efficient way for AI to interact with the internet.
- Computer Use is a transitional form.
- In the future, standardized agent communication protocols will emerge.

Directly processing underlying data through protocols is the best way for AI to interact with the internet.

AgentNetworkProtocol(ANP)

ANP

Goal

HTTP/HTML of the Agentic Web

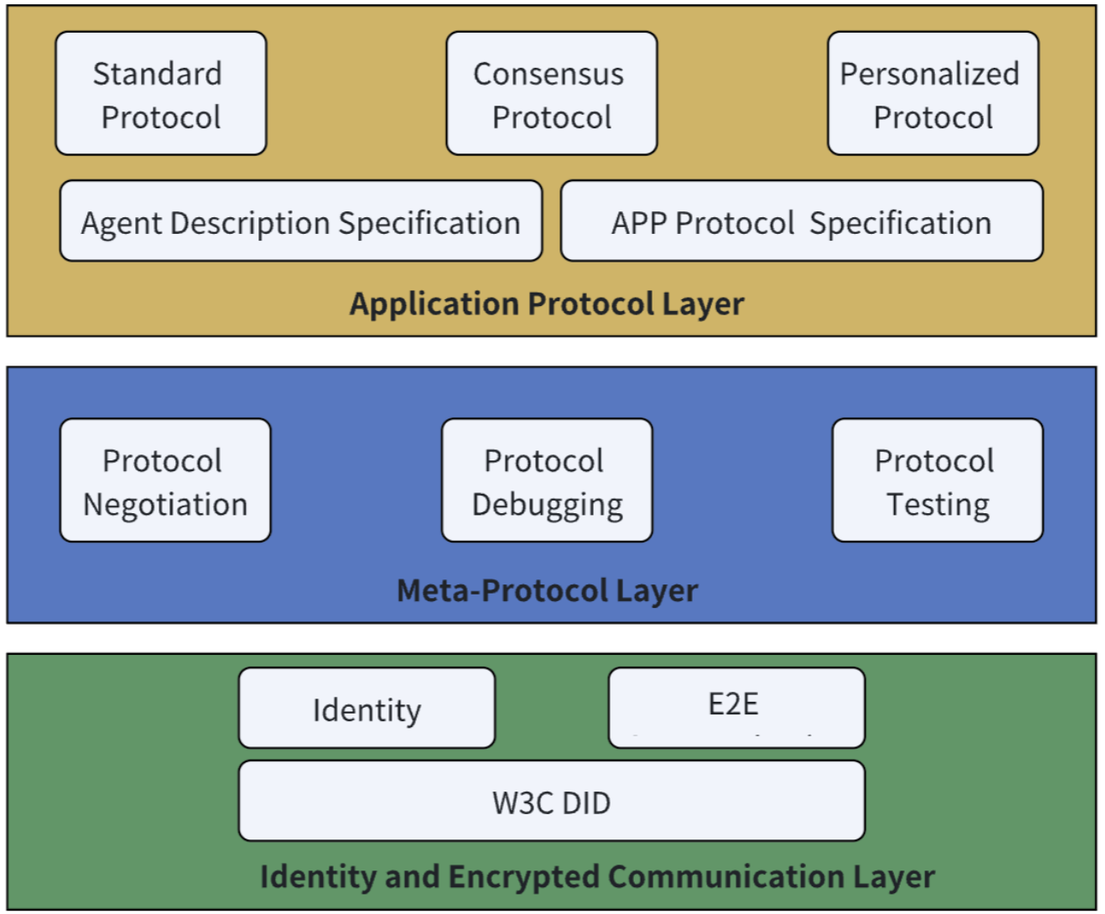
Vision

Define the connectivity between agents and build an open, secure, and efficient collaboration network for billions of agents.

AgentNetworkProtocol(ANP)

ANP

- 🔒 **Identity and Encrypted Communication Layer:** Based on W3C DID, it builds a decentralized identity authentication solution with excellent scalability, capable of supporting billions of users.
- 🌍 **Meta-Protocol Layer**: A meta-protocol is a protocol for negotiating communication protocols between agents. It is the key to the evolution of the agent network into an autonomous, self-negotiating, and highly efficient collaborative network.
- 📡 **Application Protocol Layer:** Based on Semantic Web standards, it enables agents to describe their public information, available capabilities, and supported interfaces. Using this information, other agents can discover and interact with them.



Today, we will focus on the identity layer and the application layer.

