

Driving Business with Trust:

# The Sustaining Role of Secure and Reliable Identities

March 2023

Sponsored by



Author:

**Marco Becker**

Consulting Manager

IDC Central Europe





# Introduction

In a digital and globalized world, checking the trustworthiness of a business counterpart can be difficult. While legal entity identity — or more precisely the lack of transparency into the identities and ownership structures of legal entities — became a major issue for financial markets with the financial crisis in 2008, the same issue applies to global trade and supply chains. During the pandemic, fraudulent transactions increased, making trust between business counterparts increasingly important and highlighting the need for verifiable company data, especially in cross-border trade.

Currently, there are several challenges based on the lack of identifiability, and this list is not exclusive:

- Missing trust between legal entities that prohibits business interaction and trade finance
- Various, mostly non-standardized and -digitized national and international identification schemes
- Adherence to numerous regulations, such as know your customer (KYC), antifraud, and AML (anti-money laundering)
- Cost and efficiency of thorough identity verification and risk management
- Limited flexibility, agility, and resilience to tackle accelerating disruptions

This IDC Technology Spotlight shows the importance of trust as an enabler for global trade, how identities for legal entities and their representatives can enable and maintain trust, and how secure identities can be used to mitigate risk, raise efficiency, and foster resilience. It introduces the Legal Entity Identifier (LEI) (ISO-17442) for B2B identity and verification and shows how application of the LEI and vLEI, the digital, cryptographic version of the LEI code, can contribute to cross-border legal entity identification and to more efficient, secure, and innovative supply chain management.



# Table of Contents

Digital Trust: The Foundation of a Digital-Enabled World	4
Reliable Identity Becomes the Heart of Physical and Digital Interactions	6
"Identity and Digital Trust" — A Hot Growth Market	7
Identities Are Vital for Agile and Resilient Worldwide Trade	9
Ensuring Identities and Authentication of People in Organizational Roles with Global LEI System and vLEI	12
Use Case: Using LEI and vLEI in Supply Chain Management to Enhance Compliance, Efficiency, and Innovation	14
Conclusion	16
Resources	17

# Digital Trust: The Foundation of a Digital-Enabled World

The world is fast becoming “digital first.” IDC believes that by 2024, 80% of the people around the world will have access to the web and that spending on goods and services on the internet will reach more than \$10.5 trillion — a huge amount given that overall consumer household spending reached \$53 trillion in 2021, according to the World Bank. Not only are enterprises striving to create new digital-first business models to drive revenues and growth, but governments are also digitizing their economies and services.

All this comes with advantages for economies, trade, and consumer experience. It also comes with challenges, especially in terms of risk. According to IDC research, mitigating risk that threatens digital trust is often the most challenging aspect for digitally mature companies in running their digital business. And that's a huge problem because trust already is a key business asset in a global, digital context. Household customers are increasingly opting to only interact with trustworthy and purpose-driven organizations; this is increasingly the case for business-to-business interactions too. More than 90% of European organizations say trust is relevant, important, or a competitive advantage. About 74% of organizations already have formal trust programs of varying maturity in place, some for now primarily focused on security and privacy while others already encompass customer experience, reputation, sustainability, and diversity. 79% of organizations worldwide say trust programs — investments in security, privacy, and compliance to improve risk posture — will be a priority in 2023.

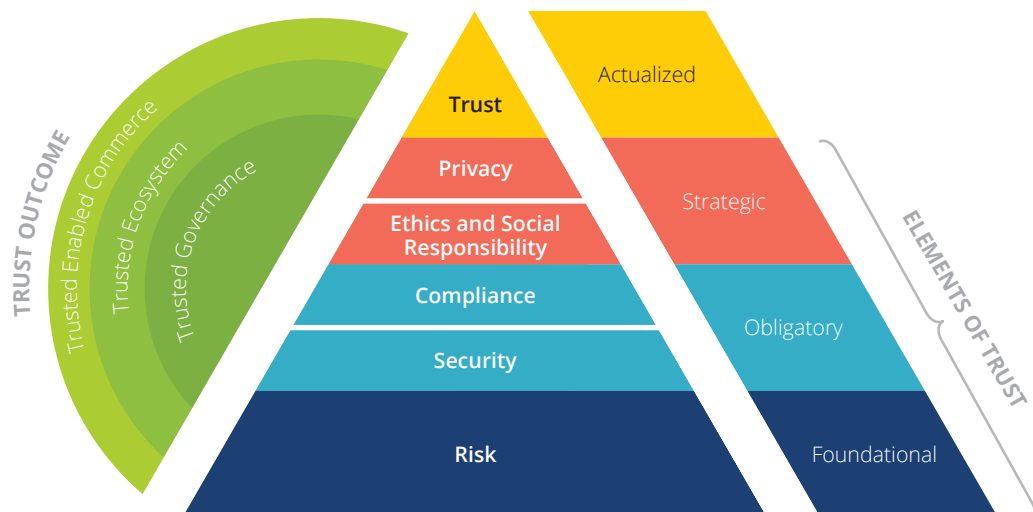
For **79%** of organizations, trust programs will be an investment priority in 2023. For 37%, a **high-priority** investment.

Source: IDC Future Enterprise Resilience and Spending Survey, Wave 5, June 2022

**37%** of digitally mature companies say **mitigating risk that threatens digital trust** is a major challenge when running a digital business.

