FUTUREMATTERS™
CENTRE OF EXCELLENCE

GFTN
GLOBAL FINANCE & TECHNOLOGY NETWORK

Verified Machine Identity: Foundational Digital Infrastructure For Trusting Granular Green Data

June 2025

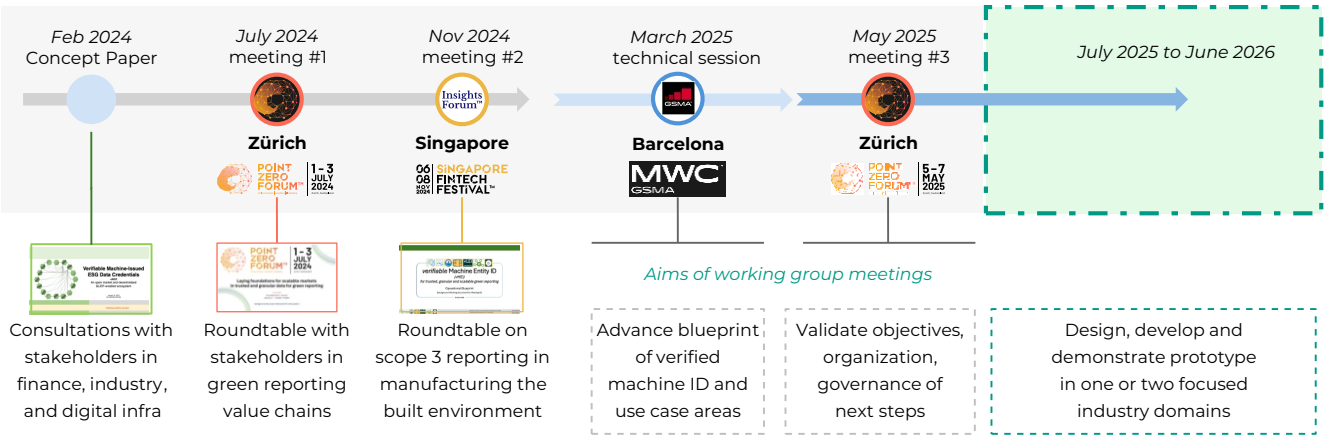
Contents

Introduction

This note presents an update from the working group on Machine-verified green data, held on 4th Nov at the Insights Forum in Singapore. This is the second meeting of a consultative working group that convened for the first time at the Point Zero Forum in Zurich in July 2024 to develop proposals for enhancing scalable, trusted markets in granular green data for reporting and climate action.

Today, data is collected in repetitive ways that do not allow provenance to be tracked, or integrity verified. Companies can collect data from sources, including machines, over which they exercise direct control. But they are also often the ones feed those specialist data aggregators and analytics platforms. While they may have strong domain expertise, analytics and procedures, it may not be possible for them to demonstrate precisely where the data was sourced from, with what authority, and how it was transformed. Traditional audit and reporting methods

Figure 1: Working group progress and milestones



Collection of data for green reporting across the value chain has become an acute challenge. Regulations and commercial interests alike drive companies to better analyze, monitor and adjust their supply chain structures, partners and inputs, not only to reduce their carbon footprint but to enhance the efficiency and resilience of their business. The emission reporting defined in Scope 1, 2 and 3 categories requires data collection from external partners, often in other jurisdictions, facing different rules and standards, using different methodologies and facing their own reporting obligations; it is very difficult to scale up bilateral data sharing agreements or even extend centralized platform models across complex supply chain networks and industries.

