



Carillon eShop User's Guide



Contents

1		Intr	oduc	tion	3
2		HO	W-TC	: SET UP A CA CERTIFICATE CHAIN (TRUST CHAIN) IN WINDOWS 10	4
	2.	.1	Inst	alling the Carillon CA Trust Chain	5
		2.1	.1	Download & Install the Carillon Root CA Certificate	5
	2.1.2 2.1.3 2.2 Ins ⁻ 2.2.1		.2	Download & Install Carillon Intermediate CA Certificate	9
			.3	Validate the Root Certificate Thumbprint	14
			Inst	alling the Boeing Trust Chain	16
			.1	Download Boeing Certificates	16
		2.2	.2	Install the Boeing Root CA Certificate	17
		2.2	.3	Install Boeing Intermediate CA Certificate	21
	2	.3	Veri	fying the Trusted Site and Validating the EVSSL	26
3		CEF	RTIFI	CATE RETRIEVAL PROCESS	30
4		THE	E ACK	NOWLEDGING PROCESS	39
5		HO	W TC	EXPORT ID, SIG, & ENC CERTIFICATES	13
	5.	.1	Exp	ort ID, SIG & ENC Certificates from Your Personal Store	13
	5.	.2	Dele	etion of Certificates from Hard Drive	18
	5.	.3	To I	mport Certificates	18
	5.	.4	Sett	ing Up Access to the Carillon LDAP Proxy	52
	5.	.5	Con	firming LDAP is Properly Configured	55
6		HO	W TC	USE YOUR CERTIFICATES IN OUTLOOK	57
	6.	.1	Sett	ing up Outlook or Office 365 to use your Certificates	57
	6.	.2	Sigr	ning and Encrypting E-mail	52
7		NET	rwof	RK ADMINISTRATOR TROUBLESHOOTING	54
	7.	.1	Test	t link to the Carillon LDAP Proxy	54
8		CUS	STON	IER SERVICE	56





1 Introduction

This document serves as a guide to assist you through the various steps that need to be performed using the Carillon eShop Interface: from downloading the Carillon CA Certificate Chain (Trust Chain), retrieving and acknowledging your certificates, through to setting up Outlook in order to be able to use these certificates on your computer or laptop.

PLEASE NOTE:

The instructions in this handbook are typical guidelines of how to download and install CA certificates on your system. There may be some variance between what is presented here, and what your own system will display. Should you have any issues after you have completed these steps, please contact your System Administrator.

Please be aware that you may require Administrator rights to perform these actions. If you do not have Administrator rights on your workstation, seek assistance from your System Administrator to help with this setup.





2 HOW-TO: SET UP A CA CERTIFICATE CHAIN (TRUST CHAIN) IN WINDOWS 10

This section describes the steps for installing the Carillon Trust Chain and the Boeing Trust Chain on a Windows 10 computer or laptop. We refer to the Carillon CA and Boeing Trust Chains as our principle examples because these are the ones we use for Carillon CA issued certificates purchased from our Carillon eShop.

Installing the appropriate Trust Chain certificates on your computer or laptop ensures that your personal certificates will then be correctly installed, recognized and trusted by your applications, such as your web browser or email client.

You will need to first download the *Carillon Trust Chain* certificates. These trust chain certificates are required in order to validate the certificates that will be purchased from the Carillon Certificate eShop.

The Carillon Trust Chain is comprised of the following two certificates:

The https://pub.carillon.ca/CAcerts/CISRCA1.cer (Root Certificate); and

the Carillon PKI Services CA 1 <u>https://pub.carillon.ca/CAcerts/CISCA1.cer</u> (Intermediate or Signing Certificate).

These certificates can also be downloaded directly from the Carillon PKI public repository website: <u>https://pub.carillon.ca/</u> by clicking on the **DER** button for each certificate.

If you are using these certificates as part of the Boeing supply chain, you need to download the **Boeing Trust Chain** certificates. The Boeing Trust Chain certificates are required for secure email communication between Boeing and its partners.

The Boeing Trust Chain is comprised of the following two certificates:

The Boeing Root CA certificate (The Boeing Company Root Certificate Authority.crt); and

The Boeing Secure Messaging G2 certificate (Boeing Secure Messaging G2.crt)

These certificates can be downloaded individually from the Boeing PKI public repository website: http://www.boeing.com/crl/





2.1 Installing the Carillon CA Trust Chain

2.1.1 Download & Install the Carillon Root CA Certificate

The following link: <u>https://pub.carillon.ca/CAcerts/CISRCA1.cer</u> will bring you to your View Downloads – Internet Explorer window.

1. Under name **CISRCA1.cer** (Root CA) file; click on the **Open** button.

🛃 View Downloads - Internet Explorer 🦳 🗆							
View and track your	downloads	Sea	arch downloads			٩	
Name		Location	Actions				
CISRCA1.cer pub.carillon.ca	1.41 KB	Do you want to open or save this file?	Open	Sav	e 🔻		

2. The Certificate window will appear; click on the Install Certificate button.

📻 Certificate	×
General Details Certification Path	
Certificate Information	_
This certificate is intended for the following purpose(s):	_
 Proves your identity to a remote computer Protects e-mail messages 	^
 Ensures software came from software publisher Protects software from alteration after publication 	
Allows data to be signed with the current time Allows data on disk to be encrypted	~
	_
Issued to: CISRCA1	
Issued by: CISRCA1	
Valid from 10/16/2012 to 10/16/2032	
Install Certificate Issuer Statem	ient
	ОК





3. The following **Certificate Import Wizard** window will appear, click the **Next** button.



4. Select the **Place all certificates in the following store** option and then click the **Browse** button.

Certificate St	re		
Certifica	e stores are system areas where	certificates are kept.	
Window: the certi	can automatically select a certific icate.	ate store, or you can speci	fy a location for
OA	tomatically select the certificate s	tore based on the type of o	ertificate
Pl	ce all certificates in the following	store	
C	rtificate store:		
			Browse





5. Click on Trusted Root Certification Authorities and then click OK.

Select Certificate Store	×
Select the certificate store you want to use.	
Personal Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Intrusted Certificates	^
Show physical stores	
OK Cancel	

6. The following information will appear in the **Certificate Store** window, click on the **Next** button.

Certificate	Store				
Certific	cate stores are s	system areas whe	ere cer <mark>ti</mark> ficates a	re kept.	
Window the cer	ws can automati rtificate.	ically select a cert	ificate store, or	you can spec	fy a location for
0	Automatically se	elect the certificat	e store based o	n the type of	certificate
۲	Place all certifica	ates in the following	ng store		
	Certificate store	e: Certification Auth	orities		Browse
					browsern





7. The following window will appear, click on the **Finish** button.

Comple	ting the Cert	ificate Import V	Vizard	
The certifica	te will be imported a	fter you dick Finish.		
You have sp	ecified the following	settings:		
Certificate	Store Selected by L	Iser Trusted Root Certi	fication Authorities	
Content		Certificate		

Throughout the installation of the Trust Chain, you will get Security Warning pop-ups. This is normal as you are installing the certificates for the first time. It is okay to trust and install these certificates.

8. The **Certificate Import Wizard** pop-up will appear advising the Import was successful; click the **OK** button to complete the installation of the Carillon Root CA Certificate.

Certificate Import Wizard	×
The import was successful.	:
ОК	ו





9. Click **OK** to close the certificate windows, and click **Close** on the downloads window.

Certificate	×
General Details Certification Path	
Certificate Information	
This certificate is intended for the following purp	ose(s):
 Proves your identity to a remote computer Protects e-mail messages 	^
Ensures software came from software publisher Protects software from alteration after publication	
Allows data to be signed with the current time Allows data on disk to be encrypted	~
Issued to: CISRCA1	
Issued by: CISRCA1	
Valid from 10/16/2012 to 10/16/2032	
Install Certificate Issue	er Statement
	ОК

2.1.2 Download & Install Carillon Intermediate CA Certificate

The following link: <u>https://pub.carillon.ca/CAcerts/CISCA1.cer</u> will bring you to your View Downloads – Internet Explorer window.

