Australian Government

New Zealand Government

A-NZ PEPPOL FRAMEWORK GUIDANCE NOTE

Know Your Customer (KYC)

Guidance note 04

Issue date	**Version**
15 November 2019	1.0
Effective from	**Artefacts impacted**
November 2019	

Introduction

The purpose of this document is to provide instructions on how Access Point (AP) Providers and Service Metadata Publisher (SMP) Providers in Australia and New Zealand can meet the requirements of the Know Your Customer (KYC) principle in the PEPPOL Compliance Policy. This document also includes recommended practice for accounting/invoicing software providers.

It is essential that the identity of end-users is reliable to maintain confidence and trust in the e-invoicing network. Appropriate validation checks reduce the risk of fraudulent behaviour which impacts end-users and can damage the reputation of the network and its participants. The requirements in this document consider current industry best practice and create a baseline level of validation, which PEPPOL Authorities will work with Service Providers to continue to strengthen as the network matures.

KYC validation:

- provides greater assurance of the identity of the end-users,
- provides end-users with a seamless service experience,
- mitigates the risk of potential bad customer behaviour, and
- increases protection against the fraudulent misuse of a business's identity.

Note, this guidance note should be read in conjunction with the ABN and NZBN validation guidance notes.

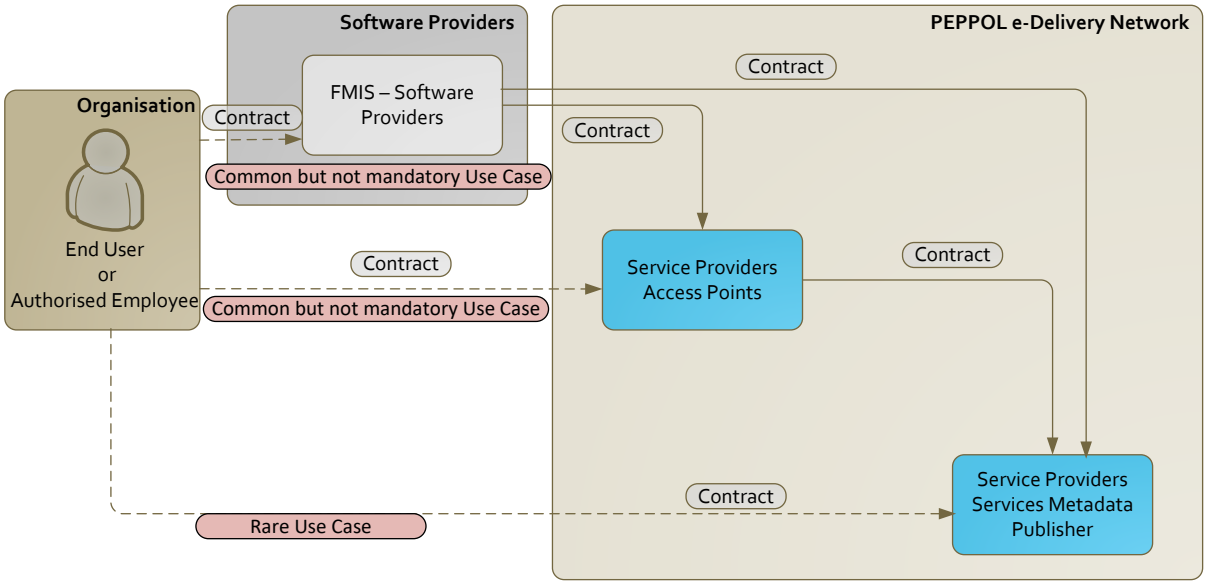
Issue

To ensure a high level of data integrity is achieved and to reduce the potential for misuse to occur, OpenPEPPOL has developed a Compliance policy that all PEPPOL AP and SMP Providers, and PEPPOL Authorities must adhere to. Within the compliance policy, overarching principle 8 states the requirement to undertake KYC.

> *Each AP service provider must have a written service contract with its customers carrying forward the minimum requirements defined by OpenPEPPOL.*

Until the minimum requirements are defined for the PEPPOL Framework, the requirements within this guidance note will be applied as the minimum requirements for APs and SMPs operating in Australia and New Zealand.

Roles and Responsibilities



The KYC checks identified in this table are defined in detail in the guidance section below.

Role	Responsibility
Organisation (end user)	Provide accurate information and keep entity details up to date. Ensure only authorised representatives have access to act on behalf of the business
Software providers	Define and implement relevant KYC processes Ensure appropriate KYC is implemented for contracted end-user customers Perform regular checks to ensure accuracy of information
Access Point Provider	Define and implement appropriate KYC processes Ensure KYC is implemented for contracted end-user customers

	Perform regular checks to ensure accuracy of information Verify that service providers have validated pre-existing KYC checks, or performed KYC checks for their contracted end-user customers. Only allow updates from software providers that the AP provider is in a contract with.
Services Metadata Publisher Provider	Define and implement appropriate KYC processes Ensure KYC is implemented for end-user customers Perform regular checks to ensure accuracy of information Verify that access points and service providers have performed or validated pre-existing KYC checks for their contracted end-user customers. Only allow updates from access points or software providers that the SMP provider is in a contract with.

Guidance

Requirements for AP and SMP Providers

1. Customer identification process (**Mandatory**)

   All AP and SMP providers are to ensure KYC identification and verification checks have been performed, either directly as part of their on-boarding, or by their contracted Software Providers as part of their on-boarding procedures.

   This must include documented processes for:

   - How information is collected and verified; and
   - How discrepancies will be handled.

2. Verify Entity Registration details (**Mandatory**)

   Verify the end-user customer's identifier and name:

   - ABN – via the Australian Business Register
   - NZBN – via the New Zealand Business Number Search
   - GLN – via the GS1 Company Database
   - DUNS – via the D-U-N-S Number Lookup

   Note: For existing end-user customers, if verification has not previously been performed, verification should be undertaken for those customers within 18 months.

3. Verify Representative (**Recommended**)

   AP and SMP Providers should verify the person registering is a representative of the end-user customer.

Possible options for verification include:

- checking via the entity's official webpage, email, or telephone number/s,
- checking a public register to identify listed office holders of the entity (e.g. ASIC registers in Australia, Companies Register in New Zealand),
- confirming with an office holder that the representative is authorised,
- leveraging off other authorisation processes or evidence of existing business activity (e.g. bank, ATO, tax agent, utility bills, rates bills).

Note: For existing end-user customers, if verification has not previously been performed, verification should be undertaken for those customers within 18 months.

4. Updating key information (**Mandatory**)

   Where key information is updated or changed on the end-user customer's record, the customer identification process in item 1 must be applied, including verification requirements in item 2 (Entity Registration details).

Accounting/invoice software providers (Recommended)

Accounting/invoicing software providers who create the e-invoice can significantly contribute to ensuring the integrity of the information used in the eDelivery network.

Accounting/invoicing software providers should implement the KYC checks described in this guidance note.

AP and SMP Providers should inform accounting/invoicing software providers of the benefits of KYC checks and encourage their implementation.

Further information

Further guidance on identity validation can be the Identity Verification Code of Practice 2013 released by Department of Internal Affairs. A copy of the Code can be found here.

The Guideline document for the "Accountants" for complying with the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 can be found here.

Version history

Version	Date	Change
1.0	15 November 2019	Initial published version