A&M TAX MIDDLE EAST

Digital Identity and Invoice Fraud Risks in Peppol Based E-Invoicing

Belgium's case and what it means for UAE businesses

Executive Summary

The United Arab Emirates' (UAE) implementation of the Pan-European Public Procurement Online (PEPPOL) based mandatory e-invoicing and e-reporting regime is well underway with the first wave going live on 1 January, 2027. While businesses are busy getting ready to comply with this new regulation, it is worth analyzing recent live PEPPOL mandates, particularly Belgium – to de-risk implementation activities and Accredited Service Providers (ASP) selection to a minimum.

While PEPPOL's structured, machine-to-machine e-invoicing infrastructure strengthens auditability and transparency, a recent cybersecurity report in Belgium by SalesBridge and SafeByte* demonstrates that the shift to mandatory e-invoicing introduces digital identity governance and operational fraud risks that are frequently underestimated. The research further highlights that it is technically possible to transmit fraudulent e-invoices through PEPPOL that appear entirely legitimate to recipients.

This article explores this cybersecutiy threat in more details, drawing on the Belgian research and highlight some of the key governance risks to consider for UAE businesses.

This article explores these cybersecurity risks in greater detail, drawing on Belgium's experience, and highlights key governance considerations for UAE businesses operating in an environment where financial resilience, cost control, and supplier risk management have become increasingly critical.Q

In addition, UAE businesses are currently operating in an environment characterized by heightened financial discipline, tighter liquidity conditions, and evolving strategic priorities. In such a context, the margin for operational error, fraud exposure, or control failure is significantly reduced. As organizations reassess cost structures, supplier relationships, and cash management practices, the implementation of e-invoicing must be approached not only as a compliance requirement but as a critical control mechanism to safeguard working capital and financial integrity.

What are the cyber-security risks relevant to e-invoicing?

01

Digital Identity Fraud:

In a PEPPOL environment, each company is identified by a PEPPOL Participant Identifier (PEPPOL ID), which functions as its digital trade identity. The PEPPOL ID is needed to receive any e-document through the PEPPOL network.

PEPPOL IDs typically consist of a numerical code of two parts such as 0208:0123456789, if we take a standard Belgian company as an example.

In the case of Belgium, many Belgian companies had PEPPOL IDs automatically created via the national Hermes platform, which served as a temporary government platform until 31 December, 2025, to help businesses unable to directly use PEPPOL send digital structured invoices.

In several cases, companies were unaware that their PEPPOL ID existed in the first place and were left unclaimed or unmanaged.

This situation resulted in a vulnerability window in which malicious actors could attempt to exploit dormant or unclaimed PEPPOL IDs and attempt to pose as the legitimate business itself.

In the UAE context, where organizations are increasingly focused on cash preservation and supplier payment accuracy, the misuse of a digital identity could have immediate financial consequences. Fraudulent invoices processed through automated systems may directly impact liquidity positions, particularly in organizations with high transaction volumes or centralized shared service centers.

02

Access Point Onboarding Vulnerabilities & False Delivery Assurance:

PEPPOL operates through certified Access Points (APs) that onboard businesses and route e-invoices through its network. One of the key risks identified by the report highlighted risks associated with weak identity verification (KYC/KYB) during onboarding.

If onboarding controls at the AP level are insufficient, a malicious actor could attempt to register using a legitimate company name or a valid VAT number.

If successful, any invoice generated by the malicious actor would then travel through the certified e-invoicing infrastructure and produce a “successful delivery” status, thereby appearing compliant.

Despite the delivery confirmation being merely evidence of a technical transmission between APs, without validation of the invoice content or its commercial legitimacy, some companies have equated it to an authenticity corroboration and allowed these invoices to be processed through their standard Procure-To-Pay (P2P) processes.

This risk is particularly relevant in the current UAE environment, where many organizations are streamlining procure-to-pay processes and increasing automation to drive efficiency. While automation improves speed and reduces manual intervention, it also increases dependency on upstream data integrity. Without reinforced validation controls, erroneous or fraudulent invoices may flow through systems more quickly, amplifying financial exposure before detection.

It is, however, important to note that these risks don’t lie in PEPPOL’s encryption architecture itself but in the insufficient governance framework by its various participants.

03

Cloud Exposure Risk:

**As recently as October 2025, a company called Invoicely used by 250,000 businesses globally, accidentally exposed a repository in its cloud infrastructure with over 178,000 sensitive and financial documents, including Personally Identifiable Information (PII), which is one of the most critically protected categories of data globally.

PII data can be leveraged by malicious actors for a multitude of purposes including identity theft, social engineering, and targeted invoice fraud to name a few.

This situation did not result from a sophisticated cyberattack on Invoicely’s infrastructure but a simple misconfiguration of one storage component as “public read” in their Amazon Web Services instance by Invoicely themselves.