Goals and Principles of Agent Identity Design

ANP

Goals

- All agents can authenticate each other's identity.

Principles

- **Decentralization**: Identity should not be provided by a few vendors.
- **Interoperability**: Identities between different systems should be easily authenticated with each other.
- **Scalability**: The system should support large-scale user usage.

W3C DID(Decentralized Identifier)规范：https://www.w3.org/TR/did-core/

W3C DID

What is DID:

- **Full Name**: Decentralized Identifier
- **Definition**: A user-controlled, self-sovereign digital identity identifier, widely applicable in decentralized systems.
- **Officially became a W3C Recommendation in 2022**.

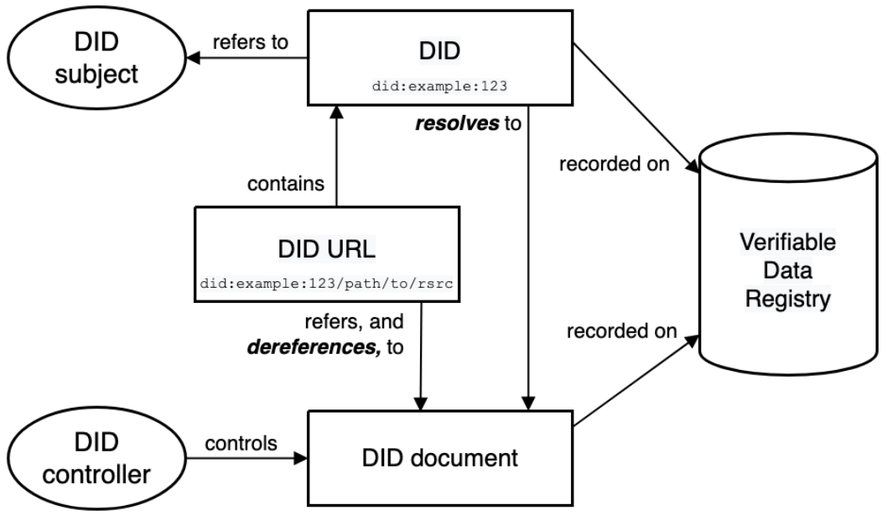
EXAMPLE 1: A simple DID document

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ]
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }]
}
```

Scheme: `did` | DID Method: `example` | DID Method-Specific Identifier: `123456789abcdefghi`

Features of DID:

- **Decentralized Identity**: Users manage their identity independently, avoiding reliance on centralized service providers.
- **Interoperability**: Supports cross-platform usage, enhancing compatibility between different systems.
- **Privacy and Security**: Ensures the privacy and security of user identity data, preventing abuse.
- **Typical Application**: Bluesky.



W3C DID(Decentralized Identifier)规范：https://www.w3.org/TR/did-core/

DID Method： Web-Based Agent

ANP

Method Design Principles:

- **Do not pursue complete decentralization,** feasibility is prioritized over decentralization features.
- **Reuse existing web infrastructure** to reduce implementation costs.
- Build upon the existing **did:web method** and add agent-related features.

Did:wba DID Defines：

did:wba:example.com:user:alice

-> https://example.com/user/alice/did.json


