

## 2.01 Acceptable Use of Electronic & Digital Signature Policy

<b>Policy Owner</b>	Executive Director Corporate & Commercial Services
<b>Responsible Officers</b>	Manager Governance & Risk
<b>Date of Approval</b>	31/08/2017
<b>Amended/Revised/Revised</b>	6/11/2024

### Objective

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

### Scope

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

### Purpose

### This policy aims to:

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

### Definitions

- **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). Also known 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.
- **Scanned Signature:** *Also known as a "Digitized Signature," this refers to capturing a wet signature and attaching it to electronic documents, certificates, letters, and correspondence. It identifies the person and their intention towards the material it is attached to.*  
**Scanned signatures should not be used.**

### Policy Statements

- The City of Albany permits the use of digital signatures as alternatives to handwritten signatures.
- **Scanned signatures are not to be used.**
- Transactions between the City of Albany and external parties are allowed only when approved and when both parties agree to conduct transactions electronically.
- The Chief Information Officer (CIO) has delegated the responsibility for this function to Directorate Executive Directors.
- Directorates will maintain a comprehensive list of document types and correspondence not covered by this policy.

- Digital signatures must be linked to metadata that includes the individual's name and position title.

### Summary

- This policy allows for the use of electronic or digital signatures instead of handwritten signatures within the City of Albany.

### 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:

[Your Name]  
[Your Position]  
City of Albany  
[Your Contact Information]

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

#### Digital Signatures (Using PDF Signing Feature)

Digital signatures, such as those created with Adobe, can convey an individual's intent to sign a record for both low and high-risk transactions.

#### Example: Signing a document electronically with Adobe.



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

Digital signatures may be utilised in situations where electronic signatures are deemed acceptable and authorised. 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 electronic signatures 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, the following may be necessary:

- **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 myGovID 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 authorization administrator acting on behalf of the City online, is responsible for authorizing individuals in RAM to act on behalf of the business.
- **Authorised Users using City of Albany’s RAM Credential Signature:** To access online services on behalf of the City of Albany, authorised users must link their personal myGovID to the City of Albany using RAM. This allows them to utilise the RAM Credential Signature for authentication purposes.

### Electronic & Digital Signature Implementation Guidance:

The Chief Information Officer (CIO) - CEO has delegated the responsibility to Directorate Executive Directors 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:

**Table**

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

**Table 1 - Risk Matrix**

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

### Signing Activities for Electronic Signatures:

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

**Table 2 - Signing Activities**

### 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 authorise exceptions to a designated individual.
- **Non-Compliance:** Employees found to violate this policy may face disciplinary action, up to and including termination of employment.

### 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.

- **Document Retention:** Individuals who submit documents (such as plans, forms, etc.) must ensure they retain their own copies in a manner that allows for easy retrieval if needed.
- **Email Retention:** It is recommended to also retain copies of any related emails regarding document submission.
- **Electronic Records:** The Act permits the retention of records in electronic form if desired.

## Legislative and Strategic Context

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

Federal Act: Applies specifically to transactions governed by Federal law.

State and Territory Acts: 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 and Date

The policy and procedure are to be reviewed annually.

## 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.

---

## 2.01 Acceptable Use of Electronic & Digital Signature Procedure

---

### General Guidelines:

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

### Scanned Signature Usage:

- **Scanned Signatures should not be used.**


### Creating a Digital Certificate for Digital Signature:

- **Digital Signature Basics:** A digital signature (or certificate) provides electronic identification. This procedure outlines how to digitally sign PDF documents and create your own digital ID.
- **Setup Instructions:** Refer to Attachment 1: Cheat Sheet - Setup and Adobe Digital Signature for step-by-step guidance on setting up your Adobe eSignature with your City email address.

### Accessing Government Services with myGovID and RAM:

- To access Australian Government services on behalf of the City of Albany, use RAM for authentication.

## Attachment 1: Cheat Sheet: Setup an Adobe Digital Signature

Setup Adobe Digital Signature - Cheat Sheet v2.docx  
15/02/2021 11:07:00 AM / Adam Catterall

**OPEN THIS PDF IN ADOBE ACROBAT**

### Cheat Sheet: Setup an Adobe Digital Signature

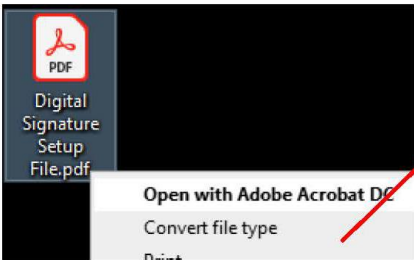
Adobe Acrobat is the default PDF reader at the City. This cheat sheet explains how to setup a digital signature to sign Adobe PDF forms.

