|  |
| --- |
| A-NZ e-Invoicing  Security Questionnaire  November 2019 |

unCLASSIFIED

External



Contents

[Document Details 3](#_Toc23751762)

[Version History 3](#_Toc23751763)

[Document Purpose 4](#_Toc23751764)

[How to complete this questionnaire 4](#_Toc23751765)

[Minimum evidence requirements 4](#_Toc23751766)

[What’s next? 5](#_Toc23751767)

[Provider Lifecycle Overview 5](#_Toc23751768)

[Questions 5](#_Toc23751769)

[Section A: General Information 6](#_Toc23751770)

[Section B: Evidence requirements 7](#_Toc23751771)

[Section C: Access Points (AP) only 10](#_Toc23751772)

[Submitting your questionnaire 12](#_Toc23751773)

[Terms and Conditions 12](#_Toc23751774)

## Document Details

|  |  |
| --- | --- |
| **Attributes** | **Details** |
| Date Latest Release | **November 2019** |
| Document Name | A-NZ e-Invoicing Security Questionnaire |

## Version History

|  |  |  |
| --- | --- | --- |
| **Version** | **Changes** | **Date Released** |
|  |
| V1.0 | Initial release of A-NZ e-Invoicing Security Questionnaire | November 2019 |
|  |  |  |

## Document Purpose

Trust and integrity of the PEPPOL e-delivery network is critical to achieving benefits like increased efficiencies and reduces rework for A-NZ Inc. This questionnaire is prepared to establish the specific security posture of PEPPOL Service Providers of Access Points (APs) and Service Metadata Publisher (SMP).

The security requirements include:

* Self-assessment or independent audit against ISO/IEC 27001 or ASD/NZ ISM.

This includes 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 in transit (Access Points only)
* Encryption at rest
* Security monitoring practices
* Multifactor authentication (Access Points only)

## How to complete this questionnaire

**Please complete the relevant sections of this questionnaire**

[**Section A – General information**](#SectionA)

[**Section B – Evidence required**](#Section B: Evidence requirements)

**Section C – Access Points only**

## Minimum evidence requirements

* Where you have answered ‘yes’ to a question, evidence must be provided in line with the requirement.
* You can submit the questionnaire to *support@nzpeppol.govt.nz*
* Evidence can be embedded directly into the questionnaire, or separately as an appendix document or combined into a .zip file and submitted with your questionnaire. Clearly reference your attached evidence documentation, aligning to the questionnaire sections.
* If you want to securely send your completed evidence then New Zealand PEPPOL Authority can provide a secure channel facility to transfer your data upon request.
* Responses to this questionnaire need to be true and correct to the best of your knowledge. Providing false or misleading information in this questionnaire could lead to your access to the network being revoked.
* You will need to complete one questionnaire per product i.e. AP or SMP

## What’s next?

After completing this questionnaire the A-NZ PEPPOL Authority will review the suitability of the evidence provided and issue a notification of approval. The approval includes any additional conditions and a date for the annual review.

## Provider Lifecycle Overview

The below diagram illustrates a high level overview of the key stages for a AP/SMP

#### New e-Invoicing Service Provider (AP/SMP) On-boarding



## Questions

If you need assistance in completing this questionnaire please contact The New Zealand PEPPOL Authority,at any time through *support@nzpeppol.govt.nz*.

## Section A: General Information

|  |  |
| --- | --- |
| **Date of questionnaire completion** |  |
| **Business identifier e.g. ABN,NZBN** |  |
| **Entity Legal/Trading Name** |  |
| **Registered address** |  |
| **Product Name** |  |
| **Link to Website** |  |
| **Contact Name** |  |
| **Contact Email** |  |
| **Contact Phone Number** |  |
| **Are you registered with OpenPEPPOL?** | Yes No |
| **Are you an Access Point (AP) Provider?** |  |
| **Are you a Service Metadata Provider (SMP)?** |  |

