SECURE IDENTITY ALLIANCE

Internal Rules

Secure Identity Alliance

20th December 2022 – Version 2

Table of Contents

The terms used in these Internal Rules and their Annexes have the same meaning as in the Articles of Association of the SIA.

1. Membership & Governance

1.1. Membership criteria

1.1.1. Certifications

Full Members need to hold at least two (2) security certifications or certifications of information technology security, recognized by Member States of the European Union.

1.1.2. Definitions

- Registration/ Enrolment: The process of capturing and recording key identity attributes.
- Validation and Assurance: The process of validating the attributes presented.
- Biometrics: the process of managing attributes which are inherent—i.e., based on an individual's personal biometric (biophysical, biomechanical, or behavioural) which can be used for identification or deduplication (i.e., as used to establish an individual's identity and uniqueness) or as authenticators.
- Credentialing/ Issuance: The process of issuing a credential as a proof of the identity in physical and/or digital formats.
- Authentication: The process of validating credentials to verify identity.
- Authorisation: The process of determining whether the authenticated identity has the ability to access the system and up to what extent.
- Federation: The process of allowing identity to be portable and convey identity and authentication information across a set of networked systems.

> Decentralisation: The process of sharing control of identity lifecycle management among several independent entities and/or under control of the user.

1.2. Probation

No probation period, in the meaning of Article 9.7 of the Articles of Association of the SIA is presently applied to companies admitted as new Members.

1.3. Due Diligence

All applications to become a Member or an Affiliated member are subject to a standardized due diligence process overseen by an external consultancy, to ensure that applicants are in good standing with relation to applicable legal and ethical standards and that they are aligned with the Alliance's guiding principles.

The public reputation and any past or current legal, financial, regulatory, or ESG issues involving the applicant are examined along three pillars: corruption, governance/human rights and IP breach. They depend on the country of incorporation of the applicant.

	Corruption (reference: https://www.transparency.org/)	Governance/Human Rights (reference: https://fragilestatesindex.org/)	IP Breach (reference: media coverage)
Level 1: Check	- Non-flagged countries	- Non-flagged countries	- All countries
Level 2: Due Diligence	- Flagged countries - Or if issue identified in Level 1 and no satisfactory answers (cost to be paid by applicant if industry applicant and candidacy maintained)	- Flagged countries - Or if issue identified in Level 1 and no satisfactory answers (cost to be paid by applicant if industry applicant and candidacy maintained)	- All countries
Level 3: Enhanced Due Diligence	- If issue identified in Level 2 and no satisfactory answers (cost to be paid by applicant if candidacy maintained)	- If issue identified in Level 2 and no satisfactory answers (cost to be paid by applicant if candidacy maintained)	- All countries

If results are green, candidacy can be considered further.

If results are orange, explanations are required. If no satisfactory answer is given, next level of due diligence is required for candidacy to be considered further.

If results are red, candidacy cannot be considered further. Results are red when serious risk factors have been identified (relationship with sanctioned entities, espionage, terrorist financing, corruption, governance/human rights issues, money laundering, tax evasion, etc).

1.4. Governance

The positions of Chair and Vice-Chair are held exclusively by Founding Members.

2. Representation of Members and Affiliated members

2.1. Representatives

Full, Founding and Associate Members and Affiliated members designate a Representative.

To the extent allowed in accordance with Articles 16.3 and 24.4 of the Articles of Association, any temporary substitution or definitive change of Representative shall only be effective once it has been declared to the Chair by, as the case may be, the Representative or any other authorised person of the concerned Full, Founding and Associate Members or Affiliated members.

Each Representative keeps the Secretary General informed of its up-to-date full professional details.

2.2. Other participants

The Chair may invite other persons to attend Board meetings and/or General Meetings, without voting right, if that is necessary for the discussion to take place at such meetings.

3. Meetings

3.1. Preparation

Invitations to Board meetings and General Meetings are issued by the Chair or under its responsibility, together with the agenda of the meeting and relating documentation, if any. The Chair prepares these invitations with the Vice-Chair.

All notices are sent by e-mail.

3.2. Meetings

The minutes record the attendants to the meetings.

If no Member objects, the proposed resolutions as set out in the agenda may be amended by the Chair in the course of the meeting, before voting.

The minutes of the General Meetings are signed by the Chair, the Vice-Chair and the Secretary General. The minutes of the Board meetings are signed by the Chair, the Vice-Chair, the Secretary General and the Directors who so request.

The Vice-Chair substitutes the Chair as Chair of the Board and of the General Meeting when the Chair is not available.

3.3. Votes

Board Members vote by raising hands. The Chair may however organize secret voting. The Chair has no casting vote.

4. Working Groups

Working Groups are Chaired by a person designated by the Board, and who must be a staff member of a Member.

The person heading a Working Group organizes the agenda, the structure, and the activities of the Group, within the framework determined by the Board and in accordance with Annex 2.

The person Chairing a Working Group is responsible for calling meetings, determining the agenda, inviting participants, and drafting the minutes of its meetings. However, this person must obtain prior approval from the Chair or the Secretary General before inviting at meetings persons that are neither staff members of a Member, an Affiliated member, or the SIA.

The person Chairing a Working Group reports to the Chair, the Board and the Secretary General at least every two (2) months, and at their request. This person implements the instructions received from the Chair, the Board or the Secretary General.

5. Documents relating to the activities of the SIA

The Secretary General collects and keeps the documents relating to the activities of the SIA, notably the minutes of the Board meetings and General Meetings.

The persons Chairing a Working Group must forward to the Secretary General the documents relating to the specific activities of their Working Group.

6. Compliance

A Charter of Compliance is annexed to these Internal Rules. Each Member and Affiliated member complies with its provisions.

7. Ethics

A Code of Conduct is prepared by the Secretary General and approved by the Board. The Board may amend its content from time to time. Each Member and Affiliated member complies with its provisions.

8. Diversity & Equality

A Diversity & Equality Policy is annexed to these Internal Rules. Each Member and Affiliated member complies with its provisions.

9. Personal Data

A Data Protection & Privacy Policy is annexed to these Internal Rules. Each Member and Affiliated member complies with its provisions.

10. Intellectual Property Rights

A Charter of Intellectual Property Rights is prepared by the Secretary General and approved by the Board. The Board may amend its content from time to time. Each Member and Affiliated member complies with its provisions.

Specific, additional intellectual property rights policies may be adopted for specific projects.

11. Budget

The documentation sent to Members ahead of the General Meetings where the annual budget is to be discussed includes the report of the person in charge of controlling the accounts of the SIA.

12. Language

The internal documents of the SIA are in English or in English and French.

In its relations with the authorities, the working language of the SIA is French. English translations may be provided by the Secretary General if necessary.

13. External Communication

Discussions within the framework of the SIA's activities are confidential. Communications Guidelines are prepared by the Secretary General and approved by the Board. The Board may amend them content from time to time. Each Member and Affiliated member complies with their provisions.

The Secretary General is to choose external marketing and communications advisor with approval of the Chair, the Vice-Chair being consulted.

1. Annex 1: Charter of Compliance

The Secure Identity Alliance does not play any role in the competitive decisions of its Members and Affiliated members nor in any way restrict competition. Its activities are conducted in compliance with all applicable antitrust and competition laws and regulations.

Members and Affiliated members commit themselves, under their own responsibility and taking their own appropriate legal advice, to strict adherence to applicable legal and regulatory antitrust and competition requirements. They remain, as the case may be, independent market stakeholders, players, and competitors. In particular, they forbid themselves at all times to use the Alliance's activities, directly or indirectly, as a support or framework for any behaviour whatsoever that would be contrary to the requirements of all applicable competition laws that may apply directly or indirectly to the activities of Members and Affiliated members.

As a consequence, they notably:

- Uphold the ground principles of the Alliance, as an open organisation working in the interest of the public authorities and the general public;

- Actively pursue full and fair competition with their competitors, including Members and Affiliated members, through independent industrial and commercial strategies;

- Do not disclose confidential commercially sensitive information in any form about their respective strategies, figures, and know-how;

  Do not concert to alter the functioning of the market, whether, notably, through fixing prices or quotas, allocating contracts, territories, or customers, restricting innovation, boycotting or preventing access to the market;

Devise and implement awareness including training and compliance procedures towards all their staff participating in the activities of the Alliance regarding prohibited practices and the risks associated with infringements of competition law.

It is the responsibility of each Member and Affiliated member to oppose and refuse to take part to any attempt to break these rules, including by leaving any meeting where such behaviour would take place and referring immediately the matter to the Chair and the Secretary General. The persons Chairing Working Groups are specifically in charge of upholding these rules within their respective Working Groups.

Infringements of competition law are among the most serious breaches of the Alliance's rules that a Member or Affiliated member may be responsible for. Such occurrence would trigger sanction procedures and make the concerned Member(s) or Affiliated member(s) liable for any adverse consequence that the SIA might bear as a result.

The SIA as an association will follow a policy of full cooperation with competition authorities.

2. Annex 2: Working rules for Working Groups

2.1. Establishment and Termination of a Working Group

2.1.1.

When resolving to establish a new Working Group, the Board shall decide on

- its scope;
- its Chair.

2.1.2.

A Working Group is established when the following steps have been completed:

- the Board has resolved to establish the Working Group;
- the Secretary General has set up an initial meeting of the Working Group;
- the Secretary General has invited all the Members who have signed up to the Working Group at that time to attend the initial meeting by communicating to them the time, the place, and the agenda of the initial meeting.

2.1.3.

A Working Group may be terminated by the Board if the Working Group has achieved its goals, which the Board may decide at its absolute discretion.

2.2. Working Group Members

2.2.1.

Working Group(s) relating to Industry Services and Solutions will collectively constitute the "College 1" of the NPA. Working Group(s) relating to Open Standards Development will collectively constitute the "College 2" of the NPA.

2.2.2.

Founding, Full and Associate Members are entitled to participate in any Working Group, in either College. The same applies to Affiliated members, with the exception of Affiliated members that have a commercial activity, which may only participate in College 2.

2.3. Contributors of Working Groups

2.3.1.

With respect to each Working Group, a person designated by a Working Group Member is a Contributor if he or she:

- regularly attends the meetings of the relevant Working Group;
- actively contributes to work carried out, during the meetings and in-between the meetings, providing reasonable levels of input;
- executes assigned tasks within given time frame as agreed with Chair and other Contributors.

2.3.2.

Each Working Group Member shall appoint at least one Contributor per Working Group and has the right to replace any of its Contributors or appoint another Contributor at any time. In case of a replacement, a Working Group Member shall inform the Chair of the relevant Working Group and the Secretary General without undue delay.

2.4. Chair of Working Group

2.4.1.

The Board has the right to replace the Chair of a Working Group at any time and at its sole discretion. The Chair may resign without cause to the end of a month with a notice period of three months.

2.4.2.

In addition to the responsibilities specified elsewhere in these Internal Rules, the Chair is responsible for the following tasks and has the right to make the following decisions:

- manage the Working Group program according to the goals, milestones, and deliverables defined and approved by the Working Group;
- propose any necessary organizational changes and/or improvements needed to carry out the work of the Working Group;
- Communicate with the public on behalf of the Working Group in accordance with the “Communication Guidelines”. Any external communication drafted by a Working Group, or the Chair must be approved by the Board before its release;
- in particular, the Chair shall:
  - Organize the efficient and timely work of the Working Group and plan budget and budget requirements for the Working Group.
  - Maintain the list of Contributors and the Working Group Members.
  - Ensure the quorum is met.
  - Try to reach consensus in the Working Group.

- Plan meetings of the Working Group in time, communicate meeting schedules of the Working Group to the Working Group Members and the Secretary General, and maintain a forward-looking meeting schedule according to the working plan approved by the Working Group.
- Prepare the agenda for meetings of the Working Group and notify the Working Group Members of the agenda and work in time
- Conduct the meetings of the Working Group in an efficient manner.
- Agree on tasks to be done by the Working Group, assign tasks to Working Group Contributors with a given time frame for execution, and close the action successfully.
- Ensure meeting minutes are correctly taken, communicated, and filed in the SIA internal repository. Minutes shall be sent no later than 5 working days after a meeting to the Working Group Members for approval.
- Remind the Charter of Compliance at the beginning of each Working Group meeting and appears in the minutes.
- Ask, during each meeting, whether anyone has knowledge of intellectual property rights issues, including patents, copyright for software or text, marks, the use of which may be required to implement or publish the recommendation being considered. The fact that the question was asked shall be recorded in the working party or study group meeting report, along with any affirmative responses.
- Participate in individual or group coordination meetings organized by the Secretary General to coordinate the Working Group.
- Communicate in a reasonable manner, preferably in a written report, to Working Group Members, any results from coordination meetings (see xi. of this subsection), Board related requests and any other external meetings related to the activities of the working group.
- Report to the Secretary General and, if need be, refer to the Secretary General any issues the Working Group is not able to resolve within a reasonable time.
- Provide, with the help of the Contributors answers to the Board's or Secretary General's requests for information and report in a reasonable manner, at the Board's re-quest, any Working Group results at a meeting of the Board.
- Set working rules to maintain efficiency in the Working Group on a fair, reasonable, and non-discriminatory basis and in accordance with the Charter of Intellectual Property Rights and the Charter of Compliance of the Secure Identity Alliance.

2.5. Management of a Working Group

2.5.1. Responsibilities of the Working Group

In addition to the powers and responsibilities defined elsewhere in these Internal Rules and within the purpose of the Working Group as defined in these Internal Rules and by the Board, the Working Group is responsible for the following tasks and has the right to make the following decisions:

> drafting the technical and marketing deliverables;
> managing external communication, including electronic means and Internet web site, in accordance with the Communication Guidelines;
> providing input to the Secretary General on legal and commercial aspects related to its work (licensing, IPR etc.);

- on the initiative of the Secretary General or the Chair of a Working Group, reviewing Working Group objectives and agreed milestones and proposing changes to the Board and the Secretary General.

2.5.2. Meetings

Working Groups shall hold regular meetings coordinated at the Chair ’s discretion. The Chair decides the time, the place, and the agenda for each meeting and ensures timely communication to all Working Group Members and, at his or her discretion, to the SIA Members and/or Affiliated members.

2.5.3. Decision-making

Working Group Members are involved in the decision-making process of a Working Group, as defined in the following:

- for any decision of the Working Group, the quorum must be met (as defined below);
- all Working Group Members shall aim to reach consensus on a decision. If a consensus cannot be reached, the Chair of the Working Group shall notify the Board. Within one month from the Chair ’s notification, the Board may either decide the matter itself by resolution or instruct the Working Group to reach the decision by vote, by a simple majority and with the Chair holding a casting vote.

2.5.4. Quorum

The meetings of the Working Groups are valid if at least three Members attend.

2.5.5. Decisions by Correspondence and Participation in Meetings by Telephone/ Online Conference

Working Group Members may participate in a meeting of the Working Group by conference call or similar means.

The Working Group may adopt decisions in writing (either in tangible or electronic form), which shall be valid as a decision reached at a meeting provided the requirements established within the relevant group are complied with. The Chair shall file appropriate documentation of such written decisions.

2.5.6. Sub-working groups

The Working Group may be organized in sub-working groups defined by the Chair, each one with a lead appointed by the Chair. Sub-working groups will organize their calls/meetings as appropriate, and otherwise apply the same rules as the Working Group.

2.6. Approving Budgetary Expenses

Any expense of a Working Group must be approved by the Board.

The Chair of the Working Group is responsible for the activity for which the expense was approved and for monitoring that the approved budget for this activity is not exceeded. Any expenses in excess of the approved budget must additionally be approved by the Board.

Expenses not attributable to any of the Working Groups must be approved by the Board.

2.7. Advisory Committees

2.7.1. Principles

The Board may decide that a Working Group work with an Advisory Committee alongside an Operational Working Group.

The rules applicable to the Operational Working Group are those applicable to Working Groups pursuant to this Annex 2. to the Internal Rules.

The purpose of the Advisory Committee is to provide the Operational Working Group with advice on the general development of its work, and long-term perspective. It helps spread awareness of, and communicate on, the work of the Operational Working Group.

2.7.2. Participation

The Advisory Committee is open to governmental and academic Affiliated members.

2.7.3. Working program and internal organisation

The Advisory Committee is headed by a Chair who supervises work by the Committee, Chairs its meetings and synthetises its recommendations.

The first Chair is appointed by the Board, for a term determined by the Board. Following Chairs are appointed by the members of the Advisory Committee for two-year-terms (two civil years), by consensus. In the case of lack of consensus, the Board organizes an election by and among the members of the Advisory Committee, with any new Chair elected when gathering the votes of two thirds of the validly voting members of the Advisory Committee (i.e. excluding abstention and void votes if any). The Chair remains in place while a following Chair has not been appointed.

The Advisory Committee meets at least twice per year (for a call and a physical meeting) with the members of the Operational Working Group. The Secretary General of the Secure Identity Alliance is invited. Members of the Board may also attend, through their Representative and/or other delegated staff.

The Chair of the Advisory Committee may organise other meetings as necessary.

The Chair of the Working Group provides secretariat to the Advisory Committee, notably regarding the preparation of the meetings and the drafting of the minutes. It is in charge of the co-ordination of the work undertaken by the Operational Working Group with the advice provided by the Advisory Committee.

Public announcements or other documents may be released, by agreement between the Chair of the Advisory Committee and the Chair of the Working Group. In case of a disagreement, the Chairs refer the decision to the Board.

2.7.4. Contributions

Members of the Advisory Committee are not requested to contribute financially to the work of the Working Group. Voluntary contributions may however be agreed with the Board.

3. Annex 3: Working methods for Open Standards Identity APIs (OSIA)

3.1. Purpose of the OSIA Initiative

The Secure Identity Alliance has launched the OSIA Initiative. OSIA stands for Open Standards Identity API. The aim of the OSIA Initiative is to develop a framework of open standards for the interoperability of identity systems.

This Initiative is part of the Secure Identity Alliance's purpose under Article 7.1 (ii) of its Articles of Association:

- Promote innovation, open standards and technical frameworks to guarantee a level playing field for all market players (owner, open source, large companies, SMEs, start-ups, local and international etc.).
- Develop open standards and technical frameworks to meet above objective.
- Contribute to national, regional or international standards organisations.
- Develop certification programs.

3.2. Stakeholders invited to take part in the OSIA Initiative

Founding, Full and Associate Members, as well as Affiliated members, are invited to take part in the OSIA Initiative.

3.3. Structure of the OSIA Initiative

Work on the OSIA Initiative is carried out in a dedicated Working Group hosted within College 2 of the Secure Identity Alliance, with an Operational Working Group working under the supervision of an ad hoc Advisory Committee.

In accordance with Article 33.5 of the Secure Identity Alliance's Articles of Association, the functioning rules applicable to this Working Group are those in Annex 2 (Working rules for Working Groups) to the Internal Rules, as specified in this Annex 3, which shall prevail in case of discrepancy.

3.4. The OSIA Operational Working Group

3.4.1. Purpose

The purpose of the OSIA Operational Working Group is to manage the development of, devise, update and release the OSIA technical and functional specifications.

The OSIA Operational Working Group is also charged with devising the means for testing, accrediting, and certifying the products using the OSIA specifications.

It works under the terms and conditions set out in Charter of Intellectual Property Rights, as supplemented by the Charter for the development of a set of Open Standards Application Programming Interfaces (which shall prevail in case of conflicting provisions), with which all members of the Operational Working Group must comply. More generally, all members of the Operational Working Group commit to complying with the rules governing the Secure Identity Alliance, including notably its Code of Conduct and Charter of Compliance.

The OSIA Operational Working Group is headed by a Chair who is a natural person appointed by the Board of the Secure Identity Alliance after consultation with the Operational Working Group.

The OSIA Operational Working Group comprises a Technical Authority who is a natural person appointed by the Board of the Secure Identity Alliance after consultation with the Operational Working Group. The Technical Authority is charged with checking consistency of the specifications published on the forge.

3.4.2.Participation

The OSIA Operational Working Group is open to Founding Members and Full Members of the Secure Identity Alliance.

The OSIA Operational Working Group is also open to Associate Members as well as non-governmental and non-academic Affiliated members: industry, foundations, think-tanks, associations, consultancies.

Governmental and academic Affiliated members may be invited by the Chair.

3.4.3.Working program and internal organisation

The working program and the internal organisation of the OSIA Operational Working Group are managed by its Chair. The OSIA Operational Working Group is guided by the Advisory Committee and the two meet at least twice a year (virtual and/or in-person meetings).

The OSIA Operational Working Group meets on a monthly basis for a general update.

Working sessions on specific topics are to be organised depending on ongoing developments and matters by the Chair or the Leads of the Sub-Working Groups. The timetable of meetings, including agendas, shall be prepared, and communicated to participating bodies at the beginning of the year (for the general monthly update) and at the beginning of the work session series (for specific topics). They may evolve during the course of the year depending on speed of progress.

The Chair or the Leads may schedule short additional meetings if required, for the purpose of checking whether consent or decision is reached on a draft new or revised recommendation or other topic previously discussed or that needs urgent action.

