**GGIE Identity Use Case Requirements v.1:**

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", “RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

**Privacy Requirements**

1. Online anonymity: Personally Identifiable Information (PII) shall not be provided during online activities in a manner that, either by itself or when combined with other data, be used to identify the user or the user’s device(s) without the consent of the user. PII includes
   1. Traditional personal information such as name, address, social security number, license number, memberships, travel information, etc.
      * + IP addresses
        + MAC addresses
        + Device (PC/Tablet/mobile, router, modem, other) hardware, software, firmware, and app fingerprints
        + Other PII (TBD)

Note: The requirements for anonymity do not include PII voluntarily provided by the user directly by entering information on form or via opt-in settings that enable PII to be provided.

1. Voluntarily entering information shall not enable PII of other forms to be provided without the users consent or opt-in.
2. Anonymity may use of one or more 3rd party services to block, eliminate, encrypt, or obfuscate or otherwise make unusable certain PII from being exchanged or discovered.
3. A pseudonym is a disguised identity (a pseudonym) that must not disclose the true (legal) identity of the holder.
4. Pseudonymity requires online anonymity.
5. The user shall have the ability to create or delete their pseudonym(s).

Note: The deletion of a pseudonym does not necessarily eliminate information that was previously linked to that identity.

1. An unlinked pseudonym must not be connected, without user consent, to other identities previously created, currently in use, or subsequently created by the user.
2. A linked pseudonym may be linked to other pseudonyms, to their true (legal) identity and to specific PII under the control of the owner of the pseudonym.
3. Link(s) between pseudonyms and to specific PII already linked to it under control of the user must be able to be modified or eliminated under the owner’s control.
4. Pseudonyms may use a 3rd party service to assign and/or maintain the pseudonym(s) and the links between pseudonyms and other PII.
5. Pseudonyms shall be unique to the individual creating it. See Naming Requirements.
6. Pseudonyms may require a means to ensure that the actual pseudonym being used is encrypted, obfuscated, hashed, or otherwise concealed from others while being communicated to deter tracking by unknown parties.

**Naming Requirements**

1. A pseudonym must be human readable.
2. A pseudonym must include or be linked to a unique number or code to enable the many online activities that require data and metadata to be gathered and reused for current and future activities.
3. The human readable form of a pseudonym should not have to be globally unique although some uses may require uniqueness within its domain of use. e.g. membership in an organization.
4. A 3rd party may be used to assign or otherwise create a unique pseudonym on request from a user or for a specific use.

**Ease of Use Requirements**Although there are numerous means to obtain anonymity and pseudonymity for online activities, most today are complex and not understood by the typical user. Few users are aware of the amount of information they provide in their online activities and how that information is or can be used and misused.

1. The methods necessary to achieve anonymity and pseudonymity must be simple to understand and use such as, for example, the methods used for parental control of online access for children today.
2. Due to the lack of understanding of the issues and complexity of accessing settings e.g. for routers, settings should be set by default to anonymous or such settings should be made simple, clear and obvious to users during initial setup with simple temporary or application specific user driven overrides available for services that require it under control of the user.

**Issuer Requirements**

1. An issuer of a pseudonym shall create a unique pseudonym based on the user’s input (the human readable form).
2. An issuer of a pseudonym shall maintain anonymity for the user except as specified by the user and any legal/regulatory requirements.

**User Requirements**

1. Users should only be required to understand the higher level goals of online anonymity and the use of unique identities (pseudonyms). They should not be required to understand the underlying mechanisms and settings required to achieve them.
2. In situations where achieving these goals crosses device and/or application boundaries standards may be required to allow the user to propagate their choices across the boundaries without having to coordinate individual settings at each point. For example, a setting to “anonymous” should inform multiple devices and/or applications to ensure PII is not made available through local settings (e.g. a router with a fixed IP address) without the user having to make changes to each device and application settings. This may be accomplished by the use of a trusted 3rd party as an intermediary, a proxy service, or other means.

**Processor/Workflow Requirements**



**Device Requirements**

1. Devices shall include the ability to block, obfuscate, encrypt or otherwise ensure that PII associated with the device such as MAC addresses, IP addresses assigned to it, device related fingerprints, etc., is not made available without user consent.
2. Devices may be required to store PII in a secure manner. This may include the ability to secure PII associated with different pseudonyms separately to ensure it is only accessible to services/applications associated with that pseudonym.

**Security Requirements**The concept of PII is somewhat vague and defined differently in different domains and regulatory regimes. To secure PII some assumptions will need to be made with respect to exactly what this group includes in its definition.

1. Device PII: IP address; MAC address; hardware, firmware fingerprints; location; S/N; make/model; others
2. Software PII: Software, browser and app fingerprints; Software, browser and app user-specific PII (settings, name, address, business, registration numbers, location, memberships, history, etc.).

**Business Requirements**

Many business require PII of various types for their business models and will not provide their services to users/devices that do not provide it to them.

1. A pseudonym must be linkable to specific PII as needed to fulfil the business requirements of the service provider.
2. A pseudonym should be able to be linked to one or more businesses/services.
3. A trusted 3rd party, if directed or configured to do so by the user, may be used to either provide the necessary PII to the service without necessarily identifying the true (legal) identity of the user (unless required by the service), or to authenticate the person represented by the pseudonym has the necessary credentials “on file” to use the service r.
4. The PII linked to that pseudonym should be persistent to enable a service to authenticate the user based on the pseudonym.
5. The user shall be able to delete the pseudonym and/or its link(s) to the PII effectively severing the link to the business/service(s) for which it was used.