

Anti-Money Laundering Council Manila, Philippines

Transaction Security Protocol Manual



TRANSACTION SECURITY PROCESS

GUIDELINES

- A. The File Transfer and Reporting Facility using the Hypertext Transfer Protocol over Secure Socket Layer (FTRF v 2.0) shall be used by the CPs in transmitting their respective reports.
- B. Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) is a private, secure and graphical method of accessing web page information and/or sending information across a web. It is especially useful for encrypting forms-based information as it passes between clients and servers. HTTPS which is implemented under the File Transfer and Reporting Facility (FTRF v 2.0) will address the efficiency, integrity and security concerns of data collection from the Covered Persons.
- C. File Transfer and Reporting Facility (FTRF) has the following features:
 - a. Secure upload provides data encryption, server authentication and message integrity;
 - b. Self-signed Digital Identification & Certificate allows encrypting and digital signing of messages; and
 - c. Transactional Security Agreement serves as a memorandum of agreement between AMLC and CP. It documents the details, terms and conditions and the use of the self-signed digital certificates.
- D. The self-signed digital identification shall be implemented for all CPs. AMLC and the CPs shall use the Gnu Privacy Guard (GPG) software for their encryption and authentication and the GPG supported algorithm (MD5) for their signing. Installer of the said software shall be provided by AMLC upon registration.
- E. The key of AMLC shall be used by the CPs in filling out/verifying the information stated in the Transaction Security Agreement.
- F. The compliance officer of the CP shall likewise generate his private key as well as public key using GPG which shall be given to AMLC during the exchange of public keys.
- G. The signed public key of the AMLC shall be used by the CPs to:
 - a. Encrypt the electronic files (CTR/STR in csv format) to be submitted to AMLC; and
 - b. Verify the signature of the files they will receive from AMLC.
- H. The signed private key of the AMLC shall be used by AMLC to:
 - a. Decrypt the encrypted files sent by the CPs which were encrypted using AMLC's signed public key; and
 - b. Sign the electronic files they will send to the CPs.
- I. The signed public key of the CP shall be used by the AMLC to:

- a. Encrypt the validation messages that AMLC will send to the CP; and
- b. Verify the signature of the files AMLC will receive from the CPs.
- J. The signed private key of the CP shall be used by them to:
 - a. Decrypt the AMLC validation messages from AMLC; and
 - b. Sign the electronic files they will send to AMLC.
- K. The CPs shall submit the duly accomplished notarized Transaction Security Agreement to Data Collection and Management Staff of the IMAG at the 6/F EDPC Building, BSP Complex, Malate Manila.
- L. The form shall be enclosed in a sealed envelope with a signature on its flap.
- M. After the exchange of keys, CPs are required to perform the back-up procedures of his public and private keys.
- N. CPs are required to encrypt and sign the electronic CTR/STR files before transmitting them to AMLC via https (AMLC portal).
- O. In cases wherein the public key is compromised, superseded or no longer in use, CPs should perform the recovery procedure, only if they have successfully performed the backup procedure of their existing private and public keys, to be able to continue to encrypt file. Otherwise, a new pair of public and private keys shall be generated and newly accomplished Transaction Security Agreement shall be issued. CPs shall follow the same procedures discussed above.

TRANSACTION SECURITY PROTOCOL

1. Installing the GnuPG for Windows Software (Gpg4win 2.1.0)

- Download the gpg4win 2.1.0 from <u>www.amlc.gov.ph</u>, under Reporting Tools, then save this to your local drive.
- Double click gpg4win-2.1.0.exe. You will be asked if you want to allow the program to make changes in your computer.
- Click **Yes**. The Installer Language window will be displayed on the screen.
- Select *English*, then click Ok.



Gpg4win is a installer package for Windows for EMail and file encryption using the core componenent GnuPG for Windows. Both relevant cryptography standards are supported, OpenPGP and S/MIME. Gpg4win and the software included with Gpg4win are Free Software. Click Next to continue.
This is Gpg4win version 2.1.0 file version 2.1.0.1641 release date 2011-03-15

The Gpg4win Setup window will be displayed on the screen. Click **Next**.

