SPECIFIC CONDITIONS FOR THE SUPPLY OF SOFTWARE IN SAAS MODE
Closed Wallet

Section I - General Provisions

1. Value of these Specific Conditions

These specific contract conditions ("Specific Conditions") govern the supply of the software indicated in the subject.
These Specific Conditions integrate the Additional Conditions and refer to the services indicated in the Commercial Proposal.
In the event of a conflict between the Additional Conditions and the Specific Conditions, the latter shall prevail.
The Definitions indicated in the General Conditions apply to these Specific Conditions.

Section II - Specific Conditions

1. Definitions

In addition to the definitions set forth in the General Conditions, the following definitions shall also be taken into consideration, in addition and/or as replacements where applicable:

- **"Attribute"**: a characteristic or quality of a natural or legal person; the Attribute data is provided by an authenticated Source.
- **"EAA":** "*Electronic Attestation of Attributes*", an electronic attestation enabling the presentation and authentication of Attributes.
- **"Authenticated Source"**: the entity that provides the Attribute, which is transformed, through the Wallet infrastructure, into an EAA; it may coincide with the Customer.
- **"ID Wallet"**: "*Identification Data Wallet*", a dataset allowing the unique identification of the User, consisting of digital credentials associated with that User for authentication through the Wallet.
- **"Namirial Wallet"** or **"Wallet"**: the digital wallet containing the User's ID Wallet and EAAs.
- **"Platform"**: the set of software components, applications, interfaces, and modules provided by Namirial in SaaS mode and intended for the provision of the Service.
- **"Relying Party"**: the third-party enabling Users to authenticate within its systems via the ID Wallet and any specific Attribute.
- **"User"**: the subject using the Wallet and to whom the Attributes refer.

2. Object of the Service

Namirial provides the Client with the Closed Wallet Service, which enables the Client, delivered through the Platform, allowing the Customer, via an API call or web interface (GUI), to issue Wallets to Users containing the ID Wallet and EAAs.
Such Wallet may be used as an authentication tool within the closed context defined by the Client.

3. Service Delivery Methods

The Service consists of a SaaS model provided by Namirial, which includes the following functionalities:
The Service is provided by Namirial in SaaS mode and consists of a technological platform designed for Wallet management, developed in compliance with the European Digital Identity (EUDI) framework and the EUDI Architecture and Reference Framework.
The provision occurs within the limits and configurations set out in the relevant Commercial Proposal.
The Service is structured in functional modules, which can be used individually or in combination, as described below. The activation and use of each module take place within the perimeter of the closed context defined by the Customer and in compliance with applicable security rules and access policies:

a. *Namirial Wallet Gateway*: acts as an integration component between the Relying Parties and the Wallet, which:
   - exposes API application interfaces for interaction according to supported communication protocols;
   - governs identity verification and credential issuance/validation flows related to approved use cases (including, by way of example, KYC, Strong Customer Authentication (SCA), and corporate onboarding).

b. *Namirial Wallet App:* a tool available to the User to receive, store, and present digital credentials (ID Wallet and EAAs) in both online and offline contexts. Specifically, it:
   - enables linking of the ID Wallet to the User and managing authentications at Relying Parties via the Wallet;
   - provides the User with information about the Relying Parties' identity and authorization, the purposes, and the scope of data requests, enabling informed consent;
   - uses device-level security mechanisms and cryptographic verifications;
   - is made available as a white-label application or SDK for distribution by the Customer to end Users solely for Wallet management purposes.

   It is understood that use of the Wallet App does not grant the Customer any rights beyond the usage license granted, nor does it entail any obligations on Namirial's part toward Users other than those set forth in these Conditions and/or the Contract.

c. *Namirial Wallet Studio:* the centralized administrative and analytical interface of the Service, intended for system management and related operational entities. Wallet Studio allows, among other things, to:
   - configure and import User Attributes from authenticated Sources and define credential models, access policies, and sharing

constraints through configurable rules and parameters;
- create, suspend, and revoke EAAs based on Attributes identified by the Customer;
- configure, where applicable, white-label web pages and interfaces of the Service;
- perform monitoring and operational analysis activities (including issuance/validation volumes and performance), recording events and cryptographic artifacts, with the possibility of long-term qualified archiving via Namirial services for traceability purposes.

The above functionalities are exercised in compliance with configured authorization profiles and applicable security measures.

4. Specific Obligations of the Client

The Client shall be responsible for:

- the Attributes entered into the Wallet platform to be transformed into EAAs; the Client shall have the right to select the types of Attributes to be associated with Users, assuming full responsibility therefor. Namirial shall be expressly excluded from any and all liability of any kind in relation to the Attributes identified by the Client;
- the identification of the actors (Users, Authenticated Sources, and Relying Parties) within the closed environment in which the Wallet is made available;
- any and all relationships, including commercial ones, with the Users, the Authenticated Sources, and the Relying Parties.

5. Compliance with Technological Standards

Namirial guarantees that the Service complies with applicable regulations, maintaining a high level of security and reliability. In particular, Namirial undertakes to comply with the following technological standards and their possible evolutions, to the extent applicable to the Service:

- OpenID for Verifiable Credential Issuance 1.0 (OID4VCI) – https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html;
- OpenID for Verifiable Presentations 1.0 (OID4VP) – https://openid.net/specs/openid-4-verifiable-presentations-1_0.html;
- ISO/IEC 18013-5 – *Personal identification – ISO-compliant driving licence Part 5: Mobile driving licence (mDL) application*;
- ISO/IEC 18013-7 – *Personal identification – ISO-compliant driving licence Part 7: Mobile driving licence (mDL) add-on functions*;
- ETSI TS 119 471 – *Electronic Signatures and Trust Infrastructures (ESI); Policy and Security requirements for Providers of Electronic Attestation of Attributes Services*.