Reported data lacks the integrity, provenance and quality needed to meet legal reporting standards. Data underpinning legally binding statements (to regulators, to investors) needs to merit and reaffirm our trust. If obligations not only to report but commit to the veracity of statement on climate impact are to be backed up by enforcement measures, then companies will want to have means to verify and eventually prove the accuracy and pertinence of their statements in court. Enforcement of climate policy and reporting obligations are expected to eventually entail imposition at least of financial and reputational penalties if data is incomplete, inaccurate or falsified.

are not bad per se, but they may not be well adapted for scalable, complex tracking and aggregation of data. Reporting is largely 'best effort' reliant on our confidence in new platforms and 'controlled' through non-scalable, costly sample audits. Yet this data is used by investors to fix their terms of financing; it is relied upon to avoid looming statutory penalties for false reporting or compliance. In the wider community, reporting quality suffers from claims of *greenwashing*.

Incentives and capacity for firms to systematically record and share data are weak. The burden of reporting falls on a wide cross section of countries and companies. Many consider demands for data as solving “other people's problems”: a one-way street, helping banks and corporates in other jurisdictions to meet their obligations, but generating little tangible benefit for them. The time, effort and tools required to collect and manage data is not trivial. **Sharing data also can also entail a loss of control** and agency over sensitive meta data.

Starting from Meeting 1 in Zurich, the working group has been discussing the aims and approach for what has become defined now as a framework for “Machine-Issued Data Assurance” (MIDAs). The core principles and elements of this developing proposal are outlined below.

Scalable, reliable reporting should draw on data from connected machines and devices. Industry 4.0, 'smart manufacturing', and IoT generated data can -and should- be better, more widely harnessed. Digital technology advances make it easier to record granular data and manage production with the aid of digital devices; in the near future, more widespread application of AI tools may make it necessary for the source and integrity of granular data to be verifiable in order to enable users to assess the overall quality of reporting produced in that manner.[1] Machine or device-issued data can be attributed to specific processes, secured against tampering, controlled, tracked, and traced. It can complement other methods and inputs to track emissions and environmental impact.

Machine sourced data needs to be underpinned by trusted controls and identity. Companies that control machines and processes may know what *their own* data represents and its source. But companies receiving other partners data are less well equipped to interrogate and track its origin and integrity. They therefore may have to fall back on complicated data sharing agreements and tools to 'translate' data from source into higher level indicators that are then mapped by third parties to product and process schemas for climate reporting.[2] Mechanisms are needed to verify data attribution and quality *across* organizations.

MIDAs is a framework for verifiable machine identity and data sharing. It will provide foundations for an open and economically sustainable ecosystem of market-driven, trusted data sharing, analysis, and reporting. Foundations for MIDAs entail three elements for co-development by industry stakeholders and public sector partners:

- A governance framework for assigning **trusted, unique machine identifiers**
- A registry of firms' **legal and economic rights to machines and data assets**
- A governance framework for **data access consent** enabling control and monetization

Machine Identity would become part of a broader, new generation of digital foundations for the economy. Trusted identity framework for machines/devices and data would align with the emerging ecosystem of other identifiers and data verification mechanisms needed for the Ledger Economy.

Insights Forum Singapore – Discussion Summary

Discussion focused on (i) design proposals for foundations, (ii) comparison with existing industry solutions and approaches, (iii) a review of business model and deployment challenges in specific industries and domains, and (iv) the role of policy makers in setting requirements and standards.

