Privacy, Cybersecurity & Identity (PCI) Domain Working Group Charter

FINAL

Approved by the Oversight Committee August 23, 2023

1. Status and Change History

This charter is a proposal from the Privacy, Cybersecurity & Identity (PCI) Exploratory Group and approval from the Metaverse Standard Forum's Oversight Committee will ensure the status of the group becomes "The Working Group" for Privacy, Cybersecurity & Identity (PCI). The charter was approved on August 23, 2023 by the Metaverse Standards Forum Oversight Committee.

2. Officers and Processes

2.1 Working Group Officers

The Exploratory Group Chairs are:

1. Kathleen Moynahan - katmoynahan@microsoft.com
2. Louis Rosenberg - louis.rosenberg@responsiblemetaverse.org
3. Chad Wollen - chad@wearepea.co.uk

The Working Group will follow the standard election process as in section 3, of the Cohort Process Policy with a minimum of 3 and maximum of 4 elected co-chairs, with election balloting after at least three Working Group meetings so that Members can establish good standing, but before the sixth meeting.

2.2 Approval of Public Deliverables

As per section 6.4 of the Cohort Process Policy, the Working Group shall seek Oversight Committee Approval before releasing significant public updates or deliverables.

2.3 Internal Coordination

The Working Group will determine the frequency and cadence of meetings throughout various phases. Meeting agendas will be posted to its space within the Forum portal. After each meeting, the minutes and a recording of the meeting will also be posted. In addition to the meeting agendas, minutes, and recordings, the Working Group will provide a quarterly update and an annual report on its progress on key deliverables and initiatives to the Oversight Committee and, where appropriate, other Domain Working Groups. At the request of the Oversight Committee, specific review meetings can be arranged and updates can be provided to general Forum membership.

3. Motivation and Goals (and NON-Goals)

3.1 Background

The reason to primarily address the three key focus areas is that Privacy, Cybersecurity, and Identity are critical aspects of the Metaverse that impact trust, confidence, and credibility. In the Metaverse, humans, companies, and AI agents will interact with each other and with virtual entities, exchanging and inferring personal and sensitive information. This makes privacy and cybersecurity crucial for stakeholders to feel safe and confident in the ecosystem. The protection of personal data, control over data, transparency in data collection and usage, and interoperability standards will all contribute to building trust and confidence among stakeholders.

Furthermore, identity is also crucial in the Metaverse, as humans, companies, and AI agents will need to establish and verify their identities in order to participate in virtual transactions and interactions. A secure and reliable system for identity verification will not only protect humans from identity theft and fraud, but it will also increase the credibility of virtual transactions and interactions, and simplify the facilitation of their rights, fostering a more robust and trustworthy virtual society and economy. Ultimately, without strong privacy, cybersecurity, and identity measures in place, stakeholders may be hesitant to engage with the Metaverse, reducing its potential for growth and innovation.

3.2 Scope & Goals

The Working Group will focus on three key topics, i.e. privacy, cybersecurity, and identity, while following adjacent distinct but interconnected domains. We aim to influence the development of standards for the Metaverse by aligning the technical, legal, and human-centered discourses of each of these domains: social, technical, and regulatory. We want to consider both traditional and contemporary approaches to define these subject domains.

It is a priority to support the efforts of other working groups across the Forum and beyond by providing knowledge of existing systems, the gaps within, and advising on their particular use cases in a timely manner as changes may arise that impact these three PCI domain areas.

We realize this is an important and sensitive area, all messaging will be approved by the oversight committee and the board according to Forum policies etc etc .

Privacy

The protection of privacy (data protection) is crucial to building trust and promoting responsible Metaverse development. By promoting privacy as a key consideration in Metaverse development, adoption, and governance, the Working Group can help ensure that Metaverse stakeholders understand, design and implement privacy protections that are commensurate with the risks posed by the Metaverse environment.

The following activities are within the scope of Privacy in the context of the Metaverse:

1. **Landscape and Historical Analysis:** Conducting research to understand privacy risks in the Metaverse.
2. **Expert Presentations:** Inviting subject matter experts to educate on novel privacy approaches and support member outreach.
3. **Forum WG Collaboration and Use Case Study:** Establishing priority topics and use cases for privacy in the Metaverse through interviews with other Forum Groups and PCI WG members.
4. **Gap Analysis:** identifying gaps in privacy-enabling technologies, regulations, and user experiences that we can recommend being developed. At the heart of the gap analysis will be interoperability, in the context of our working group it means looking beyond just technical interoperability and understanding the convergences and divergences at a legal and policy level and how bridges can be built across different regulatory regimes with different laws and expectations of outcomes and impacts
5. **Privacy Protection Recommendations:** Research over the decades has shown the privacy or data protection requirements are left as an afterthought (as per Privacy by Design). This group will review scenarios, use cases, lifecycle frameworks and requirements from other Forum groups and relevant SDOs in order to ensure there is an early and constructive dialogue.