1. Under name **CISCA1.cer** (Intermediate or Signing CA 1 certificate) file; click on the **Open** button.

丞 View Downloads - Internet Explorer					-		×
View and track your o	Search downloads				٩		
Name		Location		Actions			
CISCA1.cer pub.carillon.ca	2.48 KB	Do you want to open o save this file?	or	Open	Sav	e 🔻	×





2. The Certificate window will appear; click on the Install Certificate button.

😱 Certificate	×
General Details Certification Path	
Certificate Information	-
This certificate is intended for the following purpose(s):	_
Proves your identity to a remote computer Protects e-mail messages	
 Ensures software came from software publisher Protects software from alteration after publication Allows data to be signed with the current time Allows data on disk to be encrypted 	
* Refer to the certification authority's statement for details.	
Issued to: Carillon PKI Services CA 1	-
Issued by: CISRCA1	
Valid from 10/23/2014 to 10/23/2027	
Install Certificate Issuer Statemen	it
OK	:

3. The following Certificate Import Welcome Wizard window will appear, click the **Next** button.

🔶 🛿 🐉 Certificate Import Wizard	×
Welcome to the Certificate Import Wizard	
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
Store Location	
Current User	
O Local Machine	
To continue, click Next.	
Next Cancel	





4. Select **Place all certificates in the following store** option and then click the **Browse** button.

Certificate Store				
Certificate st	ores are system ar	reas where certif	îcates are kept.	
Windows can the certificat	automatically sele e.	ct a certificate s	tore, or you can spe	cify a location for
Autom	atically select the (certificate store b	pased on the type of	certificate
Place a	all certificates in the	e following store		
Control of the second s				
Cerun	cate store:			
				Browse

5. Click on Intermediate Certification Authorities and then click OK.

Select Certificate Store	×
Select the certificate store you want to use.	
, Personal ,	^
Intermediate Certification Authorities	
	×
Show physical stores	
OK Cancel	





6. The following information will appear in the window, click on the **Next** button.

Certificate Store	
Certificate stores are system areas where certificates are kep	ot.
Windows can automatically select a certificate store, or you c the certificate.	an specify a location for
O Automatically select the certificate store based on the	type of certificate
Place all certificates in the following store	
Certificate store:	
Intermediate Certification Authorities	Browse

7. The following window will appear, click on the Finish button.







8. The **Certificate Import Wizard** pop-up will appear advising the Import was successful; click the **OK** button to complete the installation of the Carillon Intermediate CA 1 Certificate.



NOTE:

Throughout the installation of the Trust Chain, you will get Security Warning pop-ups. This is normal as you are installing the certificates for the first time. It is okay to trust and install these certificates.

9. Click OK to close the certificate windows, and click Close on the download window.

Certificate	×
General Details Certification Path	
Certificate Information	_
This certificate is intended for the following purpose(s):	-
Proves your identity to a remote computer Protects e-mail messages	
 Ensures software came from software publisher Protects software from alteration after publication Allows data to be signed with the current time Allows data on disk to be encrypted 	
* Refer to the certification authority's statement for details.	
Issued to: Carillon PKI Services CA 1	
Issued by: CISRCA1	
Valid from 10/23/2014 to 10/23/2027	
Install Certificate Issuer Statement	
OK	





This completes the installation of the Carillon Trust Chain Certificates.

- 2.1.3 Validate the Root Certificate Thumbprint
- 1. Click on the **Start icon**:



2. Type in the Search programs and files box: certmgr.msc and press enter.

Ask me anything	
-----------------	--

3. The certmgr window will appear. Click **Trusted Root Certification Authorities**, and then click **Certificates.** On the right panel, locate and double-click the **CISRCA1** certificate.

🚟 certmgr - [Certificates - Current	User\Trusted Root Certification Au	thorities\Certificat — 🛛	\times
File Action View Help			
🗢 🄿 🙋 📅 📋 🧔 🛃	?		
 Certificates - Current User Personal 	Issued To	Issued By	^
 Trusted Root Certification Au Certificates Enterprise Trust Intermediate Certification Au Active Directory User Object Trusted Publishers Untrusted Certificates Third-Party Root Certification Trusted People Client Authentication Issuers Other People Local NonRemovable Certific MSIEHistoryJournal Certificate Enrollment Reques 	CISRCA1	CISRCA1	
> 📔 Smart Card Trusted Roots			~
< >	<		>





4. A Certificate window will open. Click the **Details** tab. In the Show: dropdown, select **<All>** in the field column, scroll down to Thumbprint. It should read:



a6 9e 03 36 c4 e5 90 23 ff 65 3c 71 f9 28 eb 73 f2 1c 00 f0.

5. Click **OK** to close the window.





2.2 Installing the Boeing Trust Chain

2.2.1 Download Boeing Certificates

1. Visit the Boeing website at the following address:

http://www.boeing.com/crl/

2. Under the column *Enterprise Production Authority Information* heading, download the **The Boeing Company Root Certificate Authority.crt** by **right-clicking** on the link, then in the drop-down menu select the **Save target as...** to save the file.

A ttp://www.boeing.com/crl/ P - C M The Boeing C	Company PKI P ×
Boeing Class 2 Windows Machines.crt	Apr 10 05:33:06 2019 GMT
Boeing Company OSCA.cer	Nov 23 22:51:06 2016 GMT
Boeing Company OSCA.crt	Nov 23 22:51:06 2016 GMT
Boeing Company OSCA G2.crt	Dec 31 23:59:59 2020 GMT
Boeing e-Enabled Products Issuing CA(1).crt	May 1 22:37:08 2019 GMT
Boeing e-Enabled Products Issuing CA.crt	May 1 22:37:08 2019 GMT
Boeing e-Enabled Products Issuing CA G2.crt	Nov 19 20:57:18 2025 GMT
Boeing e-Enabled Products Policy CA.crt	Aug 28 23:07:56 2028 GMT
Boeing e-Enabled Products Root CA.crt	Aug 20 23:26:48 2048 GMT
Boeing Network Devices CA.crt	Oct 11 11:14:22 2016 GMT
Boeing PCA G2.crt	Sep 21 17:58:13 2029 GMT
BoeingPCAG2.p7c	Apr 30 23:59:59 2017 GMT
Boeing PCA G3.crt	Nov 29 17:20:01 2030 GMT
BoeingPCAG3.p7c	Apr 30 23:59:59 2017 GMT
Boeing PREPROD SecureBadge Medium G2.cer	Feb 1 00:12:58 2022 GMT
Boeing PREPROD SecureBadge Medium G2.crt	Feb 1 00:12:58 2022 GMT
Boeing SecureBadge Basic G2.crt	Feb 28 23:00:46 2023 GMT
Boeing SecureBadge Medium G2.crt	Feb 3 19:28:47 2022 GMT
Boeing Secure Messaging G2.crt	May 30 01:43:26 2019 GMT
Boeing SUG Root.crt	Dec 4 21:36:59 2017 GMT
saml.boeing.com.cer	Mar 25 23:59:59 2018 GMT
saml-ciefrz.boeing.com.cer	Jul 3 23:59:59 2017 GMT
saml-cie-prod.boeing.com.cer	Nov 4 23:59:59 2017 GMT
saml-cite.boeing.com.cer	Jan 13 23:59:59 2018 GMT
Secure Messaging.crt	Jan 20 19:28:53 2015 GMT
The Boeing Company Class 2 Certificate Authority.crt	Jan 11 19:02:14 2014 GMT
The Boeing Company Class 2 Certificate Authority G2.crt	Nov 15 22:15:15 2017 GMT
The Boeing Company Root Certificate Authority.crt	Dec 15 00:16:20 2021 GMT

3. Select a directory on your computer to save the file to and click the **Save** button.





4. Repeat steps 2 and 3 for the downloading of **Boeing Secure Messaging G2.crt** and **Boeing Secure Messaging G2 Exp 2019.crt** then close your browser.