## Section B: Evidence requirements

|  |  |  |
| --- | --- | --- |
| 1. **Self-assessment or independent audit against ISO/IEC 27001 or ASD/NZ ISM.**   The self-certification requirement seeks to provide the A-NZ PEPPOL Authority with a level of assurance that you have robust security practices in place across your organisation.  Suitable evidence is required 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  Notes The scope of self-certification/independent audit should cover relevant organisational policies, procedures and data repositories that hold or manage e-Invoice business documents. | **Examples of suitable evidence**  Completed documentation demonstrating your conformance with the requirements (full control suite) of one of the approved security standards. | Yes  No |
| *[Your response here with suitable evidence attached]* | | |
| 1. **Encryption at Rest**   This requirement seeks to protect information from unauthorised access.  Encrypting data at rest can be full-disk, container, and application or database level encryption techniques.  Approved algorithm (for example, AES-256) to encrypt data at rest are as per [AUS](https://www.cyber.gov.au/ism) or [NZ](https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/) Information security Manual. Notes The scope of encryption at rest covers data repositories that hold or manage e-Invoicing related information. | **Examples of suitable evidence**     * 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 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 including restrictions such as ‘need to know’ principles. | Yes  No |
| *[Your response here with suitable evidence attached]* | | |
| 1. **Security Monitoring Practices**   This requirement seeks to detect and respond to cyber-attacks, channel or e-Delivery network misuse and business threats | **Examples of suitable evidence**  **Network / Infrastructure layer – relevant combinations of the below:**   * Screen shots (product page, the management console page) * Product purchase/ownership doco (e.g. receipts, front page of a contract of product/support/service) * Configuration files * Photos of the product * Photos of SOC/SIEM centre (using the products)   **Application layer – relevant combination of the below:**   * Screen shots of the function page in the application * Reports from the backend system   **Transaction (data) layer – relevant combination of the below:**   * Reports from the backend system * Previous unusual cases | Yes  No |
| *[Your response here with suitable evidence attached]* | | |

## Section C: Access Points (AP) only

|  |  |  |
| --- | --- | --- |
| 1. **Encryption in Transit**   This requirement seeks to protect the confidentiality and integrity of e-Invoicing Information (business documents) that are sent and received by an Access Point  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](https://www.cyber.gov.au/ism) or [NZ](https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/) Information security Manual. | **Examples of suitable evidence**  When directly connected, provide a screenshot of one of the below:   * SSL certificates * Showing HTTPS protocol being enforced * Call to API * TLS handshake protocol being enforced. | Yes  No |
| *[Your response here with suitable evidence attached]* | | |
| 1. **Multifactor Authentication**  This requirement seeks to minimise the opportunity for unauthorised users to access invoice related information. It is required for:   * Internal users with privileged administration permissions (system/ database level)   It will need to include a combination of two of the below factors:   * Something you know * Something you have * Something you are   There are examples of Authentication factors in the [ACSC Implementing MFA](https://www.cyber.gov.au/publications/multi-factor-authentication) (April 2019) and NZISM  MFA will need to be implemented at login for external users accessing data of another entity.  or  Internal users who perform a privileged user role as defined by the [AUS](https://www.cyber.gov.au/ism) or [NZ](https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/) Information security Manual  It will need to include a combination of 2 of the below factors:   * Something you know * Something you have * Something you are   There are examples of Authentication factors in the [ACSC Implementing MFA](https://www.cyber.gov.au/publications/multi-factor-authentication) (April 2019) and NZISM | **Examples of suitable evidence**  User manual, user description or instruction paired with screen shots of the user interface. | Yes  No |
| *[Your response here with suitable evidence attached]* | | |
| 1. **Will you be providing your solution to market or using it to service your own commercial products?** | | |
| *[Your response here]* | | |
| 1. **Please supply an architecture, infrastructure or application diagram for your AP solution(s)** | | |
| *[Your response here]* | | |

## Submitting your questionnaire

Thank you for completing the required sections of A-NZ e-Invoicing Security Questionnaire

Please submit your completed questionnaire and evidence to The New Zealand PEPPOL Authority through the *support@nzpeppol.govt.nz*.

## Terms and Conditions

Following approval for the A-NZ e-Invoicing there will be an expectation that the following terms and conditions are met.

1. The New Zealand PEPPOL Authority must be notified of any changes to your business or product environment in relation to the information you supplied in your questionnaire. Failure to do so may result in your product being de-listed. The New Zealand PEPPOL Authority reserves the right to undertake ad hoc reviews to ensure e-Invoicing service providers maintain alignment to the security requirements.
2. Monitoring is considered a joint responsibility between the New Zealand PEPPOL Authority and the e-Invoicing service provider. If anomalies or areas of concern are identified, we may re-assess your listing suitability. We will generally contact you or your representative before making changes to your listed status unless exceptional circumstances apply.
3. Where a breach is identified by any means e.g. monitoring, client advice, you must contact The New Zealand PEPPOL Authority immediately to ensure appropriate action can be taken.
4. In line with standard industry practice, certification (both independent and self–assessed) must be current. Where certification lapses before the review date below, you must take the appropriate steps to update and supply the New Zealand PEPPOL Authority with a current copy of your certification.