The OSIA Operational Working Group strives to conduct all its work via online collaboration.

The Chair is specifically in charge of upholding the Charter of Compliance and the Charter of Intellectual Property Rights of the Secure Identity Alliance within the OSIA operational Working Group. The Chair drafts the minutes of the meetings. The Leads are charged with the same tasks as the Chair within their respective sub-working groups.

3.4.4. Contributions and release of the specifications

Contributions to the specifications are submitted via the forge at least one month before the meeting where they are to be discussed.

The approved OSIA specifications are published on the forge after consistency review by the person responsible for the forge and the OSIA Technical Authority, and approval by the OSIA Operational Working Group.

The decision is to be reached by consensus. If consensus cannot be reached, the decision is approved through a vote at a later meeting, where (i) the quorum is half of the participating Members and Affiliated members, (ii) the majority is 3/5 of the Contributors of the Members and Affiliated members present at this meeting and (iii) no power of attorney will be allowed.

3.4.5.Version control

Versions of the OSIA specifications will be controlled using the following rules:

1. Document dates: the author of the document will ensure the date the document is created or revised is identified on the first page and, when possible, is incorporated into the header or footer of the document and appears on every succeeding page.

2. Version numbers: the author of the document will ensure the current version number is identified on the first page and, when possible, is incorporated into the header or footer of the document and appears on every succeeding page.

3. Draft document version number

a) The first draft of a document will be Version 0.1.
b) Subsequent drafts will have an increase of “0.1” in the version number (e.g., 0.2, 0.3, 0.4, ...0.9, 0.10, 0.11).

4. Final document version number and date:

a) The Chair will deem a protocol or other document (consent/assent form, case report form, manual of procedures) final after all reviewers have provided final comments and the comments have been addressed.

b) The first final version of a document will be Version 1.0. Include the date when the document becomes final. Generally, the final version is submitted to the Advisory Committee.
c) Subsequent final documents will have an increase of “1.0” in the version number (1.0, 2.0, etc.).

5. Final documents undergoing revisions

a) Final documents undergoing revisions will be Version X.1 for the first version of the revisions.
b) While the document is under review, subsequent draft versions will increase by “0.1” (e.g., 1.1, 1.2, 1.3, etc.).
c) When the revised document is deemed final, the version will increase by “1.0” over the version being revised (e.g., the draft 1.3 will become a final 2.0).

6. Documenting substantive changes: a list of changes and historical versions from the previous draft or final documents will be kept on the forge. The list will be cumulative and identify the changes from the preceding document versions. The list of changes made to a protocol and consent/assent should be submitted to the Advisory Committee with the final protocol and consent/assent documents.

3.4.6. Fees

Non-governmental and non-academic Affiliated members that are members of the OSIA Working Group are requested to contribute financially to the Initiative, for an amount that is determined annually by the Board and may vary or be waived depending on the status and size of the Member. At the beginning of each civil year (and in the year of admission, if admission occurs by 30 June), they pay a non- refundable fee for an amount to be determined by the Board. Founding, Full and Associate Members will contribute via the membership fees paid to the Secure Identity Alliance.

Specific accounting lines in the accounts of the Secure Identity Alliance identify the resources and expenses linked with the Initiative.

3.5. The OSIA Advisory Committee

The purpose of the OSIA Advisory Committee is to provide the Operational Working Group with advice on the general development of the Initiative, including notably issues linked to the use of OSIA, its consistence with its aims (inter-operability, consistence with authorities’ needs…), and long-term perspective. It helps spread awareness of, and communicate on, the Initiative.

3.5.1. Participation

The OSIA Advisory Committee is open to governmental and academic Affiliated members.

3.5.2. Working program and internal organisation

The Advisory Committee is headed by a Chair who supervises work by the Committee, Chairs its meetings and synthetises its recommendations.

The first Chair is appointed by the Board, for a term ending end 2020. Following Chairs are appointed by the members of the Advisory Committee for two-year-terms (two civil years), by consensus. In the case of lack of consensus, the Board organizes an election by and among the members of the Advisory Committee, with any new Chair elected when gathering the votes of two thirds of the validly voting members of the Advisory Committee (i.e. excluding abstention and void votes if any). The Chair remains in place while a following Chair has not been appointed.

The Advisory Committee meets at least twice per year (for a call and a physical meeting) with the members of the Operational Working Group. The Secretary General of the Secure Identity Alliance is invited. Members of the Board may also attend, through their Representative and/or other delegated staff.

The Chair of the Advisory Committee may organise other meetings as necessary.

The Chair of the Working Group provides secretariat to the Advisory Committee, notably regarding the preparation of the meetings and the drafting of the minutes. It is in charge of the co-ordination of the work undertaken by the Operational Working Group with the advice provided by the Advisory Committee.

Public announcements or other documents may be released, by agreement between the Chair of the Advisory Committee and the Chair of the Working Group. In case of a disagreement, the Chair s refer the decision to the Board.

3.5.3. Contributions

Members of the Advisory Committee are not requested to contribute financially to the Initiative. Voluntary contributions may however be agreed with the Board.

4. Annex 4: Code of Conduct

4.1. Purpose

The Secure Identity Alliance is dedicated to supporting sustainable worldwide economic growth and prosperity through the development of trusted digital identities and the widespread adoption of secure eServices.

The Alliance offers support and expertise to allow government agencies and other public bodies to implement their Digital ID projects and realize the wide range of economic, public health, electoral and sustainability opportunities offered by the shift to digital service provision.

The Alliance brings together public, private and non-government organizations to foster international collaboration on Digital ID challenges and the issues of data security, citizen privacy, identity, authentication and more.

The Alliance plays a key role in sharing best practice and uncovering the new generation of eIdentity and eDocument technologies crucial to building the trusted framework on which to drive eGovernment, and global economic growth, forward. Trusted digital identities are necessary to both public and private eService deployments.

To help fulfil this mission, the Alliance has adopted this Code of Conduct, as an ethical framework for interventions by public, private and non-government organizations. It is the Alliance's firm belief that strict adherence to high ethical standards is key to meeting the challenges and reaching the full potential of digital identities and secure eServices, to the benefit of all stakeholders.

The Code of Conduct provides general guidelines and principles, to serve as references on which to build concrete behaviour depending on the relevant situation at hand. It is conceived around the core notion of respect.

4.1.1. Respecting human dignity

Every human has a fundamental right to the respect of their dignity.

Members and Affiliated members refrain from using forced labour, child labour, or labour provided under conditions that disrespect the workers' fundamental rights of association, no-discrimination, due compensation and appropriate resting periods.

4.1.2. Respecting legality

Members and Affiliated members are committed to respecting the laws, rules and regulations applicable to their activities depending on the jurisdiction at hand.

In doing so, they take into full consideration prevailing international decisions, treaties, and conventions. They comply in particular with the applicable sanctions' regimes set up against countries, companies, or individuals, as well as with import/export legislations.

They do not use threats, bribes, or other illegal means to influence the adoption or implementation of laws, rules or regulations, or the content of court decisions.

They abide by the Secure Identity Alliance's Charter of Compliance.

4.1.3. Respecting honesty

Members and Affiliated members:

- Enact policies designed to identify, prevent, or end conflicts of interest.
- Ensure proper use of their assets, so as to avoid them being used for purposes of bribery.
- Respect the principle of fair competition, notably in the context of tender procedures.
- Negotiate and perform contracts in good faith.
- Refrain from infringing intellectual property rights.
- When establishing a relationship with a third party (contractors, consultants…), do so with reputable and qualified parties, in writing. Remunerations shall reflect the services actually rendered. Payments shall always be traceable and duly registered in the accounts.
- When communicating to other parties or to the public, refrain from providing false, inaccurate, or otherwise misleading information.

4.1.4. Respecting safety

Members and Affiliated members actively seek to provide a safe and healthy environment at the workplace.

They maintain working conditions designed to reduce the risks of occupational injuries or diseases.

They enact policies to prevent and sanction inappropriate behaviour such as harassment (notably sexual harassment), violence, threatening, intimidation, proselyting or working under the influence of substances such as alcohol or illegal drugs.

4.1.5. Respecting sustainability

Members and Affiliated members respect the applicable legal framework for the protection of the environment and design their activities so as to minimize their environmental impact.

Through their activities, they seek a durably positive impact on the concerned stakeholders, notably local communities.

4.1.6. Respecting neutrality

Members and Affiliated members :

- Enact policies of no-discrimination on the basis of, notably, race, origins, social group, sexual orientation, religion, beliefs, opinions, or language. This principle of no-discrimination applies notably to workers.
- Respect the principle of free speech, inasmuch as freedom of speech is not invoked to justify claims, slogans, affirmations, or questions designed to degrade adherence to the principles spelled out by this Code of Conduct.
- Do not make payments to governmental bodies (central or local), political parties or other individuals, groups, entities, and organizations that aim the implementation of a political agenda, notably by supporting violent action.

4.1.7. Respecting equality

Members and Affiliated members respect the principles of equal treatment and equal opportunities between human beings. They notably oppose gender-based discrimination or discrimination against persons suffering from disabilities

4.1.8. Respecting confidentially

Members and Affiliated members respect the confidentiality of the information provided to them by third parties on a confidential basis, in accordance with the terms under which such information was provided and with the applicable legal framework. They enact policies designed to safeguard such information from disclosure to unauthorized persons.

They respect and safeguard the confidentiality of personal data, in accordance with the applicable legal framework.

4.1.9. Implementation

All Members and Affiliated members adhere to this Code of Conduct, in addition to their own internal ethical and compliance rules.

They observe this Code of Conduct when they act independently, as well as when they act in conjunction with third parties, which they must hold to the same standards to the best of their knowledge.

They actively promote awareness of the Code of Conduct, internally and externally. They set up or extend internal mechanisms to assess compliance with this Code of Conduct, allow reporting of inappropriate behaviour and sanction disrespect of the principles it spells out.

5. Annex 5: Communication Guidelines

5.1. Purpose

The Secure Identity Alliance is a forum of reference, where collective actions can be designed and implemented, in full compliance with competition law requirements, and in an open public/private collaboration perspective, to address questions of common interest in the field of Government-issued e-Identity.

The ultimate aim of these actions is to raise general awareness on these questions, and spread best practices, to the benefit of the public.

To this purpose, communication is key. It comprises such actions as (but is not limited to) issuing statements, responding to the media, meeting stakeholders, or taking part to industry or other public events.

It is of utmost importance that these efforts be conducted in a consistent and professional manner, so that the Alliance fulfil its role and uphold fruitful co-operation between its Members and Affiliated members, as well as with external stakeholders.

In this perspective, the Alliance has adopted these Communications Guidelines, as a framework for communication actions taken in the name of the Alliance.