**Example**

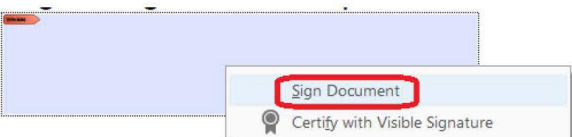
Adam  
Catterall

Digitally signed by Adam  
Catterall  
Date: 2021.02.03  
17:35:48 +08'00'


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



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

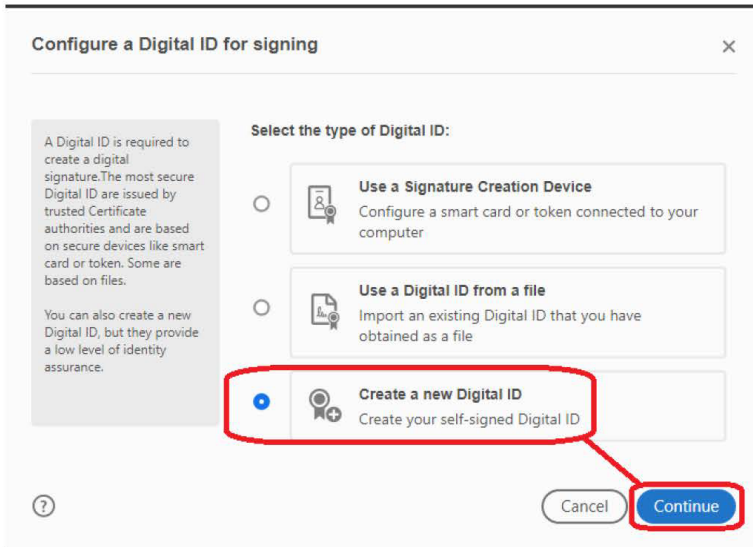


- Click on **Select Configure Digital ID**



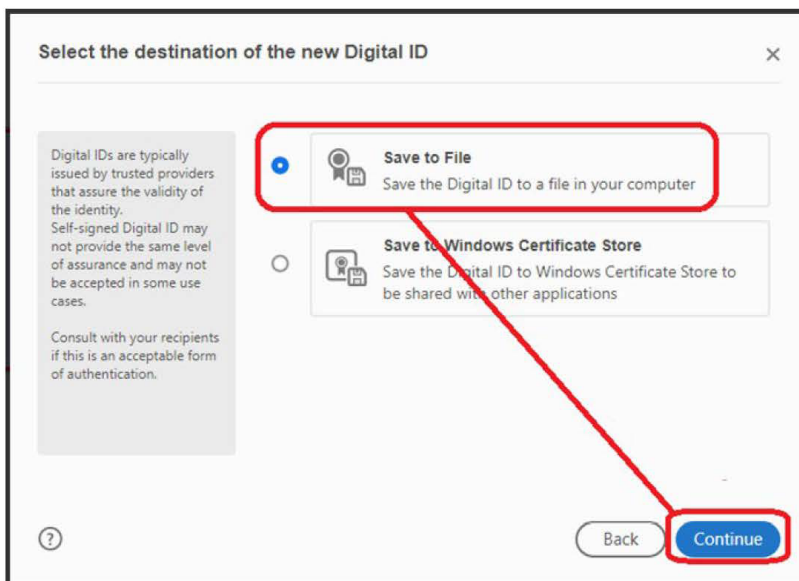
[www.albany.wa.gov.au](http://www.albany.wa.gov.au) | Page 1 of 4

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



The screenshot shows a dialog box titled "Configure a Digital ID for signing". On the left, there is a text box explaining that a Digital ID is required for digital signatures and that self-signed IDs have a lower level of assurance. The main area is titled "Select the type of Digital ID:" and contains three radio button options: "Use a Signature Creation Device", "Use a Digital ID from a file", and "Create a new Digital ID". The "Create a new Digital ID" option is selected and highlighted with a red box. Below the options are "Cancel" and "Continue" buttons, with the "Continue" button also highlighted in red.

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



The screenshot shows a dialog box titled "Select the destination of the new Digital ID". On the left, there is a text box explaining that Digital IDs are typically issued by trusted providers and that self-signed IDs may not be accepted in some cases. The main area contains two radio button options: "Save to File" and "Save to Windows Certificate Store". The "Save to File" option is selected and highlighted with a red box. Below the options are "Back" and "Continue" buttons, with the "Continue" button also highlighted in red.



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	<input type="text" value="Adam Catterall"/>
Organizational Unit	<input type="text" value="IT Team"/>
Organization Name	<input type="text" value="City fo Albany"/>
Email Address	<input type="text" value="adam.catterall@albany.wa.gov.au"/>
Country/Region	<input type="text" value="AU - AUSTRALIA"/>
Key Algorithm	<input type="text" value="2048-bit RSA"/>
Use Digital ID for	<input type="text" value="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 :

Browse

**Apply a password to protect the Digital ID:**

Confirm the password:

Back
Save

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



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



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