While this relates, strictly speaking, to online-generated invoicing as opposed to e-invoicing meant via PEPPOL, most e-invoicing providers are cloud-based (Software as a Service (SaaS)) and therefore exposed to this risk.

What Does This Mean for UAE Businesses

Given the UAE's e-invoicing and e-reporting framework is based on PEPPOL, the risks laid out above are directly relevant to businesses in the country and should be viewed as additional justifications to introduce a strong governance framework while getting ready for the country's mandate:

Beyond regulatory compliance, UAE businesses must consider e-invoicing implementation within the broader context of operational resilience and financial risk management. As organisations reassess supplier ecosystems, renegotiate contracts, and optimise working capital, the integrity of invoicing processes becomes increasingly central to maintaining financial stability.

Active Identity Management

A business's digital identity must be actively managed, including claiming it as soon as feasible, assigning clear internal ownership, and integrating its management into the broader internal governance and control framework. Ultimately, it should be viewed as a corporate asset.

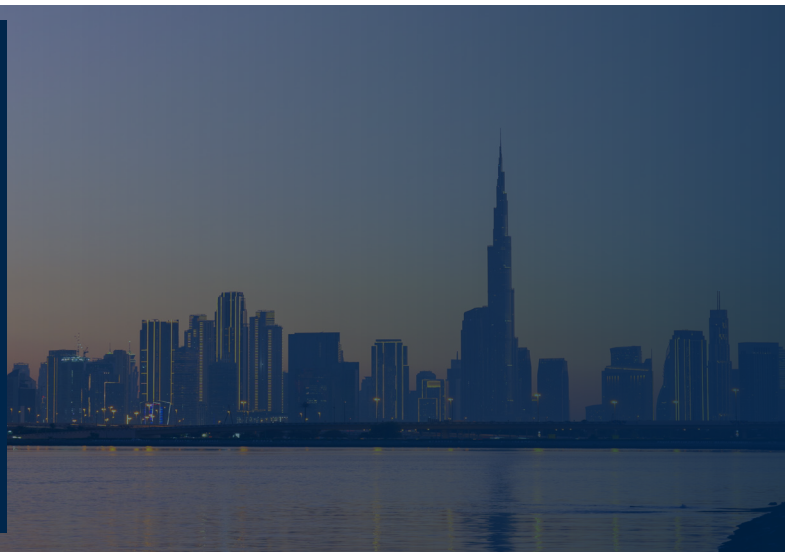
ASP Security Scrutiny

Clear understanding of Accredited Service Provider's (ASPs) security setup, official certification, cloud hosting locations including access control policies, encryption at rest/in transit, and their onboarding process controls. Your chosen ASP effectively becomes a part of your organization's overall control framework.

Retention of Internal Controls

Existing controls from vendor risk management, Know Your Customer (KYC), three-way matching or Tax Registration Number (TRN) validation as an example remains essential. The UAE e-invoicing mandate will increase the transparency and auditability of data, but it does not replace internal controls.

For UAE businesses, the implementation of e-invoicing should be seen as a finance transformation project, beyond mere compliance. It needs to be looked at holistically and strategically to ensure the maximum benefits are extracted from the investment made, which include updating the governance and internal controls framework to de-risk the consequences of operating in a machine-to-machine digital world from 1 January, 2027.



How A&M can help

A&M provides deep technical expertise in helping businesses in the UAE to get ready for e-invoicing. Our structured methodology has been proven worldwide in extracting the maximum benefits from the original investment in getting ready while de-risking the implementation to ensure compliance from day one.

How Skill Quotient can help

SMARTeIS by Skill Quotient supports organizations with a security-first, governance-led approach to PEPPOL e-invoicing implementation. Our methodology combines secure-by-design engineering, strong DevSecOps discipline, defense-in-depth architecture, and continuous monitoring to reduce digital identity and invoice fraud risks.

Key Contacts

Pierre Arman
Managing Director
parman@alvarezandmarsal.com

Sathish Reddy
CEO at Skill Quotient Group
sathish.reddy@skillquotientgroup.com

Follow A&M on:

Founded in 1983, Alvarez & Marsal is a leading global professional services firm. Renowned for its leadership, action and results, Alvarez & Marsal provides advisory, business performance improvement and turnaround management services, delivering practical solutions to address clients' unique challenges. With a world-wide network of experienced operators, world-class consultants, former regulators and industry authorities, Alvarez & Marsal helps corporates, boards, private equity firms, law firms and government agencies drive transformation, mitigate risk and unlock value at every stage of growth.

To learn more, visit AlvarezandMarsal.com

* https://www.vatupdate.com/2026/01/02/risk-of-identity-fraud-with-mandatory-e-invoicing-via-peppol/

** https://www.esecurityplanet.com/news/invoicely-178k-records-cloud-misconfiguration/

488696-59191/March 26