() Attp://www.boeing.com/crl/	, 으 ㅜ Ċ
🗴 📆 Convert 🔻 👼 Select	

The Boeing Company PKI Public Repository

Index Created: Tue Jul 11 07:26:39 2017	
Enterprise Policy Info	Document Date
Boeing_Med_Assurance_Domain_CP_v11.3.pdf	Mon Apr 3 13:03:45 2017
Boeing SecureBadge Medium G2 Certificate Templates.pdf	Thu Aug 25 08:27:05 2016
Boeing SecureBadge Medium G3 Certificate Templates.pdf	Thu Aug 25 08:26:10 2016
Enterprise Production Authority Information	Expires
Boeing Basic Assurance Hardware Root CA.crt	Sep 18 21:47:59 2038 GMT
Boeing Basic Assurance Software Issuing CA G3.crt	Jun 29 22:59:40 2026 GMT
Boeing Basic Assurance Software Root CA G2.crt	Apr 21 20:49:09 2036 GMT
Boeing Class 2 Windows Machines.crt	Apr 10 05:33:06 2019 GMT
Boeing Company OSCA.cer	Nov 23 22:51:06 2016 GMT
Boeing Company OSCA.crt	Nov 23 22:51:06 2016 GMT
Boeing Company OSCA G2.crt	Dec 31 23:59:59 2020 GMT
Boeing Company OSCA G3.crt	Jun 1 23:00:45 2026 GMT
Boeing e-Enabled Products Issuing CA(1).crt	May 1 22:37:08 2019 GMT
Boeing e-Enabled Products Issuing CA.crt	May 1 22:37:08 2019 GMT
Boeing e-Enabled Products Issuing CA G2.crt	Nov 19 20:57:18 2025 GMT
Boeing e-Enabled Products Policy CA.crt	Aug 28 23:07:56 2028 GMT
Boeing e-Enabled Products Root CA.crt	Aug 20 23:26:48 2048 GMT
Boeing Mobile Device Issuing CA G1.crt	Jun 29 23:01:08 2026 GMT
Boeing Network Devices CA.crt	Oct 11 11:14:22 2016 GMT
Boeing PCA G2.crt	Apr 30 23:59:59 2018 GMT
BoeingPCAG2.crt	Apr 30 23:59:59 2018 GMT
BoeingPCAG2.p7c	Apr 30 23:59:59 2018 GMT
Boeing PCA G3.crt	Apr 30 23:59:59 2018 GMT
BoeingPCAG3.crt	Apr 30 23:59:59 2018 GMT
BoeingPCAG3.p7c	Apr 30 23:59:59 2018 GMT
Boeing SecureBadge Basic G2.crt	Feb 28 23:00:46 2023 GMT
Boeing SecureBadge Medium G2.crt	Feb 3 19:28:47 2022 GMT
Boeing Secure Messaging G2.crt	Dec 15 00:16:20 2021 GMT
Boeing Secure Messaging G2 Exp 2019.crt	May 30 01:43:26 2019 GMT

You have now successfully downloaded the Boeing Trust Chain Certificates.

2.2.2 Install the Boeing Root CA Certificate

1. Go to the folder where the Boeing Certificates were downloaded. Double-click on **The Boeing Company Root Certificate Authority** certificate and the following window will appear, click on the **Open** button:







2. Click on the Install Certificate button.

8	Certificate	х
G	eneral Details Certification Path	
	Certificate Information	-
	This certificate is intended for the following purpose(s): • All issuance policies • All application policies	
	Issued to: The Boeing Company Root Certificate Authority	
	Issued by: The Boeing Company Root Certificate Authority	
	Valid from 3/17/2000 to 12/14/2021	
	Install Certificate Issuer Statement	
	OK	

3. The following Certificate Import Wizard window will appear, click on the Next button.







4. Select the Place all certificates in the following store option and the click the Browse button.

Cartificate Steer		
Certificate stores are s	stem areas where certificates	are kept.
Windows can automatic the certificate. Automatically sel Place all certifica Certificate store	ally select a certificate store, of ct the certificate store based es in the following store	or you can specify a location for on the type of certificate Browse

5. The following window will appear, click on Trusted Root Certification Authorities and then click OK.







6. The following information will appear in the window, click on the **Next** button.

Certificat	Store			
Cert	icate stores are system area	s where certificates a	e kept.	
Wind the o	ows can automatically select ertificate.	a certificate store, or	you can specify a	location for
C	Automatically select the cer	tificate store based or	the type of certif	ficate
0	Place all certificates in the fo	ollowing store		
	Certificate store:			
	Trusted Root Certification	Authorities	E	Browse

7. The following window will appear, click on the Finish button:







NOTE:

Throughout the installation of the Trust Chain, you will get Security Warning pop-ups. This is normal, as you are installing the certificates for the first time. It is okay to trust and install these certificates.

8. Click **OK** to complete the installation of the **Boeing Company Root Certificate Authority** certificate.



9. Click the **OK** button to close the Certificate window.

2.2.3 Install Boeing Intermediate CA Certificate

1. Go to the folder where the Boeing Certificates were downloaded. Double-click on the **Boeing Secure Messaging G2** certificate and the following window will appear, click on the **Open** button:

Open File	- Security Warning X			
Do you	want to open this file?			
	Name:\ Desktop\Boeing Secure Messaging G2.cer Type: Security Certificate From: C:\Users\ Desktop\Boeing Secure Messagi Open Cancel	1		
🗹 Alway	ys ask before opening this file			
۲	While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. <u>What's the risk?</u>	y		





2. Click on the Install Certificate button.

属 Certificate	×
General Details Certification Path	
Certificate Information	n r the following purpose(s):
• 1.3.0.1.4, 1.73, 13.3.1.2 • All application policies	
Issued to: Boeing Secure	Messaging G2
Issued by: The Boeing Co	mpany Root Certificate Authority
Valid from 5/29/2014 to	5/29/2019
Insta	Il Certificate Issuer Statement
	ОК

3. The following Certificate Import Wizard window will appear, click on the **Next** button.

Welcome to the Certific	ate Import Wiza	rd
This wizard helps you copy certificate lists from your disk to a certificate sto	s, certificate trust lists, ar re.	nd certificate revocation
A certificate, which is issued by a cert and contains information used to prot connections. A certificate store is the	ification authority, is a co ect data or to establish se system area where certif	nfirmation of your identity ecure network icates are kept.
Store Location		
Current User		
To continue, dick Next.		





4. Select on the Place all certificates in the following store and then click the Browse button.

Certificate St	re			
Certificat	e stores are system a	areas where certific	ates are kept.	
Windows the certif	can automatically selected.	ect a cer <mark>t</mark> ificate sto	ore, or you can speci	fy a location for
	tomatically select the	certificate store ba	ased on the type of o	certificate
Pla	ce all certificates in th	ne following store		
Ce	rtificate store:		1	
_				Browse

5. Click on Intermediate Certification Authorities and then click on the OK button.

Select Certificate Store	×
Select the certificate store you want to use.	
: Personal	•
	s
Enterprise Trust	
Trusted Publishers	
Certificates	~
<	<u>></u>
Show physical stores	
OK Car	ncel





6. The following information will appear in the window, click on the **Next** button.

Certificate St	ore				
Certifica	te stores are s	ystem areas whe	ere certificates	are kept.	
Window: the certi	s can automatic ificate. utomatically sel	cally select a cer lect the certificat	tificate store, o te store based o	r you can spec on the type of	ify a location for certificate
● Pl	ace all certifica	tes in the followi	ng store		
C	ertificate store	:			
	Intermediate C	Certification Auth	orities		Browse

7. The following window will appear, click on the **Finish** button:







NOTE:

Throughout the installation of the Trust Chain, you may have Security Warning popups. This is normal, as you are installing the certificates for the first time. It is okay to trust and install these certificates.

