

City of Albany
Policy & Procedure

Acceptable Use of Electronic & Digital Signature Policy

(including scanned signatures applied to documents)

Overview

Electronic Transactions Act 2011 WA: The Act provides that where the following can or have to be done under WA law, they may be done by electronic communication:

- Giving information in writing
- Providing a signature
- Producing a document
- Recording information
- Retaining a document

E-Signature Exceptions include:

- Documents that are required to be witnessed
- Documents to be personally served
- Court documents
- Powers of attorney
- Wills

The Act provides that where the following can or have to be done under WA law, they may be done by electronic communication:

- Giving information in writing
- Providing a signature
- Producing a document
- Recording information
- Retaining a document

Document Approval			
Document Development Officer:		Document Owner:	
Manager Governance & Risk (MGR)		Executive Director Corporate & Commercial Services	
Document Control			
File Number - Document Type:		CM.STD.7 – Policy CM.STD.8 – Procedure	
Document Reference Number:		NP21130538	
Status of Document:		Administrative decision: Approved.	
Quality Assurance:		Executive Management Team, ICT Steering Committee, Governance & Risk Team	
Distribution:		Public Document	
Document Revision History			
Version	Author	Version Description	Date Completed
1.0	MGR	Approved by ICT Steering Committee & EMT. Synergy Ref: NP1768439.	31/08/2017
2.0	MGR	Reviewed and approved by Document Owner. Reviewed and amended: AUSkey and Manage ABN Connections are retired in March 2020. To access Australian Government online services and other government online services, authorised persons will need to use: <ul style="list-style-type: none">myGovID – the Australian Government’s digital identity provider that allows you to prove who you are online. It’s an app that you download to your smart device and is different to your myGov account.Relationship Authorisation Manager (RAM) – an authorisation service that allows you to act on behalf of a business online when linked with your myGovID. Attachment 1: Attachment 2: Cheat Sheet: Setup an Adobe Digital Signature Acknowledges that the City of Albany has not appointed a Chief Information Officer (CIO). Therefore, the Chief Information Officer (CIO) – CEO has delegated this function to Executive Directors.	19/05/2021
2.1	MGR	Reviewed under delegated authority.	17/07/2023

Contents

Overview	1
Objective:.....	4
Purpose:	4
Scope:	4
Policy Statements:	4
A. Acceptable Use Signature Guidance:	4
B. Electronic & Digital Signature Implementation Guidance:	6
C. Responsibility for Policy Compliance:	7
D. Retention of Records:	7
Legislative & Strategic Context:	7
Review Position & Date:	7
Associated Documents:	7
Additional Definitions:	7
PROCEDURES	8
Scanned Signature Procedure:	8
Creating a Digital Certificate to Digitally Sign a Document Procedure:	8
What is a digital signature?	8
 Attachments:	
Attachment 1: Use of Scanned Signature Form 1	9
Attachment 2: Cheat Sheet: Setup an Adobe Digital Signature.....	11

Objective:

The objective of the City of Albany is to encourage the use of digital signatures in all correspondence originating from the City.

By implementing this policy, the City of Albany aims to streamline the use of digital signatures, enhance security, and ensure the integrity and authenticity of electronic documents and correspondence.

Purpose:

This policy aims to achieve the following:

- Provide guidance on when digital and electronic signatures are considered acceptable methods for validating the identity of a signer in City of Albany electronic documents and correspondence.
- Outline the approval processes and security measures to be followed when using digital and electronic signatures.

For the purpose of this policy a signature is defined as:

Digital Signature: An encrypted digital code attached to an electronic message or document to verify the identity of the sender (authentication), prevent the sender from denying sending the message (non-repudiation), and ensure that the message was not altered during transmission (integrity). A digital signature is also commonly referred to as a digital certificate.

Electronic Signature (eSignature): A signature that identifies an individual using a computer-generated method. The signature block affixed to emails is a common example of an electronic signature.

Scanned Signature: Also known as a "Digitized Signature," a scanned signature refers to the process of capturing a wet signature and attaching it to electronic documents, certificates, letters, and correspondence. It serves to identify the person and their intention towards the material it is attached to.

Scope:

This policy applies to all individuals conducting City of Albany business, including employees, contractors, and other agents.

