

A-NZ PEPPOL FRAMEWORK GUIDANCE NOTE

A-NZ Information Security Guidance for e-Invoicing Service Providers

Guidance Note 03

Copy available for download here

Issue Date	Version
15 November 2019	1.0

Effective From	Artefacts Impacted
November 2019	Annex 5

Introduction

The European PEPPOL framework has been formally adopted by both the New Zealand and Australian governments for e-Invoicing. The framework will provide businesses with the opportunity to fully digitise the invoicing process allowing them to pay invoices faster, reduce incidents of fraud and refuse costs associated with invoice handling.

While several mitigations are inherent in the OpenPEPPOL framework, an analysis of the threat landscape has identified additional controls required to respond to a number of risks rated as

high. These risks can be summarised in the threat statement below.

An external threat actor or insider motivated by financial profit, a desire to cause business disruption, state sponsored or industrial espionage, accesses an element of the e-Invoicing process. They then modify or collect business and invoice data as it is being processed, stored or transmitted by the systems involved in e-Invoicing. This results in financial losses for the affected businesses, attention from the media, a loss of stakeholder confidence in the e-Invoicing process and poor uptake of e-Invoicing by businesses due to the perceived risks.

Scope

The A-NZ Information Security Program applies to all e-Invoicing service providers, that provide (or are seeking to provide) Access Point and/or Service Metadata Publisher services.

Large organisations with diverse service/product offerings, may limit the scope of the information security program to relevant policies, procedures and systems of the business unit responsible for the e-Invoicing Access Point / Service Metadata Publisher service.

Objectives

The Information Security is a collective obligation of the PEPPOL Service Providers and the A-NZ PEPPOL Authorities.

This Information security guidance has below collective objectives

- Increased trust and assurance
- Reduce Security related incidents
- Less or no reputational damage
- Apply PEPPOL regulatory compliance

Key Requirements

Section 2.1 of the Annex 5 within the Transport Infrastructure Agreement, requires *PEPPOL SMP and AP Providers must comply with any security requirements defined by the PEPPOL Authority. PEPPOL SMP and AP Providers will be required to provide evidence of compliance against the requirements for accreditation and demonstrate their continued compliance to maintain their accreditation.*

The below table describes the information security requirements required by e-Invoicing Service Providers.

Requirement	Detail
Self-certification or independent certification against either ISO/IEC 27001 or ASD ISM/NZ ISM	Potential service providers **should** consider the applicability of all controls within the standard, however the assessment **must** include suitable evidence for the following controls: • Encryption key management • Network segregation • Audit logging • Patch and vulnerability management program • Information security awareness, education and training • Physical and environmental security • Operational procedures and responsibility • System acquisition, development and maintenance – including secure coding practices • System access control • Personnel security • Backup
Encryption at rest	Business documents when stored are encrypted at rest. Encryption may be at the disk, container, application or database level. Encryption at rest should follow [Australian Government Information Security Manual (ISM) approved cryptographic algorithms and protocols / New Zealand Government ISM cryptographic algorithm and protocols.]
Security monitoring practices	Security monitoring must be in place – including denial of service mitigations. For example: • network / infrastructure layer; • application layer; • transaction (data) layer.
(Access Points only) Encryption in transit for all e-Invoicing information (business documents) sent and received by an Access Point	Business documents are encrypted in transit utilising TLS 1.2 or higher or another [Australian Government Information Security Manual (ISM) approved cryptographic algorithm and protocols / New Zealand Government ISM cryptographic algorithm and protocols.]
(Access Points only) Multifactor authentication	End users that directly interact with a PEPPOL AP must utilise multi-factor authentication.

Further Guidance

Self-certification or independent certification against either ISO/IEC 27001 or ASD ISM/NZ ISM

Self-certification

The self-certification requirement seeks to provide the PEPPOL Authority with a level of assurance that Service Providers have robust security practices in place. This is done by way of self-certifying against one of the below standards:

- ISO/IEC 27001
- ASD ISM / NZ ISM

The scope of certification **should** cover relevant organisational policies, procedures and data repositories that hold or manage PEPPOL BIS information.

A-NZ PEPPOL Authorities do not expect Service Providers to be fully compliant with the complete range of controls of your chosen standard. The controls that Service Providers should be compliant with will be dependent on operating model and the architecture of solution. We also acknowledge there may be areas where Service Providers are unable to demonstrate compliance with particular controls. In these scenarios Service Provider will be required to offer supporting commentary to substantiate the non-compliance or the manner / timeframe in which Service Provider expect to address the gap.

Where Service Providers deem a control not applicable a short description should be provided as rational behind the inapplicability.

Service Provider's self-certification **should** be reviewed at prescribed intervals or when significant changes occur within the environment. For the purpose of meeting the requirement for self-certification, Service Provider must review self-certification annually and resubmit an updated version every 2 years. Where Service Provider have had a significant change in environment which affects the controls that have addressed as part of self-certification, Service Providers are required to submit a revised version to the PEPPOL Authority as soon as possible.

The A-NZ PEPPOL Authority is unable to prescribe which of the above methods Service Providers **should** use. The choice of what standard to self-certify against should be made on the basis of suitability to Service Provider Solution.

Service Providers are able to request to use an alternative security standard if Service Provider believes it would be more suitable for your circumstances. These requests will be assessed on a case-by-case basis.

Evidence required for Self-Certification

Completed documentation demonstrating your conformance with the requirements (full control suite) of one of the approved security standards including comments on why certain controls may or may not be applicable to Service Provider and how controls that do apply are addressed by Service Provider

Independent Certification

The independent certification requirement seeks to provide the A-NZ PEPPOL Authority with a level of assurance that Service Providers have robust security practices in place.

