ecma INTERNATIONAL

Ecma/TCXY/<year>/NN

Draft number Technical Report ECMA TR/XXX

Edition / Date

NLIP Overview Document

Rue du Rhône 114 CH-1204 Geneva T: +41 22 849 6000 F: +41 22 849 6001

is the registered trademark of Ecma International

COPYRIGHT PROTECTED DOCUMENT

Contents

Page

Introduction

The advent of large language models (LLMs) has made an interactive natural language interaction feasible between machines in a manner that did not exist before. An implication is that a natural language interface can replace many mobile applications that are used today.

Just like the advent of the browser in 1990s simplified technology by replacing a plethora of client-side applications with a single standard application, a common natural language interaction protocol can potentially replace the plethora of mobile applications that exists today, providing a universal application layer protocol. Convergence to a universal application layer protocol would bring significant benefits to all segments of society – consumers can use a single application for various interactions, businesses will have a simpler maintenance burden for their IT infrastructure, and integration among different businesses can be streamlined.

ECMA Technical Committee 56 is defining this standard. Two standards documents define the standard protocol called Natural Language Interaction Protocol (NLIP) and its binding over HTTPS/REST.

In this document, we provide the motivation, requirements and design philosophy behind the NLIP Standards. We also document some use-cases and sample interactions among different parties for various common scenarios.

This Ecma Technical Report was developed by Technical Committee 56 and was adopted by the General Assembly of <month> <year>.

NLIP Overview Document

1 Scope

This Technical Report provides a supporting documentation for the NLIP specifications and binding document. It includes the motivation, the requirements of the protocol, and examples of sample exchanges. This is a normative document and does not define a standard. In the case of a conflict between this document and the NLIP standards, the standards document take precedence.

2 References

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 12345:year, *Title*

ISO/IEC 12345:year, *Title*

ECMA-XXX, *Title*, xth edition (month year)

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
term
definition

3.2
term
definition

3.3
term
definition

NOTE Text text text.

3.4
term
definition

NOTE 1 Text text text.

NOTE 2 Text text text.

4 Abbreviations

ALG Application Layer Gateway

API Application Protocol Interface

5 Our Vision

In this section, we define our vision for the future that a protocol like NLIP can enable.

We envision a future in which there is a single application on the phone of consumers, which can interact with business services provided by various businesses or organizations. We provide some instances where the current environment causes hardships for users, and where we envision a single application in operation to provide significant benefits to users and service providers.

At the present time, almost every major city has a public transportation system that publishes its own mobile application for the benefits of its riders. The application provides many capabilities including an easy view into train timetables and status, an ability to view and buy ride tickets/passes, and an ability to find how to go from point A to point B. At the same time, every city provides its own application, which requires installing an application for every city. This imposes a significant hassle for any individual who travels to multiple cities.

Consider the case of a traveling trade-person who is on a tour to attend conferences, trade shows, and to meet with clients. The person needs to install the train/public transit/taxi application for each of the cities in order to determine how to move around conveniently. If the traveller is not a frequent visitor to the cities, the need to install the plethora of apps is a significant burden.

The same traveller is probably encouraged by each of the three trade shows he or she is attending to download and install a venue app to make the participation experience better. The lifetime of the application is that of a few days, and the experience and interfaces of each of the applications are very different.

We can further assume that the traveller needs to use a ride-sharing or taxi company in each of the different cities. Many ride-sharing and taxi operators provide their own proprietary mobile application to their customers. Some of the ride-sharing operators work in many cities, whereas others (e.g. local taxi companies) operate in a limited area only. The need to install a new application for taxi services in every city is burdensome.

In one of the international cities, the traveler wishes to see a game. Obtaining the tickets requires the installation of yet another mobile application.

Even without considerations associated with travel, a consumer needs a mobile application for every bank, credit card provider, retailer, cellular service provider, and virtually any other businesses he or she interacts with. The niggling need to install and be acquainted with so many single-use mobile apps acts as an adoption barrier to the user.

The need to create, maintain and provide a mobile application is a significant technical burden on businesses as well. In some cases, the mobile app may provide a unique competitive business advantage, but in a large variety of cases, it does not. The support, development and maintenance of the mobile app on the multitude of mobile/wearable devices imposes a significant IT burden.