Policy Statements:

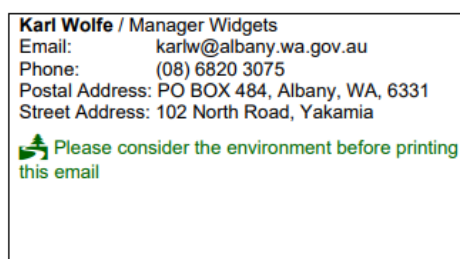
- (1) The City of Albany permits the use of electronic or digital signatures as alternatives to handwritten signatures.
- (2) While scanned signatures will be accepted, digital signatures are preferred.
- (3) Transactions between the City of Albany and external parties are only allowed when approved and when both parties have agreed to conduct transactions electronically.
- (4) The Chief Information Officer (CIO) - CEO has delegated the responsibility for this function to Directorate Executive Directors and.
- (5) Directorates will maintain a comprehensive list (detailed in this policy and procedure) of the document types and correspondence not covered by this policy.
- (6) Electronic and digital signatures must be linked to metadata that includes the individual's name and position title.

In summary, this policy allows for the use of electronic or digital signatures instead of handwritten signatures within the City of Albany.

A. Acceptable Use Signature Guidance:

Electronic Signatures (Email):

Electronic signatures, such as an email signature block, can be used to indicate an individual's intent to sign a record for low to medium-risk transactions. Example Email Signature Block:



City of Albany procedures must clearly identify the authorised person by their position who is responsible for signing, approving, and preventing unauthorised actions.

Digital Signatures (Adobe):

Digital signatures, specifically when signing a document electronically with Adobe, can convey the intent of an individual to sign a record for both low and high-risk transactions. For example: Signing a document electronically with Adobe.



City of Albany procedures must clearly identify the authorized person by their position who is responsible for signing, approving, and preventing unauthorized actions.

Digital signatures may be utilized in situations where electronic signatures are deemed acceptable and authorized. They can be permitted or required for any record or document that necessitates a signature according to Commonwealth, State law, or City policy, unless a handwritten signature is explicitly mandated.

Digital signatures must be used instead of an electronic signature when legally required or when a higher level of risk is involved.

RAM Credentialed Digital Signature

To access a range of Australian Government online services on behalf of the City of Albany, it may be necessary to utilize the following:

myGovID: An application that can be downloaded to a smart device, enabling individuals to verify their identity when logging into various government online services. It is distinct from a myGov account.

Relationship Authorisation Manager (RAM): An authorization service that allows individuals to act on behalf of a business online when linked with their myGovID. RAM is accessed using the myGovID login.

Principal Authority: The principal authority for the City of Albany must establish a link with the City in the Relationship Authorisation Manager (RAM) before authorized individuals can be granted access to government online services on behalf of the City. The principal authority, or the authorisation administrator acting on behalf of the City online, is responsible for authorizing individuals in RAM to act on behalf of the business.

Authorised Persons using City of Albany's RAM Credential Signature: To access online services on behalf of the City of Albany, authorized individuals must link their personal myGovID to the City of Albany using RAM. This allows them to utilize the RAM Credential Signature for authentication purposes.

B. Electronic & Digital Signature Implementation Guidance:

The Chief Information Officer (CIO) - CEO has delegated the responsibility to Directorate Executive Directors, who are required to develop procedures that identify, evaluate, and document the permissible use of electronic signatures, digital signatures, and wet signatures.

Signatures applied electronically must adhere to the following City of Albany electronic and digital signature standards:

Transaction Type	Level of Risk	Signature Type Required
Internal	Low, Medium	Email / Letter Signature Block (No Signature Required)
Internal	High	Email Signature Block or Adobe Digital Signature
External	Low	Email / Letter Signature Block (No Signature Required) with registered Synergy Record Number
External	Medium	Email Signature Block / Letter Signature Block (Scanned Signature) or Adobe Digital Signature with registered Synergy Record Number
External (Federal government)	High	Wet signature with registered Synergy Record Number or Credentialed Digital Signature

Table 1 - Risk Matrix

Note: Synergy Record Number refers to a registered identifier for the document.

Signing Activities for Electronic Signatures:

SUITABLE	NOT SUITABLE
Suitable for E-Signatures: <ul style="list-style-type: none"> • Building and Planning applications and approvals • Certificates of Authorization • Elected Member declarations and reimbursement claims • Employee declarations • Employment contracts, employee onboarding, and information acceptance records • Giving Notices - Local Government Act - s.3.25 Notices • Impounding Notices under the Cat Act, Dog Act, etc. • Infringement Notices (Wet signatures only) • Local Law permits / licenses - applications and approvals • Supplier contracts 	Exempt from allowing electronic signatures: <ul style="list-style-type: none"> • Common Seal - Local Laws, Local Planning Schemes • Court documents • Documents that require witnessing • Documents to be personally served • Land Transfer Forms • Legal Agreements - Deeds, Leases, Memorandums of Understanding • Powers of attorney • Wills

Table 2 - Signing Activities

C. Responsibility for Policy Compliance:

All staff members will assist Executive Directors in verifying compliance with this policy through various methods, including business tool reports, internal and external audits, and providing feedback to the policy owner.