Cybersecurity

Cybersecurity is essential in the metaverse due to the numerous cyber threats that can compromise the safety and privacy of humans and systems. The success of the Metaverse depends on its ability to protect against various threats, including hacking, malware, and phishing attacks. The Metaverse involves various activities, such as online shopping, banking, and socializing, which all require the exchange of sensitive information. Without effective cybersecurity measures, the Metaverse could face serious risks and lose stakeholders' trust, ultimately undermining its growth and adoption.

Following are the top three activities within the scope of Cybersecurity in the context of the Metaverse:

1. **Creating Metaverse-specific security guidelines:** Map and align cybersecurity standards, frameworks, and best practices from other industries and domains with the scenarios, use cases and requirements of the Metaverse environment while accounting for Metaverse related risks, existing gaps and emerging threats.
2. **Collaboration and Information Sharing:** Collaboration and information sharing between different stakeholders in the Metaverse can help in identifying and mitigating cybersecurity threats. It is essential to promote communication and cooperation among different organizations, including Forum, service providers, stakeholders, and relevant standards bodies.
3. **Cybersecurity Awareness and Education:** Providing cybersecurity awareness and education to Metaverse users can help in preventing and mitigating cybersecurity threats. This includes educating individuals (especially vulnerable populations) on the risks associated with cyber threats, promoting good cybersecurity practices, and providing resources and tools to assist in securing their digital presence within the Metaverse.

Identity

Identity is critical to the Metaverse because it establishes trust and credibility for various purposes such as accessing restricted content, participating in virtual events, or the Identity and ownership within transactions, including establishing and attesting ownership for items such as virtual objects and digital currency. The various systems of Identity and Access Management (IAM), including centralized and decentralized approaches, need evaluation to ensure that individual identities are properly authenticated and protected to prevent fraud and maintain the integrity of the metaverse ecosystem. A secure and reliable system for identity verification will also increase the credibility of virtual transactions and interactions, fostering a more robust and trustworthy virtual economy while protecting stakeholders from identity theft and fraud.

Identity, in the context of privacy, is a foundational concept. The ability to identify - single out or distinguish one individual from others - is the *de facto* definition of personal data, in this respect there needs to be an understanding of any new - direct or indirect - means of identification in the metaverse (which can lead to new means of tracking or surveillance). In addition, an individual's control over their identity (to be known or unknown) is closely linked to important human rights which go beyond the right to privacy and the right to data protection, including the rights to dignity, autonomy, and (informational) self-determination. In the security and privacy domain, it is important to understand forms of anonymization or de-identification and raise awareness about ways in which Metaverse technologies and systems may aid re-identification (and so unlawful tracking or profiling or surveillance).

Identity does not just concern natural persons, legal persons - such as organizations that have legal incorporation - increasingly are joining identity systems to establish their credibility. Organizational identity can play a significant role in increasing the confidence between individuals and companies and between companies themselves.

In this respect, the scope of Identity in this workgroup is related to natural and legal persons, and where appropriate to the identity of natural and legal persons, it will include the identity of bots, AIs, goods, assets or the full range of virtual or digital objects as it is, for example, only natural and legal persons who can own such goods, assets, etc.

Following are the top four activities within the scope of Identity in the context of the Metaverse:

1. **Risk Analysis:** Conducting a risk analysis of various forms of identity implementation in the Metaverse environment to catalog potential risks and identify best practices for mitigating them.
2. **Collaboration and Information Sharing:** Convening multi-stakeholder international groups to share knowledge and expertise on the risks, benefits, and implementation strategies for identity in the context of the Metaverse, in order to develop a shared vision and understanding of identity governance and protection.
3. **Best Practice Recommendations**: This group will review scenarios, use cases and requirements from other Forum groups and relevant SDOs in order to ensure there is constructive dialogue regarding identity.
4. **Gap Analysis**: Here we will look at scenarios and use cases where the free flow of identities and data (and goods or services attached to those identities) needs to be supported by standards which take into account data protection/privacy and security requirements. At the heart of the gap analysis will be interoperability, in the context of our working group it means looking beyond just technical interoperability and understanding the convergences and divergences at a legal and policy level and how bridges can be built across different regulatory regimes with different laws and expectations of outcomes and impacts.