8. Click OK to complete the installation of the Boeing Secure Message G2 Certificate



9. Click the **OK** button to close the certificate window.

Certificate X
General Details Certification Path
Certificate Information
This certificate is intended for the following purpose(s): • 1.3.6.1.4.1.73.15.3.1.2 • All application policies
Issued to: Boeing Secure Messaging G2
Issued by: The Boeing Company Root Certificate Authority
Valid from 5/29/2014 to 5/29/2019
Install Certificate Issuer Statement
ОК

*** Repeat steps 1 through 9 to install the Boeing Secure Messaging G2 Exp 2019.crt ***





2.3 Verifying the Trusted Site and Validating the EVSSL

To verify if: <u>https://pub.carillon.ca/; https://www.carillon.ca</u> and <u>http://certstore.carillon.ca</u> are trusted sites on your computer:

- 1. On the web browser menu click on the **Tools** menu and select **Internet Options**. In the **Internet Options** window, select the **Security** tab.
- 2. Click on the Trusted Sites check mark then click on the Sites button.







3. If in the box of **Websites** you do not see the above addresses; you will have to click on the **Add** button and add them and then click **Close** button.

Trusted sites	×
You can add and remove websites from this zo this zone will use the zone's security settings.	ne. All websites in
Add this website to the zone:	
	Add
Websites:	
https://certstore.carillon.ca	Remove
https://pub.carillon.ca	
~ ~	
Require server verification (https:) for all sites in thi	s zone
	Close

4. On the Internet Options pop-up, click on the Advanced tab.

Internet (Options					?	\times
General	Security	Privacy	Content	Connections	Programs	Advand	ed
Setting	s ———						_
	Accelerate Use sc Accessibili Alway Enable Move Play s Reset Browsing Alway Close Disable	ed graphic oftware re ty s expand e Caret Br system ca ystem sou text size zoom leve s record c unused fo e script de	s ALT text fo owsing for aret with fo unds to medium el for new v leveloper c olders in His ebugging (I ebugging (I	tead of GPU re or images new windows a cus/selection of for new window vindows and ta onsole messag tory and Favo nternet Explor Other)	endering* and tabs hanges ws and tabs abs es rites* er)	~	
*Ta	kes effect a	after you	restart you	r computer	aduanced a	attinen	
Reset I	nternet Ev	plorer set	tings	Restore	advanced s	ettings	
Rese cond	ts Internet ition.	t Explorer	's settings t	to their default	Res	et	
You	should only	use this i	f your brov	vser is in an un	usable state	2.	
			Ok	Ca	ancel	Apply	/





5. In the **Settings** window, scroll down to **Security** and make sure **Use SSL 2.0** and **Use SSL 3.0** are unchecked, and ensure that all the **Use TLS** options are checked, and then click the **OK** button.

	You should only use this if your browser is in an unusable state.
1	
	Resets Internet Explorer's settings to their default Reset
ке	eset Internet Explorer settings
	Televent Fullere entities
	Restore advanced settings
	*Takes effect after you restart your computer
	< >>
	¥
	Warn if POST submittal is redirected to a zone that does n
	Warn if changing between secure and not secure mode
	Warn about certificate address mismatch*
	✓ Use TLS 1.2

6. In the address bar, type https://pub.carillon.ca/ and press Enter. There will be a lock icon as in the following screenshot. Click the lock and click the View certificates button.







7. Click the **Certification Path** tab, which shows pub.carillon.ca in the Certification path. The Certificate status should read: **This certificate is OK**.

🐖 Certificate	×
General Details Certification Path	
Certification path	
Entrust Root Certification Authority - G2	
View Certificate	
Certificate status:	_
This certificate is OK.	
OF	





3 CERTIFICATE RETRIEVAL PROCESS

1. You will receive a Certificate Issuance email (similar to the one below) with instructions, a link to pick up your certificates and an access code. If your email has not arrived after thirty minutes of its request; go to the following link, enter your email address, and click **Request New Access Code**.

https://pub.carillon.ca/certserv

Sample email:

🗣 Reply 🛱 Reply All 🗳 Forward
Thu 11/2/2017 7:59 AM
PKI No Reply <testing@carillon.ca></testing@carillon.ca>
Carillon SHA2 TEST PKI: Certificate Issuance
To Testuser Ninetynine
Signed By testing@carillon.ca
This message was sent with High importance.

Dear Testuser Ninetynine:

The request for a Carillon SHA2 TEST PKI digital certificate has been approved. To proceed with the retrieval of your certificate(s), please go to the following URL:

https://certserv.carillon.ca/certserv

To log on: If you already have a valid Identity certificate you will automatically be logged in, otherwise please enter your email address and the access code below:

yvfw89ymjB

If you encounter any difficulties, or have any questions, please do not hesitate to contact us at:

"PKI Help Desk" <<u>testing@carillon.ca</u>> Thank you,

The Carillon SHA2 TEST PKI Team

NOTE:

Certificate Retrieval is dependent on Java to work. For the best possible results downloading and acknowledging your certificates, it is highly recommended that Internet Explorer, with the latest version of Java, be setup as your default browser on your workstation.

Should your default browser be set to anything other than Internet Explorer, you may need to export the certificates from the other browser to complete the acknowledgement process, or the process will not work altogether.

Should you encounter any issues, please do not hesitate to contact Carillon Customer Service.





2. Click on the link mentioned in the email; it will bring you to the following **Certificate Services** page. Enter your email address and click on the **Submit** button.

Carillon	we build TRUST	
		Check browser setup
CERTIFICAT	E SERVICES	🕪 Download CA Certificate Chain
Thank you for registering then be securely transmit	for a certificate from the Carillon SHA2 TEST PKI. Log in here to generate a private key and certificate request which will tted to our Certificate Authority for signing.	
Please enter your email a	address and the access code that was emailed to you.	
lf you have lost your acce	ess code, enter only your email address and a new code will be emailed to you.	
Email Address:		
SUBMIT Please contact us if you h System Messa	have any questions about this service, or problems using issued certificates.	
Posted	Message	
2016-05-19	If you have any questions or concerns, please contact us at customer_service@carillon.ca or 1.844.PKI.PIVI (1.844.754.7484)	
Other OA	Uption 2.	

3. Enter the Access Code from the email and click on the Log In and Retrieve Certificates button:

	(I* Check browser setup
CERTIFICATE SERVICES	🕫 Download CA Certificate Chai
hank you for registering for a certificate from the Carillon SHA2 TEST PKI. Log in here to generate a private key and certificate request which will then be securely transmitted to our Certificate Authority for gring.	
lease enter your email address and the access code that was emailed to you.	
f you have lost your access code, enter only your email address and a new code will be emailed to you.	
Email Address:	
codel9@carilion.ca	
Please contact us if you have any questions about this service, or problems using issued certificates.	
HELLO TESTUSER NINETYNINE	
HELLO TESTUSER NINETYNINE	
HELLO TESTUSER NINETYNINE You are scheduled to retrieve certificates. Please enter the access code you received by email and press the button to continue. Access Code (from email):	



(((•



4. Click on the Pick up your certificates button.

WELCOME, TESTUSER NINETYNINE.