Instead of an abundance of mobile apps, we envision a future where there is a single application that enables the user to type in natural text (sometimes in conjunction with an image from the phone camera or a local file) to interact with a chat-server for each app. The single application can talk to the business service of any business. This business service will be supported by means of an AI model, and it would be appropriate to refer to this business service as an agent for the business. In some cases, the conversation may happen with the user providing his/her identity to the business-agent, while in other cases, the conversation may happen with the user in an anonymous mode.

As an example, the traveling business person would be able to use this single application to find the schedule of the local public transit regardless of the city. An agent operated by the transit authority of each city allows the

traveller to check the schedule and purchase tickets for the ride. An agent operated by each conference organizer lets its attendees ask questions and get directions during the operation of the conference.

6 Need for a new Protocol

The vision of a common application interacting with an agent has many parallels to the browser accessing websites. The single browser application can interact with any web-site and allows the users to obtain information in either an anonymous or a signed-in/authorized model.

Despite the existence of the browser, many businesses feel the need to provide a mobile application to their users. The reason is that each company needs to extend the capabilities provided by the browser. A bank needs to provide the capabilities to check balances, transfer money, pay bills and similar operations to its clients. A local transit company needs to provide capabilities to check for schedules or purchases tickets. In the current browser design, these require providing new extensions to the markup tags provided by the underlying specifications, and any such additional tags, or conventions for transferring information requires a change on both the client side and on the server side. In effect, every bank introduces a new application layer banking protocol, each local transit company introduces a new application layer transit protocol, each airline introduces a new application layer airline protocol etc. The underlying hypertext markup language and protocol do not allow the introduction of such customization without modifying both the client and server sides.

In contrast, the emergence of large language models allows the development of an environment where a new protocol can be introduced merely by changing the capabilities on the agent side, without requiring new capabilities on the client-side. The basic function supported by the common application is the ability to converse in natural language to any server. The natural language implementation can support a generic protocol for customization by a specific agent. A basic set of conventions are required to enable characteristics such as security, authentication, improved performance, support of authorized model and the anonymous mode, etc. A large language model on the server side can provide customized protocols without requiring a new client, or any new capability on the client side.

The flexibility offered by the natural language text allows new dynamic relationships among agents to be established. As an example, suppose a company decides to partner with another company, and offer a new set of services that were not previously available in the mobile app, e.g. a conference is allowing rides from a local taxi provider with a discount. If the conference app did not have a provision to offer taxis at discount built in, a new customized app would need to be developed, or the current app modified. On the other hand, if the interactions are based on natural language and agents, a modified parsing of the text messages on the server side would enable the addition of the new capability of discounted taxi rides for the conference. The ability to provide extensions with only server side capability augmentation can provide tremendous flexibility, which is not possible with current set of protocols.

7 NIP Scope

The scope for use of NLIP is shown in two halves of Figure 1.

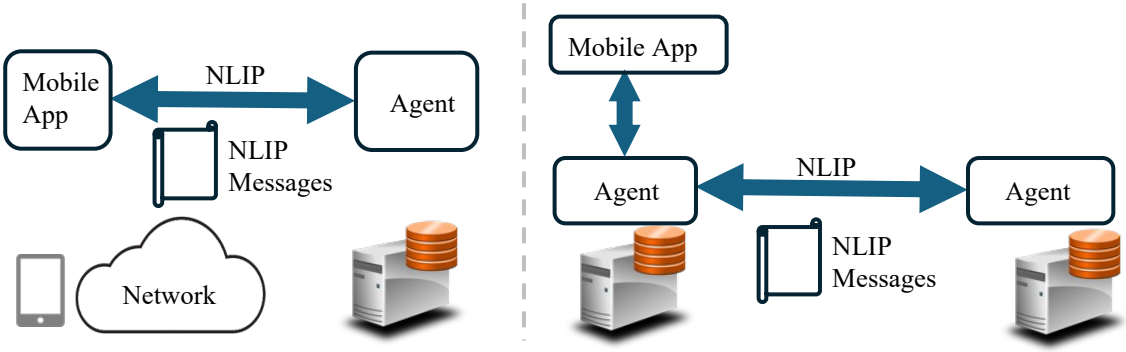

Figure 1

As shown in the left half of Figure 1, the architecture envisions a common application that provides an exchange happening using a standardized format using a standardized protocol between a mobile application and a chat service. The use of a standard convention would allow the usage of the same application across a variety of service providers. A bank, a retailer, a network service provider, an investment company -- and essentially any other businesses planning to export a chat interface to their users, would be able to use the same application to communicate without worrying about the need to provide their own chat-application.