Source: IDC Future Enterprise and Resilience Survey, Wave 7, 2022

Figure 1: IDC Trust Framework



Source: IDC, 2022

IDC's Trust Framework (see Figure 1) illustrates potential trust outcomes and how trust is systematically achieved by combining three interrelated layers of trust:



**Risk:** Risk management is a prerequisite for every company. Only proper risk management enables economically successful business operations by maintaining continuity.



**Security and compliance:** A loss of sensitive data or any significant downtime of services can quickly erode trust. To protect their economies, countries increasingly demand obligatory cybersecurity measures. This also applies to compliance with existing regulation. This layer may also include privacy for those jurisdictions that have corresponding regulations in place.

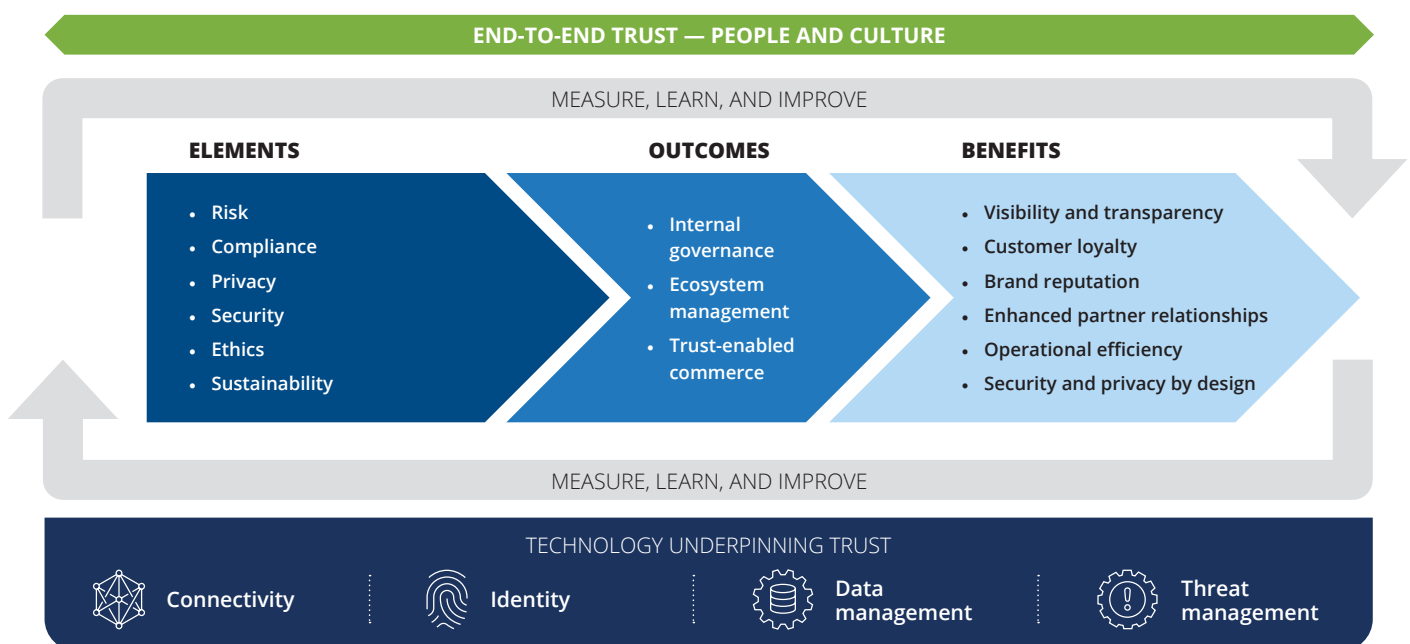


**Ethics and social responsibility:** Long seen as a “nice to have,” ESG is still largely voluntary but is becoming increasingly regulated and a key decision factor for customers and investors. Every measure that exceeds obligatory responsibilities conveys dedication and trust. When pursuing their sustainability initiatives, 31% of European organizations see increasing brand value and trust as a key driver.

Companies that adhere to the above are perceived to be trustworthy by consumers, business partners, and governments, enabling accelerated commerce, better collaboration in business ecosystems, and easier interaction with authorities. As Figure 2 shows, these can translate into benefits such as better visibility and transparency of processes, improved loyalty and enhanced reputation, stronger partner relationships, and overall operational efficiency.

At the same time, in a digital-first world that is becoming more complex and faster every day, holistic end-to-end trust must be underpinned by technology, with the ability to prove identity a key technology pillar.

Figure 2: Necessary Elements and Technologies to Achieve End-to-End Trust



Source: IDC, 2022

# Reliable Identity Becomes the Heart of Physical and Digital Interactions

Identities shape our lives. Think of how many IDs the average person already has to make sure they are eligible for activities, purchases, or legal actions: driver's license, club membership, ecommerce platform login, email addresses, to name a few. The same applies to businesses: identities shape them and are an important way to reduce risk and enable business transactions — even more so in a globalized digital world. This is also why legal entity identity and being identifiable anytime and anywhere becomes key for businesses.

