

Position paper on potential accreditation frameworks for e-invoicing and DRR purposes

The Global Exchange Network Association (GENA) supports facilitating the cross-border movement of goods and services through harmonised digital trade processes, including digitalised tax controls in the form of Continuous Transaction Controls (CTC), such as digital real-time reporting (DRR) and electronic invoicing (e-invoicing). As global markets shift towards digitalisation in trade and tax controls accelerate, with more and more governments introducing 4- and 5-corner models, service providers (as a distinct group of software vendors specialising in e-invoicing, compliance and/or process automation) have become pivotal players in the broader ecosystem. Relying on these professional parties and aggregators, who possess strong commercial incentives to deliver high quality services and robust data controls, represents a positive development for the full CTC ecosystem. With this development, quality and security assurance becomes important for all stakeholders, and it is natural that governments would assess the need for accreditation schemes for third-party intermediaries.

ViDA legislation recognises the critical role of third parties, including service providers, in facilitating e-invoicing and DRR. However, it leaves considerable discretion to Member States to take necessary measures towards taxpayers and such third parties to ensure compliance. An example of such measures mentioned by ViDA is the possible implementation of local accreditation frameworks. While such local accreditations can bring many benefits, they risk carrying conditions that may perpetuate fragmentation of the Single Market and/or add disproportionate compliance burden, which may ultimately impact the taxpayers by increasing the costs and operational complexities of compliance.

Purpose of this Document

As a proponent of the 4-corner and 5-corner models, the Global Exchange Network Association (GENA) endorses the introduction of accreditation schemes on third-party vendors (including but not limited to service providers, and ERP, accounting software, workflow and process automation vendors) operating within these ecosystems, provided that they are justified, proportionate, harmonized, and equitable, without creating unnecessary barriers to competition or imposing redundant compliance burdens.

This position paper, developed by the GENA, explores the potential implementation of accreditation frameworks for service providers. It does not advocate for or against any specific accreditation or certification scheme. Instead, it offers a set of insights and considerations aimed at supporting informed decision-making by authorities. Ultimately,

the goal is to support decisions that serve the best interests of both governments (by strengthening tax compliance and system integrity) and taxpayers, by ensuring fair, efficient, and accessible digital tax environments.

While the primary focus is on the European Union, particularly in the context of the VAT in the Digital Age (ViDA) initiative, the principles and recommendations outlined are equally relevant to other jurisdictions, that are considering similar frameworks, globally.

Guiding principles

Accreditation of third-party vendors, if implemented, could offer an approach to establish basic standards of security, reliability, and compliance, which can benefit all stakeholders from tax administrations to taxpayers. The following are a number of guiding principles that can be considered when implementing accreditation schemes.

1. Requirements must be proportionate to objectives

Effective accreditation frameworks must focus on essential requirements that are proportionate to actual risks, avoiding overengineered standards. Third-party vendors should not face multiple accreditations for identical functions. Taxpayers will ultimately bear the cost of such redundancy. Technical specifications and registration processes must facilitate rather than restrict market access, ensuring that qualified providers from any Member State can compete fairly across the Single Market.

2. Requirements must ensure equal treatment between third-party vendors

Taxpayers may leverage various kinds of instruments (software, services) to help them comply with the ViDA requirements on e-invoicing and DRR. It is important that any accreditation scheme establishes equal treatment of such instruments, regardless of whether these are service providers, accounting software, ERPs, etc., to avoid introducing distortion to the market and providing for loopholes to circumvent the accreditation schemes.

3. "Certify Once": Accreditation recognition principle

Under the "Certify Once" principle, it would be sufficient to undergo the accreditation process once in any single Member State, with this accreditation being recognised across the entire Union. This could be achieved through multiple mechanisms, including but not limited to the development of a harmonised accreditation mechanism at the European Union level, with automatic validity across all Member States, alternatively by Member States recognizing accreditation from other Member States even without such harmonized schema. It should be noted that, under such harmonised accreditation schemes, Member States may still have a need to assess technical readiness separately.

4. Clear responsibilities and liability

In an accreditation model, third-party vendors maintain clear accountability to their primary clients, the taxpayers, while meeting standards set by tax authorities. It is important that such a model also explicitly establishes responsibilities and liabilities, that flow from the accreditation for all parties.

Favourable requirements

Following the above guiding principles, the Appendix outlines accreditation requirements that could be considered either on the EU or individual, Member State level.

Unfavourable requirements requiring careful consideration

Accreditation requirements that go beyond essential technical, security, and operational standards may create significant, unwarranted impediments to effective and competitive market functioning, without delivering corresponding benefits to both taxpayers and tax administrations. Such requirements contradict Single Market principles by imposing barriers to cross-border provision of services and increase operational and compliance costs for taxpayers. Accordingly, they undermine ViDA's harmonisation objectives and warrant careful consideration to determine how and whether to implement them.

1. Local establishment

Providers established in any EU Member State, EEA members, or jurisdictions with mutual assistance agreements should be eligible to offer their services to any taxable person throughout the entire Union. A VAT number from any such trusted jurisdiction ought to provide sufficient identification of a legitimate business entity. Member States should therefore avoid requirements that a service provider should be locally established. Local VAT registration should be limited to cases where necessary strictly for taxation of the services provided, not as an identification mechanism or requirement to provide services in the jurisdiction. The same applies to requirements for local subsidiaries, branches, other establishments or even to the obligation to obtain a local tax identification number merely for the purpose of obtaining a local digital certificate.