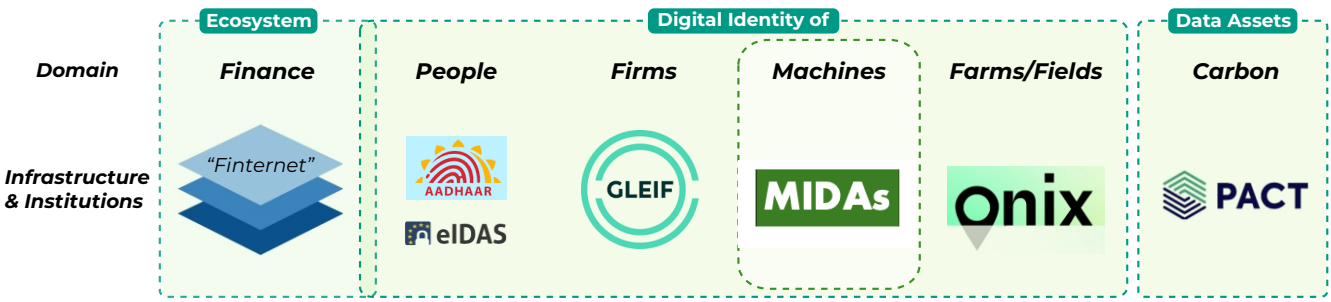
Design Issues

The working group discussed some of the practical data collection and analysis challenges, as well as promising enablers in certain sectors, such as the built environment. Debate centered on how existing monitoring technologies and analytics could be harnessed to provide more accurate, scalable climate reporting and highlighted some of the non-technical issues in standards, governance and business model incentives that need to be addressed. The starting point for discussion drew on the architecture developed in Zurich, illustrated in Figure 3 on next page.

Building Foundations

- **Machine and device identity should be based on existing serial numbers and identifiers.** Most machines and devices are already assigned identification numbers (e.g. a serial number, an IMEI (international Mobile Equipment Identity) number) managed within different industries. A system for secure and interoperable identities for

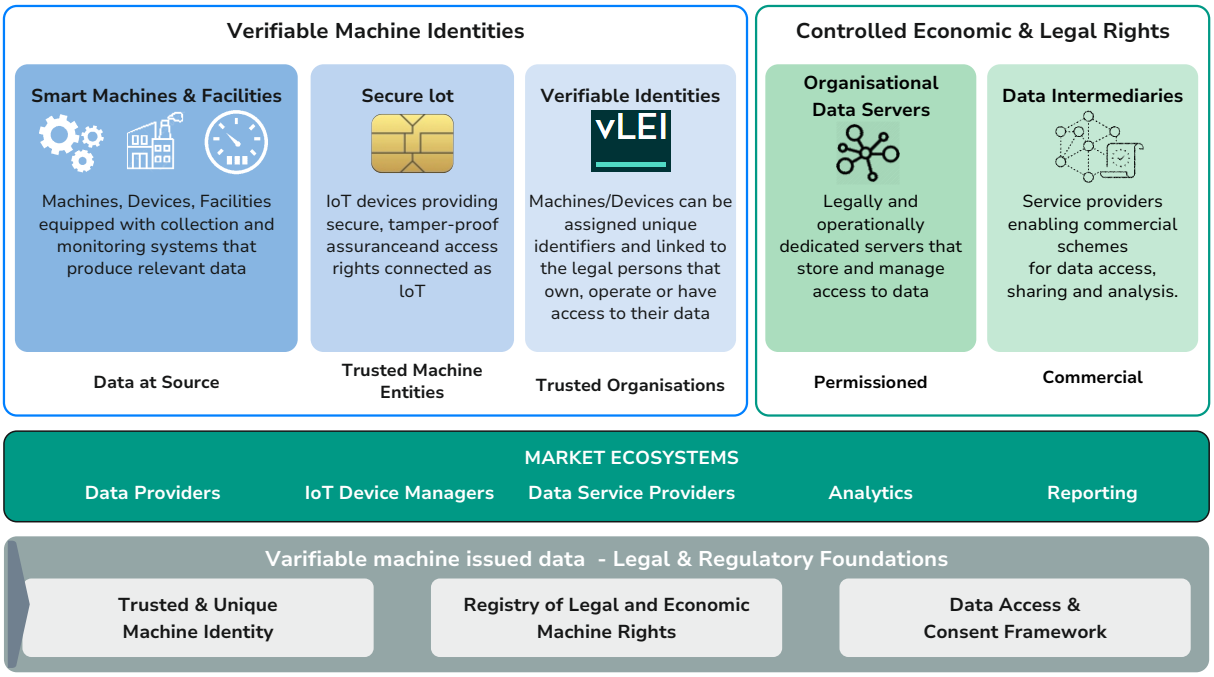
Figure 2: Foundational Digital Infrastructures – emerging pillars



1 Concerns about the quality of AI driven analysis are already widely discussed. Confidence in the outputs of AI program based analysis driving interest in ways to verify the provenance and authenticity of data inputs.