You've used a one-time password to access this page. In the future, access to this page will be supported by the Identity certificate that you will shortly be retrieving, issued by the Carillon SHA2 TEST PKI.

Your certificates:



Encryption Key Recovery

You have (or have had in the past) encryption certificates. In order to decrypt data, you may need to recover a certificate and private key if you no longer have them. Please click the 'Encryption Key Recovery' button to access this feature.

5. Click Yes:

Web Access Confirmation				
	This Web site is attempting to perform a digital certificate operation on your behalf:			
	https://certserv.carillon.ca/certserv/browsercheck.php			
You should only allow known Web sites to perform digital certificate operations on your behalf. Do you want to allow this operation?				
	Yes No			



- 🔎 Return to Main Page
- Check browser setup
- (Download CA Certificate Chain



6. Your browser will be checked, then click on the Continue button.

		CON
	we build TRUST	
CHECKING YOUR E	BROWSER SETUP	
Before you can retrieve your certificate	es, we need to ensure your web browser meets certain requirements and	
is correctly configured. If these tests d certificates at this time.	io not succeed, unfortunately you will not be able to retrieve your	
Test for valid browser:	PASSED	
Test for session cookies:	PASSED	
Test for persistent cookies:	PASSED	
Test for Java >= 1.6:	PASSED	
Test for Javascript:	PASSED	
Testing system time:	WARNING (Your system time is 27 seconds fast)	
Test for MS enrollment object:	PASSED (CertEnroll found)	
Overall result:	PASSED	
This concludes the browser compatibil	lity check. You may press "Go Back" to return to the main page.	
It appears that you have the correct Ja	iva version installed.	

7. Read and confirm the Terms of Service and place a check in the I hereby accept the terms of service box and then click **Continue**.



HELLO TESTUSER NINETYNINE.

we build

Terms of Service

By using this service, the Subscriber agrees that he has read and understood the applicable Subscriber Agreement and/or Certificate Policy, and that Certificates generated herein are to be used in accordance with those documents. Futhermore, the Subscriber, and/or the Subscriber's Employer, agrees to indemnify Carillon against any and all claims that may arise due to the Subscriber's use of this certificate.

Subscriber Agreement

Please confirm the Terms of Service:

I hereby accept the terms of service.



- (Return to Main Page
- (Check browser setup
- (Download CA Certificate Chain





8. Click Yes:



9. The following screen will appear, click on the Continue button.







11. You will have to Click Yes a few times:

Â	This Web site is attempting to perform a digital certificate operation on your behalf:
	https://certserv.carillon.ca/certserv/req-gen-ms.php
	You should only allow known Web sites to perform digital certificate operations on your behalf.
	Do you want to allow this operation?
	Ver
	Yes I INO

IMPORANT NOTE:

If you have been requested for Medium level certificates (Medium Software 256) you will need to remember and enter the retrieval code you submitted on your Digital Credential Request Form (DCR).

12. Your certificates have now been retrieved and installed. Before restarting your browser, you must first download the Encryption Certificate. Click on the DOWNLOAD CERTIFICATE button.



13. You will see a popup window at the bottom of your screen similar to the following; expand on the Save button and then click Save and Open:

Do you want to open or save	BrunoMars-ENC.p12 (3.70 KB) from certserv.carillon.ca?	Open	Save 🔻	Cancel	×





14. On the Certificate Import Wizard window, leaving the store location as Current, click next.

~	🐉 Certificate Import Wizard	×
	Welcome to the Certificate Import Wizard	
	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
	Store Location Ourrent User 	
	O Local Machine	
	To contrainde, click mext.	
	Next Cance	1

15. Click next on the following popup.







16. On the Private key protection popup window, enter the password (24 Alpha-Numeric password) in the Carillon PKI: Encryption Key Password email that you received.

	Private key protection
_	To maintain security, the private key was protected with a password.
	Type the password for the private key.
	Password:
	Display Password
	Import options:
	Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
	Mark this key as exportable. This will allow you to back up or transport your
	keys at a later time.
	✓ Indude all extended properties.

17. On the Certificate Store popup window click next, leaving the "Automatically select the certificate store based on the type of certificate" selected.

Certificat	e Store				
Certi	ficate stores are	e system areas v	where certificate	s are kept.	
Wind the c	ows can automa ertificate.	atically select a c	ertificate store,	or you can spec	ify a location for
C) Automatically :	select the certifi	cate store base	d on the type of	certificate
C) Place all certifi	icates in the follo	wing store		
	Certificate sto	ore:			
					Browse





Г

18. Click Finish on the Completing the Certificate Import Wizard popup.

÷ 🐙	Certificate Import Wizard	9	×
	Completing the	Certificate Import Wizard	
	The certificate will be impo	orted after you click Finish.	
	You have specified the fol	lowing settings:	
	Certificate Store Selecte	d Automatically determined by the wizard	
	Content	PFX	
	File Name	C:\Users\codell\Downloads\TestuserNinetynine-ENC (4).p12	
	<	>	
		Finish Cance	el

19. Click OK on the Certificate Import Wizard: The import was successful popup.







4 THE ACKNOWLEDGING PROCESS

You will receive two emails: a **Certificate Acknowledgement Instructions** email and an **Encryption Acknowledgement Code** email.

1. **OPEN** the **Certificate Acknowledgement Instructions** email (similar to the following) to acknowledge your certificates; then click on the link which will bring you to a **Windows Security** page.

🗣 Reply	🛱 Reply All 🔤 Forward
	Thu 11/2/2017 8:46 AM
	PKI No Reply <testing@carillon.ca></testing@carillon.ca>
	Carillon SHA2 TEST PKI: Certificate Acknowledgement Instructions
To Cindy (Ddell
Signed By	testing@carillon.ca
1 This m	essage was sent with High importance.

Dear Testuser Ninetynine:

Thank you for retrieving your certificates from the Carillon SHA2 TEST PKI.

In order to keep and use your certificates, it is now necessary to validate that they are working properly; therefore, you must acknowledge them within 1 month of receipt.

To acknowledge your certificates, ensure that you have CLOSED all your Internet browser windows and then go to this URL:

https://certserv.carillon.ca/certserv/acknowledge/

IMPORTANT NOTE: If you have requested and retrieved an Encryption certificate, you will have received a second, encrypted email. This encrypted email contains a code which is needed to complete the acknolwedgement for your encryption certificate.

To be able to read the encrypted email, you will need to double-click on it, so that it is opened in a separate window. It is NOT possible to read an encrypted email in the Outlook preview window.

If you encounter any difficulties, or have any questions, please do not hesitate to contact us at:

"PKI Help Desk" <<u>testing@carillon.ca</u>> Thank you,

The Carillon SHA2 TEST PKI Team





2. Select your ID certificate with the Issuer: CIS and then click **OK**.

Windows Security					
Select a Certificate					
Site certserv.carillon.ca needs your credentials:					
[e ≡]	Testuser Ninetynine	- ID			
لتتتتبا	Issuer: TEST CIS Sign	ning CA1			
Valid From: 11/2/2017 to 11/1/2020					
	Click here to view certificate properties				
More choices					
OK Cancel					

3. The following window will appear. Click on the I acknowledge button to acknowledge your Signature Certificate.

Carillon * we build	
	🕪 Return to Main Page
ACKNOWLEDGEMENT	(* Test My Certificate
Identity Certificate Acknowledgement	(* Check browser setup
	(* Download CA Certificate Chain
You have successfully generated your certificates, and used your identity certificate to view this page. I herefore, your identity certificate is now acknowledged.	
Signature Certificate Acknowledgement	
By clicking below, you will be using your Signature certificate to sign your acknowledgement of receipt of your Signature certificate.	
ACKNOWLEDGE SIGNATURE CERTIFICATE	
Encryption Certificate Acknowledgement	
You have been sent an encrypted email with an acknowledgement code in it. Please type this code below, and click "I acknowledge".	
You can also request another copy of the encrypted code by clicking "Send email again".	
Acknowledgement Code:	
I ACKNOWLEDGE SEND EMAIL AGAIN	





4. Enter your **Acknowledgement Code** from your Encryption Acknowledgement Code email and click on the **I acknowledge** button.