	License Agreement This software is licensed under the terms of the GNU General Public License (GPL).
	Press Page Down to see the rest of the agreement.
ne license Agreement	GNU GENERAL PUBLIC LICENSE Version 2, June 1991
indow will be displayed on the screen. Click Next .	Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. Preamble
	The licenses for most software are designed to take away your +
	In short: You are allowed to run this software for any purpose. You may distribute it as long as you give the recipients the same rights you have received. Nullsoft Install System v2.37-3
	< <u>B</u> ack Next > Cancel

Gro O	Choose Components Choose which features of Gpg4w	iin you want to install.
Check the components y nstall. Click Next to con	you want to install and uncheck the cor tinue.	nponents you don't want to
Select components to in	stall: V Kleopatra GPA V GpgOL V GpgEX Claws-Mail V Gpq4win Compendium	Description Position your mouse over a component to see its description,
nace required: 102 5M	B	

Select components to install. Check Kleopatra, GpgEX, and Gpg4win Compendium, then other uncheck components. Click Next.

	🚱 Gpg4win Setup
	Choose Install Location Choose the folder in which to install Gpg4win.
Specify destination folder, then, click Next .	Setup will install Gpg4win in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.
 For 32 bit machine the default directory is C:\Program Files\GNU\GnuPG. 	Destination Folder C:\Program Files\GNU\GnuPG Browse Space required: 101.0MB Space available: 123.0GB Nullsoft Install System v2.37-3 < Back

🕑 Gpg4win Setup			
	oose Install Location hoose the folder in which to install Gpg4wi	n.	
Setup will install Gpg4win in the and select another folder. Click	following folder. To install in a different fo Next to continue.	lder, dick Browse	
			• For 64 bit machine the default
Destination Folder	r		directory is C:\Program Files (x86)\GNU\GpuPG
C: (Program Files (x86) (GN	U\GnuPG	Browse	
Space required: 101.0MB			
Space available: 237.9GB			
Nullsoft Install System v2.37-3 —	↓		
	< Back Next :	Cancel	





Choose Start Menu folder for the Gpg4win shortcuts. Enter **Gpg4win**, then click **Install**.

Please wait while Gpg4win is being installed.	Gpg4win Setup Installing Please wait while Gpg4win is being installed. Extract: view-refresh.png Show details	
	Nullsoft Install System v2,37-3	

Gpg4win Setup	
Installation Complete Setup was completed su	ccessfully.
Ld Completed	
Show <u>d</u> etails	Once the setup completed successfully, clice Next.
Nullsoft Install System v2.37-3	Back Next > Cancel





Check

skip

2. Generation of Key Pairs (One time Procedure)

From your desktop,	Kleopatra Eile <u>View Certificates Tools Settings Window Help</u> Import Certificates Export Certificates Redisplay Stop Operation	Cookup Certificates on Server
double click Kleopatra. The Kleopatra main window will be displayed on the screen.	Find: Omega My Certificates Trusted Certificates Other Certificates Name E-Mail Valid From Valid Until	My Certificates

File	View Certificates Tools Set	tings Window	Help		
۶	New Certificate	Ctrl+N		<i>8</i> %	
M	Lookup Certificates on Server	Ctrl+Shift+I	n Looku	p Certificates on Ser	ver
-	Import Certificates	Ctrl+I		My Certifica	ites 👻
201	Export Cartificates	Ctrl+E	cates		×
Y GI	Export Secret Keys	GHIL	Until	Details	Key-ID
	Export Certificates to Server	Ctrl+Shift+E			
R	Decrypt/Verify Files		1		
40	Sign/Encrypt Files				
	Create Checksum Files				
	Verify Checksum Files		-		
0	Close	Ctrl+W			
×	Quit	Ctrl+Q			

Click File, then select New Certificate.

Certificate Creation Wizard will be displayed on the screen. Click Create a personal OpenPGP key pair.