Table 1: Identity Relationship Types and Their Core Goals

RELATIONSHIP TYPES	CORE IDENTIFICATION GOALS
<b>B2E (business to employee)</b>	Identifying employees and authenticating their access to company resources
<b>B2C (business to consumer)</b>	Identifying customers for creditworthiness to lower risk and deliver customized customer experiences
<b>B2G&amp;R (business to government/regulator)</b>	Identifying their business to governments and regulators worldwide, e.g., for tax or compliance
<b>B2B (business to business)</b>	Identifying business partners and suppliers, their compliance with important regulation, and their reliability

Business identity is very complex. Public or regulatory authorities sometimes provide identities to businesses, often ending up with dozens of identity schemes for just one country. Businesses create identities to represent themselves to customers or to manage online tools for customer or supplier relations. But it's not enough just to have identities. Identity crime and fraud has soared, with digitization and globalization sometimes causing huge financial damage and destroying trust. So, it's even more important to have secure and reliable identities and ways to bridge across identity schemes. At the end of 2021, about 50% of companies interviewed by IDC worldwide said identity security is a source of operational savings, a linchpin for overall security, or a technology they wanted to spend more on. At the same time, 20% said identity security is a "necessary evil," or a "resource and time sink" forced on them by requirements and compliance, showing that identity security and management can be difficult, especially when manual. The remaining 30% said it's a trade-off — useful as long as it's constrained and well managed. Too little identity security puts businesses in danger, but too much may prohibit any business at all.

Global trade financing offers a good example. On one hand, fraud is a reason why global banks often decline trade finance and loan requests especially for SMEs in emerging markets, as these pose more risk, harming global trade and inclusion. On the other hand, the number of regulatory hurdles (e.g., for AML/CFT/KYC due diligence), associated costs, and lack of international standardization for corporate identities to eventually reduce risk make interactions less profitable, resulting in less business (or even none at all). Reliable and secure identities are vital for physical and digital business interactions, but the way they are provided, managed, and verified needs to evolve to become easier, more secure, and more efficient.

For about **50%** of organizations, **identity security is a source of operational savings, a linchpin for overall security**, or a technology they want to spend more on.

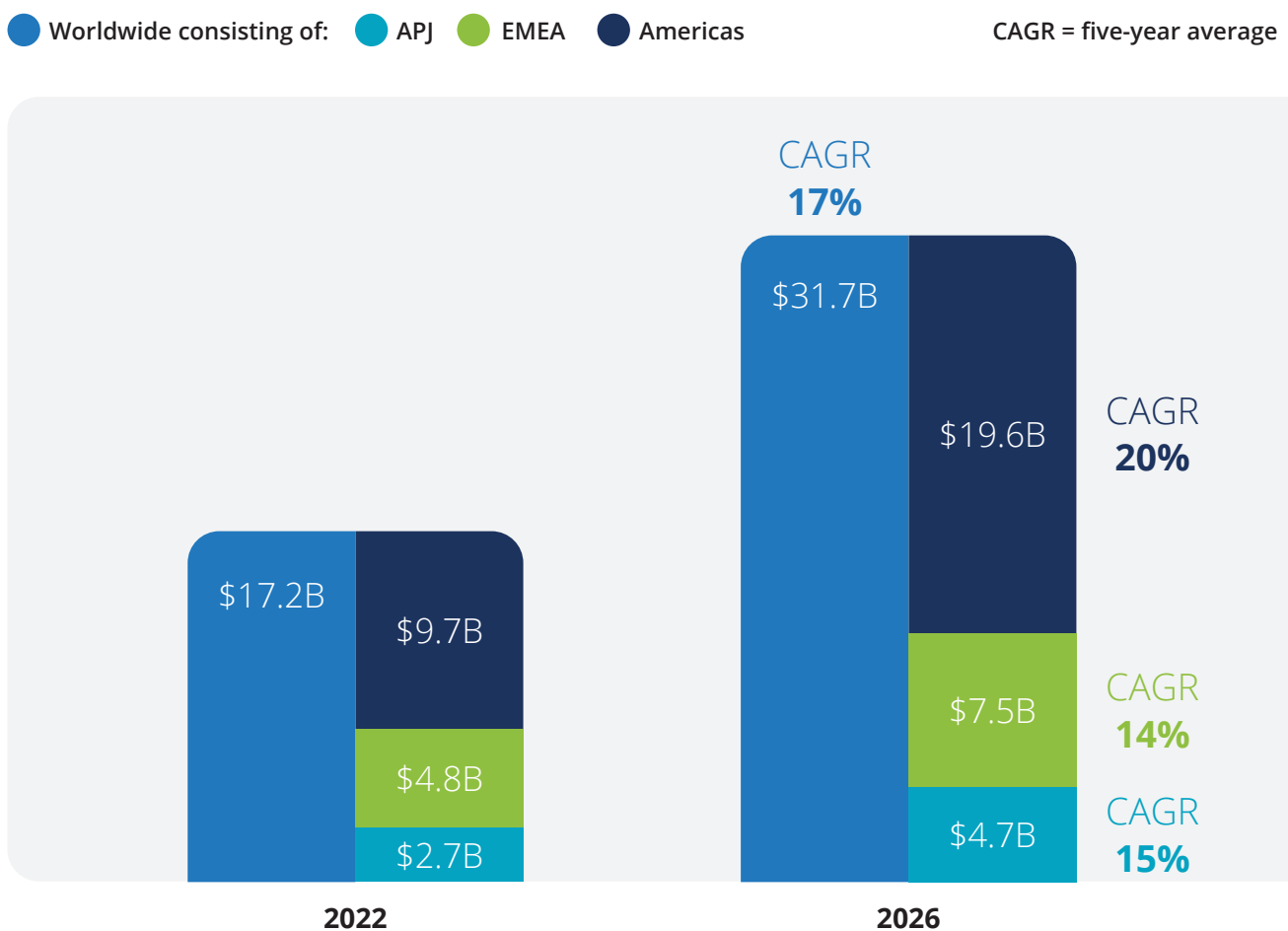
Source: IDC Security Identity Survey, September 2021



# Identity and Digital Trust — A Hot Growth Market

Identity and digital trust (IDT) is a technology market with big growth ahead of it. IDC forecasts double-digit growth worldwide and for all global regions in the coming years.