This is done by way of attaining independent certification against one of the below standards:

- ISO/IEC 27001
- ASD ISM / NZ ISM

The scope of independent certification should cover Service Provider information security practices and below mentioned areas

- Risk Management
- Auditing and Logging
- Monitoring & Reporting
- Vendor Management

Large organisations with diverse service / product offerings, may limit the scope of the certification to relevant policies, procedures and systems of the business unit responsible for the primary products or services which hold or transact e-Invoicing related information.

We don't expect Service Provider to be fully compliant with the complete range of controls. The controls that Service Providers **should** be compliant will be dependent on operating model and the architecture of the Solution. We also acknowledge there may be areas where Service Providers are unable to demonstrate compliance with particular controls. In these scenarios Service Provider will be required to offer supporting commentary to substantiate the non-compliance or the manner / timeframe in which you expect to address the address the gap.

Where Service Providers deem a control not applicable this should be addressed in the statement of applicability.

Service Provider independent certification **should** be reviewed at prescribed intervals or when significant changes occur within your environment. For the purpose of meeting the PEPPOL framework requirement for independent certification, Service Provider must maintain independent certification on going. This evidence needs to be supplied to the PEPPOL Authority. Where you have had a significant change in your environment which affects the

controls you have addressed as part of your independent certification, Service Provider **must** submit a revised version to the PEPPOL Authority as soon as possible.

The A-NZ PEPPOL Authority is unable to prescribe which of the above methods Service Providers **should** use or provide links to them. The choice of standard to complete independent certification should be made on the basis of suitability to Service Provider.

Evidence required

- Completed documentation demonstrating your conformance with the requirements (full control suite) of one of the approved security standards outlined above.
- Statement of Applicability
- Letter of Compliance
- Copy of certificate upon completion of independent certification

Encryption at rest

This requirement seeks to protect e-Invoicing related information from unauthorised access.

You can chose to apply encryption at the disk, container, application or database level. Encryption at rest should follow the relevant cryptographic controls outlined in the ASD ISM or NZ ISM.

Evidence required

- Screenshot showing encryption enabled at the database or disk level with the type of encryption at rest being used
- When using 'out of the box' encryption a licensing agreement or screenshot showing 'out of the box' encryption at rest enabled
- If using the infrastructure of a cloud provider to encrypt data at rest, an invoice or contract agreement could be provided or screenshot from within the cloud environment showing encryption enabled.

Where encryption at rest is not viable, evidence must be provided of a full range of data protection controls.

These **must** include:

- User/system (service account) access control (including authentication and authorisation) and active logging and monitoring protocols

- Intrusion Detection System/Intrusion Prevention System
- Internal employee screening or vetting
- Isolation of/and handling procedures for sensitive data (ie invoice data) including restrictions such as 'need to know' principles.

Security monitoring practices

This requirement seeks to detect and respond to cyber-attacks, channel misuse and business threats. Monitoring is a joint responsibility between the A-NZ PEPPOL Authority and Service Provider. Service Providers need to be able to demonstrate that they scan their environment for threats and take appropriate action when they detect anomalies.

Evidence required

Network / infrastructure layer - relevant combinations of:

- screen shots of an intrusion detection system or firewall that generates alerts. If a service provider uses a third party a screenshot from within the solution showing the monitoring capabilities, dashboard etc.
- photos of your Security information and event management dashboard
- If leveraging off a cloud provider you can provide either an invoice or screenshot from within the environment showing the type of monitoring captured.

Application layer – relevant combinations of:

- screen shots of the function page in the application, and
- reports from the backend system.

Transaction (data) layer – relevant combinations of:

- reports from the backend system
- Screenshots of an anomaly detection system.

Encryption in transit for all e-Invoicing information (business documents) sent and received by an Access Point

This requirement seeks to protect the confidentiality and integrity of information in transit.

You will need to provide evidence that you use an approved cryptographic protocol (for example, TLS 1.2) and algorithm to encrypt data in transit as per AUS or NZ Information security Manual.

Evidence required

Screenshot of one or more of the below:

- SSL certificates
- Showing HTTPS protocol being enforced
- Call to API
- TLS handshake protocol being enforced.

Multifactor authentication

This requirement seeks to minimise the opportunity for unauthorised users to client related information.

Multi-factor authentication (MFA) is defined as a method of authentication that uses two or more authentication factors from different categories, to authenticate a single claimant to a single authentication verifier.

The authentication factors can be categorised as:

- Something you know, such as a password or a response to a security question
- Something you have, such as a one-time pin, SMS message, smartcard, or software certificate
- Something you are, such as biometric data, like a fingerprint or user's voice

Further information on each method can be found at ACSC Protect: Multi-factor authentication (PDF)

For access point controlled products or services the following circumstance is an example of when MFA is ***not mandatory*** but is highly recommended (note: this is not an exhaustive list).

Note

- AP employees are those staff (including contractors) working for or on behalf of the AP.
- Tokens or temporary credential should be isolated to an individual device and expire once used. Any token or temporary credential should expire within 24 hours.
- APs that have not implemented MFA, should consider implementing good passphrase practices including single factor authentication controls, account lockouts, resetting passphrases, session and screen locking as described in the ASD ISM or NZ ISM.

- A privileged user is defined as a user who can alter or circumvent a system's security measures – this may include the capability to modify system configurations, account privileges, audit logs, data files or applications.

Evidence required

User manual, user description or instruction paired with screen shots of the user interface.

Version history

Version	Date	Change
1.0	15 November 2019	Initial published version

This site uses Just the Docs, a documentation theme for Jekyll.