5. Your certificates have now been acknowledged.



ACKNOWLEDGEMENT

Identity Certificate Acknowledgement

You have successfully generated your certificates, and used your Identity certificate to view this page. Therefore, your Identity certificate is now acknowledged.

Signature Certificate Acknowledgement

Your Signature certificate has been acknowledged.

Encryption Certificate Acknowledgement

Your Encryption certificate has been acknowledged.

6. Click on the **Return to main Page** option from the menu bar; you will now see serial numbers beside your issued certificates.



Encryption Key Recovery

You have (or have had in the past) encryption certificates. In order to decrypt data, you may need to recover a certificate and private key if you no longer have them. Please click the 'Encryption Key Recovery' button to access this feature.

ENCRYPTION KEY RECOVERY



(Return to Main Page

(** Test My Certificate (** Check browser setup

(Download CA Certificate Chain



5 HOW TO EXPORT ID, SIG, & ENC CERTIFICATES

5.1 Export ID, SIG & ENC Certificates from Your Personal Store

1. Click on the Start icon:



- 2. Type in the search box: certmgr.msc and press enter; the certmgr Certificates screen will appear.
- 3. Under: Personal > Certificates highlight the three certificates you want to export; right click on them, then click on **All Tasks** and click on **Export**.







4. The Certificate Export Wizard will appear; click **Next**.



5. On the Export Private Key screen; click on Yes, export the private key. Click Next.

Export Priv You ca	ate Key n choose to export the private key with the certificate.
Private certific	keys are password protected. If you want to export the private key with the ate, you must type a password on a later page.
Do you	want to export the private key with the certificate?
۲) Yes, export the private key
C) No, do not export the private key





6. The Export File Format screen will appear; ensure that the Personal Information Exchange – PKCS #12(.PFX) button is highlighted; click Next.

÷	🛃 Certificate Export Wizard	×
	Export File Format Certificates can be exported in a variety of file formats.	
	Select the format you want to use:	
	O DER encoded binary X.509 (.CER)	
	Base-64 encoded X.509 (.CER)	
	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
	Include all certificates in the certification path if possible	
	Personal Information Exchange - PKCS #12 (.PFX)	
	Include all certificates in the certification path if possible	
	Delete the private key if the export is successful	
	Export all extended properties	
	Enable certificate privacy	
	O Microsoft Serialized Certificate Store (.SST)	
	Next Cancel	

7. On the **Password** Screen; create a password and retype it; then click **Next**.

Security	
using a password.	must protect the private key to a security principal or by
Group or user names ((recommended)
	Add
	Remove
	TOLLING THE
Password:	
Confirm paceword	
••••••	
and the second second	





8. The File to Export screen will appear showing the file name to export; click Browse.

-	Certificate Export Wizard	
F	ile to Export	
	Specify the name of the file you want to export	
<u></u>		
	File name:	
	Browse	e
		200000
	Next	Cancel

9. The **Save As** window will appear; name the file and then save it to wherever you want i.e.: desktop and then click **Save**.

🚰 Save As				×
$\leftarrow \rightarrow \checkmark \uparrow$ I > This PC > Desktop	ت ~	Search Desktop		9
Organize 🔻 New folder				?
This PC Name	Da	ate modified	Туре	^
Desktop misc	10	/11/2016 11:02	File folder	
Documents				
🖊 Downloads				
👌 Music				
E Pictures				
👩 ScanSnap Fold				
Videos				
🏪 Local Disk (C:)				
DVD RW Drive				~
HP_RECOVERY V <				>
File name: test certs for export				~
Save as type: Personal Information Exchange (*.pfx)				\sim
∧ Hide Folders		Save	Cancel	





10. Click on the Next button.

	-	×
÷	🛃 Certificate Export Wizard	
	File to Export Specify the name of the file you want to export	
	File name:	
	C:\Users\Desktop\test certs for export.pfx Browse	
	Next Cance	I

11. The Certificate Export Wizard window will appear; click Finish.

Completing the Certificate Export Wizard
You have successfully completed the Certificate Export wizard.
You have specified the following settings:
File Name C:\Users\Desktop\test certs for export.pfx File Format Personal Information Exchange (*.pfx)





12. On the Certificate Export Wizard pop-up advising the export was successful; click OK.



5.2 Deletion of Certificates from Hard Drive

Any files containing your private key should be kept on removable media only. When first exporting your certificates, copy them to a local drive that is not accessible to a network. Import your certificates into applications as necessary, *then remove them and any related files from your machine after you're done!*

It is important to remember that all certificates exported from *your web browser* onto your computer be <u>DELETED</u>. Failure to do so will put the security of your certificates and keys at risk.

Also ensure that once the certificates have been deleted that your recycling bin (or trash) has been emptied.

5.3 To Import Certificates

1. Double click on certificate file you saved and the Certificate Import Wizard screen will appear; click Next.







Welcome to the	Certificate Im	port Wizard	
This wizard helps you cop lists from your disk to a ce	y certificates, certifica ertificate store.	te trust lists, and certificate rev	ocation
A certificate, which is issu and contains information connections. A certificate	ed by a certification au used to protect data o store is the system ar	thority, is a confirmation of yo to establish secure network a where certificates are kept.	ur <mark>ide</mark> ntity
Store Location			
Current User			
O Local Machine			
To continue, dick Next.			

2. On the Certificate Import Wizard; File to Import screen; click Next.

File to Import			
Specify the file you wa	ant to import.		
File name:			
C: \Users \Desktop \tes	st certs for export.pfx		Browse
Note: More than one of	certificate can be stored in a single	e file in the foll	owing formats
Personal Informatio	on Exchange- PKCS #12 (.PFX,.P1	2)	
Cryptographic Mess	sage Syntax Standard- PKCS #7 C	ertificates (.P.	/B)
MICrosoft Serialized	Certificate Store (.SST)		





3. On the **Certificate Import Wizard, Password** screen; enter the **Password** you created during export. Make sure that you check off all three boxes; especially **"Mark this key as exportable"**. This will allow you to back up or transport your keys at a later time. Click **Next**.

Private key protection
To maintain security, the private key was protected with a password.
Type the password for the private key.
Password:
••••••
Display Password
Import options:
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
Include all extended properties.

4. On the Certificate Import Wizard, Certificate Store window; click on Automatically select a certificate store based on the type of certificate; and click Next.

Carlifford	fh-r	
Certificate	store icate stores are system areas where certificates are kept.	
Wind the c	ows can automatically select a certificate store, or you can specify a locatic rtificate.	on for
۲	Automatically select the certificate store based on the type of certificate	
C	Place all certificates in the following store	
	Certificate store:	
	Browse	e





5. The Completing the Certificate Import Wizard window will appear; click Finish.



6. On the Importing a new private exchange key pop-up(s); click OK.

Importing a r	new private exchange key	Х
	An application is creating a Protected item.	
	CryptoAPI Private Key	
	Security level set to Medium Set Security Level	
	OK Cancel Details	





7. Click **OK** on the Import was successful pop-up.



5.4 Setting Up Access to the Carillon LDAP Proxy

The *Carillon LDAP Proxy* is a link to a directory of recipient encryption certificates containing public encryption keys, which can then be used to encrypt email intended for the person associated with the retrieved certificates. This is done in order to avoid having to manually enter each person's certificates so that you may send/receive encrypted e-mail with them.