- **Exceptions:** Any exceptions to this policy must receive prior approval from Executive Directors. They may also delegate the authority to authorize exceptions to a designated individual.
- **Non-Compliance:** Employees found to be in violation of this policy may face disciplinary action, up to and including termination of employment.

D. Retention of Records:

The [Electronic Transactions Act 2011](#) (the Act) sets forth specific requirements for record retention, particularly for the "First Party" involved in a transaction.

Individuals who submit documents (such as plans, forms, etc.) must ensure they retain their own copies of the documents in a manner that allows for easy retrieval if needed.

It is recommended to also retain copies of any related emails regarding document submission.

The Act permits the retention of records in electronic form if desired.

Legislative & Strategic Context:

Electronic commerce in Australia is primarily regulated by Federal, State, and Territory Electronic Transaction Acts.

The Federal Act applies specifically to transactions governed by Federal law.

The State and Territory Acts are similar to the Federal Act and apply within their respective jurisdictions.

It's important to note that the Electronic Transactions Acts do not apply to all legislation or transactions. Each Act specifies exemptions for certain legislation or transaction types.

Digital Signature Standard:

<https://info.authorisationmanager.gov.au>

Review Position & Date:

The document owner is responsible for reviewing this policy and procedure annually.

Associated Documents:

Documents that are relevant to this policy and may serve as useful references for policy users include:

Additional Definitions:

RAM: Relationship Authorisation Manager (RAM) is an Australian Government authorisation service that allows individuals to act on behalf of a business online. It replaces AUSkey as the way to access government services.

myGovID: The Australian Government's digital identity provider, which allows individuals to prove their identity online and access government online services.

Scanned Signature: An analogue representation of a handwritten signature that has been converted to an image file. It can be attached to documents to identify the person and their intention towards the material it is attached to.

Approved Person: An employee who has been authorized by a higher authority to authenticate a document by attaching their scanned signature.

Authorising Person: An employee who is authorized to produce a scanned signature and approve its use by another departmental employee.

Simple Electronic Signature (E-Signature): A computer-generated signature that identifies an individual. The most common example is the signature block found in emails.

Digitising: The process of creating a digital representation of a document or part of a document for use in electronic documents.

Document: Any form, whether on paper or electronic, used to transact business or make official statements, including letters, certificates, awards, reports, and permits.

Electronic Document: A document in a soft or electronic format, stored on a computer drive, compact disc, or other electronic device.

Hard Copy: An actual paper copy of a document, including City letters, transcripts, reports, and permits that require a signature.

Electronic Completion: The process of filling in the required input of a form using a computer, either with a PDF editing program (e.g., Adobe® Reader®) or a word processing program (e.g., Microsoft® Word).

Electronic Submission/Delivery: The completion of a form and its transmission to the intended recipient using electronic means such as email or facsimile.

PROCEDURES

Signatures should only be applied to documents that require authentication and/or approval.

Scanned Signature Procedure:

When using a scanned signature, it should resemble the signatory's usual style and format.

To ensure proper use of scanned signatures, the following steps must be followed to establish approval processes and maintain security measures for each instance:

Approval Process:

- All senior executive staff and managers are authorized persons under this policy.
- In special circumstances, the CIO delegate may appoint additional authorized persons. All authorized persons may approve the use of their scanned signature by approved persons, subject to the following conditions:
- Approval, including the specific circumstances for using the scanned signature, is provided in writing (refer to Form 1) and stored on an official departmental file. Each approval is limited to a particular circumstance or reason and a specified period of time.
- Separate approval is required for each specific circumstance. For example, an authorized person may approve the use of their scanned signature for committee reports and personal development reviews. Each instance requires a separate approval.
- The document on which the scanned signature is used must be checked for accuracy and completeness and approved by the authorized person before the scanned signature is affixed.

Security:

- Since scanned signatures are not physically bound to a document, measures should be taken to preserve the relationship between the scanned signature and its associated document over time.
- An authorized person's signature should be saved as a PDF or image document in one of the following secure storage options:
 - Secure USB drive (password protected)
 - Restricted access electronic folder in the (N) drive
 - Approved software package, with restricted access granted to the authorized person and approved person (refer to Use of Scanned Signature form)
 - A copy of the scanned signature is stored in hard copy on an official departmental file.
- Details of each document on which the scanned signature is used are recorded and maintained in an official departmental file.
- Each authorized signature must be destroyed when the specified reason given in Form 1 is no longer valid or when the specified period of time has expired, whichever is later. All hard copies and electronic copies of the signature must be destroyed.