3.3 Adjacent Distinct but Interconnected Domains

The Exploratory Group has identified adjacent topics that are distinct and interconnected that often interact with the PCI as subjects. The group will monitor these important topics but not make them a primary focus:

1. Accessibility and Inclusion*
2. Digital Ethics*
3. Disinformation
4. Generative AI
5. Safeguarding
6. Trust and Safety
7. Child Safety
8. Community Standards
9. UI/UX Design
10. 3D Assets/Avatars*
11. Networking*

12. Blockchain

*Other Exploratory Groups and Working Groups are set up which might have the above topics as their central focus, so this Working Group will liaise and collaborate with them. Until that point, the Privacy, Cybersecurity and Identity Working Group will maintain a light-touch "watching brief".

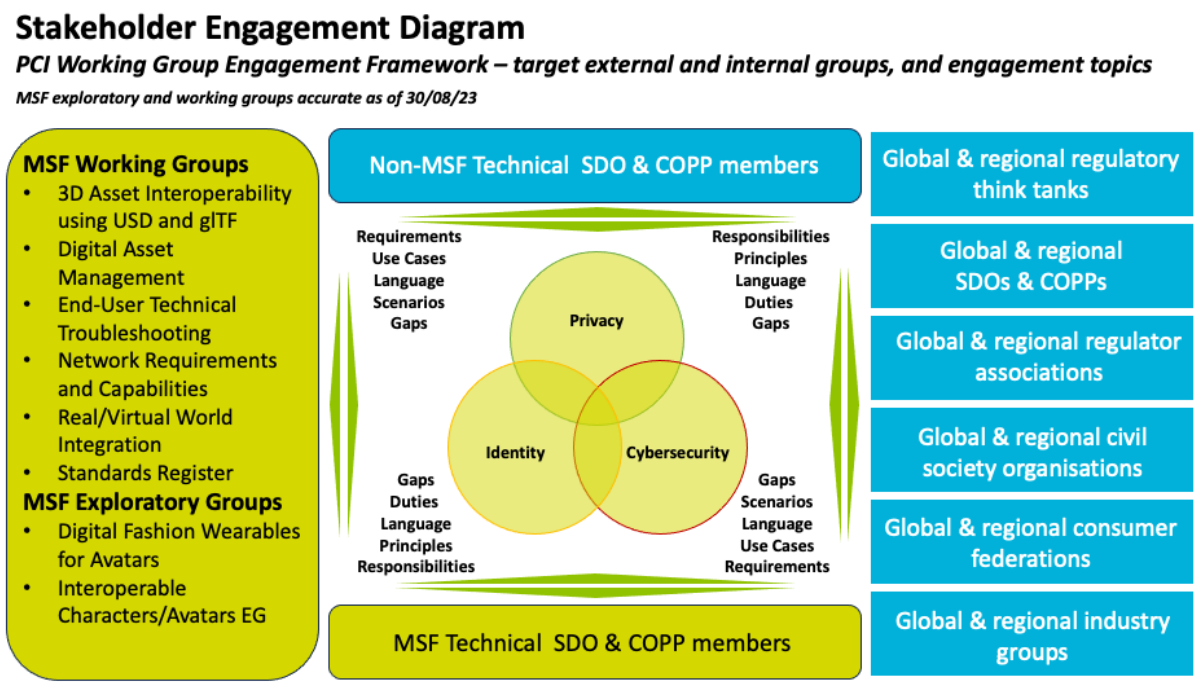
3.4 Out-of-scope Topics

The Exploratory Group purposely chooses not to go deeper into the adjacent, interconnected topics below, due to competing priorities, pre-established consensus, and to avoid scope creep:

1. Trustworthy computing (see references section for further context)
2. Trustworthy synthetic media
3. Advertising Standards
4. Digital Consumer Protection
5. Competition Policy
6. Content Standards
7. Creative Freedom
8. Virtual Economies
9. Physical Health & Product Safety

4. Stakeholder Engagement

The following chart will be used as a touchstone for developing detailed stakeholder collaboration and communication plans.



PCI Working Group Engagement Framework

5. Milestone Plan

We will follow a 6-phase roadmap: Discovery, Planning, Execution, Research & Analysis, Output & Delivery. During the Discovery phase, specialized task groups will be formed to develop domain expertise and leveraged to collaborate with and advise other working groups and sub-groups on their specific use cases and scenarios. The initially planned task groups are as follows:

1. Privacy Task Group at the PCI Working Group
2. Cybersecurity Task Group at the PCI Working Group
3. Identity Task Group at the PCI Working Group

The task groups will be assigned 6-12 months of working duration (renewable based on the outcome), within which the leads of each task group will work closely with the co-chairs of the PCI Working Group to stay aligned and execute the charter's agenda as appropriate.