Figure 3: Identity and Digital Trust Software Spending, 2022–2026



Source: Worldwide ICT Spending Guide Enterprise and SMB by Industry, January 2023

The IDT market will remain hot for the foreseeable future due to the soaring demand in B2C and B2B identity management. Most companies focus their spending on employee identity management, but consumer identity management is catching up. IDC believes there is not enough awareness of B2B identity management in terms of legal entity identities, though there are lots of potential benefits, such as digitization of manual and paper-based business processes and fraud reduction and prevention. IDC believes that when these benefits are more widely recognized or when fraud damages become too painful, the market will gain significant traction.

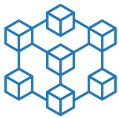
At the same time, current technological developments are driving investment:



A **zero-trust** approach (“never trust, always verify”) is set to become the default for cybersecurity. Instead of trusting known devices, users, or internal networks by default, a zero-trust approach always requests strong identity verification. It’s also important for supply chains and partner ecosystems, as it helps to secure data movement, accelerate information exchange, and improve business interactions. For 79% of European organizations zero trust is therefore a top priority, with a defined strategy or at least incorporated in developments and initiatives where possible.



**Interoperability and standardization** are needed to foster national and international use of identities and credentials and mitigate silos. An important goal is to make solutions lean and easily accessible to be attractive for all organizations, especially SMEs and companies in developing countries, which account for a large part of the global economy and trade. International institutions and foundations such as the ICC Digital Standards Initiative are taking the first steps to create open standards that can be globally utilized.



**Decentralized public key infrastructures** enable verification of digital identities and credentials without the need to exchange personal data. Decentralized identities (DIDs) and remote identity verification are the foundation of self-sovereign identities (SSIs) that enable users to control which exchange of (personal) data is needed to perform a task that requires identity information.



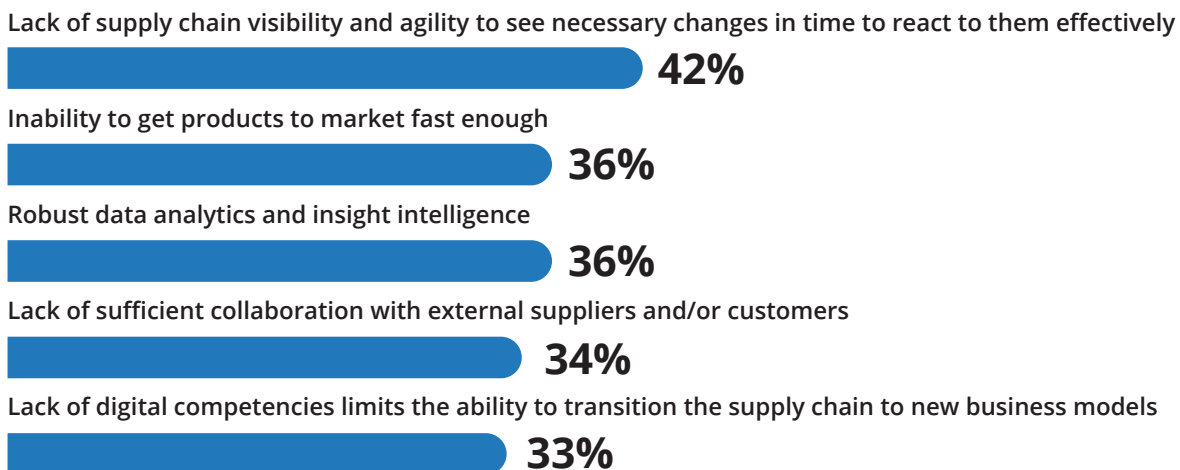


# Identities Are Vital for Agile and Resilient Worldwide Trade

Let's go back to 2008. The world slid into a financial crisis, but underlying this was a crisis of identity and trust. A lack of trust among banks and between banks and businesses led to a slump in lending and to a harsh economic slowdown. There was another crisis in 2020, in the shape of COVID-19. The pandemic had a major impact on business and trade, and identity again played a huge role. COVID restrictions led to risk mitigation by financial institutions to stop loans and letters of credit to SMEs that had no trusted identity and were therefore automatically less credible. The result was a larger than ever trade finance gap that has created new risks for global supply chains, threatened the very existence of SMEs around the world, and decelerated global trade, especially by impacting developing countries' economies and their purchasing power. Another problem with COVID was the enormous new wave of fraud. In 2021 alone, the European Anti-Fraud Office (OLAF) identified more than 1,250 suspicious traders selling medical products on ecommerce platforms. OLAF seized 100 million COVID-related products — the tip of a giant trade fraud iceberg.