These Communication Guidelines are attached to the Internal Rules of the Alliance. In no event may these Guidelines be construed in a manner that would contradict the principles set out in the other documents governing the Alliance, notably the Compliance Charter or the Code of Conduct.

5.2. Perimeter of the Guidelines

These Communication Guidelines are designed as a framework for communication actions taken in the name of the Alliance.

Communication actions are to be construed in an extensive manner. They cover all means whereby the persons involved in the work of the Alliance (directly or through their organization) may communicate with third parties in the name of the Alliance. These means include, notably (but not exclusively) :

- Connecting with the media: press interviews, press releases...
- Writing articles.
- Participating to industry or other public events.
- Managing or interacting on websites or social media.
- Contacting or meeting with stakeholders, including public authorities.

These Communication Guidelines are distinct from the actions and frameworks that Members or Affiliated members may design, or adhere to, for the purposes of communicating in their own names. Accordingly, the persons communicating in the name of the Alliance should at all times be aware of, and make clear, the distinction between their capacity within the Alliance and their external capacity. They should always ensure that there is no confusion in their audience (ie, as the case may be, journalists, event organisers, attendance at meetings or conferences...), using the appropriate means as necessary (opening statement, logo...). In addition, even when not speaking in the name of the Alliance, they should refrain from comments that would contradict or pre-empt the Alliance's communication.

5.3. Communication plan and spokespersons for the Alliance

The spokesperson of reference for the Alliance is the Chair. The Vice-Chair communicates in the name of the Alliance upon instructions from the Chair, or in case of urgency when the Chair is not available.

The Chair, with the assistance of the Vice-Chair, the Secretary General and the external marketing and communication advisor of the Alliance, is responsible for designing and implementing the communication plan of the Alliance. This plan notably covers managing the Alliance's website and social network profiles, issuing press releases, and responding to press interviews, taking part to relevant industry or other public events, or meeting with stakeholders.

The Chair submits this plan and regular updates to the Board for approval. Communication actions carried out or planned are presented to the General Meeting annually.

As part of the actions thus designed by the Chair and approved by the Board, other spokespersons may be charged of speaking on behalf of the Alliance. These other spokespersons may be Representatives of Board Members, the Secretary General, Heads of Working Groups, or advisors to the Alliance. Exceptionally, where required by a specific action, other persons may be specifically appointed.

In any event, no other person than the Chair may communicate in the name of the Alliance, if not as foreseen in an action approved by the Board.

The above does not prevent the Chair from exceptionally taking ad hoc decisions, under his responsibility and with report to the Board, where necessary and notably in the case of urgency.

5.4. General principles applicable to the design and implementation of the communication plan

The communication plan designed by the Chair and approved by the Board for actions taken in the name of the Alliance abide by the following principles:

- No Member or Affiliated member is to liaise directly with the media. The person charged with liaising with the media in the name of the Alliance is the Chair, with the assistance of the Secretary General and the Alliance's communication advisor;
- No Member or Affiliated member is to liaise directly with public authorities. The person charged with liaising with public authorities in the name of the Alliance is the Chair, with the assistance of the Secretary General and the Alliance's communication advisor. The Chair notably ensures that any such contact complies with the rules applicable to lobbying, if any. For this purpose, the Secretary General and the Alliance's communication advisor implement a supervision plan as provided for in the "Contacts with public authorities" article, hereafter;
- The Alliance's website and social media profiles are managed by the Secretary General and the Alliance's communication advisors, under the responsibility of the Chair. Members and Affiliated members are invited to connect to the Alliance's website and social media profiles to further their impacts, notably by forwarding released news. Interaction must however always comply with the general principles applicable to the messages conveyed in the name of the Alliance, hereafter;
- Individual messages to be released in the name of the Alliance shall be subject to review by the Board, with a reasonable time frame for reaction if any. Absence of reaction shall be regarded as approval.

The above does not prevent the Chair from exceptionally taking ad hoc decisions, under his responsibility and with report to the Board, or the Board from exceptionally approving ad hoc decisions, where necessary and notably in the case of urgency.

5.5. General principles applicable to the messages conveyed in the name of the Alliance

Any action implemented in the name of the Alliance must:

- Comply with the principles set out in the other documents governing the Alliance, notably the Compliance Charter and the Code of Conduct;
- Not breach the applicable legal framework, notably regarding rules on copyrights or other intellectual property rights, on confidentiality or on defamation;
- Correctly cite sources and quotes;
- Be consistent with the Alliance's communication plans and previously conveyed or approved messages;
- Be formal, respectful, informed and professional, so as to uphold the reputation of the Alliance and, indirectly, that of its Members and Affiliated members;
- Be prudent, and notably refrain from pre-empting the Alliance's communication on new issues.

Members and Affiliated members notably ensure that these principles are upheld when their agents engage in social events or on social media, where a topic concerning the Alliance is discussed.

5.6. Procedure for additional communication actions

Members or Affiliated members may be asked by third parties to take part to, or suggest initiating (notably as a result of work carried out in the Working Groups), actions in the name of the Alliance. In this case, they refer the request to the Chair and the Secretary General and specify:

- The party requesting or suggesting an action, and the party having the final say on its outcome;
- The format of the action (nature, topic, date, place...);
- The proposed course of action and message to convey;
- Whether/how it will be possible for the Alliance to control the outcome ahead of its release;
- The timeframe for approving the action.
- The request is examined and decided as an update to the Alliance's communication plan.

5.7. Logo and other image requirements

The communication plan designed by the Chair and approved by the Board covers adopting and updating the Alliance's logo and other image/brand-related tools, including presentation templates, icon libraries and biographies, which must be adhered to.

5.8. Contacts with public authorities

The Secretary General and the Alliance's communication advisor implement a supervision plan regarding all contacts made in the name of the Alliance with public authorities, for the purpose of ensuring that lobbying regulations are complied with. Relevant lobbying regulations are currently to be found mostly in the European Union institutions and in France.

Lobbying is when the Alliance, directly or through a lobbyist, initiates a contact with a public authority, for the purpose of influencing a decision:

- The Alliance means any person speaking on its behalf. As provided above, no other person than the Chair may communicate in the name of the Alliance, if not as foreseen in an action approved by the Board. Under French rules, a declaration threshold is reached when a given person has at least 10 such contacts with a French public authority over 12 months;
- Initiative means that the contact derives from a step taken by the Alliance, as opposed to a specific request from the public authority. Any such step is to be formally decided by the Alliance. However, any person who would find his/herself unexpectedly in contact with a public authority while representing the Alliance should report to the Secretary General and the Alliance's communication advisor;
- A contact means a letter, e-mail, call or face-to-face meeting. Each occurrence counts for one contact, unless it may be bundled with series of identical contacts for the same purpose: contact made simultaneously with several public authorities for the same purpose; preparation and immediate follow-up of a contact with a given person;
- Public authorities mean, in the European Union institutions, the Commission and Parliament; in France, mostly members of the Government and their advisors, and members of the Parliament and their advisors (a list set to expand);

- A decision means mostly acts of Parliament and administrative regulations but extends to “other administrative decisions” (agreements, authorisations…). This is not the case when the contact merely aims at providing general information. Any person who would find his/herself in contact with a public authority while representing the Alliance should keep to such general information unless he/she has been formally charged with conveying a specific message.

When the Alliance decides to take actions that may fall within the definition of lobbying, the Secretary General and the Alliance’s communication advisor analyse the situation in advance. Depending of the case at hand, they may suggest steps and guidance so that there would be no confusion with lobbying; or inform the Board that pre-emptive or follow-up steps have or may have to be taken. They debrief contacts to check any necessary adaptations to anticipated steps.

When external consultants are recruited by the Alliance, the Secretary General and the Alliance’s communication advisor ask these consultants to confirm that they have or will take, the relevant compliance steps.

6. Annex 6: Data Protection

SIA's mission is to support the provision of legal, trusted identity for all and drive the development of inclusive digital services necessary for sustainable, worldwide economic growth and prosperity. In doing so, SIA may process personal data. This Annex explains how we and our Members and Affiliated members handle personal data.

This Annex consists of :

- **Our data processing charter:** all Member and Affiliated members must abide by the data protection rules set forth in our data processing charter.
- **Our data processing agreement:** when we process personal data on your behalf in our capacity as data processor, the clauses of our data processing agreement apply.
- **Our privacy policy:** when we process personal data of data subjects in our capacity as data controller, the clauses of our privacy policy apply.
- **Our cookie policy:** when we place cookies or use similar technologies, the clauses of our cookie policy apply. Please refer to our website for the latest cookie policy.

6.1. Data processing charter

6.1.1. Purpose

The purpose of this charter is to establish a common set of minimum standards with regard to the processing, sharing and transfer of personal data, i.e. data relating to an identified or identifiable natural person (data subject).

It is acknowledged and agreed that this charter applies to the processing of personal data by a (Affiliated) Member.

6.1.2. Data protection principles

Each (Affiliated) Member shall comply with its obligations under applicable data protection legislation. In any case, any processing must be fair, transparent and lawful. This means, in particular, that data subjects should always be informed about the essential aspects of the processing of their personal data, including at least the contact details of the data controller, the categories of personal data, the purposes, the legal basis, the security measures and the rights they have as a data subject and how to exercise them. Where applicable, the data subject shall also be informed of the administrative authority enforcing the data protection legislation.

6.1.3. Legal basis

It is the common intention and understanding that each (Affiliated) Member shall act as a separate data controller in respect of any personal data for which it determines the purposes and the means.

As data controller, each (Affiliated) Member shall ensure that any processing of personal data for which it is responsible is based on a valid legal basis.

6.1.4. Subcontractors

If an (Affiliated) Member uses a subcontractor to process personal data, the (Affiliated) Member is responsible for selecting a reliable subcontractor with a good record of data protection compliance. In any case, and without prejudice to the obligations based on the applicable data protection law, the (Affiliated) Member shall enter into an appropriate agreement with the subcontractor which clearly defines the mandate of the subcontractor in relation to the processing of personal data on the instructions of the (Affiliated) Member and which reflects any specific language that may be required under applicable data protection law.

6.1.5. Data protection assessments

Each (Affiliated) Member agrees that if it intends to start a new processing activity, it will first assess the potential risks involved. If this assessment demonstrates that the intended processing activity entails significant risks to the rights and freedoms of data subjects, the (Affiliated) Member intending to start such processing activity shall document the potential risks and the mitigation measures taken to reduce the risks to an acceptable level. The level of a risk is determined by its probability and its possible impact on the rights and freedoms of individuals.