10	ose Certificate Format
ea	se choose which type of certificate you want to create.
•	<u>C</u> reate a personal OpenPGP key pair OpenPGP key pairs are created locally, and certified by your friends and acquaintances. There is no central certification authority; instead, every
•	Create <u>a</u> personal X.509 key pair and certification request X.509 key pairs are created locally, but certified centrally by a certification authority (CA). CAs can certify other CAs, creating a central, hierarchical chain of

Enter Det Please ent certificate	ails er your personal details below. If you want mo parameters, click on the Advanced Settings bu	re control over the	then Advance Settings.
Name:	Juan C. Dela Cruz	(required)	
EMail:	juan.delacruz@yahoo.com	(required)	
Comment:	ABC Bank	(optional)	
J	iuan C. Dela Cruz (ABC Bank) <juan.delacruz(< th=""><th>@yahoo.com></th><th></th></juan.delacruz(<>	@yahoo.com>	

Note:

Name – Name of Compliance Officer Email – Email address of Compliance Officer Comment – Name of the company

Details window	Key Material
will be displayed	RSA 2,048 bits (default)
on the screen.	● DSA 2,048 bits (default) ▼
	✓ + Elgamal 2,048 bits (default) →
From Key	Cartificata Usaga
DSA: 2 048 hits	Signing Contification
(default).	
. ,	Valid until: 2/9/2014
Check + Elgamal :	
2,048 bits	
(default).	
From Certificate	
Usage, check	
Usage, check Signing ,	
Usage, check <i>Signing,</i> <i>Encryption</i> and	
Usage, check Signing, Encryption and Certification.	
Usage, check Signing, Encryption and Certification.	

Enter Det	aiis		From	the
Please ent certificate	er your personal details below. If you want more arameters, click on the Advanced Settings butto	control over the	Certificate	14/:
Name:	Juan C. Dela Cruz	(required)	window,	clic
EMail:	juan.delacruz@yahoo.com	(required)	Next.	
Comment:	ABC Bank	(optional)		
J	an C. Dela Cruz (ABC Bank) <juan.delacruz@y< th=""><th>/ahoo.com> <u>A</u>dvanced Settings</th><th></th><th></th></juan.delacruz@y<>	/ahoo.com> <u>A</u> dvanced Settings		





Please be reminded that once you forget your passphrase, you need to generate a new public key, since AMLC cannot retrieve the said passphrase.

Creating Key			
Your key is bein	created.		
The process of o foster this proce The text itself we move this windo application.	reating a key requires la ss, you can use the ent in't be used at all, only v around with your mou	arge amounts of ran ry field below to entr the inter-character ti se, or start some dis	dom numbers. To er some gibberish. ming. You can also sk-intensive
1			

Wait until the key pair is successfully created.

	Key Pair Successfully Created					
	Your new key pair was created successfully. Please find details on the result and some suggested next steps below.					
	Result					
k Finish.	Certificate created successfully. Fingerprint: 7F2C0A8B90C6E4E83FFDFC4E09D7D50EBC5CC263					
	Next Steps					
	Make a Backup Of Your Key Pair					
	Send Certificate By EMail					
	Upload Certificate To Directory Service					

Transaction Security Process

3. Exporting Public Key

Import Certificates	Export Certificate	s Redispla Export Ce	v <u>Stop Op</u> eration rtificates	n Look	up Certificates on	Server
My Certifica	tes T <u>r</u> usted C	Certificates	Other Certific	ates	1.625	
Name E-Mail		Valid Fr	om Valid	Until	Details	Key-ID
Juan C	juan.delacru	2012-02-08	}		OpenPGP	BC5CC263

From your desktop, double click Kleopatra. The Kleopatra main window will be displayed on the screen. Click the name of the compliance officer, then click Export Certificates.