```
{
    "@context": [
      "https://www.w3.org/ns/did/v1",
      "https://w3id.org/security/suites/jws-2020/v1",
      "https://w3id.org/security/suites/secp256k1-2019/v1",
      "https://w3id.org/security/suites/ed25519-2020/v1",
      "https://w3id.org/security/suites/x25519-2019/v1"
    ],
    "id": "did:wba:example.com%3A8800:user:alice",
    "verificationMethod": [
      {
        "id": "did:wba:example.com%3A8800:user:alice#WjKgJV7VRw3hmgU6--4v15c0Aewbcvat1BsRFTIqa5Q",
        "type": "EcdsaSecp256k1VerificationKey2019",
        "controller": "did:wba:example.com%3A8800:user:alice",
        "publicKeyJwk": {
          "crv": "secp256k1",
          "x": "NtngWpJUr-rlNNbs0u-Aa8e16OwSJu6UiFf0Rdo1oJ4",
          "y": "qN1jKupJlFsPFc1UkWinqljv4YE0mq_Ickwnjgasvmo",
          "kty": "EC",
          "kid": "WjKgJV7VRw3hmgU6--4v15c0Aewbcvat1BsRFTIqa5Q"
        }
      }
    ],
    "authentication": [
      "did:wba:example.com%3A8800:user:alice#WjKgJV7VRw3hmgU6--4v15c0Aewbcvat1BsRFTIqa5Q",
      {
        "id": "did:wba:example.com%3A8800:user:alice#key-1",
        "type": "Ed25519VerificationKey2020",
        "controller": "did:wba:example.com%3A8800:user:alice",
        "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
      }
    ],
    "keyAgreement": [
      {
        "id": "did:wba:example.com%3A8800:user:alice#key-2",
        "type": "X25519KeyAgreementKey2019",
        "controller": "did:wba:example.com%3A8800:user:alice",
        "publicKeyMultibase": "z9hFgmPVfmBZwRvFEyniQDBkz9LmV7gDEqytWyGZLmDXE"
      }
    ],
    "service": [
      {
        "id": "did:wba:example.com%3A8800:user:alice#ad",
        "type": "AgentDescription",
        "serviceEndpoint": "https://agent-network-protocol.com/agents/example/ad.json"
      }
    ]
}
```

CURD Operations of did:wba

CURD Operations:

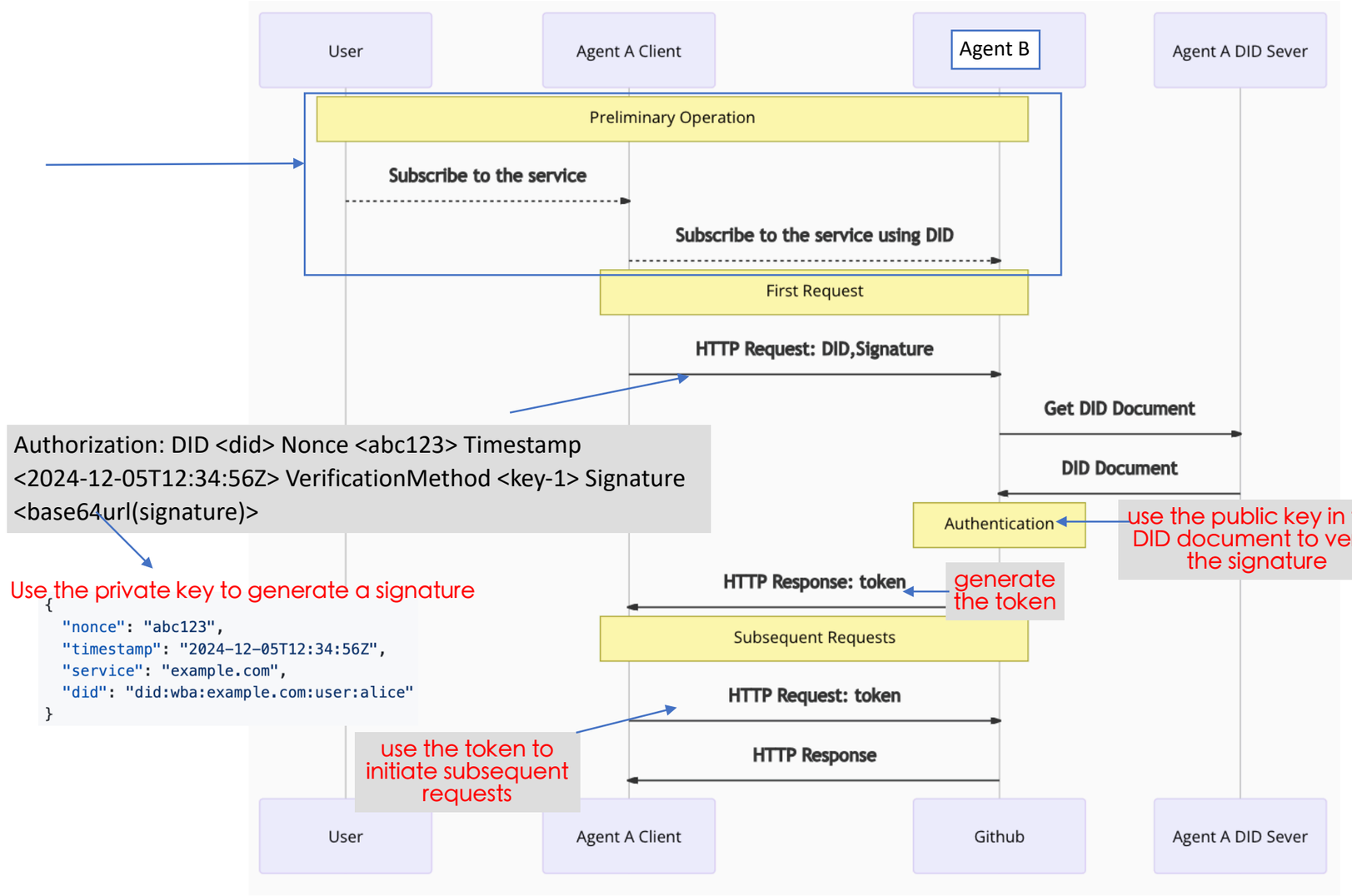
- **Create (Register)**: Defined by the implementer.
- **Read (Parse)**: Use the HTTP GET method to retrieve the DID document.
- **Update**: Defined by the implementer.
- **Deactivate (Revoke)**: Defined by the implementer.

Method Features:

- Fully utilizes existing web infrastructure, capable of serving billions of users.
- Achieves decentralization and interoperability of agent identities.
- The method is similar to the existing Email service.

DID:wba Method Identity Verification Process

- A calls the API to subscribe to B's service, and B records A's DID.
- A includes its DID and signature in the HTTP header during the first HTTP request.
- When B receives the HTTP request, it extracts A's DID and signature from the HTTP header, then retrieves A's DID document from A's DID server using A's DID.
- After B obtains A's DID document, it uses the public key from A's DID document to verify A's signature.
- Once the verification is successful, B processes A's business request and returns the business data along with an access token.
- In subsequent requests, A includes the access token, and B verifies A's identity by validating the access token.



Features: Supports automatic registration; simple process with minimal interaction; equivalent security to traditional methods.

Unresolved Issues

ANP

- For user permissions, how can we implement more granular permission control, instead of using a single ID for communication with all agents?
- How can we determine whether a request from an agent has been manually authorized by the user? Some sensitive actions should not be initiated autonomously by the agent.
- How can we ensure that the user has full ownership of their identity, rather than relying on permissions granted by the platform?

Agent Description Protocol(ADP)

ANP

What is an Agent Description Protocol?

- Used to define the Agent Description Document.
- The agent description document can be seen as an entry point for the agent, similar to the homepage of a website. Through this homepage, all aspects of the website can be accessed.

What information does an agent description document contain?

- An agent description includes the identity of the entity to which the agent belongs, the owner, authentication methods, external interfaces, and public information about the entity.
- For example, if the agent represents a coffee shop, the publicly available information would include the location, business hours, product list, purchase interface, and other related details..

Core Principles of ADP Design

ANP

- **AI-Oriented Design**: Specifically designed for AI, making it easier for AI to access.
- **Semi-Structured Protocol**: Overall, it is a structured design that facilitates programmatic processing; fields can contain natural language, making it easier to convey personalized information.
- **Multi-Agent Consensus**: Enhances the consistency of agents' understanding of data semantics.

In theory, as long as the intelligence is strong enough, ADP could entirely use natural language. However, this approach has many drawbacks, such as cost, the probability of errors at the current stage, and so on.

ADP Design Scheme

ANP

- **Linked-Data**: Using Linked-Data technology, the information of agents is linked together. The agent description document serves as the entry point for all the information about the agent, and from this entry point, all the agent's information can be traversed. In terms of document format, we use Json-LD as the primary format.
- **Schema.org**: The fields in Json-LD extensively use the predefined fields of Schema.org. If there are any undefined fields, they will be added with a definition. This ensures consistency in how multiple agents interpret the same field, while also making it easier for programs to process.
- **The specification is divided into two parts**: one is the **core ADP specification**, which describes the core framework and structure of ADP; the other part consists of **AD examples for each domain**. For example, an AD document for a coffee shop, where other agents can refer to this example to generate their own.

AD Document Example

Example URL: https://github.com/chgaowei/AgentNetworkProtocol/blob/main/examples/adp/lkcoffe/ad.json

Identity authentication information