The NLIP based component on a phone/pervasive end-point may be a stand-alone application on a mobile device, or it may be a component that gets incorporated within other mobile apps. The mobile app that incorporates NLIP may also have an embedded large language model, or it may use a human (its user) as the intelligent agent needed to interpret various modalities of information. In the former case, the mobile application may use the embedded large language model to interpret the responses from the server. In other cases, the mobile application may rely on another service running a large language model to do the interpretation.

In addition to communication between mobile apps and an Internet based service, NLIP may also be used in B2B context as communication between two businesses agents as shown in the right hand of Figure 1. In this context, the software on both ends is running on traditional servers.

The interaction shown on the right can also represent an application running on the personal machine of a user. In this case, a user may be able to use a large language model on their machine to process and interact with the responses generated by the businesses. As an example, a user AI engine may want to filter out some of the content provided by the chat application server, which are deemed to be not interesting, not useful or potentially harmful to the user on the local machine. This flexibility to the end user, that they can control information flowing into their own machine, is something which is difficult with current protocols. However, a gen-AI module under control of the user can provide the ability to manage these types of operations relatively easily.

NLIP is not designed to provide interoperability among existing business services and systems. As a migration path towards the adoption of NLIP, we envision several implementations to happen using the interaction diagram shown in Figure 2.

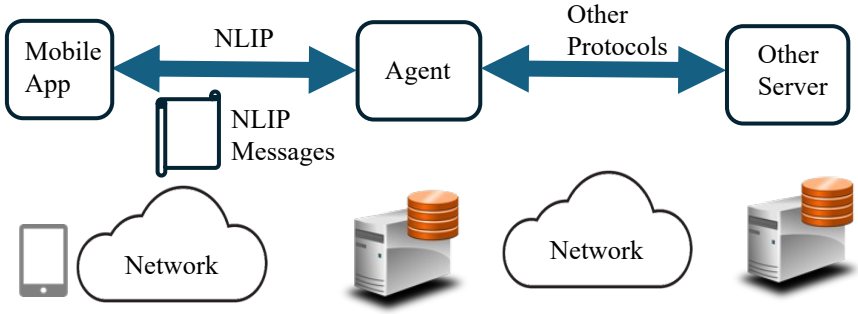

Figure 2

In these interactions, NLIP provides a mechanism for an agent to interact with its user. However, it is not designed to act as a mechanism for interaction between an agent and other existing servers.

Eventually, as NLIP gets adopted widely, we would envision it to be adopted by various business services as the primary interface. In this case, we can also envision NLIP proxy agents coming up which provide for interaction and communication among other agents. This interaction configuration is shown in Figure 3.

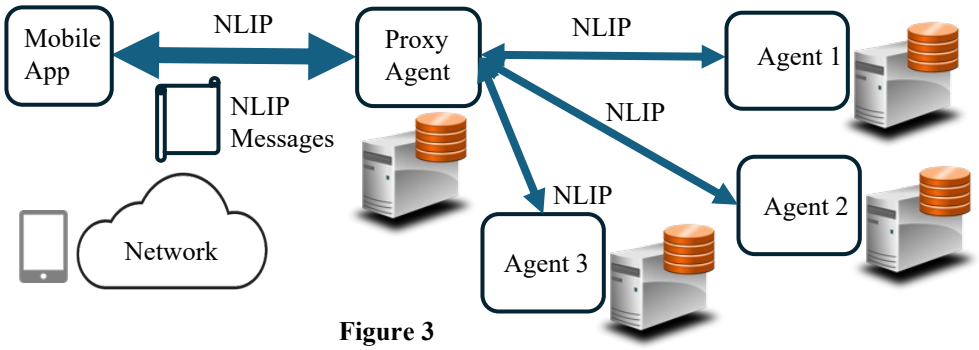

Figure 3

8 Requirements of NLIP

In order to satisfy its goal as a communication protocol between intelligent agents belonging to multiple organizations, NLIP needs to satisfy several requirements. These requirements include security, performance, and manageability requirements.

In many cases, the requirements may be satisfied by the protocols which are used for NLIP implementation. We are enumerating all requirements regardless of the layer of the protocol which implements it.

8.1 Security Requirements

A key requirement for wide deployment of any protocol is the support for proper security mechanism. Towards a goal of secure communication between the clients and the servers, we need to ensure that NLIP supports proper mechanisms for various capabilities including authentication, authorization, encryption, identity management, policy exchange support, support for anonymous mode and prevention of denial of service attacks.