1. From you Microsoft Outlook page, select the **File** tab and then **Info** tab from the corresponding menu items. Click on the **Account Settings** button, and select the **Account Settings**... pop-up.

E	Inbox - customer_service@carillon.ca - Outlook	?	-	٥	×
Info	Account Information				
Open & Export Save As	customer_service@carillon.ca MAP/SMTP				
Save Attachments	Add Account Account Settings				
Office Account	Change settings for this account or set up more connections. Account Settings -				
Options	Mailbox Settings Manage the size of your mailbox by emptying Deleted Items and archiving. Tools				
Exit	Rules and Alerts				
	Manage Rules & Allerts & Allerts				





2. In the Accounts Settings window, select the **Address Books** tab and click on the **New...** button.

count Settings				×
Directories and Address Books You can choose a directory or address book l	below to change or re	move it.		
E-mail Data Files RSS Feeds SharePoint Lists	Internet Calendars	Published Calendars	Address Books	
🛍 New 🚰 Change 🗙 Remove				
Name	Туре			^
Mobile Address Book	MAPI			
				~
			(lose

3. Make sure the Internet Directory Service (LDAP) option is selected and click the Next button.

Add New Account		×
Directory or Address Book Type You can choose the type of directory or address book you'd like to add.		×
Internet Directory Service (LDAP)		
Connect to an LDAP server to find and verify e-mail addresses and ot information.	her	
Additional Address Books		
Connect to an address book to find and verify e-mail addresses and o information.	ther	
	< Pade Next >	Cancel
	< Daux Next >	Cancel

4. Fill out the Server Name information only. The Carillon LDAP Proxy directory is dir.carillon.ca.





5. Click on the More Settings button.

Directory Servic You can enter	e (LDAP) Settings the required settings to	i	You must restart Outlook for these changes to take effect.
Server Informati Type the name of th has given you.	on ne directory server your	I	ОК
Server Name:	dir.carillon.ca		
Logon Informatio	on		
This server requi	res me to log on		
User Name:			
Password;			
Require Secu	ire Password Authentica	tion (SPA)	More Settings

6. In the Microsoft LDAP Directory window ensure that dir.carillon.ca is the Display Name and that the Connection Details Port is set to **389**; then click **OK** or **Apply** as necessary.

Connection	Search		^
Display Na The dis dir.c	me play name as it arillon.ca	appears in the Add	dress Book
Connectio	n Details		
Port:		389	
Use S Sock	ecure ets Layer		
	ОК	Cancel	Apply





7. Click the **Finish** button.

Add New Account		Х
Add New Account	Congratulations! You have successfully entered all the information required to setup your account. To close the wizard, click Finish. Add another account	
	< Back Finish	

- 8. Click the Close Button.
- 9. You will need to **RESTART** Microsoft Outlook for the email account changes to take effect.

You have now completed setting up the Carillon LDAP Proxy

5.5 Confirming LDAP is Properly Configured

To confirm that the changes have been applied, open Outlook and select the **File** tab and **Info** tab from the corresponding menu items.

1. Click on the Account Settings button and select the Account Settings... pop-up. In the Accounts Settings window, select the Address Books tab.

©	Inbox - curtomer_service@carillon.ca - Outlook	?	-	٥	×
info	Account Information				
Open & Export Save As	cuttomer, service@carition.ca MA0/SMTP				
Save Attachments	Add Account				
Print	Account Account Settings				
Office Account Options	Mailbox Settings				
Feedback	Tools Wanage the size of your mailbox by emptying Deleted Items and archiving. *				
Exit	Rules and Alerts Use Rules and Alerts to help organize your incoming e-mail messages, and receive updates when items are added, changed, or removed.				





2. Your directory should appear in the list on this page. Double click on dir.carillon.ca

	eds SharePoint Lists	Internet Calendars	Published Calendars	Address Books	
🛿 New 🚰 Change	. 🗙 Remove				
lame		Туре			1
1obile Address Book		MAPI			
Outlook Address Book		MAPI			
lir.carillon.ca		LDAP			
ub.carillon.ca		LDAP			
					*

- 3. Click on More Settings
- 4. Verify that dir.carillon.ca is the Display Name and that the Port is 389, click OK.

Server Information Type the name of ti administrator has g Server Name: Logon Information This server requ User Name: Password: Require Sect	ne directory server your Internet service jiven you. dir.carillon.ca ires me to log on	provider or system	Microsoft LDAP Directory Connection Search Display Name The display name as dir.carillon.ca Connection Details Port:	it appears in the Address Boo
		More Settings	Sockets Layer OK <back next=""></back>	Cancel App Cancel n Auth

5. Click the **Close** button to close the window.

You have now verified that you have access to the Carillon LDAP Proxy.



6 HOW TO USE YOUR CERTIFICATES IN OUTLOOK

This section gives step by step instructions on how to set up and use Secure Email (S/MIME) with your email client and how to properly import the certificates into the *Microsoft Office Outlook 2010* or higher and on Microsoft Office 365 email management tool. These instructions will guide you on how to set up your email account to use these certificates, as well as set up your email client to use the *Carillon LDAP Proxy* so that you can look up and find other users with whom you may wish to exchange secure email.

To ensure these certificates are properly recognized and trusted by your email client, be sure to install the associated Trust Chain certificates on your computer or laptop before proceeding.

NOTE:

Third party certificates aren't supported for OWA S/MIME; only Microsoft Windows Certificate Authority issued certificates are supported.

6.1 Setting up Outlook or Office 365 to use your Certificates

- 1. Start the email application.
- 2. Select the File tab and then select Options. You will see a screen similar to this one.

¢		
Info	Accou	nt Information
Open & Export	Ē	
Save As	IMAP/SM	TP
	🛉 Add Account	
		ni Na seconda de latitudo de constante totas
Print	Account Settings *	Account and Social Network Settings Change settings for this account or set up more connections. Connect to social networks.
Office Account		
Options Exit	Cleanup Tools *	Mailbox Cleanup Manage the size of your mailbox by emptying Deleted Items and archiving.
		111 Tensor 10 10 10 10 10 10
	\$	Rules and Alerts
	Manage Rules & Alerts	Use Rules and Alerts to help organize your incoming e-mail messages, and receive updates when items are added, changed, or removed.
		Slow and Disabled Add-ins
	Manage Add- Ins	Manage add-ins that are affecting your Outlook experience.







3. Select the **Trust Center tab** from the side menu, and then select the **Trust Center Settings...** button. Similarly in Office 365, select the Trust Center tab from the side menu; you will not have a Trust Center Settings button.

Outlook Options		?	×
General	Help keep your documents safe and your computer secure and healthy.		
Mail	▼ 1 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2		
Calendar	Protecting your privacy		
Contacts	Microsoft cares about your privacy. For more information about how Microsoft Outlook helps to prot please see the privacy statements.	tect your privac	у,
Tasks	Show the Microsoft Outlook privacy statement		
Notes and Journal	Office.com privacy statement		
Search	Customer Experience Improvement Program		
Mobile	Security & more		
Language	Learn more about protecting your privacy and security from Office.com.		
Advanced	Microsoft Trustworthy Computing		
Customize Ribbon	Microsoft Outlook Trust Center		
Quick Access Toolbar	The Trust Center contains security and privacy settings. These settings help keep your computer secure. We recommend that you do not change these settings.	ist Center Setti	ngs
Add-Ins			
Trust Center			
		OK (ancel
		-	_





4. In the Trust Center window, under the E-mail Security tab, click the Settings button.



5. In the Change Security Settings window, under Security Settings Name, enter a name for your security setting (this would be a name you designate to your certificates). Under the Certificates and Algorithms section, setup your Signing certificate by clicking on **Choose**.