```
"ad:securityDefinitions": {
  "didwba_sc": {
    "scheme": "didwba",
    "in": "header",
    "name": "Authorization"
  }
},
"ad:security": "didwba_sc",
```

External interfaces, including natural language interfaces and purchased APIs

```
"ad:interfaces": [
  {
    "@type": "ad:NaturalLanguageInterface",
    "protocol": "YAML",
    "url": "https://service.agent-network-protocol.com/
    "description": "A YAML file for interacting with th
  },
  {
    "@type": "ad:PurchaseInterface",
    "protocol": "YAML",
    "url": "https://service.agent-network-protocol.com/
    "description": "A YAML file for interacting with th
  }
]
```

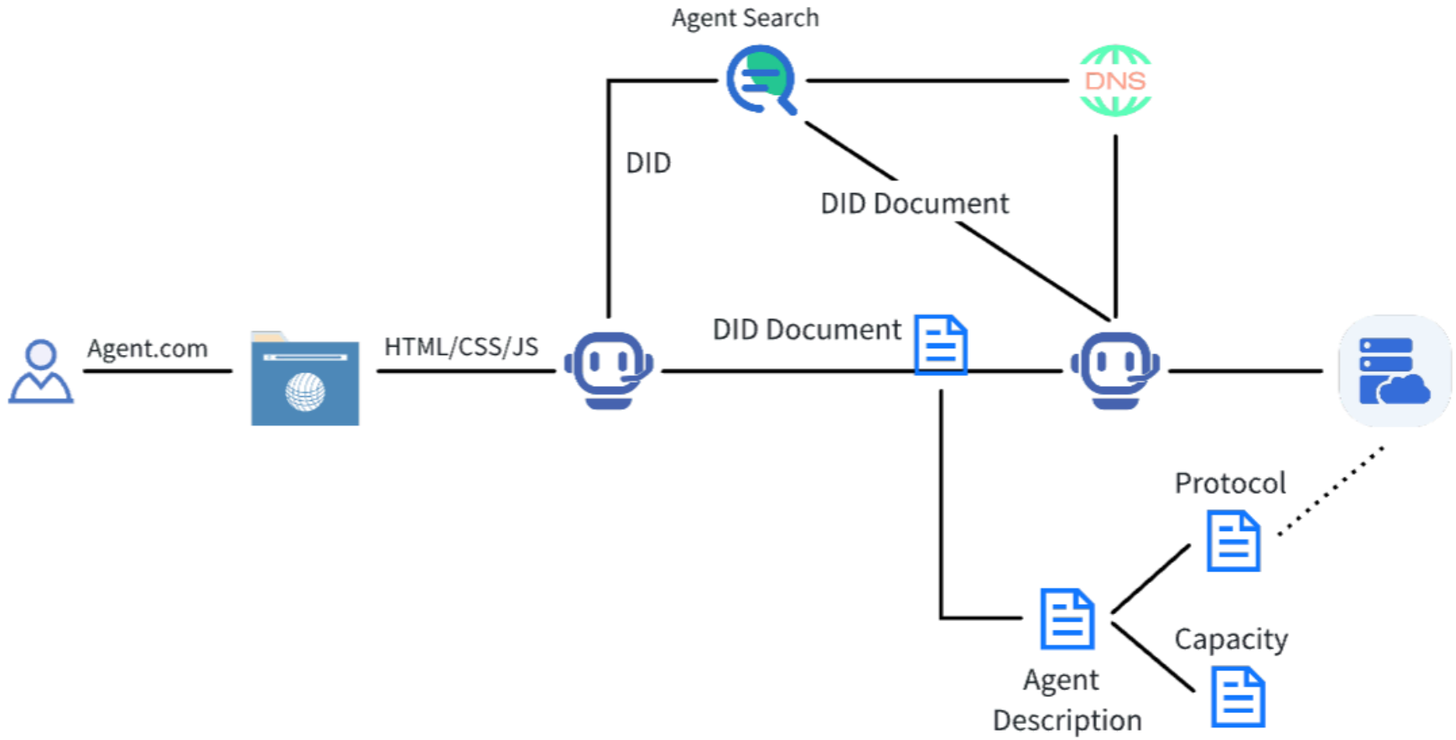
Domain entities corresponding to the agent

```
"ad:domainEntity": {
  "@type": "CafeOrCoffeeShop",
  "name": "Luckin Coffee",
  "address": {
    "@type": "PostalAddress",
    "streetAddress": "XX Road No.XX",
    "addressLocality": "Some City",
    "addressRegion": "Some Province",
    "postalCode": "123456",
    "addressCountry": "CN"
  },
```

Products provided by the entity to the outside world