All these problems are caused by mismanagement of risk. According to IDC, 26% of European companies say low business recognition of supplier risk is a severe barrier for effective supplier cyber-risk management in their organization. For an additional 47%, it's a moderate barrier. This is intensified by other supply chain challenges such as a lack of supply chain visibility and agility, a lack of collaboration with external suppliers and customers, and a lack of digital competencies, limiting new business models.

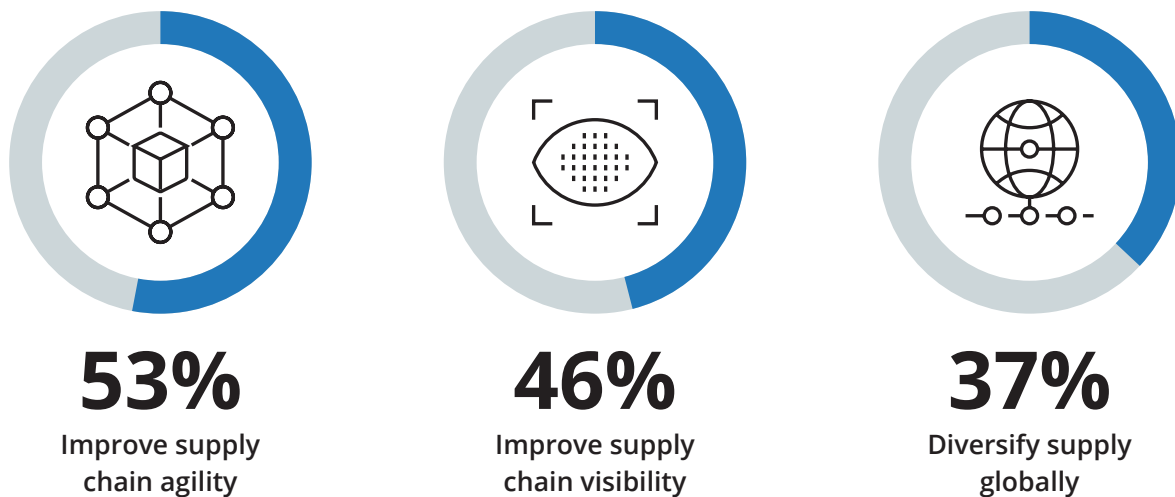
Figure 4: Current Gaps in Supply Chains That Are Likely to Be the Most Problematic in the Future If Not Addressed



Source: IDC Supply Chain Survey, March 2022

Due to the current economic uncertainty, businesses and supply chains must be more agile and resilient than ever before. To improve supply chain risk mitigation and resilience, companies are prioritizing measures such as supply chain agility, supply chain visibility, and global supplier diversification. They are also including supply chain partners in risk mitigation.

Figure 5: Top 3 Measures Worldwide to Mitigate Supply Chain Risk



Source: IDC Supply Chain Survey, March 2022

#### To implement these measures, organizations need to:

- Know all current suppliers in the supply chain, direct and indirect
- Maintain continuously monitor all supply chain participants and changes in their legal status quo, such as bankruptcy, changes in ownership, and compliance violations
- Secure exchange of relevant information for coordination and collaboration
- Be able to add new suppliers worldwide as fast as possible

Secure and reliable identities of legal entities and their representatives are at the core of all of these and are a prerequisite for agile, resilient trade. They enable reliable identification of all suppliers in supply chains, can support zero trust in physical and digital trade, and can accelerate supplier onboarding without compromising security.

Another burden for supply chains and trade is the rapid development of ESG legislation worldwide. Germany's Supply Chain Act (LkSG), for example, came into effect in January 2023, forcing companies to ensure ESG-related liabilities such as human rights and ecological protective measures in accordance with various UN social development goals in their supply chains. 64% of German organizations say supply chains are important or critical to implement ESG initiatives. Similar legislation exists or is planned in other countries, such as the U.S., Canada, Brazil, France, the U.K., and Australia. The EU has an advanced draft for a supply chain law with severe liabilities that could come into effect in 2025. 37% of worldwide organizations think that improving sustainability across the supply chain has a significant impact on organizations' sustainability goals. Again, identity plays a vital role because companies need to identify all their suppliers and related entities to check sustainability compliance.

## Despite the value of having identities and identifiability, there are also challenges:



**Validity:** Companies must check if an identifier is valid, if the counterpart really is the owner or affiliate of the identified entity, and if they are eligible to use the identifier.



**Feasibility:** Checking identities but also providing and proving identity, legal capacity, and compliance with relevant laws is a lot of work. This is especially challenging for SMEs that don't have the resources to maintain the many identities required by different business partners or business transactions.



**Time and effort:** There are multiple identification schemes — national, international, or sectoral — stored in different silos, often neither digitized nor internationally standardized or interoperable. The number of identities and the increasing cost of managing them make supply chains less efficient and agile.



**"Golden source" data:** Relevant identity information needs to be continuously maintained (name, address, operating status, etc.) and changes immediately communicated, in some cases even in real time (if compliance is threatened, for example).

