

Linux and LibreOffice User Guide for HYP2003

HyperPKI USB Token

09/09/2022

HSTE-NB0066-IND-RV1.0

HYPERSECU INFORMATION SYSTEMS INC

200-6191 Westminster Hwy, Richmond BC, V7C 4V4 Canada 1-604-279-2000 | hypersecu.com

Table of Contents

Getting Started	1
Installing HYP2003 Token Driver in Linux Ubuntu	1
Setting Up Chrome to Use the HYP2003 Token for PDF Signing	2
Setting Up LibreOffice to Use Chromium Certificates	6
Setting up Mozilla Firefox to Use the HYP2003 Token to Sign PDFs in LibreOffice	8
Digital Signing with LibreOffice	12
Digitally Signing ODF Documents	12
Digitally Signing Existing PDF Documents	16
Checking the Digital Signature on ODF Documents and Existing PDF Documents	17

Document History

Version	Release Date	Description of Changes	Document Owner	Approved By
1.0	2022-09-09	Original document	NB	JL

Getting Started

Installing HYP2003 Token Driver in Linux Ubuntu

- 1. Open the terminal and execute the command uname -m to determine if your system is 32-bit or 64-bit.
- 2. Extract the downloaded files, then find and open the config folder.
- 3. Right-click and select the open terminal here or open that path in terminal.
- 4. Enter the following command:

sudo sh config.sh

- 5. Enter the sudo user password.
- 6. After entering the password, you will receive the message Run Finish >
- 7. Enter the following command:

cd ../redist >

8. Enter the following command:

```
sudo chmod a+x pkimanager >
```

9. Enter the following command:

sudo chmod 775 >

10. Enter the following commands:

```
sudo cp libcastle_v2.so.1.0.0 /usr/lib/ >
sudo chmod 700 /usr/lib/libcastle_v2.so.1.0.0 >
sudo chown user:group /usr/lib/libcastle v2.so.1.0.0 >
```

- 11. Plug the token into the system and double-click to open the pkimanager from redist folder.
- 12. Check the status of the token to make sure you receive the message that the token is inserted and ready to use.

NOTE: This works for only CSP 2.0 tokens (as per CCA Guidelines for PKI Hardware, issued in 2018). $libcastle_v2.so.1.0.0$ is the PKCS#11 library file which communicates with the token for the certificate.

In the application where you want to use the certificate, that application must be able to browse PKCS#11 lib (libcastle_v2.so.1.0.0) in it.

If you are using a token with CSP V.10, you can update your existing token to CSP V2.0 from <u>https://update.epasstokens.com</u>.

Setting Up Chrome to Use the HYP2003 Token for PDF Signing

Chrome for Linux manages digital certificates similarly to Firefox by using Mozilla NSS as the backend. However, unlike Firefox, Chrome does not provide a graphical user interface to install PKCS#11 modules. Therefore, to set up Chrome you will need to use the command line.

NOTE: Make sure your token contains the user certificate and is plugged in before proceeding. You must also be using a HYP2003 token with **CSP V2.0**.

1. Open the terminal and install Mozilla NSS Tools if it is not already installed on your system:

```
$ sudo apt-get install libnss3-tools
$ sudo mkdir ~/.pki/nssdb
$ sudo chmod -R 0700 $HOME/.pki
$ sudo modutil -dbdir ~/.pki/nssdb/ -add "ePass2003" -libfile
/usr/lib/libcastle_v2.so.1.0.0
```

- 2. modutil will alert you that you need to close your browser if it is not already closed. Type q <enter> to abort or <enter> to continue.
- 3. Once any running browsers are closed, press **Enter**. When the command finishes, you can reopen your browser.

WARNING: Performing this operation while the browser is running could corrupt your security databases.

- 4. Module "epass2003" is added to the database.
- 5. Verify that the token has been successfully added by running the following command:

```
$ modutil -dbdir sql:.pki/nssdb/ - list
```

6. As root, to load the root CA (CCA India 2022, 2014) certificate into the NSS database, enter the following command:

```
certutil -A -n rootca -i /location_of_ca_root_cert/rootcert.pem -t
"CT,CT,CT" -d ~/.pki/nssdb
```

7. To root load each sub CA's public certificate into the NSS database, enter the following command:

```
certutil -A -n subca -i /location_of_subca_root_cert/rootcert.pem -t
"CT,CT,CT" -d ~/.pki/nssdb
```

8. To verify that the certificates have loaded, as root, enter the following command:

```
certutil -L -d ~/.pki/nssdb
```

It is also possible to verify the trust of a root CA certificate through the Chrome browser.