2 An example is the schema companies would need for mapping data to the EU Digital Product Passport.

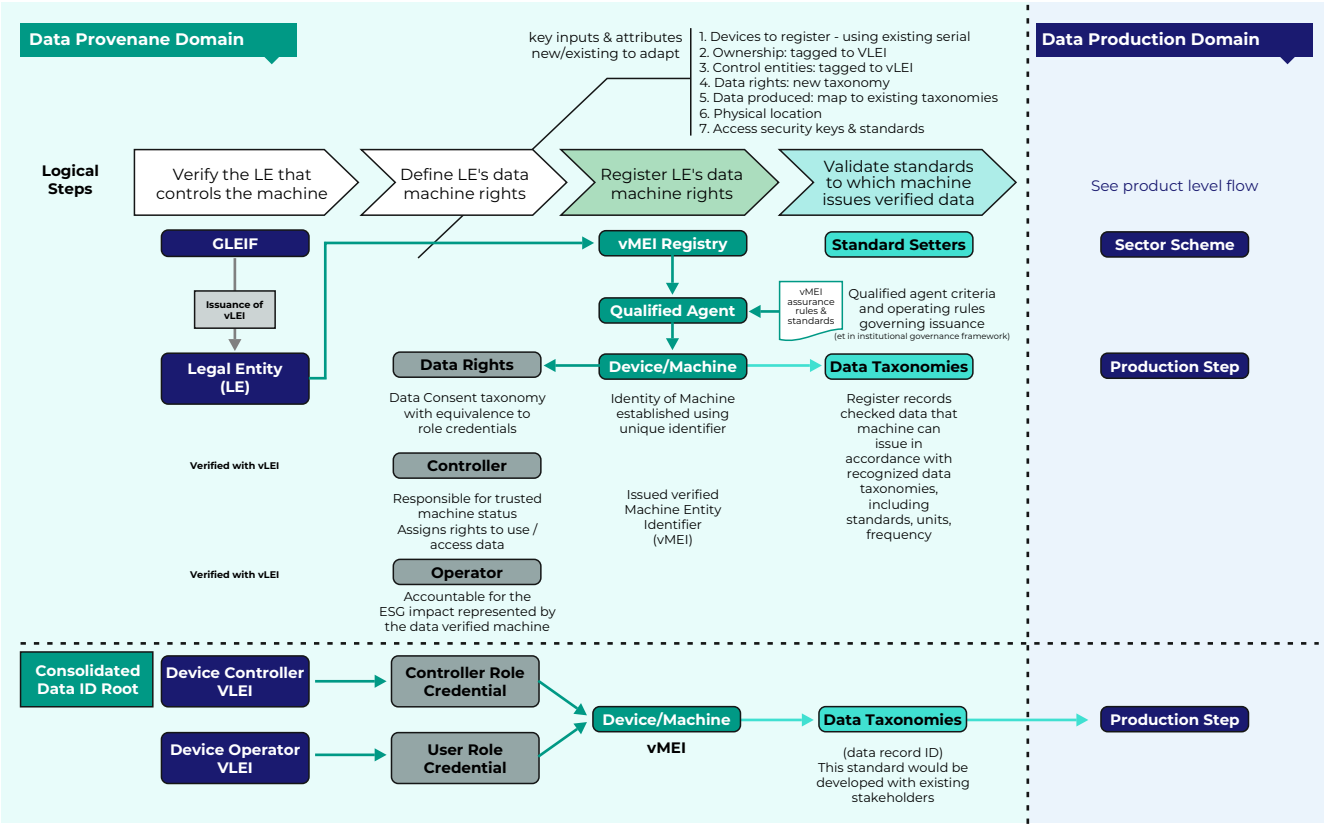
Figure 3: Base Architecture



devices could draw on the architectural approach used by the Global Legal Entity Identifier Foundation (GLEIF) to create universal identifiers for legal entities. These do not replace but complement those issued by national authorities or registries. Similarly, existing numbering systems could be used as a base for more global standards. Secondly, machines need to be linked to the companies that own or control them. The confirmation of machine identity, security controls, and attribution to legal entities could be performed by qualified issuers or certification authorities, building on existing institutional and governance structures for similar trust agent and standards assessments. Figure 4 provides an illustration of the logical relationships that would need to be established to create a chain of trust between machines and their controlling entities.

- **Building on existing industry standards and practices:** Existing sector and supply chain specific

Figure 4: Illustrative framework for trusted machine/device identity



initiatives can and should be built upon to avoid duplication and to accelerate the impact of work to date. There is potential to leverage the global database management of IMEI's and TACs[3] and their work, or for example, to integrate with the EU's Digital Product Passport initiative. Technology companies are already working on initiatives to enhance traceability of data provenance by establishing their own platforms. The time is right to avoid creating silos and set standards that make data interoperable.

Addressing specific sector needs and Implementation challenges

- **Green Finance:** Hard-wiring terms/cost of finance to climate targets is becoming more common, creating demand for practical monitoring and reporting. Some intermediaries are tackling this by deploying networks of IoT integrators, using software and sensors to collect more than just emissions, to monitor also water and air quality. But this requires scale to be efficient and someone to finance the deployment by SMEs that otherwise lack incentives or capacity. Financial intermediaries may have a growing demand for more scalable and trusted data as the legal and financial link to emissions targets strengthen and perhaps become embedded in term sheets.

- **Sustainable Buildings:** Stakeholders in the property industry have appropriate equipment and arrangements in place to manage their own data collection, for instance for electricity usage, but scaling of data reporting across multiple stakeholders is still limited. The challenge is now less about technology in this field but more about coordination and business model design. It is estimated that carbon emissions could be reduced by 17% just by applying existing technology solutions. But we need deals with suppliers and extend deployment and usage.