Creating a Digital Certificate to Digitally Sign a Document Procedure:

What is a digital signature?

A digital signature, also known as a digital certificate, is a form of electronic identification.

This procedure explains the necessity of a digital signature (or digital ID) for digitally signing a PDF document and provides instructions on obtaining or creating one.

For instructions on setting up your own Adobe eSignature attributed to your City email address, please refer to Attachment 2: Cheat Sheet - Setup and Adobe Digital Signature.

Accessing Australian Government online services with myGovID and RAM:

To access Australian Government online services on behalf of the City of Albany, RAM must be utilized.

Attachment 1: Use of Scanned Signature Form 1

Name of signatory

Designation

Location/Team

Reason for use of scanned signature

Identify the electronic and physical locations where the scanned signature is to be stored.

Identify the approved person who will have access and use of the scanned signature.

Identify when the use of the scanned signature will commence and cease and when the file will be deleted from the electronic location and destroyed in hard copy.

Please complete and sign the following declaration to authorise use of your signature.

I authorise that the signature provided on page 2 of this form can be stored, used, and then deleted in accordance with the conditions outlined in the use of scanned signatures applied to documents policy.

Printed Name

Signature

Date

Please complete and sign the following declaration when scanned-signature has been deleted

I certify that the scanned-signature created from the signature blocks on page 2 of this form has been deleted and/or access to it suspended from the computer file where it was stored in accordance with the conditions stated outlined in the use of scanned-signatures applied to documents – letters, certificates, awards and reports policy.

Printed Name

Signature

Date

Use of Scanned Signature Form 1 (continued)

It has been noticed that when people are asked to sign their signature, often they are not happy with their first attempt, feeling that it does not accurately reflect their signature. Consequently, history has shown that by obtaining 6 sample signatures, the signatory selects the most preferred signature.

- Use a black felt tip pen (preferably sizes 0.7-1.5mm).
- Ensure that no part of your signature appears outside the box.
- Once completed, this form is to be stored as a PDF document so that it cannot be altered.

DO NOT FAX THIS FORM

If this form is to be sent to another location fold the form ONCE where indicated and post, courier or deliver by hand to recipient.

— — — — — ▪ Fold ONCE Here

— — — — — ▪

--

--

--

--

--

--

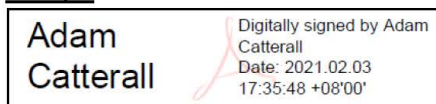


OPEN THIS PDF IN ADOBE ACROBAT

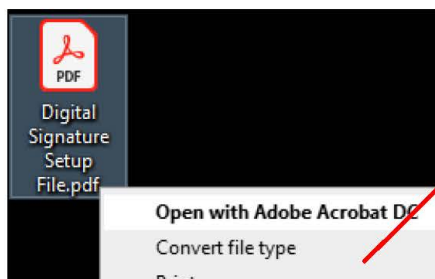
Cheat Sheet: Setup an Adobe Digital Signature

Adobe Acrobat is the default PDF reader at the City. This cheat sheet explains how to setup a digital signature to sign Adobe PDF forms.

Example



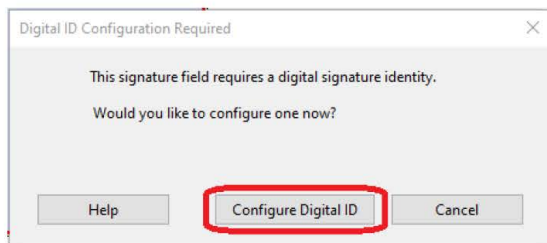
1. With the **Setup Adobe Digital Signature - Cheat Sheet** on your Desktop, **right-click** on it and select **Open with Adobe Acrobat DC**



2. Right-click on the signature field above and select Sign Document.



3. Click on **Select Configure Digital ID**



4. Select **Create a new Digital ID** and click **Continue**

Configure a Digital ID for signing [X]

A Digital ID is required to create a digital signature. The most secure Digital IDs are issued by trusted Certificate authorities and are based on secure devices like smart card or token. Some are based on files.

You can also create a new Digital ID, but they provide a low level of identity assurance.

