Digital Certificate **Renewal** (Windows Vista and Windows 7)

STEP 1 (must be done before *renewing* the certificate)

Run IE as Administrator

Right-click on the Internet Explorer (IE) icon *Run as administrator*. The way to do so differs slightly between Vista and Windows 7.

Frequent

VISTA

Open Open file location Can iexplore.exe for Viruses Pin to Start Menu Add to Quick Launch Restore previous versions Send To Cut Copy Create Shortcut Delete Rename Properties

WINDOWS 7

Tasks		Open	
🐁 Start InPrivat	19	Run as administrator	
📑 Open new ta		Unpin from Taskbar	ig.
		Properties	
Dinternet Explo	orer		_

Choose **Allow** when prompted.

ser Account Control	2
I An unidentified program wants access to your co	mputer
Don't run the program unless you know where it's from or you'v iexplore.exe Unidentified Publisher Cancel I don't inow where this program is from or what it's for.	e used it before.
Allow I trust this program. I know where it's from or I've used it	t before.
Details	
	ana againa

You may get this popup window if you aren't a local administrator.

Contact your Administrator if you get this prompt. They will need to provide you with temporary administrative privileges in order to proceed.

9	chang	es to this comp	uter?
	e	Program name: Verified publisher: File origin:	Microsoft Windows Microsoft Corporation Hard drive on this computer
lo co	ontinue,	type an administrato	or password, and then click Yes.
1		User name	
		Password	
1.4		Demains	

💁 • 🔂 · 👘 • 🖓 Page • 🎯 Tools •

.

٠

.

٠

F11

Delete Browsing History...

Pop-up Blocker

Phishing Filter

Work Offline Windows Update Full Screen

Menu Bar Toolbars

Manage Add-ons

Internet Options

Once Internet Explorer opens up, in the toolbar at the top of the browser, select *Tools* and then *Internet Options* from the drop down list.





The **Trusted Sites** window is now displayed with the Verisign website entered into the first field. If it is not pre-filled, type in https://onsite.verisign.com.

When finished, click the *Add* button.

Click *Close* after you've added https://onsite.verisign.com as a trusted link.

this zone will use the zone's security	ity settings.
Add this website to the zone:	- 12
https://onsite.verisign.com	Add
<u>M</u> ebsites:	
	Bemove
	and an
Require server verification (https:) for	all sites in this zone

Now it is time to install the Root. Go to the following website:

https://onsite.verisign.com/services/ MIBITSecurityPKI/digitalidCenter.htm

Click INSTALL CA.

Click **Open** when prompted.



A new window will open.

Click Install Certificate.

Certif	kate Information
Ad incus Ad incus Ad apple	te is interded for the following purpose(s): not policies cation policies
Issued t	er MB Grup, Inc Root CA
Issued I	nya MSB Group, Six Root CA
Valid fro	uu 9/28/2003 to 9/28/2013
	[potal Certificate] Since Statement

The Import Wizard will pop up.

Click Next.



Make sure *Place all certificates in the following store* is highlighted.

Click Next.

ertificate Import Wizard	
Certificate Store Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a locati	on for
O Automatically select the certificate store based on the type of certificate	
e Bace all certificates in the following store	
Certificate store:	
Bgows	e
< gaox	Cance

Then, click the *Browse* button and choose *Trusted Root Certification Authorities*. Then, click *OK*.



The *Completing the Certificate Import Wizard* screen will appear.

Click the *Finish* button.

You have completed the Installation of the Root Certificate Authority (CA).



Click Yes to accept the Security Warning.

You have completed the Installation of the Root Certificate Authority (CA).



STEP 2

Access the Verisign Enrollment site to renew your Digital ID:

https://onsite.verisign.com/services/ MIBITSecurityPKI/client/userRenewal.htm

***Note: The URL is case sensitive; you must
key it in exactly as it is shown.***

Select the link for Microsoft Internet Explorer.



Click Renew.



STEP 4

This screen appears. Be sure that any other open applications are minimized as the pop up window may be hidden behind them.

Click **Renew**.

Sele	ct Digital ID	
Pleas	e select digital ID	
1		
	VALID DATES	
	5/13/2003 - 5/31/2010	

STEP 5

This screen appears to allow you to set the security level.

Click Set Security Level.

Creating a	new RSA signature key	×
	An application is creating a Protected item.	
	CryptoAPI Private Key	
	Security level set to Medium	
	OK Cancel Details	-

This screen appears to choose the security level.

Select High.

Click Next.

Creating a new RS	A signature key	×
	Choose a security level appropriate for this item.	
	Cancel	

STEP 7

Now you will create a password for this certificate.

A password can consist of any alphanumeric values, however, it is case sensitive.

A password for Vista or Windows 7 must be at least 8 characters

Note: Depending on your permission level, the area beside Password for: may be grayed out. If it is blank, key in your first initial and your last name.

Re-key your password for confirmation.

The password you create is confidential; do not share it with anyone, and please remember it as you will need it to renew your Digital ID.