- **Supply Chain Adoption Incentives and Capacity:** There is a recognition of growing gaps and tensions between the context of large corporations in advanced economies and MSMEs in emerging and middle-income markets. Rules are predominantly being set in advanced economies, with obligations cascading through multinationals to less well-equipped companies in emerging markets in Asia. Questions arise not only about the incentives for MSMEs to support the green transition but also their capacity **and** the impact on climate objectives.Not all SMEs have the same impact on the result, and many have other priorities and challenges which are not being taken seriously by global stakeholders and regulators. Market incentives to provide and ultimately also fund data collection and reporting may be important. More attention may need to be paid to the proportionality of implementing measures **by focusing** on markets, products and value chains that can have the most significant impact on reducing carbon emissions.

Policy Considerations

- **Policy and Regulation:** A growing array of interconnected regulations, disclosure requirements, and policy measures create challenges for companies but also highlight the need for more scalable reporting mechanisms. Sustainable mechanisms need to be able to scale across different industries and jurisdictions; to do that, governments also need to support compatible standards and practices across sectors and countries. Governments acknowledge that existing measures are a starting point and warrant more collaboration with industry and across borders to forge scalable arrangements. That the door is open to dialogue is a first step. The EU Digital Product Passport (DPP), supply chain reporting, and carbon adjustments will accentuate the need for data sharing across borders. The EU aims to encourage technology-neutral reporting solutions and standards that can be applicable across borders and complement the broader aims of carbon emissions reduction and consumer empowerment. An interoperable machine ID would be in alignment with and support the operationalization of the DPP.

Sector Deployment

From idea to implementation requires us to design and test a prototype in areas where there is sufficient industry maturity, a clear use case and benefit, and a clear alignment with other existing industry reporting, government regulatory, or international infrastructure initiatives. The working group has begun to articulate these and other criteria that should be considered in shaping and prioritizing pilots or implementations.