To make legal entity identities not only useful for transparency, resilience, and security, but also faster and more versatile to increase business agility, efficiency, and collaboration, digitization of corporate identity will become increasingly foundational. Digital legal entity identity will be critical for a wide range of international trade transactions and processes such as contract creation, data exchange, e-documents, ESG compliance, and know-your-customer processes, while individually minimizing risk.

In summary, digital identity can improve individual supply chain risk, agility, and resilience, but also contribute to global society by fostering market integrity, financial stability, and a more inclusive trade system. To make identities globally effective, IDC proposes three core requirements for broad adoption:



**Global value chains require a global approach:** This requires globally unique identifiers to bridge local identity silos and enable efficient orchestration of worldwide trade processes.



**Agile and efficient identity checks require digitization:** Standardized, interoperable, and technology-agnostic digital identity management solutions are needed to make processes efficient and to eliminate duplicative verification workloads on similar occasions.



**Holistic inclusion requires easy accessibility:** This applies regardless of company size and jurisdiction to encompass the global trade network.



IDC assumes that **by 2028, digital trade finance transactions** could make up **30%** of trade finance if trade ecosystems become **interoperable, standardized, technology agnostic, and easily accessible.**

IDC FutureScape: Worldwide Corporate Banking 2023 Predictions, October 2022

# Ensuring Identities and Authentication of People in Organizational Roles with the Global LEI System and vLEI

The LEI is an internationally recognized standard for identification of legal entities. The LEI is a 20-digit code based on ISO 17442-1:2020. As an ISO standard, it enables unique, global identification of entities, and it is persistent, meaning the entity remains tagged by the LEI even when it ceases operations. All LEIs are part of a global register, the LEI Index, which anyone can access free of charge and at all hours. The LEI index enables anyone to access the LEI and the associated reference data including links to local business registration or other selected international identifiers such as the S&P Global Company ID, BIC, or ISIN. The LEI offers data about “who is who” and “who owns whom.”

LEI record  
transparency  
enables users to  
check information  
for all issued LEIs,  
such as:

- Entity creation date
- Last data validation date
- Last update of LEI
- Entity operating status
- Next scheduled revalidation date
- LEI issuer
- Corroboration level

Source: IDC, based on information provided by GLEIF, 2023

Organizations can easily apply for an LEI by self-registering at one of the 39 accredited LEI issuers worldwide, serving 226 jurisdictions. The LEI issuers check the submitted data with local authorities and issue the LEI for a small fee. An annual renewal requirement ensures high quality of data. Organizations can become a Registration or Validation Agent, which expands the LEI issuer network. They can help their clients obtain LEIs and thereby streamline their LEI issuance.

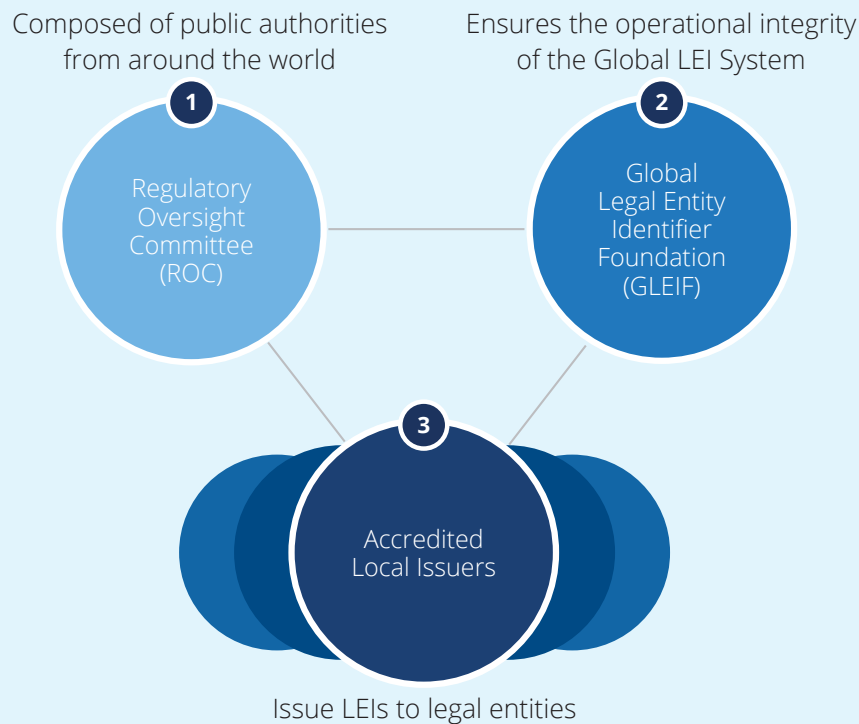
The organization operating the LEI Index, the Global Legal Entity Identifier Foundation (GLEIF), is a supranational non-profit organization based in Switzerland and founded by the Financial Stability Board (FSB), driven by the leaders of the G20 after the financial crisis in 2008. GLEIF is overseen by the Regulatory Oversight Committee (ROC) of more than 65 financial market regulators and public authorities as well as 19 observers from more than 50 countries.