Change Security Settings			23				
Security Setting Preferences Security Settings Name:							
My S/MIME Settings	My S/MIME Settings						
Cryptography Format: S/MIME							
Default Security Setting	ng for this cryptogr	aphic message for	mat				
Default Security Setting	ng for all cryptogra	phic messages					
Security Labels	Security Labels New Delete Password						
Certificates and Algorithm	ns						
Signing Certificate:			Choose				
Hash Algorithm:		•					
Encryption Certificate:			Choose				
Encryption Algorithm:		•					
Send these certificate	Send these certificates with signed messages						
		ОК	Cancel				





6. On the Windows Security window, select the signature certificate you wish to use (if you have more than one) and click the **OK** button.



7. For the Hash Algorithm, select SHA1.

ecurity Setting Preference	5		
Security Settings Name:			
My S/MIME Settings			
Cryptography Format:	S/MIME		2
Default Security Set	ing for this cryptograp	hic message fo	ormat
Default Security Set	ing for all cryptographi	c messages	
Security Labels	New	Delete	Password.
Certificates and Algorith	ms		
Signing Certificate:	Testuser Nineteer	n - SIG	Choose
Hash Algorithm:	SHA1	•]
Encryption Certificate:	-		Choose
e	AES (256-bit)	-]
Encryption Algorithm:			

8. Setup your Encryption Certificate by clicking on Choose.





9. On the Windows Security window, select the encryption certificate you wish to use (if you have more than one) and click the **OK** button.

Windows Security		_	23
Select a Cert	ificate		
	Test User Nineteen - ENC Issuer: TEST CIS Signing CA1 Valid From: 24/06/2016 to 24/06/2019		
	ОК	Can	icel

10. For the Hash Algorithm, select AES (256-bit).

Security Setting Preference Security Settings Name:	15	
My S/MIME Settings		0
Cryptography Format:	S/MIME	
Default Security Set	ting for all cryptographic messages	Password
Certificates and Algorith Signing Certificate:	ms Testuser Nineteen - SIG	Choose
Hash Algorithm:	SHA1 •	
Encryption Certificate:	Testuser Nineteen - ENC	Choose
Encryption Algorithm:	AES (256-bit) 🔹	
Send these certificat	tes with signed messages	

11. Click the **OK** button to complete your Personal Certificate setup.

You have now finished setting up your Personal Certificates for use in Outlook.





6.2 Signing and Encrypting E-mail

The reasons for digitally signing and encrypting a document are simple:

- It ensures that the document was actually sent by YOU.
- It ensures that the document wasn't modified in route.

Additionally, the reason for encrypting an email is that it ensures that no one else can read your message. To proceed:

1. Open Outlook, and select New E-mail on the htab.



2. Click on the To....

	From -	customer_service@carillon.ca
Send	То	
	Cc	
	Subject:	

3. The Select Names: Contact window should pop up and from the Address Book drop down, select: dir.carillon.ca. Type in the email address in the space to the left of the GO button; then select GO.







- 4. The name of the person should show up in the space below with ENC beside it. Select their name, then click on the **TO**, then **OK**.
- 5. Fill out your email, then open the **Options** tab and ensure that the **Encrypt** and **Sign** buttons on the Permission menu are selected.
- 6. Click Send to send the digitally signed and encrypted email.

File Message Inset Options Format Text Review Developer Adobe PDF Image: Colors of the color of the c	😰 🛃	19 (24 + 14)	-	Untitled -	Message ((Plain Text)			_		×
Colors Permission Defects Color Permission P	File	Message	Insert Optic	ons Format Text F	Review	Developer	Adobe PDF				۵ 🕜
Themes Page Bcc Permission Show Fields Permission Permission Tracking Tomes Customer_service@carillon.ca	Aa	A Fonts -		Encrypt		Request	a Delivery Receipt		Þ	8	
Themes Show Fields Permission Tracking More Options Image: Contract of the contrac	Themes	Effects T Cold	ge Bcc or∵	Permission 🚘 Sign	Use Voti Buttons	ng 🔲 Request	a Read Receipt	Save Sent Item To 🔻	Delay Delivery	Direct Replies	То
From • customer_service@carillon.ca To		Themes	Show Fields	Permission		Tracking	Es.	Mor	e Option	5	5
To Image: Construction of the second		From - customer_service@carillon.ca									
Cc Subject:	Send	То									
Subject:		Сс									
		Subject:									
	<u>X</u> ·		1	2	3 1		. 4	. 5			
		1									
											_
											=
											-

Delivered messages display the signing icon, encryption icon, or both, depending on the options you selected.

You have now successfully sent a signed and encrypted email.

NOTE:

If you are using Windows 7, recipients of your emails may not be able to read your encrypted messages if they are using an older email client. To fix this problem, follow the steps below:

- 1. From the File menu, select **Options**, then click the **Trust Center** tab, **Trust Center** button.
- 2. Under the Encrypted email header, click the Setting button. Under the Certificates and Algorithms section, from the Encryption Algorithm drop-down menu, select 3DES.
- 3. Click **OK**, and then click **OK** again.





7 NETWORK ADMINISTRATOR TROUBLESHOOTING

This section is to assist **Network Administrators** in diagnosing certain common problems that may occur after setting up the certificates on your system. References are made to tools that the Network Administrator will have at their disposal in order to perform these tasks.

7.1 Test link to the Carillon LDAP Proxy

To test your configuration to the *Carillon LDAP Proxy*, click the Start Menu button *Search programs and files* field type *cmd* and press the [Enter] key to open the Windows Command Prompt.



2. The following window will appear; type the command: ping dir.carillon.ca



3. If you were successful in connecting to the directory, you should have 0% lost packets, receiving the following output:

C:\Windows\system32\cmd.exe	_ D X
C:\Users\John Smith> ping dir.carillon.ca	
Pinging dir.carillon.ca [207.115.107.27] with 32 bytes of data: Reply from 207.115.107.27: bytes=32 time=64ms TTL=242 Reply from 207.115.107.27: bytes=32 time=63ms TTL=242 Reply from 207.115.107.27: bytes=32 time=63ms TTL=242 Reply from 207.115.107.27: bytes=32 time=63ms TTL=242	11
Ping statistics for 207.115.107.27: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 63ms, Maximum = 64ms, Average = 63ms	
C:\Users\John Smith>	▼

4. If no connection was established (100% packet loss), try again.



-



- 5. Telnet to port 389 if you get a connected message, the firewall from your organization will let the traffic through. If you get a connection denied message, please open your company firewall to allow traffic on TCP 389 to dir.carillon.ca.
- 6. To ensure that you can, in fact, lookup certificates, open the shell and make sure you are in the directory with *OpenLDAP* (or equivalent tool) in order to do an "Idapsearch".
- 7. Then type this command:

ldapsearch -xh dir.carillon.ca mail=captainbob@carillon.ca

Where captainbob@carillon.ca is the email address of the certificates you are looking for. If the search was successful, you should see a user Certificate entry returned (a giant block of text (certificate) should be displayed.) This means the email is correct. If you're still unable to send the person email, it is likely due to their certificate being expired or revoked.



If the search was not successful, the following output will be returned.



This means that this email address is not in the certificate directory. Contact the owner of the email address and make sure the email address you typed in is correct. If the email address is spelled correctly, the owner does not hold a certificate and should not be communicated with.

NOTE:

You CANNOT use a directory browser to verify connectivity. The directory is configured to answer specific queries for user Certificate entries by people knowing email addresses, and to not allow for browsing. This is to ensure confidentiality.





8 CUSTOMER SERVICE

Should you require assistance at any time, please feel free to contact us and we will be happy to assist you:

Carillon Information Security Inc., Customer Service Group 8:00AM-8:00PM Eastern Telephone: 1-514-485-0789 Email: customer_service@carillon.ca