```
"ad:products": [
  {
    "@type": "Product",
    "name": "Silk Latte",
    "description": "Made with high-quality
    "@id": "https://service.agent-network-p
  },
```

Interaction Flow



- We have placed the agent description document link in the DID document, meaning that as long as there is a DID, the agent description document can be found.
- In the future, there will be **a data network that makes it easier for AI to access**.

Others

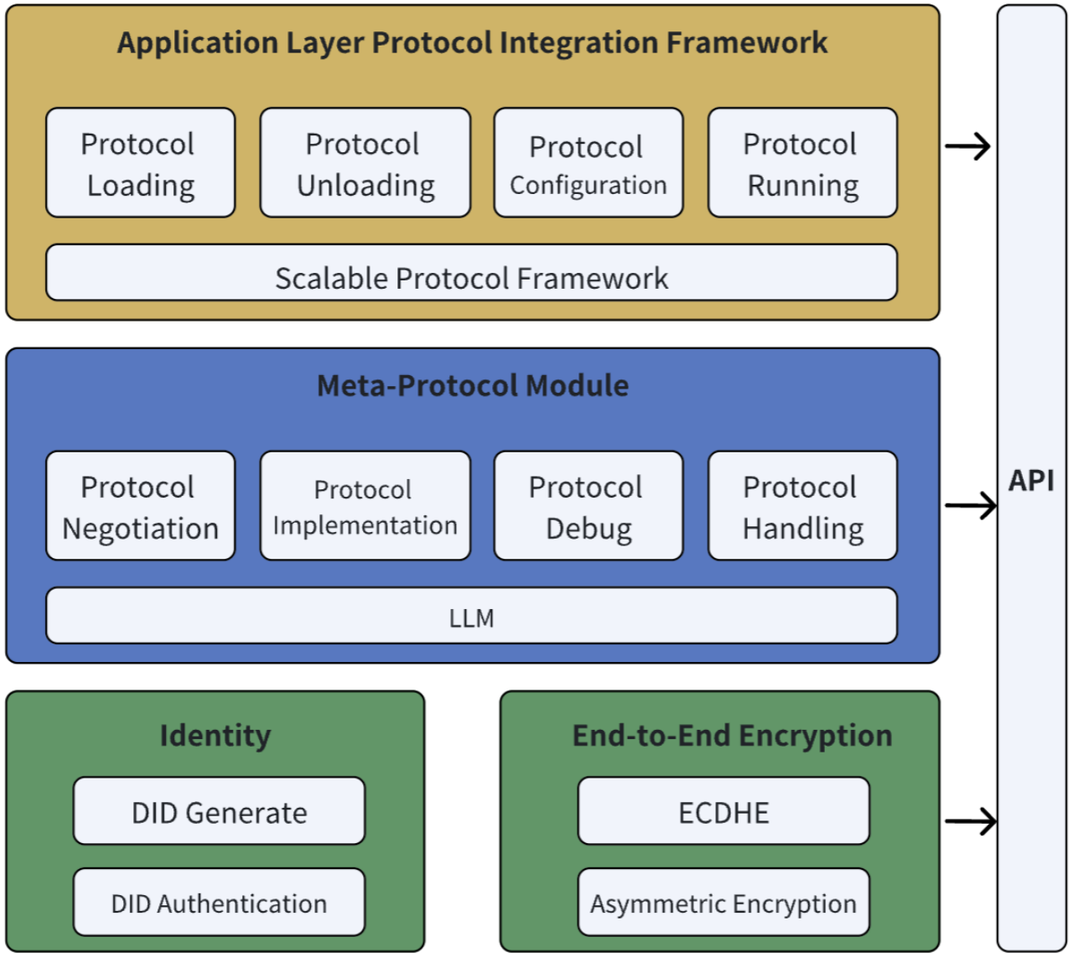
- **Supporting ADP during LLM training**: ADs specifications, along with examples and interfaces from various industries, can be incorporated into the LLM through training data or fine-tuning. This enhances the LLM's speed and accuracy in processing ADP and reduces the length of prompts required.
- Agents can independently define and upload AD document examples for reference by other agents. The specification examples defined by agents may surpass those defined by humans.

Demo Presentation

ANP

Through the coffee ordering scenario, demonstrate how a personal assistant interacts with the coffee shop's agent using DID and AgentDescription.

Code



ANP Open Source Code: https://github.com/chgaowei/AgentConnect

Thanks

The historical meeting records of WebAgents provide valuable resources and inspiration for our design.

Finally

ANP

ANP is still in its early stages, and if possible, we are willing to contribute ANP and continue improving it together with everyone in WebAgents.

Question & Answer