1. Open Chrome, then open the menu and click **Settings**.

S Settings ×	Root Certificate CCA	× New Tab	× +			• – •	3 (2
→ C A Not secure cca.gov.in	rroot_certificate.html		Å* A⁻ A 📑 Skip to	main cor	New tab New window New incogni	x V (to window Ctrl+Sh	Ctrl+T Ctrl+N hift+N
meder used	nics & Information Technology ndia	Home About C	CA Services FAQ	Conta	History Downloads Bookmarks	1	Ctrl+J
PKI Framework Root CA	of India Licensed CAs	Root Certificate	CA Certificates	eSigr	Zoom	- 100% +	53
Home Root Certifying Authority of	» Root Certificate	Root Certificate			Print Cast Find More tools	ļ	Ctrl+P Ctrl+F
India	SON.	Root CA of			Edit	Cut Copy	Paste
Certificate Practice Statement	N/S	India			Settings		
Root Certificate	CITETED A				Help		
Expired Root Certificate	A root certificate is a self-s	igned certificate A root o	artificate the ton-most of	artificat	Exit		
	standard. All certificates be Existing Root Certificates	ow the root certificate inh	erit the trustworthiness of	the root ce	rtificate.		
	Name	Valid From	Valid To	Certif	Icate	Latest Cri	
				(2 KB)	1.54	(1 KB)	
	CCA India 2015 SPL	29.01.2015	29.01.2025	(2 KD)		(=	

2. Select **Privacy and Security**, then select **Security**.

🎯 Google Chrome 🔫	Aug 6 18:29	🔷 📢 🕂 🛨
S Settings	🗙 🍘 Root Certificate CCA 🛛 🗙 New Tab 🛛 🗙 🕂	🗢 – 🕫 🙆
\leftrightarrow \rightarrow C \odot Chrome ch	rome://settings/privacy	🖈 🗳 🛊 😩 E
Settings	Q Search settings	
You and Google	Privacy and security	
Auto-fill Safety check	Clear browsing data Clear history, cookies, cache and more	
Privacy and security Appearance	Cookies and other site data Third-party cookies are blocked in Incognito mode	
Q Search engine	Security Safe Browsing (protection from dangerous sites) and other security settings	
 Default browser On start-up 	또 Site settings Controls what information sites can use and show (location, camera, pop-ups and more)	
Advanced	Appearance	
Extensions	Theme STK+ Use Classic Use Classic	
	Show Home button Disabled	
	Show bookmarks bar	

3. Navigate to Manage Certificates and click on the Authorities tab.

s 💿 Google Chrome 🔫	Aug 6 18:30	💎 🌒 🕯 🗸
S Settings – Security × 🙆	Root Certificate CCA × New Tab × +	
← → C © Chrome chrome://settings	/security	x 🔮 🛊 🚢 E
Settings	Q Search settings	
 You and Google Auto-fill Safety check Privacy and security Appearance Search engine Default browser On start-up 	Help Improve security on the web for everyone Sends URLs of some pages that you visit, limited system information and some page content to Google, to help discover new threats and protect everyone on the web. Warn you if passwords are exposed in a data breach Chrome periodically checks your passwords against lists that have been published online. When doing this, your passwords and usernames are encrypted, so they can't be read by anyone, including Google. When you sign in to your Google account, this feature is turned on. No protection (not recommended) O Does not protect you against dangerous websites, downloads and extensions. You'll still get Safe Browsing protection, where available, in other Google services, like Gmail and Search. Advanced	
Advanced • Extensions 🖸 About Chrome	Manage security keys , Reset security keys and create PINs , Manage certificates , Manage HTTPS/SSL certificates and settings , Google Advanced Protection programme Safeguards the personal Google Accounts of anyone at risk of targeted attacks	

4. Navigate to **org-India PKI** and expand the section to find the CCA India 2014, which is the root-certifying authority in India. Root certificates available on the HYP2003 token will appear in the list here.

Settings – Manage certific ×	Root Certificate CCA × New Tab	× + •	- 0
→ C	ttings/certificates?search=org-India+PKI	A	6 x Z
ettings	Q, org-India PKI	Q	
You and Google	arg-IdenTrust	~	
Safety check	org-india PKI	^	
Privacy and security	CCA India 2014	View	
Appearance	org-Internet Security Research Group	Edit	
λ Search engine	org-IZENPE S.A.	Export Delete	
コ Default browser り On start-up	org-Japan Certification Services, Inc.	~	
dvanced +	org-Krajowa Izba Rozliczeniowa S.A.	Ŷ	
standare F2	org-LuxTrust S.A.	*	
bout Chrome	org-Microsec Ltd.	~	
	org-NetLock Kft.	*	
	org-Network Solutions L.L.C.	~	

NOTE: If you can't find the CCA India 2014, you will need to import manually.

5. Click **Edit**, then check all available checkboxes and click **OK**.

🌍 Google Chrome 🔫	Aug 6 18:03	🗢 🌒 🕂 🛨
📀 Linux Cert Management 🛛 🗙 Skype	× 🕏 Settings – Manage certific × 🔮 Root Certificate CCA × 🕂 +	
\leftrightarrow \rightarrow C \odot Chrome chrome://settings/	certificates	🕸 😜 🌲 🗄 E
Settings		
You and Google	org-Hellenic Academic and Research Institutions Cert. Authority	*
📋 Auto-fill	org-Hongkong Post 🗸 🗸	
Safety check	pro-IrienTrust	
Privacy and security	The certificate 'CCA India 2014' represents a Certification Authority	
Appearance	Trust settings	
Q Search engine	Trust this certificate for identifying websites	
() On start-up	 Trust this certificate for identifying entail users Trust this certificate for identifying software makers 	
Advanced +	· · · · · · · · · · · · · · · · · · ·	
Extensions	Cancel	
About Chrome	org-Lux Trust S.A.	
	org-Microsec Ltd.	
	org-NetLock Kft.	

Setting Up LibreOffice to Use Chromium Certificates

Chromium users do not need to install and set up Firefox to sign documents with LibreOffice. Instead, they can set up LibreOffice to use the Chromium public key infrastructure.

To do so:

- 1. Open the Tools menu, then click **Options**.
- 2. Click **LibreOffice** to expand the tree on the left side panel, then select **Security** and click **Certificate**.

	Options - LibreOffice - Security	×
 LibreOffice 	Security Options and Warnings	
User Data General View	Adjust security related options and define warnings for hidden information in documents.	Options
Print	Passwords for Web Connections	
Paths Fonts	Persistently save passwords for web connections	Connections
Security	Protected by a master password (recommended)	
Application Colors	Passwords are protected by a master password. You will be	1
Accessibility	asked to enter it once per session, if LibreOffice retrieves a	Master Password
Advanced	password from the protected password list.	
OpenCL	Macro Security	
Load/Save Language Settings LibreOffice Writer	Adjust the security level for executing macros and specify trusted macro developers.	Macro Security
► LibreOffice Writer/Web	Certificate Path	
 LibreOffice Base Charts Internet 	Select the Network Security Services certificate directory to use for digital signatures.	Certificate 🔖
- internet	TSAs	
	Maintain a list of Time Stamping Authority (TSA) URLs to be used for digital signatures in PDF export.	TSAs
Help	Reset Apply	Cancel OK

3. In the Certificate Path window, click Add.

n		Certificate Path _ 🗆 🗙	
c	ertificate Path Select or add the c digital signatures:	orrect Network Security Services Certificate directory to use for	Mas
gs er	Profile	Directory	M
en			
			-



- 4. In the Select Path field, press **Ctrl+L** to manually enter the location.
- 5. Enter ~/.pki/nssdb/ and click OK.

Cancel	Select Path Enter location or URL	٩	ок 📐
⊘ Recent	~/.pki/nssdb/		
🔂 Home	Name	 Size	Modified
🖿 Desktop	🛅 bin 🔯 Desktop		11 Mar 2019 21:21
Documents	Documents		22:15
🕹 Downloads	Downloads		21:25
J Music	 Music Pictures 		21:21 22:20
Pictures	🔯 Public		21:21
	🛅 Templates		21:21
圖 Trash	🐱 Videos		21:21

- 6. Click **OK** in the Certificate Path window to close the window, then click **OK** in the Options window to close the window.
- 7. Restart LibreOffice to complete setup.

Setting up Mozilla Firefox to Use the HYP2003 Token to Sign PDFs in LibreOffice

NOTE: Before getting started, be sure Mozilla Firefox can browse PKCS#11 lib (libcastle_v2.so.1.0.0) in it.