Select the type of Digital ID:

- ☐ **Use a Signature Creation Device**
Configure a smart card or token connected to your computer
- ☐ **Use a Digital ID from a file**
Import an existing Digital ID that you have obtained as a file
- ☒ **Create a new Digital ID**
Create your self-signed Digital ID

[?] [Cancel] [Continue]

5. Select **Save to File** and click **Continue**

Select the destination of the new Digital ID [X]

Digital IDs are typically issued by trusted providers that assure the validity of the identity. Self-signed Digital ID may not provide the same level of assurance and may not be accepted in some use cases.

Consult with your recipients if this is an acceptable form of authentication.

- ☒ **Save to File**
Save the Digital ID to a file in your computer
- ☐ **Save to Windows Certificate Store**
Save the Digital ID to Windows Certificate Store to be shared with other applications

[?] [Back] [Continue]

6. **Enter the information** in the fields and click **Continue**

Create a self-signed Digital ID

Enter the identity information to be used for creating the self-signed Digital ID.

Digital IDs that are self-signed by individuals do not provide the assurance that the identity information is valid. For this reason they may not be accepted in some use cases.

Name	Adam Catterall
Organizational Unit	IT Team
Organization Name	City fo Albany
Email Address	adam.catterall@albany.wa.gov.au
Country/Region	AU - AUSTRALIA
Key Algorithm	2048-bit RSA
Use Digital ID for	Digital Signatures

?

Back Continue

7. Enter a **Password** and Click **Continue**

Save the self-signed Digital ID to a file

Add a password to protect the private key of the Digital ID. You will need this password again to use the Digital ID for signing.

Save the Digital ID file in a known location so that you can copy or backup it.

Your Digital ID will be saved at the following location :

C:\Users\adam.catterall\AppData\Roaming\Adobe\Acro Browse

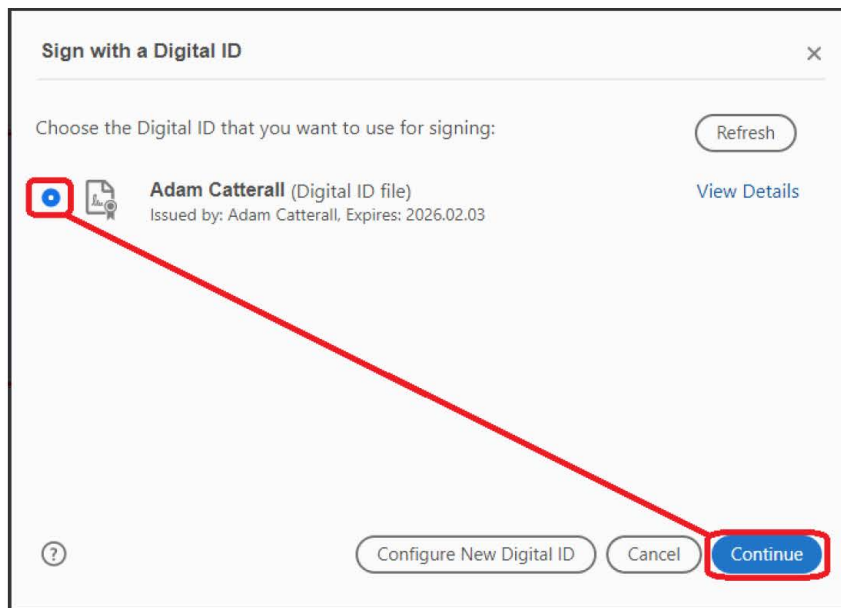
Apply a password to protect the Digital ID:

Confirm the password:

?

Back Save

8. **Select your Digital ID** and Click **Continue**



Sign with a Digital ID

Choose the Digital ID that you want to use for signing:

Refresh

Adam Catterall (Digital ID file)
Issued by: Adam Catterall, Expires: 2026.02.03

View Details

Configure New Digital ID Cancel **Continue**

9. Enter your **password** and Click **Sign**



Sign as "Adam Catterall"

Appearance Standard Text Create

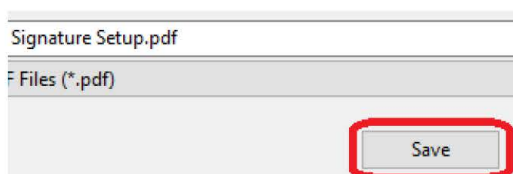
Adam Catterall Digitally signed by Adam Catterall
Date: 2021.02.03 17:14:53 +08'00'

☐ Lock document after signing View Certificate Details

Review document content that may affect signing Review

Back **Sign**

10. Click Save to save the PDF with your digital signature included



Signature Setup.pdf

Files (*.pdf)

Save