opentext™

OpenText Active Invoices with Compliance

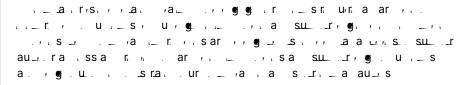**Meet**

Maintain

Simplify

In much of the world, sending and receiving invoices electronically requires compliance with government regulations, and increasingly, these regulations are becoming mandatory both for business to government (B2G) and business to business (B2B) invoice transactions often requiring invoices to be submitted directly to the tax authority or a government approved portal/agent before they can be sent to customers.

Global e-Invoicing network

Name	Description
Onboarding	Automatically provides PDF invoices via email to SME customers with no human intervention, allowing for large-scale deployment
	Provides largest team of specialists dedicated to rapidly enabling a global partner community using OpenText Community Onboarding for EDI-based partners
Data validation	Provides configurable rules to ensure that invoice data meets government requirements as well as internal business rules
Country validation	Validates as per rules configured for the sender country for different types of documents, such as invoices, credit notes, etc
Duplicate invoice check	Ensures that a sender cannot send multiple invoices with the same invoice number within a fiscal year
Currency check	Ensures the currency used in sender invoice documents is from a pre-approved list
Legal entity relationship check	Ensures an explicit relationship is established between legal entities before they start transacting, as is required for some countries and processes (non-signed EDI)
Authenticity and integrity	Guarantees authenticity (e-Invoice comes from the claimed source) and integrity (the e-Invoice has not been altered) through the application of digital signatures/electronic seals in accordance with country-specific legislation
	• Several formats and signature parameters available using locally approved certificate authorities • Support for Batch signing for EANCOM format invoices • Revalidation of the signature in the Archive UI
	Non-signed EDI can be used within the EU and UK, providing a process-based method to demonstrate integrity and authenticity Typically, this means keeping additional reports and evidence:
	• Human readable version of EDI data • Summary lists • Partner list • Audit trail demonstrating use of secure communications (VAN, sFTP/FTPs, AS2, VPN) •

o   n