





**BUSINESS HOW-TO GUIDE** 



### How to check a Digital Licence

The Digital Licence contains visual features to help you identify that it is current and genuine. The below items should all appear on the user's Digital Licence. (This does not include all the credentials - some users may only have one or two).



## **Security**

The Digital Licence app includes security features to ensure a user's data is protected against cybercrimes and theft.

Their information is encrypted on their device, and protected by both their phone's security features, and a PIN and password which they set when they are onboarding.

## **Privacy**

Every time a user shares their information, using the Share button at the bottom of a credential, they must confirm what information they are sharing

You can ask a user to present their Digital Licence, so you can sight it, or scan it with your own Digital Licence, Verifier app or other device.

However, you should not ask the user to hand their device to you. Their device should stay in their posession at all times.

## Verifying visually

There are a number of different elements that you can look for when visually verifying a Digital Licence.

No feature is more important than the others - you should look for at least a couple of the items to ensure you are looking at a legitimate Digital Licence.

## **Refreshing the screen**

If you have any concerns or suspicions about the user's Digital Licence, you can ask them to return to the app's Home Screen, and pull down on the screen, which will refresh their information.

### How to scan a Digital Licence

When a user shares their Digital Licence with you, they will select a bundle of information to share. The Digital Licence then provides a QR code, which you can scan with your Digital Licence, Verifier app, or other device.



) reference

### How to verify a PDF copy of a Digital Licence

You have the ability to check the PDF version you have received is legitimate and hasn't been altered in any way. There are a few steps to take to ensure the Digital Licence PDF is a trusted certificate. Follow the instructions provided to visually check the PDF is digitally signed.

**Please note:** At the top of the PDF, there is a line stating when the document was generated and digitally signed, with a date and time. This is the date and time that the user onboarded, securely reset, or last had their information change within the app. It does not get updated when the user selects the printable copy sharing bundle, which means it could be a date/time that is not recent. If you have any concerns, please visually check the information in the PDF against their Digital Licence app screen.

Categories:	Trust Manager		
Commenting Documents Full Screen General Page Display Accessibility Forms Identity Internet JavaScript Language Measuring (3D) Measuring (3D) Measuring (Geo) Multimedia & 3D Multimedia & 3D Multimedia (legacy) Multimedia Trust (legacy) Reading Reviewing Search Security	PDF File Attachments Allow opening of non-PDF file attachments with external applications Restore the default list of allowed and disallowed file attachment types:		
	Internet Access from PDF Files outside the web browser Unless explicitly permitted, PDF files cannot send information to the Internet. Change Settings		
	Automatic Adobe Approved Trust et (AATL) updates Load trusted certificates from an Adobe AATL server Ask before updating Update Now		
	Automatic European Union Trusted Lists (EUTL) updates           Load trusted certificates from an Adobe EUTL server           Ask before updating   Update Now		
Security (Enhanced) Signatures Spelling	Help		
Trust Manager Units			

	2	Signature Verification Preferences		×
Categories:	Digital Sir			
Commenting	Signal Sile	Verify signatures when the document is opened		
Documents	Creat	When document has valid but untrusted signatu	res, prompt to review and trust signers	
Full Screen		Varification Polyavian		
General	. 5	Verification behavior		
Page Display		when veniging:		
		<ul> <li>Use the document-specified method; p</li> </ul>	rompt if unavailable	
Accessibility	Verifi	Use the document-specified method: if	unavailable use default method	
Forms		0.000		
Identity		Always use the default method:	Adobe Default Security 🗸	
Internet				
JavaScript	Require certificate revocation checking to succeed whenever possible during signature verification			
Language	ident	Use expired timestamps		
Measuring (2D)	• 0	Inners desument validation information		
Measuring (SD)	- N			
Multimedia & 3D		Verification Time	Verification Information	
Multimedia (legacy)	Docu	Verify Signatures Using:	Automatically add verification information when	
Multimedia Trust (legacy)	0000		saving signed PDF:	
Reading	• C	Time at which the signature was created		
Reviewing		<ul> <li>Secure time (timestamp) embedded</li> </ul>	Ask when vehication information is too big	
Search		in the signature	○ Always	
Security		<ul> <li>Current time</li> </ul>	() Never	
Security (Enhanced)				
Signatures		Windows Integration		
Spelling		Trust ALL root certificates in the Windows Certif	ficate Store for:	
Trust Manager		Validating Signatures		
Units				
		Validating Certified Documents		
		Selecting either of these options may result Take care before enabling these features.	t in arbitrary material being treated as trusted content.	
		Help	OK Cancel	

### How to validate the PDF

You will only need to go through steps 1-9 once, and you will then be able to validate all Digital Licence PDFs.

### Before you open the PDF:

- 1. Open Adobe Acrobat Reader.
- 2. Click Edit, and then Preferences.

3. In the window that appears, select Trust Manager.

4. In the main window, the third option will be 'Automatic Adobe Approved Trust List (AATL updates)'. In this box, ensure 'Load trusted certificates from an Adobe AATL server' is ticked, and click 'Update Now'.

5. In a few moments, a window will come up saying 'Security settings have been successfully updated.' Click OK in the bottom right corner.

6. In the left column, select Signatures.

7. In the main window, you will see a box titled Verification. Click the 'More...' button in that box.

8. At the top, tick the box next to 'Verify signatures when the document is opened'.

9. Click OK, and then OK again.

### **Open the PDF**

When the PDF is open, after a few moments, you should see a blue bar at the top that says 'Signed and all signatures are valid.'

In the blue bar, click 'Signature Panel'.

In the Signatures panel that appears, you should see, 'Rev. 1: Signed by Department of Transport and Main Roads <dlpki@qld.gov.au'.

This means the PDF is a valid export of a customer's driver licence, marine licence or photo identification card.

If you see anything else in the blue bar, or in the Signatures panel, this means the PDF was not created by the Digital Licence, and is not valid.

### **Digital Licence Verifier**

The Queensland Digital Licence Verifier app (DLV) verifies the Queensland Digital Licence App (DLA). The DLV app allows you to quickly check the validity of the credential by performing a secure check of TMR credentials.



Verify a Digital Licence

Open the Verifier app and select Scan QR Code to access the camera.

Scan the user's QR code when they present it to you. The Verifier app will provide you with the information to determine the validity of the credential. Other information which the user has selected to share will also be included.

The driver licence status will be shown through colours - green represents Current, while red represents Cancelled or Suspended. A cancelled or suspended licence may still be used as a form of identification, however the user no longer has authority to drive.

Note: Once the DLA has been verified, the information is only displayed for a limited time and can not be saved.



If a customer shares their full driver licence

If a customer shares that they are over 18