In parallel, **ideas have developed about specific industry or use case domains** in which demonstration cases or pilots could begin to be elaborated. These would need to be further developed by working group members and then

3 TAC: Type Allocation Code. This is required under 3rd Generation Partnership Project, an umbrella term for a number of standards organizations which develop protocols for mobile telecommunications, for all devices, including IoT devices, payment terminals and connected vehicles. It is the 8-digit number that forms the first part of the 15-digit IMEI (International Mobile Equipment Identity), which uniquely identifies each individual connected device, so they can be transported around the world.

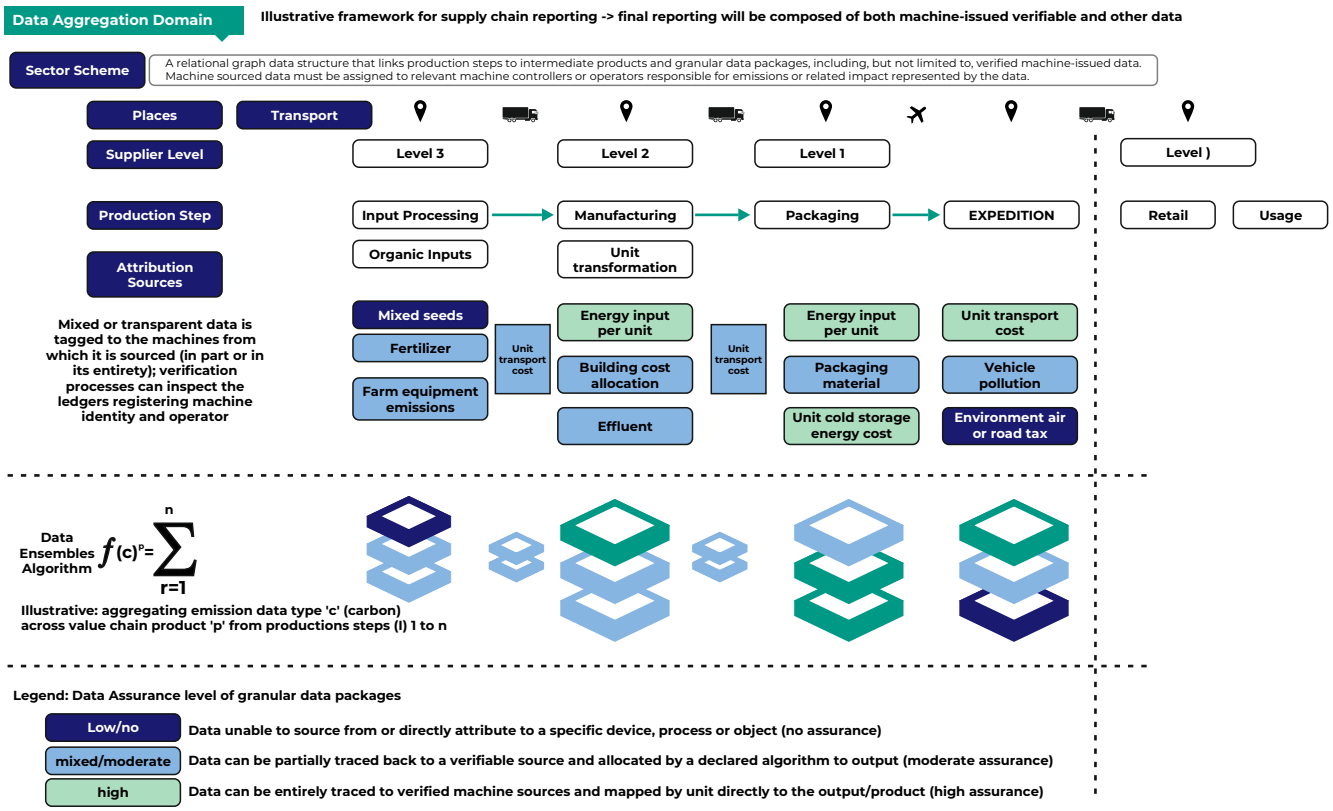
reviewed against the feasibility and success criteria needed to warrant action. Three domains have emerged recently as potential areas in which to shape pilot proposals. They are:

1. **Sustainable Buildings and Finance:** A practical use case could be developed to support the capture and handling of data to feed monitoring of sustainable buildings. Many input and equipment providers are already able to trace and share data on carbon emissions related to materials and energy usage by buildings. Meanwhile, financial intermediaries are providing lending at terms linked to the achievement of energy and emissions savings measures. Compliance with these contractual conditions can benefit from more scalable and robust mechanisms to monitor emissions.

2. **Digital product Passports:** Machine identity could support plans for supply chain ESG reporting and EU digital product passports. A trusted independent identifier may facilitate the sharing of data between entities and jurisdictions while enhancing trust and traceability. A practical application of the verifiable machine identity should be designed around existing initiatives.

3. **Digital Public Infrastructure** (DPI): Developments in DPI and market practices will eventually also require machines to have verifiable identities. DPI discussions are currently focused more on the role of digital identity for natural persons and access to basic financial services like payments- the aim here is to provide interoperable 'stacks' that connects users, assets, and data in scalable ways across borders and silos. A key initiative is embodied in the the Finternet[4] initiative noted in the 2023 speech by A. Carstens, General Manager of the BIS[5]. A similar approach could be taken, reutilizing or integrating elements of this nascent architecture to apply to machines and the data that they produce. The Finternet architecture foresees its application in areas of green reporting and will require machines to have identities that enable integration into programable or 'smart' contracts. Machine identity prototypes could be integrated with test versions of the Finternet lab program to inform design requirements and demonstrate benefits from links between financial and real economy transactions.

Figure 5: Illustrative Data Aggregation Scheme, aligned with DPP



4 https://finternetlab.io/#mustRead

5 This initiative sets our a roadmap and framework for a future financial system where multiple financial ecosystems interconnect, similar to the internet, empowering individuals and businesses with greater control over their financial lives. It envisions a universally accessible digital financial system where transactions are cheap, secure, and near-instantaneous, with the ability to transfer any financial asset to anyone, anywhere, at any time.

Next Steps

Practical pilot developments are required to inform design and demonstrate the potential impact that a machine identity framework can have on scaling trusted green data sharing. The aim is to develop a set of pilot plans and a minimum viable organization for supporting the program by the next milestone at the PZF in Zurich in May 2025. A multi-stakeholder working group is advancing blueprints for the operational design of this framework and identifying a small-scale coalition to run a pilot.

Working hypotheses are that the initiative started through this group would focus on a very thin, interoperable layer of the emerging data ecosystem, focusing on designs for three elements:

(i) A Federated Trusted Machine Registry

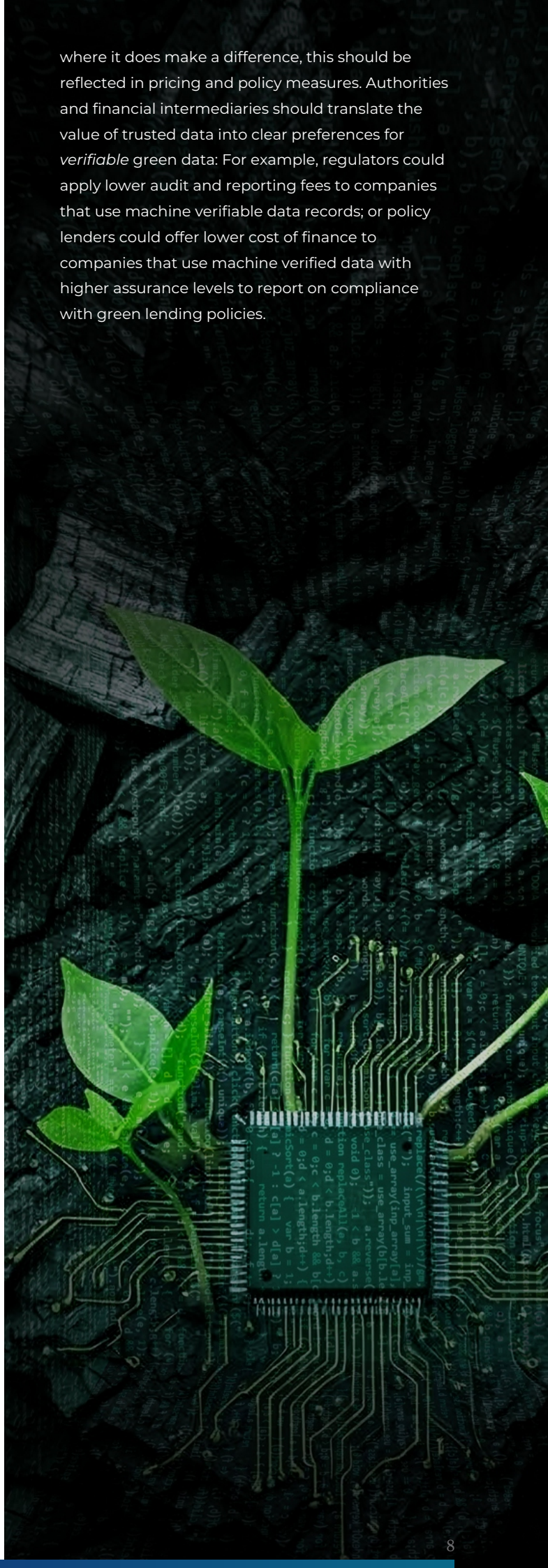
This would probably be a decentralized registry, building upon existing practices, machine identification mechanisms and registers, and establish a trust framework and set of rules to be complied with for issuance of trusted ID numbers as well as an oversight mechanism that provides a link to national organization and authorities; the plan should entail an interim arrangement for the hosting and guardianship of this register but with a pathway to integrate it with existing standards and bodies, such as ISO.

(ii) An Administrative Framework for Green Data

This would enable companies that own or operate machines to assign economic control over the data produced by or shared from devices and enable one or more jurisdictions to treat 'green data' as an intangible asset. That would complement frameworks for data consent with not just the legal rights over data access but mechanisms to price access and control, enabling market forces to incentivize and finance a shift towards high assurance granular data , thus enabling firms to manage global data assets, legal rights, and derived revenues on a consolidated basis.

(iii) Regulatory and Financial Incentives

Regulatory reporting and disclosure requirements as well as financing and risk instruments should acknowledge the different levels of quality and assurance that can be attributed to trusted and verifiable machine-issued data. While high assurance and granular data may not be warranted from a cost/benefit perspective in all circumstances, where it does make a difference, this should be reflected in pricing and policy measures. Authorities and financial intermediaries should translate the value of trusted data into clear preferences for *verifiable* green data: For example, regulators could apply lower audit and reporting fees to companies that use machine verifiable data records; or policy lenders could offer lower cost of finance to companies that use machine verified data with higher assurance levels to report on compliance with green lending policies.



Authors

Ivan Mortimer-Schutts
Global Head of vLEI,
Global Legal Entity Identifier Foundation (GLEIF)

Sophia Hasnain
CEO, Linked Things

Contributors

Akanksha Rath
Senior Manager, Knowledge Hub

Goh En Ci
Student, St Joseph Institution

Production

Sachin Kharchane
Graphic Designer

Global Finance &
Technology Network (GFTN)

6 Battery Road, #28-01, Singapore 049909
gftn.co | hello@gftn.com