

Signature requirements for approved electronic tax file number declaration – payee to payer process

Information to assist in the development of software for the input, transfer of data and use of a virtual tax file number (TFN) declaration completed electronically by a payee.

- !** These guidelines are intended for:
- commercial software developers
 - payers developing in-house software
 - computer service providers developing in-house software
 - payers who intend to provide payees with an electronic TFN declaration.

PAYER ELIGIBILITY TO USE ELECTRONIC PAYEE SIGNATURES ON VIRTUAL FORMS FOR TFN DECLARATIONS

Payers who lodge their TFN declaration report electronically to the Australian Taxation Office (ATO) are eligible to use electronic payee signatures on virtual forms for TFN declarations.

An electronic payee signature on a virtual TFN declaration form must be in an acceptable format and captured in a manner consistent with these guidelines.

A virtual TFN declaration form must be developed in conjunction with the 'Electronic reporting specification' for TFN declarations and apply standard ATO format. For information on standard ATO format and reporting specifications go to www.ato.gov.au/softwaredevelopers

PAYEE ELECTRONIC SIGNATURE REQUIREMENTS FOR TFN DECLARATIONS

Payers who are registered with the ATO to report TFN declarations electronically can now accept electronic signatures on virtual TFN declaration forms. The electronic signature must meet electronic lodgment requirements described in *Law Administration Practice Statement 2005/20 (PS LA 2005/20) Signature requirements for approved virtual forms, which are forms which are to be lodged electronically or given by telephone.*

An electronic signature is a unique identification of a payee in electronic form that is approved by the Commissioner of Taxation. For the purposes of a payee completing a TFN declaration and lodging it with their payer, the Commissioner of Taxation has approved virtual forms that include an electronic signature that satisfies the following criteria:

- adequate to authenticate the identity of the payee
- minimise risk of repudiation to declarations made by a payee when signing the virtual declaration form
- unique to the payee and secure using a password
- applies to the declaration the payee is required to make
- provides the payee and payer with ease of access to information
- a secure transmission method.

ACCEPTABLE FORMS OF ELECTRONIC SIGNATURE

- !** The list of examples provided is not exhaustive and software developers may use other solutions to meet the requirements within these guidelines.

The process for establishing a secure and safe environment for payees to provide an electronic signature on a virtual TFN declaration form is self assessed and these guidelines are to assist payers in assessing adequacy.



Examples of what constitute an approved electronic signature for approved forms are provided in PS LA 2005/20.

As a guide for establishing an electronic signature between the payee and payer for the TFN declaration, each of the following examples are an acceptable form of electronic signature:

- 1 Where the payee has access to the TFN declaration form through an internal computing network. That is, the form resides in a specified location on a payer's IT system which the payee accesses using a unique identifier (username) and password (controlled by the payee) and which other persons do not know or have access to.
- 2 A TFN declaration form provided in a secure data environment which is used by the payee to provide reportable information and identifies the payee as the person providing the information to the payer, and where it is possible to monitor access to the functions undertaken by those authorised to access it (for example, a HR personnel system).
- 3 Where information is provided across the internet, a secure channel between the parties must be established. Providing access to complete and transmit the declaration must be controlled by a password, restricting access to only the specified payee whose identity is already known to the payer and whose corporate identity and/or password has been established with the payer.

The above examples describe systems that:

- would log data relating to the transaction occurring within the payer's system by a specified user, and
- keep a record of this data transaction for the required period.

! The required period for a payer to retain a copy of the TFN declaration is, according to s202CD of the *Income Tax Assessment Act 1936*, until the second 1 July after the day on which the declaration ceases to have effect. A payer is required to keep a record of the transaction, that is, a copy of the electronic transaction or audit trail of the electronic TFN declaration form.

Payee declaration

The virtual TFN declaration must have a section entitled 'Declaration by payee'. This section will have a statement that reads 'I declare that the information I have given is true and correct'.

The payee will need to signify in some way that they agree to the declaration only after they have completed the form. The form must have a date completed feature for the declaration. The payee will then electronically submit the form.

EXAMPLES OF ELECTRONIC SIGNATURE FORMS THAT ARE NOT ACCEPTABLE

As a guide only, examples of electronic signature forms that are **not** acceptable include:

- exchanging a form between payee and payer by public access email. An email is not a secure form of transmission and could be accessed by another person. Alternately, it may not be the payee's email address (that is, the address was created by another person who has no connection with the employee). An email address is **not** an identity that can be authenticated, and can be repudiated
- a form which relies on a shared secret which could be known by many people. For example, the colour of the uniform shirt would be a shared secret known by many people.