1. Open Firefox, then enter about:preferences#privacy into the address bar and press **Enter**.



2. Click Security Devices to open the Device Manager.

- 3. Click Load.
- 4. In the Module Name field, enter ePass2003.
- 5. In the Module File Name field, enter /usr/lib/libcastle_v2.so.1.0.0.

Formula Medular and Daviese	Data	ile	Malua		
security modules and Devices	Deta	IIS	value		Log I <u>n</u>
V NSS Internal PKCS #11 Module					Log Out
Software Security Device		Load PKCS#11 Device	e Driver	0	Change Password
∨ Builtin Roots Module	Enter the inform	ation for the module you w	vant to add.		Load
NSS Builtin Objects	Module Name ePass2003			Unload	
✓ OS Client Cert Module	Module <u>f</u> ilename	/usr/lib/libcastle_v2.so.*	1.0.0	Browse	Enable <u>F</u> IPS
		[Cancel	ок	

6. Click **OK** to close the Device Manager.

Activities	s 🕴 Firefox N	Web Browser 👻	May 16	16:32	🔹 👍 🤹 🕈
	袋 Settings	× +			- • 🤇
	$\leftarrow \rightarrow G$	Sirefox about:preferences#	^t privacy		☆ 🗢 =
				Transa and Antonio	
			Device Mar	O Find in Sottings	×
Â	5 G			1800	
		Security Modules and Devices	Details	Value	Log In
2	۵ H	~ NSS Internal PKCS #11 Module	Status	Not Logged In	Les Out
	Q Se	Generic Crypto Services	Description	ES SLOT 1	Logout
		Software Security Device	Manufacturer	EnterSafe	Change Password
	e Pi	~ Builtin Roots Module	HW Version	1.0	Load
>_	() Sy	NSS Builtin Objects	FW Version	1.0	Unload
		v ePass2003	Label	ePass2003	
	m M	ES SLOT 1	Manufacturer	Feitian Technologies Co., Ltd	Enable <u>F</u> IPS
		∨ OS Client Cert Module	Serial Number	2315BB5980108034	
			HW Version	1.0	
DYD			FW Version	1.0	
0					
	ව Ex	·	X		
::::	⑦ Fir				

7. Click **Certificate**.

8. In the Your Certificates tab, you can view the current user certificate on the HYP2003 token.

NOTE: Make sure the token is with root chain of CCA and Issuer CA.



9. Click the **Authorities** tab and find the India PKI. Click **Edit Trust**, then check both checkboxes and click **OK**.



- 10. Open the LibreOffice writer and go to **Tools > Options > Security > Certificate**.
- 11. Make sure Firefox:default-release is selected, then click **OK**.

Activities May 16 17:32 🖹 LibreOffice Writer 🔻 A 🐠 🔱 ¢ Untitled 1.odt - LibreOffice Writer File Edit View Inse Options - LibreOffice - Security E - - - - -10.00 LibreOffice Security Options and Warnings Default Style 👻 🖌 User Data ≡ • 4≣ ≭≣ Adjust security related options and define warnings for hidden information in documents. Options.. General At least one signat × Â lignatures View Passwords for Web Connections Print Persistently save passwords for web connections Paths ? ? ? ? ? Protected by a master password (re Fonts A Certificate Path Personalization 1 Application Colors Certificate Path Select or add the correct Network Security Services Certificate directory to use for digital signatures: Accessibility 0 Macro Security... Advanced OpenCL Profile Directory Load/Save firefoxed /home/bharat/.mozilla/firefox/ywo3ztnf.default-releas Certificate.. Language Settings LibreOffice Writer LibreOffice Writer/We LibreOffice Base TSAs.. Charts Internet Help Select NSS path.. Cancel OK • Help Revert Apply Cancel OK is 0 chai

Digital Signing with LibreOffice

If you have a digital certificate, you can sign documents before sending them to ensure the recipient is confident about the documents' authenticity and integrity. LibreOffice can sign not only Open Document Format (ODF) documents, but also any PDF documents including those created by other programs.

Although capable of digitally signing documents, LibreOffice does not have its own public key infrastructure. Instead, it uses the infrastructure of a web browser to sign documents.

Mozilla Firefox Browser

By default, LibreOffice looks for certificates and cryptographic media in the Mozilla Firefox configuration. If you use Firefox, you must set it up before signing documents with LibreOffice. To do so, follow the procedures described in the documents below:

- How to install website certificates on Linux
- Using smart cards on openSUSE Linux

Chromium-Based Browsers

Linux Kamarada 15.1 brings Chromium as default web browser. If you use Chromium (or a Chromium-based browser, such as Google Chrome, Opera, Vivaldi or Brave), you can set up LibreOffice to use it instead of Firefox.