Figure 6: Global LEI System and GLEIF Governance Framework

### Strong governance in place for LEI, the Global LEI System, and GLEIF

The LEI, the Global LEI System, and GLEIF are based on a strong global governance framework to protect the public interest, while promoting an open, flexible, and adaptable operational model:



Source: IDC, based on information provided by GLEIF, 2023

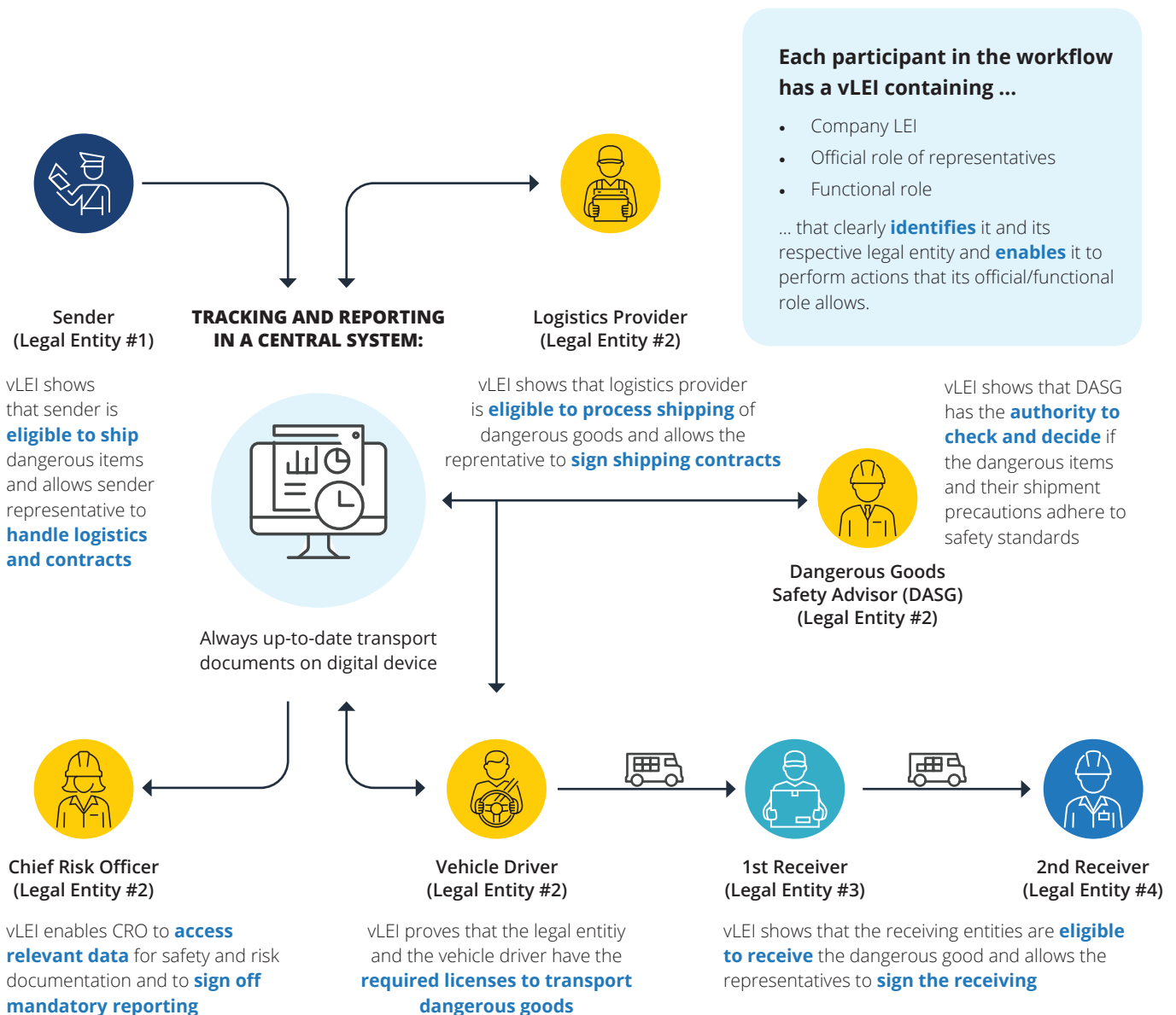
In December 2022 GLEIF launched the verifiable LEI (vLEI) to support automation of identity validation processes and add authentication and verification layers for organizational roles. This means the vLEI can also include person and role identity for representatives, either based on official organizational roles listed in ISO 5009 or on their own creations, for example, based on local organization types or relationship structure. With that, it becomes a digital credential, cryptographically bound to its owner.

The vLEI is based on open ACDC Credential (IETF draft) and Decentralized Identifier (W3C foundation) standards and is therefore interoperable. vLEIs are cryptographically bound to each other, building a trust chain with GLEIF the root of trust. Using the KERI network protocol, the vLEI is robust and quantum safe. KERI also gives organizations full control over the vLEIs, their identity data usage, and the transportation to the network of their own choice, enabling it to be operated on blockchain, distributed ledger technology (DLT), on premises, or in clouds. From an IT perspective, very little investment is required and the technological complexity for set up is low. A standard server is sufficient to operate the KERI protocol and to manage the self-issued vLEIs. Local software on every device is needed to log in and authenticate access to the vLEIs.

# Use Case: Using LEI and vLEI in Supply Chain Management to Enhance Compliance, Efficiency, and Innovation

Looking at the benefits of legal entity identities in supply chains, the handling of dangerous goods illustrates how vLEIs can contribute to compliance, efficiency, and innovation. This can also be translated to other goods, such as fakes (e.g., designer apparel) or those that fall under supply chain regulations (e.g., conflict minerals or protected resources such as rainforest wood).