Phase	Description	Milestone	Start	Duration
1	a. Set up 3 task groups, assign leads for each task group and establish the scope of execution for each task group b. Establish liaisons for connecting with SDOs to coordinate communications. c. Create social media and PR campaigns for creating awareness around PCI group's work and scope in collaboration with the Forum Marketing team. d. Finalize the ongoing list of Working Group Priority Topics and Use Cases based on the charter scope and agenda	Discovery	On Oversight Committee approval	T0+ 3, 3 months
2	a. Set up regular SME presentations and discussions to share organizational approaches to address the three key subjects in scope. b. Coordination with task group leaders to gather submissions from diverse organizations including non-Forum member orgs) on the unique approaches taken to address the respective domain use cases and challenges.	Planning		T0+ 9, 6 months
3	a. Identify, revise, and establish the scope of emerging sub-topics in coordination with the task groups b. Generate a consensual glossary for publishing by the Forum Registry Group c. Finalize task groups' collaboration and communication plan for the year 2024 (subject to renewal for another year). Submit an annual Report to the Oversight Committee including any amendments in the scope of the WG charter	Execution	On completion of Phase 2	T0+12, 3 months
4	a. Establish and start implementing the task groups' collaboration and communication plan for the year 2024 (subject to renewal for another year) including emerging sub-topics. b. Analyze the Privacy Landscape including Historical and Emerging Developments c. Analyze applicable cybersecurity implementations, approach, and use cases d. Analyze Identity System Implementations, approaches, and use cases	Research & Analysis	On completion of Phase 3	T0+18, 6 months
5	a. Establish technical test beds to leverage those capabilities in the form of "regulatory sandboxes"(as appropriate), in collaboration with other Forum Working Groups b. Create Education and Awareness Material pertaining to the scope of research undertaken by the Working Group.	Research & Analysis	**On completion of Phase 3	T0+21, 3 monthsFROM
6	a. Publish Best Practices White Paper for Working Groups' 3 key scoped domain Priority Topics and Use Cases. b. Publish Guidance on Metaverse-specific Privacy Protections. c. Publish Guidance on Metaverse-specific Cybersecurity guidelines d. Publish Guidance on Metaverse-specific Identity Implementation and Interoperability Best Practices. e. Submit a final Report to the Oversight Committee including links to all related publications and material produced via the Working Group	Output and Delivery	**On completion of Phase 4	T0+24, 3 months

** indicates the proposed work could be undertaken or begin in parallel to the previous phase.

6. Risk Factors

The effectiveness of the Working Group may be adversely affected by various obstacles, including but not limited to the following:

- A lack of subject matter experts joining the group which limits the PCI Groups ability to have an impact and generate desired outcomes.
- A lack of understanding of all or any of the three domains - privacy, cybersecurity or identity - across the wider Forum membership which constrain, out of ignorance, the PCI Groups ability to have an impact and generate desired outcomes.
- Conflicts of interest between individuals within the group and organizations represented within the group or the wider Forum leading to biased or unrepresentative communications or conduct
- PCI Group and wider Forum power dynamics can affect how decisions are made and which voices are heard.
- Cultural differences can affect how the Working Group sets project priorities and sets its goals. As a team within a global organization, the Working Group must actively seek input from different members and encourage supporting the opinions and beliefs of others.
- Lack of consensus can lead to ineffective decision-making or stagnation which will delay the creation of deliverables.
- Lack of resources, commitment, or follow-through may hamper the Working Group's ability to develop standards effectively and in a timely manner.
- Inability to engage other stakeholders which can hamper the free flow of ideas and information and may ultimately lead to the Working Group having difficulty getting support.
- The enforcement of cumbersome and overly bureaucratic procedures which unnecessarily delay PCI workplan implementation and create poor perceptions of the Forum among members
- A lack of trust between members of the PCI Working Group and Oversight committee members which create a difficult working environment.
- The perception of or actions which lead to the PCI Group being subject to standards or rules of governance that are different to those other working groups operate under.

7. Working Group Renewal

The duration of this working group will be 2 years. Before the Working Group has reached its first anniversary, it will have a project plan with specific deliverables and due dates.

8. Project Funding and Resources

Exact process for funding is to be determined by the Forum Board. For any project listed here, a cost estimate will be provided, if needed, and a specific proposal will be submitted to the Board.