Some of the security requirements are shared with performance requirements and they are described in the performance requirements section.

8.1.1 Authentication

Both interacting parties must be able to authenticate each other. NLIP must ensure authentication support using all commonly used authentication mechanisms.

8.1.2 Authorization

The authenticated remote party may only be authorized to request a restricted set of services to the local party. Appropriate mechanisms to restrict the unauthorized requests among interacting agents must be supported.

8.1.3 Encryption

The support for both current and future secure encrypted mechanisms for transfer of information must be supported. In many cases, this support may be obtained by means of underlying protocols and their support of encrypted communications.

8.1.4 Identity Management

Most business and social contexts require some form of digital identity for the users to interact with them.

The notion of digital identity is quite complex. For the present discussion, we consider the simplest form of digital identity, i.e., the user login name, which uniquely identifies a user in each name space. Authentication and access control are typically performed against login names, even though today with multi-factor authentications additional information about users are leveraged for authentication. There are various approaches according to which these digital identities are issued. In the simplest form, service providers issue digital identities, with the associated credentials for authentications, to its own customers. In other cases, there are parties, referred to as identity providers, that give users digital identities, with the associated credentials. A service provider can then demand the identity management and related authentication to the identity providers. A drawback of this approach is that the identity providers end up being involved in the transactions users perform with the service providers (unless more complex protocols are used). In our context, it is important to observe that users may have different digital identities, and it is important for the NLIP being developed to understand, based on the user preferences/behaviours and the requirements of the service providers, which identity to use, or whether to even to let the user be anonymous.

8.1.5 Privacy and Policy Support

When clients and servers support an interactive chat, issues arise regarding the ownership and privacy of the data exchanged between the client and server. To a large extent, privacy and regulatory compliance have been relegated as an after-thought to network specifications and generative AI technologies. In order to become useful and acceptable to a broad audience, NLIP must enable a mechanism for the interacting parties to learn and be aware of each other's policies for matters such as data privacy, regulatory compliance and attribute disclosure.

8.1.5.1 Data Privacy Policies

Each party involved in the protocol should be able to query their peer’s policies and specify their policies for preserving the privacy of the data being exchanged between them, and mutually agree upon them prior to actual communication.

8.1.5.2 Regulatory Compliance Policies

Each party involved in the protocol should be able to query their peer’s jurisdiction to which they comply to, and the expectations of the jurisdiction to which the other party belongs to. Some agents may refuse to communicate with parties in other jurisdictions, and some of the parties would only communicate if the other party agrees to specific terms for arbitration and conflict resolution.

8.1.5.3 Attribute Disclosure Policies

During a protocol interaction, each party may or may not be willing to disclosure some of their attributes, e.g. their physical location, to the other party. NLIP should enable an exchange among the parties so that they are all agreeable to the attributes being disclosed or not disclosed. A taxi server agent, for example, may insist that the clients hailing it disclose their exact physical location.

8.1.6 Anonymous Mode

In many business contexts, it is important that a user be able to access services without logging in. People want to be able to access some types of information without logging in first, and businesses would like to offer some information to anyone without validating their identity. Note that some information may still need authorization

and authentication of user. Examples of information that may be offered in anonymous mode include a list of items and their prices available from a retailer, the sets of flights and tickets from an airline company, the agenda of a conference etc.

8.2 Flexibility

NLIP needs to be designed to be flexible and support a multiplicity of choices for many different aspects of communication. In this section we list out some of the common multiple options that NLIP needs to support.

8.2.1 Support of Multiple Modalities

While text is the most common modality for user interaction using LLMs, common usage requires other modalities in the interactions as well. A bank check deposit would need images to be uploaded for the deposit, and some interactions may have the bank sending documents such as tax forms or account statements to the users. Users with accessibility needs may require use of video-based interactions. NLIP must support the various modalities required for enabling a diverse set of users and applications. Sentiment analysis based on tonal and facial analysis would be one such example of applications enabled by multi-modalities. Content encoding aside, multi-modality support has implications such as prioritizing standard interface definition for WebRTC, for mobile video chat, and additional real-time streaming performance requirements.

8.2.2 Support of Multiple Concurrent Sessions

NLIP should enable the beginning and termination of multiple sessions, in other words, parallel conversations, between the client and the server. One session could be in the “foreground”, to be the primary interacting agent interfacing with the user while others could be in the “background”. An assembly of interrelated sessions forms a conversation.