To do so, follow the procedures described in the document below:

• <u>Setting up smart card authentication on Google Chrome / Chromium</u>

Digitally Signing ODF Documents

The Open Document Format (ODF) is the default file format for LibreOffice. The following file types and extensions are all considered ODF documents and can be digitally signed:

- .odt for text documents, opened with Writer
- .ods for spreadsheets, opened with Calc
- .odp for presentations, opened with Impress
- .odg for graphics (diagrams, vector images), opened with Draw
- .odb for databases, opened with Base
- .odf for mathematical equations (formulas), opened with Math

This section will use a .odt file to demonstrate how to digitally sign an ODF document. The steps will be similar for all ODF files using a LibreOffice Suite application.

		test.odt - LibreOffice Writer
File Edit View Insert F	ormat Styles	Table Form Tools Window Help
New Open Open Remote Recent Documents Close Wizards Templates) Ctrl+O)	digitally signed.
Versions Save Save As Save Remote Save a Copy Save All	Ctrl+S Shift+Ctrl+S	
Export Export As Send Preview in Web Browser	Þ	
 Print Preview Print Printer Settings 	Shift+Ctrl+O Ctrl+P	
Properties		
Digital Signatures	2	Digital Signatures 📡
Exit LibreOffice	Ctrl+Q	Sign Existing PDF

1. Open the **File** menu, then navigate to Digital Signatures and click **Digital Signatures**.

- 2. If you are prompted to save the document, click **Yes**.
- 3. In the Digital Signatures window, click **Sign Document**.

	test.od	t - LibreOffice Write	er:	-	• ;
ile Edit View Insert Forr	nat Styles Table Form To	ols Window Help			3
🖹 • 🔛 • 💽 • 🚺 🚔	🔍 🐰 🗟 🛍 🖌 🛓 🧇	• 🧼 - 😪 abç	1 🔜 - 📖 🗎	Α 🚧 🚝 • Ω •	P4
Default Style - A A	Liberation Seri 💌 12	- RIU	- A ² A ₂ A	A • / • = =	=
	Di	gital Signatures			>
he following have signed the	document content:				
Signed by	Digital ID issued by	Date	Descriptio	n Signature type	
Use AdES-compliant signati	ure when there is a choice				
View Certificate	Sign Document		Remove	Start Certificate Manao	er
View Certificate	Sign Document	k	Remove	Start Certificate Manag	er
View Certificate	Sign Document	<u> </u>	Remove	Start Certificate Manag	er
View Certificate Help	Sign Document	<u> </u>	Remove	Start Certificate Manag	er Close
View Certificate	Sign Document	k	Remove	Start Certificate Manag	er Close
View Certificate	Sign Document		Remove	Start Certificate Manag	er Close
View Certificate	Sign Document	k	Remove	Start Certificate Manag	er Close
View Certificate	Sign Document		Remove	Start Certificate Manag	er
View Certificate	Sign Document		Remove	Start Certificate Manag	er

4. Enter the token's PIN, then select the certificate you want to use to sign the document and click **Sign**.

	Select Certificate				×
Select the certificate you want to use for s	igning:				
Issued to	Issued by	Туре	Expiration date	e Certifi	icate usage
ANTONIO VINICIUS MENEZES MEDEIROS	Autoridade Certificadora SERPRO	X.509		Digital	signature, l
				View C	ertificate
Description:					
Help				Cancel	Sign N
Tich				currect	Jight R

5. In the Digital Signatures window, confirm that the document has been digitally signed and click **Close**.

		Digital Signatures			×
The fo	llowing have signed the document con	tent:			
	Signed by	Digital ID issued by	Date	Description	Signature type
۲	ANTONIO VINICIUS MENEZES MEDEIF	ROS Autoridade Certificadora SERPRO	03/12/2020 22:24:42		XAdES
🤵 Th	ne signatures in this document are valid				
🕑 Us	e AdES-compliant signature when there	is a choice			
	View Certificate Si	gn Document	Remove	Start Certific	ate Manager
_					

	test.odt (Signed) - LibreOffice Writer	_ = ×
File Edit View Insert Forma	t Styles Table Form Tools Window Help	×
	View Certificate	× A 🔤 ≅ • Ω • 🖧 »
31	General Details Certification Path	×
The following have signed the d	Certificate Information	
Signed by		Signature type
ANTONIO VINICIUS MEN	This certificate is validated. Issued to: ANTONIO VINICIUS MENEZES MEDEIROS	XAdES
	Issued by: Autoridade Certificadora SERPRORFBv5 Valid from: Valid to:	
👒 The signatures in this docun		
✓ Use AdES-compliant signatur View Certificate		Start Certificate Manager
Help		Close
	Неір ОК	
Page 1 of 1 8 words, 46 characters	Default Style English (USA) I 💷 🐼 🦉	D DD 00

Digitally Signing Existing PDF Documents

LibreOffice also sign any existing PDF documents, including those created by other applications outside LibreOffice.