6.1.6. Record of processing activities

Each (Affiliated) Member shall keep a register of the processing activities it carries out. This register enables the (Affiliated) Member to have a global and structured overview of the personal data processed within the organisation, including its purposes, legal basis and whether the personal data is shared with subcontractors or other third parties. If applicable data protection legislation requires a more comprehensive register, the (Affiliated) Member will comply with it.

The (Affiliated) Member shall organise itself in such a way that the register is updated periodically.

6.1.7. Security and breaches

Each (Affiliated) Member agrees that it shall implement appropriate technical and organisational measures, in particular against viruses and theft, unauthorised copying, accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, especially where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation.

If an (Affiliated) Member suspects that any of the security measures have failed, or that a security incident has occurred, the (Affiliated) Member will immediately and thoroughly investigate the incident and take measures if necessary or useful to ensure that the security incident cannot occur again in the future. If there is an obligation to report under applicable data protection law, the (Affiliated) Member will comply with this reporting obligation in a timely manner. The (Affiliated) Member shall also establish a clear internal information security procedure.

6.1.8. Confidentiality and sharing

Each (Affiliated) Member shall treat personal data in the strictest confidence This means that, in principle, personal data are only shared with third parties if this is strictly necessary for the fulfilment of a legitimate processing activity about which the data subject has been informed or if this is necessary to fulfil a legal obligation.

Personal data may be processed by staff members of the (Affiliated) Member on a need-to-know basis. This means that the (Affiliated) Member shall put in place measures to ensure that staff members only have access to those personal data which are necessary for the performance of their professional tasks.

6.1.9. International data transfers

In the event that personal data are processed, shared, or transferred in an international context under the responsibility of an (Affiliated) Member as a data controller, that data controller shall determine all the data protection laws applicable to the processing, sharing or transfer of such personal data, and it shall fully comply with the provisions of such data protection laws. If more than one data protection law is applicable simultaneously, the data controller will take the necessary measures to comply with the provisions of each applicable data protection law.

(Affiliated) Members that have their head office in the EEA prefer not to transfer personal data outside the EEA if it is not strictly necessary for the purpose of processing that personal data. However, if they do transfer personal data outside the EEA, they will ensure that a valid protection mechanism for the international transfers of personal data is in place.

6.1.10. Data retention

The (Affiliated) Member will only keep personal data for a period of time necessary to achieve the purpose of the processing. Thereafter, the (Affiliated) Member will anonymise or delete the personal data, unless the applicable data protection law requires further storage.

6.1.11. Data subject rights

(Affiliated) Members shall always facilitate and respect the rights of data subjects as applicable under applicable data protection law.

Unless the applicable data protection legislation provides for stricter rules, an (Affiliated) Member who receives a request from a data subject in relation to the data subject's personal data shall respond and deal with that request as soon as possible and within one month of receipt of the request at the latest. Only in exceptional circumstances may this time limit be deviated from. In such a case, the data subject must be informed in writing of the reason(s) for the delay in processing the request.

6.1.12. Data protection management team

Each (Affiliated) Member shall organise itself internally in such a way that it can meet the obligations arising from the applicable data protection law and the obligations arising from this charter. This means that each (Affiliated) Member shall appoint at least one person (or a data protection management team) responsible for ensuring compliance with the data protection law and this charter within the organisation.

The (Affiliated) Member shall ensure that this person (or the data protection management team) can be reached via a functional e-mail address by SIA. This e-mail address will be communicated to SIA.

6.1.13. Compliance

The (Affiliated) Member must always be able to demonstrate compliance with this charter upon request by SIA.

Each (Affiliated) Member shall immediately notify SIA in writing of any event that could lead to that (Affiliated) Member being unable to comply with its obligations under this charter.

6.2. Our privacy policy

This Privacy Policy sets out how we collect, use, process and disclose your personal data when you:

- use our website (www.secureidentityalliance.org);
- use our social media;
- enter into an agreement with us or communicate with us in that context;
- register for or participate in our events; and
- communicate with us by email, phone or any other digital communication channel.

“We” in this Privacy Policy refers to: Secure Identity Alliance asbl [Company N° 0785 731 573 – Address: Boulevard Auguste Reyers 80, 1030 Schaerbeek]. We are responsible for the collection and use of your personal data in the manner explained in this Privacy Policy. If you have any questions, please contact us by e-mail: privacy@secureidentityalliance.org. In certain circumstances, third parties may (also) be responsible for the processing of your personal data. In that case, we recommend that you consult the privacy policies of these third parties.

We can change this privacy policy on our own initiative at any time. If material changes to this privacy policy may affect the processing of your personal data, we will communicate these changes to you in a way that we normally communicate with you (e.g. via e-mail or via a message on our website).

We invite you to read the latest version of this privacy policy on our website (www.secureidentityalliance.org).

6.3. Which personal data do we process and why?

We will only process your personal data for a specific purpose and to the extent permitted by law. We further explain below in which cases we collect and use your personal data. If we do not receive your personal data directly from you, we will also inform you of this below.

6.3.1. When you use our website or social media

When you use our website or use our contact form or other digital communication channel, we collect and use the following personal data.

What personal data?	Why?	Legal basis?
Technical information (e.g. server log files) about your visit and the device you use. We cannot identify you on the basis of this information, but third parties may be able to identify you (e.g. you internet service provider).	In order to ensure the most fault-free operation of our website and to detect and prevent malware, illegal content and conduct and other forms of potential abuse.	Our legitimate interest in keeping our online presence safe
Identity and contact details provided by you and the content of the message and the technical details of the message itself (e.g. date and time) .	To enable communication between you and us	Our legitimate interest in being able to respond to requests, questions, or comments or to contact you proactively for questions of any kind.
Your email address.	To send you our newsletter or other electronic communication.	Your consent unless you are an existing customer whom we wish to keep informed of our products or services.

6.3.2. When you conclude an agreement with us

When you or your employer is one of our service providers, or when you make use of or take part in providing our services (e.g. by participating in a Working group), we collect and use the following personal data.

What personal data?	Why?	Legal basis?
Identity information, contact details and business or professional information provided by you in the context of the agreement	To fulfil our contractual obligations, and if you are a customer, to provide our services, and to communicate with you in this context.	If you are our customer or supplier as an individual, we rely on the necessity of processing your personal data for the performance of the contract we have with you. However, when you act on behalf of a company or other legal entity, we rely on our legitimate interest in being able to contract with customers and suppliers
Identity and contact details provided by you within the framework of the agreement and, if applicable, your company and invoicing details.	To carry out our normal business administration (e.g. invoicing and relationship management).	Our legitimate interest in managing our business activities in a responsible and professional manner.

. .

6.3.3.When you participate in one of our events

When you register for or participate in our events, we collect and use the following personal data.

What personal data?	Why?	Legal basis?
Identity and contact details provided to you us in connection with, where applicable, your registration and participation in our events.	To process your registration and prepare, organize and secure our events.	Our agreement with you by your acceptance of the applicable terms and conditions.
Photos taken during an event on which you are clearly recognizable.	To capture and share ambience images of the event (e.g. on our website).	Your consent.

6.3.4. When you communicate with us

When you communicate with us via telephone, email, or any other digital communication channel, we collect and use the following personal data.

What personal data?	Why?	Legal basis?
Identity and contact details provided by you to us, the content of the communication, the technical details of the communication itself (e.g. date and time) and, if applicable, the device you used.	To enable communication between you and us (e.g., when you use our contact form or contact us via telephone or email).	Our legitimate interest in being able to respond to requests, questions or comments or to contact you proactively for questions of any kind.

6.3.5. In other cases

For all personal data that we collect in the above circumstances, we would like to make it clear that we will also process your personal data in the following cases.

What personal data?	Why?	Legal basis?
Above-mentioned personal data.	To comply with our legal obligations or to comply with any reasonable request from competent police authorities, judicial authorities, government institutions or bodies, including competent data protection authorities.	Our legal obligation.
Above-mentioned personal data.	To prevent, detect and combat fraud or other illegal or unauthorized activities.	Our legal obligation.
Above-mentioned personal data.	To defend ourselves in legal proceedings.	Our legitimate interest in entering into business transactions.
Above-mentioned personal data.	To inform a third party in the context of a possible merger with, acquisition of/by or demerger by that third party, even if that third party is located outside the EU.	Our legitimate interest in using your personal data in these proceedings.
If you are a director of SIA, we will process your identity and contact details, including your place and date of birth, address details and national registration number.	These data are necessary for registration in the CBE.	Our legal obligation.

6.4. With whom do we share your personal data?

In principle, we do not share your personal data with anyone other than the persons who work for us, as well as with the suppliers who help us process your personal data. Anyone who has access to your personal data will always be bound by strict legal or contractual obligations to keep your personal data safe and confidential. This means that only the following categories of recipients will receive your personal data:

- You;
- Your employer or business partners, but only when this is necessary for the purposes mentioned above (e.g. when your employer is our supplier or customer);
- Our employees, members of the Board, individuals of the Working group, or any individual acting under the authority of us;
- Our suppliers; and
- Government or judicial authorities to the extent that we are obliged to share your personal data with them (e.g. tax authorities, police, or judicial authorities).

We do not transfer your personal data outside the European Economic Area (EEA) (the European Economic Area consists of the EU, Liechtenstein, Norway, and Iceland). We will only transfer your personal data outside the EEA if you or your employer, as a customer or supplier, have offices outside the EEA with which we need to communicate. If a transfer were to take place, we will take sufficient safeguards to protect your personal data during the transfer (e.g. by entering into an agreement based on standard data protection clauses approved by the European Commission).

6.5. How long do we keep your personal data and how do we keep your personal data secure?

6.5.1. Data retention

Your personal data will only be processed for as long as necessary to achieve the purposes described above or, when we have asked you for your consent, until you withdraw your consent. In this article we provide you with the information you need to evaluate how long we will keep your personal data identifiable.

As a general rule, we will de-identify your personal data when it is no longer needed for the purposes described above or when the retention period, as explained in, has expired. However, we cannot delete your personal data if there is a legal or regulatory obligation or a court or administrative order preventing us from doing so.

We retain all personal data collected through our website for as long as necessary to protect the legitimate interests stated above or to perform our agreement with you or your employer.

All personal data we collect through our social media we retain as long as necessary to protect the legitimate interests stated above.

We will retain all personal data collected in connection with our events for as long as necessary to protect the legitimate interests stated above or until you withdraw your consent. If you wish to object to a published photo of you during an event, please let us know.

All personal data we collect through our interactions with you through social media, telephone, email, or other digital communication channels will be retained for as long as necessary to communicate with you, but also to maintain a historical record of our communications. This allows us to return to previous communications when you come back to us.

6.5.2. Security

The security and confidentiality of the personal data we process is very important to us. That is why we have taken measures to ensure that all personal data processed is kept secure. These measures include technical and organizational measures to protect our infrastructure, processes, systems, and applications.

6.6. Your rights and questions

You have certain rights related to the processing of your personal data: the right of access, rectification, erasure, and data portability as well as the right to object to or restrict the processing of your personal data and to withdraw your consent. More information about these rights and how to exercise them, can be found on our website. To exercise one of your rights, you can submit a written request to privacy@secureidentityalliance.org stating the right to which your request relates. For security reasons, we may request proof of your identity. If you are still dissatisfied, you have the right to contact the competent data protection authority.

Should you have any further questions about the processing of your personal data, please do not hesitate to contact our data protection manager. You can contact our data protection manager by e-mail: privacy@secureidentityalliance.org .

6.6.1. Cookie policy

When you visit our website, we use cookies or similar technologies. We will inform you of this as soon as you visit our website and ask your consent if necessary.

7. Annex 7: Diversity & Equality Policy

As an association of organisations, the Secure Identity Alliance encourages its Members and Affiliated members to devise and implement internal policies for the respect of diversity and for equality.

These policies should cover the internal organisation of Members and Affiliated members, as well as their impact on societies as responsible stakeholders.

These policies should be comprehensive and address, notably, discriminations between men and women, or on a religious, ethnical, sexual or national basis. They should aim, notably, at:

- Promoting the recruitment of women and their access to senior levels of responsibility.
- Devising awareness programs to be delivered to staff members.
- Enforcing effective mechanisms for people denouncing a discrimination to have their claims heard and investigated.
- Providing adequate and timely answers to actual discrimination cases, depending on the nature of the discrimination.
- Explaining these policies and their outcomes in corporate communication documents.

The Secure Identity Alliance believes that respect of diversity and equality are key factors to further innovative and successful initiatives. They are both one of the conditions and one of the goals of e-identity programs.

8. Annex 8: Charter of Intellectual Property Rights

Secure Identity Alliance (SIA)

Version 1 – 31st May 2022

8.1. Introduction / Purpose

8.1.1.

The purpose of this Charter of Intellectual Property Rights (the "IPR Charter") is to support the protection of intellectual property while achieving compliance with the goals of the Secure Identity Alliance (the "SIA") to foster awareness, openness, and competition in the identity management / eGovernment market, to the benefit of the public authorities and the general public.

8.1.2.

The IPR Charter notably seeks to reduce the risk that investment in the preparation, adoption and application of standards and specifications by the SIA, if any, could be lost as a result of an Essential IPR for a standard or specification being unavailable. The IPR Charter therefore seeks to balance the needs of standardization, if any, with the rights of IPR holders.

8.1.3.

IPR holders should be adequately and fairly rewarded for the use of their IPRs in the implementation of standards and specifications.

8.2. Definitions

8.2.1.

Capitalized terms used in this IPR Charter shall have the meaning set forth in the SIA's Articles of Association and Internal Rules (as amended from time to time).

8.2.2.

In addition, the capitalised terms listed below shall have the following meaning:

- **"Copyright"** means any copyright in a standard or specification or any other document, including copyright in software, written, created, designed, or developed by a Member or any of its directors, officers, or employees either individually or jointly within a Working Group or any other working structure of the SIA or as a result of any work carried out on behalf of such Working Group or structure;

- **"Equipment"** means any system or device conforming to a standard or specification;

- **"Essential"** when used in relation to IPR means that it is not possible, taking into account normal technical practice and the state of the art generally available at the time of definition of a standard or specification, to implement that standard or specification, and in particular to manufacture, sell, lease, otherwise convey or make available, repair, use or operate Equipment or Methods which comply with a standard or specification without infringing that IPR, unless the right to use that IPR is granted. For the avoidance of doubt, in exceptional cases where a standard or specification can only be implemented by certain technical solutions, all of which would cause infringements of IPRs, all such IPRs shall be considered Essential;

- **"IPR"** shall mean any intellectual property right conferred by law, such as patents, copyrights, copyrights in software code, design rights, utility models, trademarks, service marks, trade secrets, know-how, database rights and other rights in the nature of intellectual property rights (whether registered or not) including pending applications for such rights;

- **"Manufacture"** means production of Equipment;

- **"Method"** means any method or operation conforming to a standard or specification;

- **"IPR Charter"** means this SIA's Intellectual Property Rights policy;

- **"Secure Identity Alliance Document"** means any document written, created, designed, or developed by a Member or any of its directors, officers, or employees either individually or

jointly within a Working Group or any other working structure of the SIA or as a result of any work carried out on behalf of such Working Group or structure and identified as a document of the SIA.

8.3. Disclosure of Essential IPR

8.3.1.

Each Member shall inform the SIA of Essential IPRs known to it, including known pending applications, either of itself or of any other organization, that may fully or partially cover elements of standards or specifications that are being developed by a Working Group or any other working structure of the SIA, as early as possible in the process and at least prior to such standards or specifications being submitted to a voting procedure.

8.3.2.

The information referred to in Clause 8.3.1 shall be provided to the Secretary general of the SIA according to the IPR Information Statement, attached in the annexed Schedule.

8.3.3.

In the event that a Member intentionally omits to declare Essential IPRs with respect to a given standard or specification, the Member shall be deemed to have forfeited its right to withhold a perpetual license on fair, reasonable and non-discriminatory conditions from anyone who desires to implement the said standard or specification. In addition, the Board may decide to terminate the Member's membership of the SIA.

8.3.4.

For the avoidance of doubt, the obligations set forth in Clause 8.3.1 must be fulfilled in good faith and on a best-efforts basis, but do not imply an obligation on a Member to conduct IPR searches.

8.3.5.

In the event that a Member informs the SIA of any Essential IPR of a third party, the SIA Secretary general will contact the third party IPR holder and will request the submission and the confirmation as set forth in clauses 8.3.2 and 8.4.1. respectively.

8.4. Licensing Declaration

8.4.1.

When an IPR that is an Essential IPR with respect to a standard or specification that is being developed by a Working Group or any other working structure of the SIA is brought to the attention of the Secretary General, the latter shall immediately request the relevant IPR holder to give, within three months, a written confirmation that it is prepared to grant perpetual (for the life of the IPR in

question), worldwide licenses to such Essential IPR on fair, reasonable and non-discriminatory conditions to each Member of the SIA and any third party applying for such license. Such license will remain valid regardless of changes in the Member's membership in SIA.

8.4.2.

The written confirmation to license referred in Clause 8.4.1 shall cover the use of the Essential IPRs to at least the following extent:

- Manufacture, including the right to make or have made customised components and sub-systems to the licensee's own design for use in Manufacture;
- Sell, lease, or otherwise convey or make available any Equipment so Manufactured;
- Repair, use, or operate Equipment;
- Use Methods.

8.4.3.

The written confirmation referred to in Clause 8.4.1 shall be provided to the Secretary general according to the IPR Licensing Declaration, attached in the annexed Schedule.

8.4.4.

Notwithstanding Clause 8.4.1, a Member shall have no obligation to license third parties pursuant to Clause 8.4.1 in cases where a third party has obtained the standard or specification in violation of the confidentiality obligations of a Member.

8.4.5.

The Essential IPR holder's obligations under Clauses 8.4.1 to 8.4.4 are subject to the following conditions:

a) Any licensee or Equipment manufacturer shall agree to grant a licence of their Essential IPR in accordance with Clauses 8.4.1 and 8.4.2 on reciprocal terms and conditions, where applicable;
b) The portion of the licence that relates to a party to whom the licensee sells, leases, or otherwise conveys or provides Equipment can be terminated if that party refuses to grant a licence of its Essential IPR in accordance with Clauses 8.4.1 and 8.4.2 on reciprocal terms and conditions, where applicable;
c) The licensee will use its best efforts to notify Clause 8.4.5(b) to whomever it sells, leases, or otherwise conveys or provides Equipment.

8.4.6.

The Essential IPR holder who assigns the ownership of the Essential IPR which is subject to a Licensing Declaration to a third party, shall include appropriate provisions in the relevant

assignment documents to ensure that the Licensing Declaration is binding on the transferee, and that the transferee will include similar provisions in the event of future assignments in order to bind and commit all successors in this respect.

8.5. Record of IPR Information Statements and Licensing Declarations

A record of the Essential IPR Information Statements and IPR Licensing Declarations shall be placed and retained in the files of the SIA and shall be accessible to Members and third parties with reasonable interest upon request.

8.6. Notice of Essential IPRs and Licensing Declarations

Any published standard or specification containing Essential IPRs shall refer to the claimed Essential IPRs as well as the IPR holders' licensing declarations.

8.7. Non-availability of Licensing Declaration

Where, prior to the publication of a standard or specification, an Essential IPR holder does not provide a Licensing Declaration in accordance with Clauses 8.4.1 and 8.4.2, the Secretary General shall, in consultation with the Board, suspend the adoption of the standard or specification until the matter has been resolved.

8.8. Call for IPRs

8.8.1.

Every Working Group meeting shall start with an oral "call for IPRs" by the Chair of the Working Group in order to remind the Members of their obligation to inform the SIA of Essential IPRs, including pending applications therefore, under Clause 8.3.

8.8.2.

If it becomes apparent that an IPR information statement or a licensing declaration is unlikely to be provided, the Chair of the Working Group (or other working structure of the SIA, as the case may be) shall inform the Secretary General, who will take the appropriate action in accordance with Clause 8.7.

8.8.3.

The Chair of the Working Group (or other working structure of the SIA, as the case may be) shall record in the minutes of each meeting that a call for IPRs was issued and the responses that were

received. For the avoidance of doubt, if there is no response, the absence of any response shall be recorded.

8.9. Copyrights

8.9.1.

Any copyright in a standard or specification, written, created, designed, or developed by a Member or any of its directors, officers or employees either individually or jointly within a Working Group or any other working structure of the SIA, or as a result of any work carried out on behalf of such Working Group or structure (the "Copyright") will exclusively belong to and automatically and royalty free vest in the SIA to the extent possible.

Insofar assignment of Copyright would not be validly possible, a Member grants to the SIA a perpetual (for the duration of the applicable copyright), worldwide, non-exclusive, no-charge, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, sublicense, and distribute, any standard or specification to the full extent of the Member's copyright interest in the Member's contribution to that standard or specification.

8.9.2.

Any copyright in any Secure Identity Alliance Document will belong to and automatically and royalty free vest in the SIA to the extent possible.

Insofar transfer of copyright would not be validly possible, a Member grants to the SIA a perpetual (for the duration of the applicable copyright), worldwide, non-exclusive, no-charge, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, sublicense, and distribute, any Secure Identity Alliance Document to the full extent of the Member's copyright interest in the Member's contribution to that Secure Identity Alliance Document.