A session may or may not have accompanying windows like in a browser, and each sessions will likely need to have identifiers to enable end-points to distinguish among them. Further, end-points may need to support a certain amount of information about the session in a “conversation state” such as the language(s) being used, timestamps of when the first and last utterance were transmitted, parties to the chat (possibly more than two) and so on. Since large language models can take advantage of voluminous prompts, a conversation can be set up to allow the entire history of the conversation, including timestamps and the identity (to the extent known) of the party making each utterance, to be retrievable or to limit the history kept to a fixed horizon. In some cases, end-points may want to trade-off bandwidth versus local storage to optimize their performance. NLIP should enable these interactions.

Another requirement of NLIP would be to enable headless sessions. These are agent-initiated sessions that do not directly involve a human user. As an example, an agent can query another agent for additional information in support of a user query.

8.2.3 Support of multiple underlying protocols

The dominant paradigm for applications to communicate with each other today is using some variant of REST and standardization in those cases would mean identifying the URI and parameter encoding for NLIP. At the same time, there are several other protocols that can provide alternative approaches, including but not limited to QUIC, gRPC, WebRTC, websockets and ZeroMQ. The binding of NLIP to the different underlying protocols should be defined and the specifications made in a manner so that any desired protocol binding can be supported. The main advantage of NLIP being ``hot-extensibility'' of deployed instances and continuous customization of installed interactions.

We will initially define the protocol on top of HTTPS and JSON, to take advantage of their ubiquitous availability and accessibility. However, this should not preclude the use of other underlying protocols.

8.2.4 Support of multiple platforms

Since we envision NLIP to be used across many devices and many systems, it is important that NLIP does not make implicit assumptions about programming languages and underlying hardware. The common application should be easily implementable on multiple mobile platforms, each of which has its own preferred operating system and development languages. Similarly, server-side systems may be implemented on Linux, Windows Servers, etc. using languages such as C or C++, Go, Java, JavaScript, Python, Rust, Zig, etc. NLIP specifications should support all platforms and all languages.

8.3 Performance Requirements

In order to be used effectively, NLIP must support proper mechanisms for low-latency high-performance interactions. This requires supporting the following mechanisms:

8.3.1 Caching of Context

Chat interactions require maintaining the context of interactions, namely the sequence of interactions that may already have happened. Instead of exchanging the context on the wire repeatedly, context should be able to be stored and reused on each side based on prior interactions.

8.3.2 Rate Controls

When implementing caching mechanisms for performance, care has to be taken to allow one or both parties to specify limits on how much context they would store, and prevent denial of service attacks. The servers may want to impose limits on the length of context, or the length of chat messages they would support, or the rate at which requests may be sent to the server from a client, and vice-versa. These limits should be negotiable, and designed to enable most interactions to happen in a performant and secure manner.

8.3.3 Denial of Service Prevention

A common problem with any performance optimization such as saving context on both client/server side is the potential of an untrusted client or server to launch denial of service attacks, e.g. launching attacks parallel to those enabled by TCP session establishment mechanisms~\cite{harris1999tcp} such as SYN floods or half-open session state attacks. NLIP specification must take into account such potential attacks when defining any performance optimization and incorporate safeguards.

8.3.4 Real-time Streaming

Interactive multi-modal chat may require separating the session into separate streams with diverse inter-stream priority and delay bound requirements. Sustained two-way communications may require support for streaming services with customized intra-stream timing and ordering requirements.

9 NLIP Use Cases

In this section, we enumerate some of the various use-cases that a single chat application using NLIP can provide.

One use-case would be that of a user attending multiple conferences at different times. Each of the conferences have setup a conference chat server which the user can query to find details about the conference. The common application can be used to inquire information about the conference agenda from the conference chat server. A generative AI model can be used on the user side, the server side or on both side to handle the interactions. The model may perform tasks such as filtering the agenda only to meet those that are of interest to the user, or to other entities.

Another use-case would be that of a user inquiring about their bank account from the chat server operated by the bank. The user can instruct the bank to transfer money between accounts held by the bank, or at another

bank. When transfers are made across banks, the chat servers at two banks coordinate to make the transfer happen seamlessly.

The use-cases for public transportation, including ride-sharing, airlines, trains and taxis has been discussed earlier. An analogous use-case can be made for retailers and shoppers where any user can use a standardized chat application to search through the catalogue for items and make purchases from any retailer with an online presence.