2. Data sovereignty

It is important that requirements for data processing and storage balance legitimate sovereignty concerns with practical business realities. The focus should be on security outcomes and accessibility for tax audits rather than strict localisation. A balanced approach might include whitelisted or safe countries for data storage and processing,

with reasonable operational requirements ensuring necessary oversight without imposing disproportionate infrastructure costs.

Cloud computing security requirements, if applied, should not recognise only domestic frameworks of particular Member States and/or otherwise require that data must be processed on servers located solely in that particular Member State, thereby disqualifying other Member States corresponding frameworks.

To ensure that data sovereignty goals are met, cloud computing regulations should not apply solely to intermediaries handling data on behalf of taxpayers but must also apply to the source systems in the framework.

3. Restrictions through technical implementations

Requirements that mandate specific technical configurations indirectly achieve the same restrictive effect as explicit localisation requirements. One example includes restrictions on the use of IP addresses to the effect that only local IP addresses can be used to connect with the tax administration. Another example is the requirement for a local digital certificate for identification purposes, as opposed to using a certificate that complies with eIDAS, or the use of local digital signature standards that do not exist in other Member States or are otherwise not compatible with the European Norm for electronic invoices.

4. Financial stability judged on years of existence based on geography

Requirements mandating a specific number of years of financial history or operational presence within a particular jurisdiction, rather than accepting proven track records from other Member States can be unnecessarily prohibitive and disproportionate to the intended objective.

5. Localised language or onshore staff

Requirements to have local personnel who speak the local language, requiring all contracts and documentation to be in the local language and/or having employees in one, specific country, create significant operational burdens for the cross-border provision of services. Such aspects should not be a requirement in an accreditation scheme, but a market driven requirement.

6. Restrictions on taxpayers to use a single vendor

It is essential that accreditation frameworks and their technical specifications do not create structural barriers that inadvertently hinder taxpayers to leverage multiple kinds of instruments, regardless of whether these are service providers, accounting software, ERPs, etc., ensuring that compliance mechanisms remain adaptable and supportive of diverse business models. Taxpayers should not be hindered in their decision to select multiple, accredited solutions best suited to their individual needs, fostering innovation

and competition within the marketplace. Imposing a single-vendor dependency, as we have seen in some jurisdictions, not only constrains business continuity and growth, but can also lead to increased costs for taxpayers and reduced resilience.

Conclusion

The decision on whether to implement service provider accreditation/certification schemes remains at the discretion of individual Member States under ViDA.

For Member States pursuing accreditation/certification schemes, we strongly recommend a practical, harmonised approach based on mutual recognition and essential requirements. Well-designed frameworks support both trust and competition, while fragmented requirements create unnecessary compliance costs, market barriers and bureaucracy.

We urge jurisdictions to prioritise harmonisation, proportionality, and recognition of the critical role third-party vendors play in enabling effective e-invoicing and digital reporting implementations, to ensure that any accreditation scheme benefits both tax administrations and taxpayers alike. This aligns with the Commission's vision to ensure interoperability and deployment of European standards, ultimately facilitating a simple, fair and seamless Single Market.

Appendix: best practice requirements

This appendix outlines best-practice requirements that jurisdictions may consider when implementing their accreditation frameworks. This list should not, by any means, be considered as exhaustive or a ready-to-use template. Rather, careful consideration should be given to each criterion to determine its application in their domestic framework.

Requirement category	Key components
Service provider identification and validation	<ul style="list-style-type: none"> • Establishment and VAT registration from any EU Member State or jurisdictions with mutual assistance agreements, including EEA members. • Proportionate verification procedures confirming legitimate business status. • Provide information relating to legal representatives, board members, partners, shareholders, and direct and indirect controllers.
Demonstrated performance record	<ul style="list-style-type: none"> • Absence of significant negative compliance events or violations. • No outstanding tax debt in country of establishment. • Having a business continuity and contingency plan. • Not being included in a regime of restructuring or bankruptcy.
Technical security and operational resilience	<ul style="list-style-type: none"> • Maintaining agreed information security certification, e.g. ISAE, ISO or equivalent. • Comprehensive data security infrastructure. • Documented business continuity and disaster recovery provisions. • Appropriate user access controls and security monitoring mechanisms.
Data protection rules and regulations	<ul style="list-style-type: none"> • Compliance with applicable personal data protection legislation, such as the GDPR.
Know Your Customer framework	<ul style="list-style-type: none"> • Fulfilling established Know Your Customer (KYC) frameworks.
Financial Stability Assessment	<ul style="list-style-type: none"> • Financial stability demonstrating sufficient resources to maintain reliable service provision. • Business sustainability appropriate to the services offered.
Professional indemnity insurance	<ul style="list-style-type: none"> • Professional indemnity insurance with coverage levels proportionate to service volume, business risk, and potential liabilities.
Technical capabilities	<ul style="list-style-type: none"> • Support for EN16931 with requirements not to refuse accepting this format from end-users and other accredited providers, unless otherwise mutually agreed by end-users or otherwise stipulated in legislation.

Requirement category	Key components
	<ul style="list-style-type: none"> • Support for other, locally required structured formats besides EN16931. • Ensure document legibility for their end-users • Support for and offering at least the most common document exchange protocols towards other providers, such as Peppol AS4, CEF AS4. • Obligated to interoperate with all other accredited providers in their jurisdiction and across the EU. • Offering to customers a minimum set of the most common communication protocols such as SFTP, AS2, rest API etc. • Support for and offering Peppol as the minimum common denominator for, at least, intra-Community traffic. • Successfully completing a defined testing process to prove e-invoicing and DRR capabilities. • Capacity to meet reporting timelines and transmission requirements or uphold specified uptime SLAs. • Evidence of underwriting of common standards and service provider collaboration, i.e. participation of a common industry network, such as GENA.