8.9.3.

A Member shall not have the right to distribute, transmit, broadcast, communicate or make available the standards or specifications or Secure Identity Alliance Documents to parties other than its internal units or associates, without prejudice however to more specific SIA policies that would provide deviating rules in respect hereto.

8.9.4.

The copyright in all documents, literature and material owned by the Member which are not Secure Identity Alliance documents, or standards or specifications, or do not form part of a standard or specification and which are submitted by it to any Working Group or other working structure of the SIA, or to the Board, General Meeting, Chair or Secretary General of the SIA, shall remain vested in the Member and the following terms shall apply to such material:

a) The SIA shall have a non-exclusive, royalty-free licence to use (including the right to sub-license) such copyright material for the purposes of work carried out in the development of

standard or specifications unless the Member notifies the SIA, at the time of submission, that the copyright material is not licensable to the SIA;

b) The Member shall grant a non-exclusive, royalty-free licence to all other Members of the SIA on request to use such copyright for the purposes of work carried out in the development of a standard or specification;

c) The Member agrees to mark all such documents, literature, and material clearly with an appropriate copyright notice.

8.9.5.

A Member will do all acts and execute all documents or instruments and perform all formalities as are necessary to validly vest the copyright in a standard or specification or the copyright in a Secure Identity Alliance document in the SIA and in the meantime will hold all interest in the same in trust for the SIA.

8.9.6.

A Member shall not denigrate the integrity of the Copyright or the copyright in a Secure Identity Alliance document by (but without limitation) either removing the copyright notice contained thereon, varying or removing its title, or using all or any part of it as part of a specification or standard not emanating from the SIA and in any event it shall not publish nor disclose the standard or specification to any third party until the standard or specification is published by the SIA by posting the same on the SIA's website.

8.9.7.

A Member will promptly notify the SIA of any threatened or actual infringement of the Copyright or of the copyright in a Secure Identity Alliance document which comes to its notice and shall, at the SIA's request, do all such things as is reasonably necessary to assist in defending and enforcing the SIA's rights in the Copyright or such copyright.

8.10. Ownership of IPR jointly created by Members within the SIA

8.10.1.

Subject to Clauses 8.9.1 and 8.9.2 any IPR created jointly by two or more Members of the SIA within a Working Group or any other working structure of the SIA or as a result of any work carried out on behalf of such Working Group or structure shall be owned by such Members and licensed to the other Members in accordance with the provisions of Clauses 8.9.4, 8.4.1 and 8.4.2.

8.10.2.

The Members owning such IPR shall jointly make and share equally the cost of any applications for patent or other registration of the IPR.

8.10.3.

In case a joint owner refuses to share the costs or reasonably assist in applying for a patent or other registration of the IPR within 30 days of a written request to do so, the other owner(s) shall have the right to apply for a patent or other registration in its (their) name and account and shall own all rights to such registration.

8.10.4.

A joint owner refusing to share the costs or to reasonably participate in applying for a patent shall execute all such documentation and assignments that are reasonably necessary for the other joint owner(s) to apply for a registration.

8.11. Open standards and specifications

The SIA aims to promote innovation and interoperability via open standards, specifications, and technical frameworks to guarantee a level playing field for all market players in the ID ecosystem.

The SIA aims to develop open standards and technical frameworks to meet these objectives. Similarly, the SIA aims to contribute valuable input to national, regional, or international standards organizations.

The procedures within the SIA and its Working Groups will ensure that the development of the standards and specifications is a balanced, inclusive, and collaborative process, and that the publication is publicly available to interested implementers, market players and organizations, but controlled by the SIA in order to safeguard the quality and unambiguous origin of the standards and specifications. The SIA's IPR Charter shall ensure that the implementation of standards and specifications can be done by market players under reasonable and non-discriminatory conditions. Furthermore, the SIA may issue specific IPR charters applicable to specific Working Groups, in the framework of open standards and specifications, that will focus on specific issues and concerns in this respect, and which will prevail on this IPR Charter in case of conflicting provisions.

The Copyright in standards and specifications shall vest exclusively in the SIA as stated in clause 8.9.1.

The SIA grants worldwide licenses under fair, reasonable, and non-discriminatory conditions to interested market players to implement the standards and specifications in order to manufacture, sell, lease, convey, make available, operate, and use Equipment and Methods conforming to the standards and specifications.

The SIA grants worldwide licenses under fair, reasonable, and non-discriminatory conditions to standardization organizations, their member states and members, permitting them to copy and distribute its standards and specifications, and to incorporate and refer to its standards and specifications for standardization-related purposes, including the development and publication of recommendations and standards.

8.12. Copyrights in software code

In case a standard or specification includes programming code, the SIA will grant a royalty-free, non-exclusive, worldwide, sub-licensable copyright to reproduce, prepare derivative works of the software (including translations, adaptations, and alterations), to display, distribute and execute the contributed software for the following purposes:

- To a standardisation organisation and its members to evaluate the software and any derivative works thereof in order to determine whether to support the inclusion of the software code in any standard or recommendation, and to publish the software code in the standard or recommendation;
- To any organisation or market player implementing the standard or specification, to evaluate the software code and any derivative works thereof for inclusion in their own implementation of the standard or specification and to test whether its implementation conforms to the standard or specification.

In case a market player or organisation, that wants to implement the standard or specification, wants to include the software programming code in its own implementation, such as, without limitation, manufactured Equipment, the SIA shall grant a copyright license for such inclusion, under fair, reasonable, and non-discriminatory terms and conditions.

The SIA may issue specific policies in relation to specific software code, which may deviate from this Clause 8.12. Such specific policies may provide more extensive rights to third parties in relation to software code and will not be more restrictive than this Clause 8.12.

8.13. Marks

The SIA will grant a royalty-free license to standardisation organizations and other third parties, granting permission to use the trade names, trademarks, service marks, or product names of the SIA, as required for reasonable and customary use to describe or reference the origin of certain standards or specifications or other Secure Identity Alliance Document.

The Working Groups and any other entity within the SIA will act with due care whenever trademarks, service marks, trade names and similar denominations of third parties (in general “Marks”) are included or referenced within standards, specifications, or any other Secure Identity Alliance Document. Under certain circumstances it may be required to obtain a license to be able to use a Mark in a published document.

The SIA should avoid publishing any document where Marks of third parties are displayed as a graphic logo, rather than the use of the Mark as a simple word. Any intended display of a logo must be notified to the Secretary General, who may seek legal advice on such use or examine whether a license has been obtained.

The SIA must avoid any endorsement of a proprietary product or service that is referred to through its Mark, even if it is used as a word and not as a logo. It is allowed to use a Mark in a descriptive, neutral way, e.g. when it is important to state that a product, service, standard, certification etc. is compatible with a product, process, or service of the SIA. This is in particular allowed when reference is made to standards including the marks ISO, ETSI etc., or standardised technology

such as Bluetooth technology. In such case it will be important to refer to the Mark as a reference to the source of a certain product, technology, service or process, without creating any confusion about the ownership of the product, technology, service or process, and without explicitly endorsing or favouring it. Thus, it is important to refer to the Mark always in combination with a noun (such as “service”, “technology”, “infrastructure”, “protocol” etc.). E.g. it would be correct to state that a process is compatible with “Bluetooth technology”, but it would not be correct to simply refer to “Bluetooth”. Furthermore, Marks should always be cited as a single reference, and not in combination with other Marks, and Marks should always be written in full, not in an abbreviated manner.

Sometimes it is important to add the ® or ™ symbol to a referenced Mark.

In case any doubt arises when a Working Group or any other entity within the SIA intends to include a Mark in any standard, specification, or other Secure Identity Alliance Document, it is important to ask the Secretary General for advice on the matter.

8.14. Representations, Warranties and Disclaimers

Each Member represents and warrants that it is legally entitled to grant the rights and promises set forth in this IPR Charter.

Any standard and specification is provided “as is”. To the extent possible, each Member expressly disclaims any warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to a standard or specification. The risk of implementing or using a standard or specification is assumed by the implementer and user.

8.15. Law and Regulation

The obligations contained in this IPR Charter will be construed and interpreted in accordance with Belgian law.

8.16. Affiliated Members

For avoidance of all doubts, the obligations of Members in this IPR Charter are applicable to Affiliated Members.

Schedule to Annex 8 – IPR Information Statement and Licensing Declaration Form

IPR Licensing Declaration

IPR Holder/Organisation

Legal Name: _____

Signatory

Name: _____

Position: _____

Department: _____

Address: _____

Tel: _____

E-mail: _____

IPR Licensing Declaration

Secure Identity Alliance has been informed that the above designated person or Organization is the proprietor of the IPRs listed in the attached IPR Licensing Declaration schedule and that these IPRs may be considered Essential IPR with reference to the following Secure Identity Alliance standard or specification:

The Signatory hereby declares that the above designated person or Organization is willing to grant perpetual licenses under the Essential IPRs to an unrestricted number of applicants, worldwide, on fair, reasonable and non-discriminatory terms and conditions in accordance with Clauses 8.4.1 and 8.4.2 of the Secure Identity Alliance IPR Charter, in respect of the standard or specification, to the extent that the IPRs remain Essential.

This undertaking is made subject to the condition that those who seek licenses agree to reciprocate same in respect of the standard or specification in accordance with Clause 8.4.5 of the Secure Identity Alliance IPR Charter (delete this paragraph if this condition is not required).

The Signatory declares that the above designated person or Organization, in case it will assign the ownership of Essential IPR which is subject to the IPR Licensing Declaration to a third party, shall include appropriate provisions in the relevant assignment documents to ensure that the IPR Licensing Declaration is binding on the transferee, and that the transferee will include similar provisions in the event of future assignments in order to bind and commit all successors in this respect.

The construction, validity and performance of this statement shall be governed by the laws of Belgium.

Place, Date: **Signature:**

_____ _____

(Place, Date) (Signed for and on behalf of the SIGNATORY)

Please return this form duly signed to: Secure Identity Alliance Secretary general

Postal address: Secure Identity Alliance – Bluepoint - Boulevard August Reyers 80, 1030 Schaerbeck or contact form at www.secureidentityalliance.org

IPR Licensing Declaration Schedule

Secure Identity Alliance standard or specification				IPR Proprietor	Application No.	IPR	Country of Registration	OPTIONAL INFORMATION : Other IPRs/Application No. In same family*	
Project	Standard or specification	Illustrative specific part of the standard or specification (e.g. section)	Version					Patent/ Application No.	Country Applicable

9. Annex 9: CHARTER for the development of a set of Open Standards Application

Secure Identity Alliance (SIA)

Version 1 – 31st May 2022

This Charter applies to the OSIA Working Group (it does not apply to any other Working Group of the SIA).