Click Finish.

STEP 8

This screen appears. Confirm that the security level is set to High.

Click OK.



Create a password to protect this item.
Create a new password for this item. Password for: CryptoAPI Pervate Key
Password J Contem

This *Congratulations* web page appears indicting that your Digital ID has been successfully renewed.

The next step is to remove the old certificate.



STEP 10

In the toolbar at the top of the browser, select *Tools* and then *Internet Options* from the drop down list.

This screen will appear.

Click on the *Content* tab.

Seneral	Canadan	Dimen	Cantant	Connetions	Deserves	Adverser
renicial	security	Privacy	Content	Connections	Programs	Advanced
Home	page					
	Varias	n ebanan	inhish and	an ha cura for um	a kome nas	
	Touca	in change	which pag	je to use tor yo	ur nome pag	le.
	Addres	16 N	p://intran	et/		
		Use <u>C</u>	unent	Use Default	Use	lank
Temp	orary Inten	net files				
2	Pages	you view (on the Inte	met are stored	in a special	folder
10	for quic	1 marine	Inter			
	1 100.002	A VIEWEY	later.			
-		A VIEWING	liacer.			_
	, (Delete Co	okjes)	Delete <u>Fi</u> les] <u>S</u> ettin	gs
	, (Delete Co	okjes	Delete <u>Fi</u> les] Settin	gs
Histor	, , ,	Delete Co	okjes)	Delete <u>F</u> iles] Settin	98
Histor	The Hi	Delete Co story folde	okjes)	Delete <u>Files</u>	<u>S</u> ettin	gs
Histor	y The Hi quick a	Delete Co story folde	r contains	Delete Files links to pages ; swed pages.) <u>S</u> ettin vou/ve visite	gs
Histor	y The Hi quick a	Delete Co story folde	okjes) r contains recently vie	Delete Eiles links to pages ; swed pages.	<u>S</u> ettin vou've visite	gs
Histor	y The Hi quick a Days to	Delete Co story folde access to r	okjes) r contains recently vie ges in histo	Delete Eiles links to pages y swed pages. wy: 10 0) <u>S</u> ettin you've visite	gs d. for [istory]
Histor	y The Hi quick a Days tr	Delete Co story folde access to r	okjes	Delete Files links to pages ; swed pages. xy: 10 ©	<u>S</u> ettin vou/ve visite	gs d, for listory
Histor	The Hi quick a Days tr	Delete Co story folde access to r	okjes) (r contains recently vie ges in histo	Delete Files links to pages y swed pages. ary: 10 ©) <u>S</u> ettin vou've visite Clear <u>H</u>	gs d, for [istory
Histor	The Hi quick a Days tr	Delete Co story folde access to r b keep pa	nater. okjes (r contains recently via ges in histo	Delete Files links to pages y swed pages. my: 10 Languages.	you've visite	gs d, for (istory
Histor	y The Hi guick a Days tr	Delete Co story folde access to r b keep pay	r contains recently vir ges in histo	Delete Files links to pages y swed pages. my: 10 Languages.	Clear H	gs d, for listory ssibility
Histor	The Hi quick a Days tr	Delete Co story folde access to r b keep par	racer. okjes (r contains recently vir ges in histo	Delete Files links to pages y swed pages. my: 10 Languages.) <u>S</u> ettin rou/ve visite Clear <u>H</u> , Accg	gs d, for listory sability

This screen appears.

Click on *Certificates* in the middle of the screen.



STEP 12

The certificates installed on your computer show in this next screen.

Click on the older of the two certificates, and then click *Remove*.

stended purpose:	<a< th=""><th>Þ</th><th></th><th></th><th></th></a<>	Þ			
Personal Other P	eople	Intermediate Certification	Authorities Tr	usted Root Certification	4
Issued To		Issued By	Expiratio	Friendly Name	
PAUL FRADE		MIB Group, Inc CA MIB Group, Inc CA	3/2/2005 3/2/2006	<none></none>	
Import Certificate intende cAlb	Export.			(Advance	ed.

STEP 13

This alert message asks if you want to delete the certificate you have selected.



Certific	afes
	You cannot decrypt data encrypted using the certificates. Do you want to delete the certificates?
	yes to

Now, only the most recently installed certificate appears on the screen.

Click Close.



STEP 15

WEB-TERM users:

In order to fully activate your renewed digital ID, please access ://www.knowledgenow.com and click on "WEB-TERM".

WEB-DIRECT users:

If you are a WEB-DIRECT client, then you must export your certificate to the appropriate directory in your application.

Please follow this link to get to the export instructions: ://www.mib.com/registrations/html/exportinstructions.html

After completion, the submission of your first transaction to MIB will activate your renewed digital ID. If you require assistance, please contact MIB Help Desk/Customer. Congratulations, you are done!

> For more information, contact us at the Member 800 Number, option 1 or email <u>helpdesk@mib.com</u>



02/19/14