ALTERNATIVE FORMS OF APPROVED ELECTRONIC SIGNATURES

Where the payer cannot provide a secure electronic solution for a payee to sign a virtual TFN declaration form with an electronic signature, there may be other shared secrets that would support the identity of the payee.

The ATO will accept an electronic TFN declaration completed and 'locked' by the payee, when it is transmitted through an internal electronic mail process that includes within the message the payee's agreed shared secret that is known by the payer. The shared secret needs to meet the requirements for an acceptable signature.

It is the payer who needs to identify that the form was completed by the payee and a shared secret solution may be appropriate. Examples of shared secrets include but are not limited to:

- employee number
- bank account into which salary or wages are paid
- a PIN.

When determining whether one or more of the shared secrets is sufficient to uniquely identify the payee, the payer should consider:

- the extent to which the information would be publicly known. For example, employee number would not be appropriate if it is used to publicly allocate tasks
- safeguarding the personal information of the payee.

! A payee's TFN **must not** under any circumstances be used as a shared secret.

ADDITIONAL INFORMATION

TFN privacy statements and privacy of TFN information

In the electronic capture of information, payers need to meet privacy requirements regarding the person's identity data and capture of the TFN.

The method in which the payee completes the TFN declaration should state at a minimum:

'These details are required in order to determine the amount of tax to withhold from your pay. Your information is protected by our privacy statement.'

The payer is required to reference or place in full their corporate privacy statement regarding the treatment of the completed form.

As a guide, the following is an example of a corporate privacy statement:

'When capturing your personal information, it is passed through our secure server using encryption technology which scrambles the information to ensure it is protected over the Internet. Your stored information is further protected from unauthorised access through the use of firewalls, passwords and sign in processes.'

GLOSSARY

Approved form	Meets the requirements under <i>Law Administration Practice Statement 2005/19</i> , that is: <ul style="list-style-type: none"> ■ it is in the form approved in writing by the Commissioner for that kind of document (paragraph 388-50(1)(a)), Schedule 1 to the <i>Taxation Administration Act 1953</i> (TAA) ■ it contains a declaration signed by a person or persons as the form requires (paragraph 388-50(1)(b)) ■ it contains the information that the form requires, and any further information, statement or document as the Commissioner requires, whether in the document or otherwise (paragraph 388-50(1)(c)) ■ if it is to be given to the Commissioner, it must be given in the manner that the Commissioner requires (which may include electronically) (paragraph 388-50(1)(d)).
Locked	A lock is a means of controlling edit functionality. This may be achieved by a variety of means such as saving the file content upon submitting as a graphic file or having edit controls through software or encryption measures.
Payer	A business or individual making payments under the pay as you go (PAYG) withholding system.
Payee	An individual being paid under the PAYG withholding system.
Repudiation	Refuse to acknowledge, ratify or recognise as valid. For example, to reject having signed a declaration.
Shared secret	Unique information that is personal and known only to the payee and payer that can be provided between the parties to enable authentication.

 MORE INFORMATION

Contact the Software Industry Liaison Unit (SILU):

- phone **1300 139 052**
- email **SILU@ato.gov.au**

For information about ATO e-reporting requirements, email **ATO-eReporting@ato.gov.au**

For enquiries relating to the legislative requirements for lodgment of TFN declaration reports and general enquiries about TFN declaration matters, phone **1800 679 974**.

OUR COMMITMENT TO YOU

We are committed to providing you with accurate, consistent and clear information to help you understand your rights and entitlements and meet your obligations.

If you follow our information in this publication and it turns out to be incorrect, or it is misleading and you make a mistake as a result, we must still apply the law correctly. If that means you owe us money, we must ask you to pay it but we will not charge you a penalty. Also, if you acted reasonably and in good faith we will not charge you interest.

If you make an honest mistake in trying to follow our information in this publication and you owe us money as a result, we will not charge you a penalty. However, we will ask you to pay the money, and we may also charge you interest. If correcting the mistake means we owe you money, we will pay it to you. We will also pay you any interest you are entitled to.

If you feel that this publication does not fully cover your circumstances, or you are unsure how it applies to you, you can seek further assistance from us.

We regularly revise our publications to take account of any changes to the law, so make sure that you have the latest information. If you are unsure, you can check for more recent information on our website at **www.ato.gov.au** or contact us.

This publication was current at **March 2012**.