9.1. Introduction / Purpose

The purpose of this Charter (the "OSIA Charter") is to set the principles of support by the Secure Identity Alliance (the "SIA") for the development of a set of Open Standards Application Programming Interfaces ("APIs") for the interoperability and sustainability of ID systems while achieving compliance with the goals of the SIA to foster awareness, openness, and competition in the identity management / eGovernment market, to the benefit of the public authorities and the general public.

This Charter applies to the OSIA Working Group (It does not apply to any other Working Group of the Secure Identity Alliance). This Charter is a specific IPR Charter as is meant in clause 8.11 of the (general) IPR Charter of the SIA (Annex 8 of the Internal Rules of the SIA). The provisions of the general IPR Charter apply to the OSIA Working Group unless there are conflicting provisions in this Annex 9.

Collaborative, open standard development implies a waiver of intellectual property rights in the sense that the SIA Member (as well as Affiliated member), shall have no right to claim for a reward when a third party will implement an open standard and will manufacture equipment or use a method using the SIA Member's Contributions.

This charter seeks to make SIA Members aware of this principle. It implies the adoption of an open and collaborative culture at the opposite of the proprietary one.

9.2. Definitions

Capitalized terms used in this Charter shall have the meaning set forth in the SIA's Articles of Association and Internal Rules (as amended from time to time).

In addition, the capitalized terms listed below shall have the following meaning:

- **"IPR"** shall mean any intellectual property right conferred by law, including copyright;
- **"Contribution"**: any work of authorship made by a SIA Member or any third party, jointly or separately, intentionally submitted to the OSIA Working Group for inclusion in the Project;
- **"Forge":** The platform used to manage, coordinate, lead, promote and track the Project;
- **"Input"**: any Contribution in the Project, deposited in the Space;
- **"Space"**: the area dedicated to the OSIA Project, managed by the SIA, on the "Forge";
- **"OSIA Charter"** means this SIA's Intellectual Property Rights policy dedicated to the OSIA Working Group;
- **"OSIA License"** refers to the license undertaking set forth in the annexed schedule;
- **"Project":** The Project identified and promoted by SIA, with the given name "OSIA" ("Open Standards Identity APIs"), and with a dedicated Space on the Forge, managed by SIA. "OSIA" or "Project OSIA" refers to the Project and vice-versa. The OSIA Project is limited to APIs development. An API is an Application Programming Interface defined as a standardized set of classes, methods, functions and constants that serves as a front end through which one piece of software provides services to, and communicates with, other pieces of software.

9.3. Status of the Contributions

In order to participate in the Project each SIA Member shall be bound by the OSIA License terms set forth in the annexed Schedule (hereafter referred as the "OSIA License"), evidencing it is aware of the licensing terms applying to its Contributions.

As a rule, any participation in the OSIA Working Group shall presume that the Member or any invited third party has accepted the said OSIA License and has no IPR or other rights to claim in this regard.

At the beginning of each meeting of the OSIA Working Group, the Chair of the OSIA Working Group will make it clear to all participants that the meeting is dedicated to the OSIA Project and that they shall not be entitled to claim any rights about the Contribution they bring in the Working Group, and that their participation implies they have understood and accept that the Working Group is dedicated to the OSIA Project, and to APIs development, and that they waive to claim the contrary. The Call for IPRs, mentioned in clause 8.8.1. of the IPR Charter, will apply.

Any third party that may access the publicly available Space is entitled to download the OSIA documents and works, including text and/or software code in object code or source code format, including the Contributions therein, and to use these materials in conformity with the OSIA License. Such third party is entitled to submit proposed Contributions to the OSIA Working Group. Proposed Contributions of SIA Members and third parties will only be incorporated in works published by the SIA after their approval by the OSIA Working Group in conformity with the applicable procedures.

For the avoidance of doubt, the obligations set forth in Clause 9.3.1 do not imply an obligation of a Member to conduct IPR searches, nor an obligation of SIA to adopt a Contribution.

9.4. Licensing

SIA collects the suggested Contributions of SIA Members and third parties through the OSIA Working Group, and in conformity with the applicable decision-making procedures it may decide to publish them, or not, in the Space, as an Input in the Project.

SIA Members and third parties, when they submit or develop their Contributions (individually or jointly) to / within the OSIA Working Group, license their Contributions under the OSIA License set forth in the annexed schedule and to SIA, and the related IPR will belong to and vest in SIA, without further conditions, AND, in all cases:

- Allow SIA to publish these Contributions in the Space under the sole SIA name;
- Shall not publish these Contributions in the Space or elsewhere without mentioning SIA's exclusive titularity (by a clear mention "©Secure Identity Alliance / Year") and shall refrain to publish these Contributions other than in the Space. SIA shall be further entitled to add this said mention, unilaterally and directly to any Contribution.

9.5. Law and Regulation

The obligations contained in this Charter will be construed and interpreted in accordance with Belgian law.

9.6. Members and other contributors

The obligations of Members in this Charter apply to Affiliated members and any other invited persons, who shall execute a binding agreement before participating in the work of SIA, as well as any third party contributing under the OSIA Licence.

10. SCHEDULE TO ANNEX 9 –OSIA License

Secure Identity Alliance (SIA)

Version 1.0, 31st May 2022

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

10.1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, modification, and distribution stated in this document.

"Licensor" or “SIA” or “Secure Identity Alliance” shall mean the copyright owner that is granting the License.

"You" (or "Your") shall mean an individual or legal entity exercising permissions granted by this License.

"Work" or “Project” shall mean the work of authorship, including where applicable text, software programming code in object code and/or source code and its documentation, drawings, schemas, figures, and other creations, created in the framework of the OSIA Working Group of the SIA, that is made available under the License, as indicated by a copyright notice that is included in or attached to the Work.

"Derivative Works" shall mean any work, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is by its author or copyright holder intentionally submitted to Licensor for inclusion in the Work. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work.

"Contributor" shall mean any individual or legal entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

10.2. Grant of copyright License.

This License is applicable to works of authorship created in the framework of the OSIA Working Group that are published as a Work with a reference or link to this License.

By using and/or copying the Work that includes a reference to this License or to which this License is linked, You agree that you have read, understood, and will comply with the terms and conditions of this License.

10.3. License to reproduce and distribute the unmodified Work.

Subject to the terms and conditions of this License, the Licensor and each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, evaluate, test, reference, implement, display and distribute the unmodified Work, in any medium and for any purpose, provided that You include the following on all the copies of the Work or the portions of the Work that you copy and/or distribute:

- A link or URL to the original Work, clearly visible to any recipient;
- The copyright notice of the Licensor, indicating the SIA as the original copyright owner, in the form: “Copyright © Secure Identity Alliance (2022)”;
- A copy of this License or a link or URL to this License, clearly visible to any recipient.

You must include the copyright notice in any documents, software or any other items or products that you create pursuant to the implementation of the contents of the Work or any portion thereof.

10.4. Modifications.

The Licensor does not grant You the right to create modifications of the Work or Derivative Works pursuant to this License, except as follows.

Solely in order to facilitate, evaluate or test the implementation of the technical specifications set forth in the Work, You may create and distribute Derivative Works in software and in methods, in documentation of software and methods and in supporting materials accompanying software and methods, provided that all such Derivative Works include the following notices:

NOTICE OF ANY CHANGES OR MODIFICATIONS TO THE WORK ;

The following copyright statement:

“Copyright © (the name of Your organization) (year)

This software or document includes material copied from or derived from [title and URL of the Work]

Copyright © Secure Identity Alliance (2022)”

However, the publication, display, or distribution of Derivative Works for use as a technical standard or specification, or any representation thereof as a technical specification, is expressly prohibited unless such use is expressly allowed by the Licensor to You in writing.

10.5. Distribution of Derivative Works.

You may reproduce, display and distribute copies of the Work and/or Derivative Works thereof (which are allowed in accordance with clause 4), in any medium, provided that You meet the following conditions:

- You must give any recipients of the Derivative Works a copy of this License, clearly visible to the recipient;
- You must cause any modified files to carry prominent notices stating that You changed the files of the Work.
- You must provide a link or URL to the original Work and the most recent version thereof, clearly visible to any recipient;
- You must provide the copyright notice as set forth in clause 4.

10.6. Submission of Contributions.

You may submit proposed Contributions to the Licensor for inclusion in the Work. By doing so, You intend to contribute to the further development of the Work.

Any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License. Any submitted Contributions may be included in the Work by Licensor after review and approval by Licensor in accordance with Licensor's policies and decision-making processes. Only Licensor is entitled to publish a modified version of the Work including Your Contributions, without prejudice to Your limited right to create modifications and Derivative Works as allowed under Clause 4.

You assign to the Licensor Your right, title, and interest, including Your rights under copyright, in Your Contributions, for all present and future forms of exploitation and use, and in all technological solutions, at no cost.

If and insofar transfer or assignment of Your rights is not validly possible, You hereby grant to the SIA, its Members and to recipients of the Work distributed by the SIA, a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, sublicense, and distribute Your Contributions and such Derivative Works. Furthermore, You grant a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable patent license to make, have made, use, sell, lease, or otherwise convey or make available the Work and implementations of the Work, including Your Contributions, where patent claims would be infringed by such use and/or such implementation. You declare that You will not use any patent claim nor any other intellectual property right to undermine the effect of such assignment.

You represent that you believe in good faith that Your Contributions are Your original creations and that You have sufficient right to submit these for inclusion in the Work.

10.7. Trademarks.

This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work.

10.8. Disclaimer of warranty.

Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

10.9. Limitation of liability.

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless and insofar required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall Licensor or any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if Licensor or such Contributor has been advised of the possibility of such damages.

10.10. Accepting warranty or additional liability.

While distributing the Work or (insofar allowed) Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License.

However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of Licensor or any other Contributor, and only if You agree to indemnify, defend, and hold Licensor and each Contributor harmless for any liability incurred by, or claims asserted against, Licensor and such Contributor by reason of Your accepting any such warranty or additional liability.

10.11. License versions.

The SIA is the publisher of this License and may publish revised and/or new versions of this License from time to time. Each version will be given a distinguishing version number. No one other has the right to modify this License.

10.12. Severability.

If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable.

10.13. Applicable law and jurisdiction.

This License shall be governed by the law of the jurisdiction specified in a notice contained within the Work, except to the extent that any applicable law provides otherwise. Any litigation relating to this License shall be subject to the jurisdiction of the courts of the jurisdiction and venue specified in a notice contained in the Work.

END OF TERMS AND CONDITIONS

www.secureidentityalliance.org