Figure 7: Use Case: LEI and vLEI in Supply Chain Management for Compliance, Efficiency, and Innovation



Source: IDC, based on information provided by GLEIF

Figure 7 shows one supply chain link in a supply chain that could have dozens of links worldwide. Four companies, the sender, the logistics provider, and the two receivers have entity LEIs for the trade documents. The logistics provider has issued different role vLEIs for the officials in charge, the dangerous-goods safety advisor (DSGA), the risk prevention officer, and the vehicle drivers. With this, the individual vLEI representatives can perform actions that their role allows for, such as signing off the trade documents or even only parts of documents for which they are responsible, transporting the dangerous goods, checking the dangerous goods for proper handling, and submitting regulatory filings. Embedding the vLEI in all processes enables easier and faster identity and trade verification up to real-time speed, enhances the security and efficiency of operations, and helps reporting; it is also traceable compliant.

It also enables process innovation. This can be done by reinventing a process, such as making the automated, digital processing of all documents in a central platform accessible by eligible participants with defined roles, expressed digitally via the vLEI. Or it can be done by implementing a new technology, for example, to ensure that suppliers really are who they claim to be or do what they claim to be doing. IDC expects that by 2024, 15% of supply chain transactions will use blockchain for the provenance of ethical and sustainable practices. It can also be done by inventing a completely new way of doing things, such as setting up a circular economy with a large partner ecosystem based on strong reporting, holistic supply chain control capabilities, and using identities for the goods itself in the future.



## Conclusion

Every piece of software or system that provides visibility, transparency, or security adds a piece to the puzzle of building trust and mitigating risk in global supply chains. Secure and reliable identities are a prerequisite for trust, and trust is a foundation for secure, resilient, and prosperous trade — especially cross-border. Establishing a universal way to digitally verify legal entities and their key individuals can contribute to global society by fostering market integrity, financial stability, and a more inclusive worldwide trade system.

That makes the Global LEI System and the LEI important pieces of the puzzle. A key aspect is that the Global LEI System was established by the regulatory community as a public good and the system operations are managed by a foundation that is non-profit and based on an open governance framework, meaning the system is reliable and has no vendor lock-in risk. The digital vLEI can enable more efficient and agile business operations and can improve customer experience while ensuring security and compliance. In the emerging sustainability compliance area, the vLEI can support supply chain due diligence and sustainability reporting.

IDC believes interconnectivity, ease of access, and a critical mass of participants are key success factors for digital identity and trade digitalization. To reach critical mass, IDC believes large enterprises and organizations, regulators and policy makers, financial institutions, and vendors and service providers should be the driving force here. They must work together to particularly enable small businesses worldwide, standardize methods and solutions, and promote the sharing and exchange of data.



## Resources

- IDC European Identity and Digital Trust Forecast, 2022–2026 (IDC #EUR148752522, June 2022)
- IDC European IT Security Survey, May 2022
- IDC Europe Sustainable Strategies and Technologies Maturity Survey, January 2022
- IDC Future Enterprise Resilience and Spending Survey, Wave 5, June 2022
- IDC Future Enterprise Resilience and Spending Survey, Wave 7, August 2022
- IDC Future Enterprise Resilience and Spending Survey, Wave 12, January 2022
- IDC FutureScape: Worldwide Corporate Banking 2023 Predictions (IDC #US49830222, October 2022)
- IDC FutureScape: Worldwide Blockchain 2021 Predictions (IDC #US45927420, October 2020)
- IDC Security Identity Survey, September 2021
- IDC Sustainability in Germany 2022 — Greening of and by IT, March 2022
- IDC Worldwide Identity and Access Management Forecast, 2022–2026 (IDC #US48670522, July 2022)
- The OLAF Report 2021, European Anti-Fraud Office, European Commission, Publications Office of the European Union, 2022

## ABOUT THE ANALYST



### **Marco Becker, Consulting Manager, IDC Central Europe**

Marco Becker has been a senior consultant at IDC since 2019. He mainly prepares studies and implements customer projects, for which he is in contact with both provider and user companies. His focus is on (I)IoT technology, cloud, cybersecurity, sustainability, and network technologies.

## ABOUT IDC

IDC is the world's leading provider of market information, consultancy services, and events in the information technology and telecommunications field. IDC analyzes and forecasts technological and industry-related trends and potential, enabling clients to plan business strategies and IT purchasing. Drawing on its network of more than 1,300 analysts in 110 or so countries with global, regional, and local experience, IDC offers clients comprehensive research on the IT, TC, and consumer markets. Managers and IT professionals have been placing their trust in IDC for decision making for more than 50 years.

For more information, please visit [www.idc.com](http://www.idc.com) and [www.idc.de](http://www.idc.de).

## COPYRIGHT NOTICE

External publication of IDC information and data, including all IDC data and statements used for advertising purposes, press releases, or other publications, requires prior written approval from the appropriate IDC vice president, country manager, or managing director. A draft of the text for publication should accompany any such request. IDC reserves the right to deny approval of external publication for any reason.

For more information, please contact:

Lynn-Kristin Thorenz, Associate Vice President, Research and Consulting, IDC • eMail: [lthorenz@idc.com](mailto:lthorenz@idc.com)

© IDC, 2023. Reproduction of this document without written permission is strictly prohibited.