To sign an existing PDF document using LibreOffice:

- 1. Open the **File** menu, then navigate to Digital Signatures and click **Sign Existing PDF**.
- 2. Open the PDF document you want to sign. LibreOffice will open the document in Read-Only mode.

					wikipedia.p	df (read-on	ly) - Libr	eOffice	Draw			_ =	×
File	Edit V	iew Insert	Format	Page	Shape Tools	Window	Help						×
	• 🗀 •	•		81	1 Q - 1	$\langle \phi \circ \phi \rangle$	-	:#: 27		<u>Δ</u> · Δ	0	• • • • •	»
k	1	This PDF is o	pen in rea	d-only	mode to allow	signing the	existing f	file.		Edit Docum	ent	Sign Document	×
1.	+	5 I 4 I	3 I Z	(j	1 0 1 Î I	ž I š I	4 I 5	1 6 1	- Ż - 1	i g i ti		i i 12 i 13 i 14	1
0.	0				3/12/2020		PCF Wilepedia			an 100 and 100 100 100 100 100 100 100 100 100 10			
					WIKIPEDIA PDF								
1	-				The Portable Data file format develop including text form	ment Format (PDF) (roduct od by Addre in the 1990s atting and images, in a n	anty: PDF format) o to prevent document anner independent 178.9 a	of Portable Do	ocum ent Format				
	2				PostScript language of a fixed-layout fla meter images and	mentioner, and operating of such PDF file encapsulat document, including the on- the information needed to	s a complete descrip , from, vector graphi display it. PDF w	ar dan ar	PDF				
	-				standardiost as ISO for its implementat Today, PDF files m	32000 in 2008, and no longe a ^[4] ty contain a variety of conten	requires any royaltic	n Adab					
	- 4				graphics including l in armotations and content) and threed other data formats.	agical sinucturing elements, t form-fields, layers, rich n mensional objects using U33 The PDF specification also	teractive elements a edua (including vid) or PRC, and various provides for encry	stonFilename	.pdf fices 1]				
20.	- 01 -				and digital signature propiring these four	s, file attachments and metac nus.	ata to enable work fio	wis loc terms form Intrame t me dia, type	application/pdf [1]				

3. Click **Sign Document** and follow the procedures described in steps 3-5 in *Digitally Signing ODF Documents* to complete the digital signing process.

Checking the Digital Signature on ODF Documents and Existing PDF Documents

When you open a digitally signed ODF document or a digitally signed existing PDF document, LibreOffice will inform you that the document is signed. It will also display the Digital Signature icon on the status bar.

	-
test.odt (Signed) - LibreOffice Writer	x c
File Edit View Insert Format Styles Table Form Tools Window Help	×
🖸 • 🖬 • 💽 • 🚺 🖶 🔍 🐰 🖄 🖄 - 🎍 🧇 • 🛷 • 😪 🕸 👖 🧮 • 🔜 🛍 🗛 🚧 🚝 • Ω • 🥔	2 »
Default Style \bullet Ag Ag Liberation Seri \bullet 12 \bullet B $I \ U \ S \ A^2 \ A_2 \ A \ A \ A \ C \ C \ C \ C \ C \ C \ C$	≣ »
7 This document is digitally signed and the signature is valid. Show Signatures ×	0
	A!
This document is going to be digitally signed.	
Page 1 of 1 8 words, 46 characters Default Style English (USA) I_< I	100%
Digital Signature: The document signature is OK.	

To view the document's digital signature:

- 1. Double-clickthe **Digital Signature** icon on the status bar or click **Show Signatures** on the system message.
- 2. In the Digital Signatures window, select a digital signature and click **View Certificate** to view more details.

NOTE: The Certificate Information "This certificate is validated" and the Certification status "This certificate is OK" indicates that LibreOffice has established the Certification Path up to the certificate of a known certificate authority.