

## Signature Validation Instruction

When opening a PDF file in Adobe Acrobat Reader, if it contains a signature, it is automatically verified. OCPP certificates are signed, if a downloaded OCPP certificate PDF leads to the following warning:

F	File Edit View Sign Window Help	×
	Home Tools Document 🖺 📩 🖶 🖂 🔍 $\bigcirc$ 1 /6 🗒 $\mathscr{L}$	Q Share
	🚣 At least one signature has problems.	(Signature Panel) @

please follow the instructions below to verify the signature on a certificate PDF using Adobe Acrobat Reader.

## 1. Go to "Edit" - "Preferences"



2. Click "Signatures" in the left column and click the "More..." button in the "Identities & Trusted Certificates" block

Preferences		>
Categories:	gital Signatures	
Commenting Documents	Creation & Appearance	
Full Screen General Page Display	Control options for signature creation Set the appearance of signatures within a document	More
Accessibility Email Accounts	Verification	
Forms Identity	Control how and when signatures are verified	More
Internet JavaScript	Identities & Trusted Certificates	
Measuring (2D) Measuring (3D)	Create and manage identities for signing Manage credentials used to trust documents	More
Multimedia & 3D Multimedia (legacy) Multimedia Trust (legacy)	<u>Document Timestamping</u> Configure timestamp server settings	
Reading Reviewing		more
Search Security		
Security (Enhanced) Signatures		
Tracker		
Trust Manager Units		



3. In the pop up that opens, click "Trusted Certificates" on the left and click "Import".

Digital	ID and Trusted Certificate	Settings					×
$\sim$	Digital IDs	1	🦱 Import	≓ Export	Tertificate Details	Remove	•
	Roaming ID Accour	Name	^		Certificate Issuer		Expires \land
	Digital ID Files	Air Cana	Air Canada Enterprise Root CA1		Air Canada Enterprise Root CA1		2037.0
	Digital ID Files		AKD QTSA 2021 1	KIDCA		2026.0	
	Windows Digital IDs		A 2021 2		KIDCA		2026.0!
			A1		KIDCA		2024.0!
	PKCS#11 Modules a	AKD QTS	A1		KIDCA		2022.1;
	Trusted Castificator	AKD QTS	A2		KIDCA		2022.1;
	Irusted Certificates		A2		KIDCA		2024.0!
		AlfaSign	Public CA		ALFATRUST ROOT CA		2015.1(
		AlfaSign	Qualified CA		ALFATRUST ROOT CA V2		2031.1
		Alfasign	Qualified Public CA		Alfasign Qualified Root CA		2037.0
		Alfasign Qualified Root CA		Alfasign Qualified Root CA		2047.0	
		AlfaSign	Time Stamping Aut	hority <office@alfasi< td=""><td>Alfasign Qualified Public CA</td><td></td><td>2027.0</td></office@alfasi<>	Alfasign Qualified Public CA		2027.0
		AlfaSign	Time Stamping Aut	hority G3 < office@al	Alfasign Qualified Public CA		2025.0
		`					
		- BNL S.p.A. Corporate Firma Certification Service Provider					
		Issued by: - BNL S.p.A. Corporate Firma					
		Certification Service Provider					
		Valid from: 2003.09.09 08:24:28 Z					
		Valid to: 2014.09.30 23:59:59 Z Intended usage: Sign Certificate (CA), Sign CRL					

4. In the pop up that opens, browse to the OCA certificate that can be downloaded from https://www.openchargealliance.org/uploads/files/OCA-Certification-Root-CA.cer

Name	E	mail	Remove
			Browse
			Search
This list displays the	e certificates associated	with the currently selected con	tact.
Subject	lssuer	Expires	Details
			<b>-</b> .



5. Next, select the certificate in the "Contacts" section, click the certificate in the "Certificates" section and click "Trust".

Choose Contacts to Import			×
This dialog will allow you to sel any certificates associated with Contacts	an also set the trust for		
Name	Email		<u>R</u> emove
🖾 Open Charge Alliance	Certificate info@open	chargealliance.org	
			<u>B</u> rowse
			Search
Certificates			
This list displays the certific	ates associated with the c	urrently selected contact.	
Subject	lssuer	Expires	Details
Open Charge Alliance	Open Charge Alliance	11-7-2063 16:00:57	
			<u>T</u> rust
Help		l <u>m</u> port	Cancel



6. Select the option to trust the root certificate as a trusted root and click ok.

Import Contact Settings	$\times$
Certificate Details	
Subject: Open Charge Alliance Certificate Root <info@openchargealliance.org></info@openchargealliance.org>	
Issuer: Open Charge Alliance Certificate Root <info@openchargealliance.org></info@openchargealliance.org>	
Usage: Sign Certificate (CA), Sign CRL	
Expiration: 11-7-2063 16:00:57	
Trust	
A certificate used to sign a document must either be designated as a trust anchor or chain up to a trust anchor in order for signature validation to succeed. Revocation checking is not performed on or above a trust anchor.	
Use this certificate as a trusted root	
If signature validation succeeds, trust this certificate for:	
Signed documents or data	
Certified documents	
Dynamic content	
Embedded high privilege JavaScript	
$\square$ Privileged system operations (networking, printing, file access, etc.)	
Certificate Details	
Help OK Cancel	

7. Click OK when the import is completed.

8. As a final step, close the PDF and open it again. It will now indicate that the signature is valid:

