# NICDSign Installation Manual for Ubuntu

National Informatics Centre, Kerala State Centre

# Contents

1. NIC	CDSign installation in Ubuntu	. 3
1.1.	DSC token driver installation	. 3
1.2.	NICDSign installation	. 3
1.3.	Remove NICDSign	. 5
2. Bro	owser Configuration	. 6
2.1.	Mozilla Firefox	. 6
2.2.	Google Chrome	. 9

# 1. NICDSign installation in Ubuntu

For Ubuntu operating system the following prerequisites are required:

- DSC token driver
- Java8

However, Java 8 runtime is bundled along with the NICDSign Debian package and will be installed and configured along with installation.

### 1.1. DSC token driver installation

To install DSC driver,

- Make sure you have JRE 1.8 installed
- Use key combination Ctrl+Alt+t open terminal
- Enter java -version to check installed java version
- Proceed installation, if java -version shows to be 1.8, otherwise install and proceed

```
gst@gstnode1:~$ java -version
java version "1.8.0_144"
Java(TM) SE Runtime Environment (build 1.8.0_144-b01)
Java HotSpot(TM) 64-Bit Server VM (build 25.144-b01, mixed mode)
```

• Copy driver to Desktop. Here for Eg: ProxKey Token.



- To install token driver, open terminal Ctrl+Alt+t
- Type cd Desktop to go to Desktop
- Install driver using command:

sudo dpkg -i wdtokentool-proxkey\_1.1.0-1\_all.deb

```
gst@gstnode1:~$ cd Desktop
gst@gstnode1:~/Desktop$ sudo dpkg -i wdtokentool-proxkey_1.1.0-1_all.deb
[sudo] password for gst:
(Reading database ... 524714 files and directories currently installed.)
Preparing to unpack wdtokentool-proxkey_1.1.0-1_all.deb ...
```

If installation Completes successfully, we can proceed with NICDSign Installation.

#### 1.2. NICDSign installation

Uninstall previous version of DSCS igner already installed by running the following command in the terminal:

National Informatics Centre, Kerala State Centre

#### sudo dpkg --purge dscsigner

To install NICDSign, open the Terminal and type the following command



After installation, NICDSign will starts automatically once DSC token is connected to the system. Once NICDSign is started, NICDSign status window will be displayed with running status.



• To select the token driver to TrustKey, Install Trustkey driver in your machine click on **Settings** button.



If DSC token is not listed by default, a custom driver selection can made available where user can provide their custom driver and reinitialize with new driver next time.



If DSC token is listed by default then use the dropdown and select appropriate driver, here for example choose TrustKey and Click Save button to save driver selection.

😸 🖨 DSCSigner Settings				
If DSC token is not listed below, Select Custom and provide path to the driver				
Select DSC token				
Token Driver RUSTKEY/lib/libwdpkcs_TRUSTKEY.so Save				
😣 DSCSigner Info				
Your driver selection was saved successfully.     Please remove & reconnect the USB token to reinitialize.     OK				

Then you will be shown a message saying token driver saved successfully. Now remove and reconnect your token to reinitialize with new driver.

## 1.3. Remove NICDSign

To uninstall NICDSign from Ubuntu, run the following command from terminal: sudo dpkg --purge nicdsign

# 2. Browser Configuration

The browser must be configured prior to the use of NICDSign tool to configure the browser to trust the NICDSign Client. The configuration for the browsers are given below.

## 2.1. Mozilla Firefox

1. Open Mozilla Firefox and type the following in the address bar and press enter.

#### about:preferences#privacy

2. Scroll down to view the Certificate section and click on the **View Certificates** button to open the certificate manager.

Options	× +				24	-	0	$\times$
+ Ofinitier aboutpreferen	noes#privacy	+ C Q. Search	\$ D	+	ń	•	68	=
General     Search     Privacy & Security     Firefox Account	Block dangerous and deceptive content     I    Slock dangerous downloads     I    Warn you about unwanted and ungommon software     When a server requests your personal certificate     Select one automatically     Select one automatically     Ask you every time     Query OCSP responder servers to confirm the current validity of certificates	D Find in Options View Certificates Security Devices						~
① Firefox Support	Offline Web Content and User Data Your application cache is currently using 0 bytes of disk space ✓ Jell you when a website asks to store data for offline use The following websites are allowed to store data for offline use:	Clear Now Exceptions						

3. In the Certificate Manager popup, click on the Authorities tab and then click on Import button.

	Certifica	te Manager	
Your Certificates People Servers	Authorities	Others	
You have certificates on file that identify these	certificate authorities	:	
Certificate Name		Security Device	e,
✓AC Camerfirma S.A.			,
Chambers of Commerce Root - 2008		Builtin Object Token	
Global Chambersign Root - 2008		Builtin Object Token	
✓AC Camerfirma SA CIF A82743287			
Camerfirma Chambers of Commerce Root		Builtin Object Token	
Camerfirma Global Chambersign Root		Builtin Object Token	
~ACCV			
ACCVRAIZ1		Builtin Object Token	
✓Actalis S.p.A./03358520967			
Actalis Authentication Root CA		Builtin Object Token	
View Edit Trust	port Delete o	r Distrust	
			OK

4. Browse to NICDSign/ssl folder and select the rootCA.crt file and click on the Open button.

😣 🗊 Select File co	ontaining CA certificate(s) to import		
🔿 Recent	✓ ✿gst Ubuntu_Backup Documents DSCSigner ssl ▶		
✿ Home	Name 🔺	Size	Modified
🛅 Desktop	🗋 dscsigner.dev.crt	1.6 kB	Wed
Documents	rootCA.crt	2.2 kB	Wed
🕹 Downloads			
J Music			
D Pictures			
▶ Videos			
+ Other Locatio			
		Certific	ate Files 🔻
	Can	cel	Open

5. Check the **Trust this CA to identify websites** and click on OK button to complete the root certificate export.

😣 🖨 💷 Downloading Certificate
You have been asked to trust a new Certificate Authority (CA).
Do you want to truct "DECE inner Doot CA" for the following overses?
Do you want to trust. Discigner Root CA Tor the rollowing purposes?
Irust this CA to identify websites.
Trust this CA to identify email users.
Trust this CA to identify software developers.
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).
View Examine CA certificate
Cancel OK

The configuration is complete and now you can use Mozilla Firefox for digital signing using NICDSign.

# 2.2. Google Chrome

1. Open Google Chrome browser and type the following in the address bar and press enter:

#### chrome://flags/#allow-insecure-localhost



Click on Enable link to enable

2. On the address bar type

#### chrome://settings/certificates

× Settings ×					
chrome:// <b>settings</b> /certificates					
	Q Sear	ch settings			
	← M	anage certificates			
	YOU	R CERTIFICATES	SERVERS	AUTHORITIES	OTHERS
	You have	ecertificates on file that io	dentify these certificate au	thorities	IMPORT

Choose Authorities tab from available tabs and click on the IMPORT link Choose root Certificate file from your file system, then a popup appears with options

Certificate authority	×
The certificate 'DSCSigner Root CA' represents a Certification Authority	
Trust settings	
Trust this certificate for identifying websites	
Trust this certificate for identifying email users	
Trust this certificate for identifying software makers	
CANCEL	ОК

Choose 'Trust this certificate for identifying website' and click OK. The root certificate will be listed under the tab.

org-National Informatics Centre	^
DSCSigner Root CA	:

Now chrome can be used for signing in Ubuntu.