	C Export Certificates C C C C C C C Certificates C C C C C C Certificates C C C C C C C C C Certificates C C C C C C C C C C C C C C C C C C C	5 x
	Organize 🔻 New folder) • • • • • • • • • • • • • • • • • •
	Name Date mo	odified Type
elect the directory where	Libraries 1/7/2012	2 2:49 PM File f
he public key is to be	Documents 2/7/2012	2 2:49 PM File f
aved then click Save	Ib 2/7/2012	2 2:49 PM File f
saved, then click Save .	Pictures Jugins 2/7/2012	2 2:49 PM File f
	uideos 2/7/2012	2 2:49 PM File f
 he public key is to be aved, then click Save. For 32 bit machine: c:\Program 	share 5/9/2011	1 3:25 PM File f
	translations 2/7/2012	2 2:49 PM File f
	New Volume (D:)	2 9:34 AM GPG
 For 64 bit machine: c:\Program Files (x86)\GNU\GnuPG\ 	File name: 7F2C0A8B90C6E4E83FFDFC4E09D7D50EBC5CC263.asc Save as type: OpenPGP Certificates (*.asc *.gpg *.pgp)	Cancel

Note: The default filename of the public key is the key fingerprint.

Please be ready with the exported asc file as you will need this for ONLINE REGISTRATION

4. Saving AMLC public key

Get a copy of the AMLC public key (amlc.asc) from <u>www.amlc.gov.ph</u> under Reporting Tools then save this to your local drive.

- For 32 bit machine: c:\Program Files\GNU\GnuPG\
- For 64 bit machine: c:\Program Files (x86)\GNU\GnuPG\

5. Importing of AMLC public key

mport Certificates	Export Certificates	C Redisplay	CO Stop Operation	Lookup Cer	tificates on 1	Server		desktop, d click Kleo j
nd:		. 19 - 19 -			My Certific	ates	•	The Kleo
My Certificate	s T <u>r</u> usted Cert	ificates	<u>O</u> ther Certificat	es				nain windo. A displaye
Name	E-Mail	Valid From	n Valid Ui	ntil	Details	Key-ID	-	he screen
Juan C ji	uan.delacru 20	012-02-08		Оре	nPGP	BC5CC263		ine sereen.
								Click Import
								Certificates.

Select the directory where you have saved the **AMLC.asc**, then click **Open**.





The Certificate Import Result window will be displayed on the screen. Click Ok.

The imported public key will be displayed on Kleopatra – Imported Certificates tab.	Import Certificates Export Certificates Export Certificates Stop Operation Lookup Certificates on Server							
	Find: Artertificates							
	My Certificates	Trusted Certificates	<u>O</u> ther Certificates	Imported Certificate	es 🚺			
	Name	E-Mail Valid Fr	om Valid Until	Details	Key-ID			
	Anti-Mone amlo	:@bsp.go 2010-01-12		OpenPGP 1	17B9F65			

6. Certifying AMLC Key

Import Certificates	xport Certificates Redi	play Stop Operation	Lookup Certificates on	Server	From yo desktop, dou
Find:			All Certific	ates	click Kleopatra.
My Certificates	Trusted Certificate	s Other Certifica	tes Imported Certi	ficates	
Name	E-Mail Valio	From Valid U	Intil Details	Key-ID	From Kleopatra
Anti-Mone an	nlc@bsp.go 2010-0	-12	OpenPGP	117B9F65	main window,
٠		III			click Anti-Mone Laundering Council's public key.

Transaction Security Process



Certify Certificate: Anti-Money Laundering Council (AMLC Institutional Key Pair 1 Check Anti-Money Step 1: Please select the user IDs you wish to certify. Laundering 🔽 Anti-Money Laundering Council (AMLC Institutional Key Pair) <amlc@bsp.gov.ph> Council, then check I have verified the fingerprint. Click Next. Certificate: Anti-Money Laundering Council (AMLC Institutional Key Pair) <amlc@bsp.gov.ph> (117B9F65) Fingerprint: 500E59DCCDA03F2CDE3E553E1710B3CF117B9F65 VI have verified the fingerprint Next Cancel Certify Certificate: Anti-Money Laundering Council (AMLC Institutional Key Pair) Step 2: Choose how to certify. Certification will be performed using certificate Juan C. Dela Cruz (ABC Bank) <juan.delacruz@yahoo.com>. Select Certify only for myself, then click Certify. Certify only for myself Certify for everyone to see Send certified certificate to server afterwards <u>Certify</u> C<u>a</u>ncel

bar,

click

Certificate.

pinentry	
Please enter the passphrase to unlock the secret key for the OpenPGP certificate: "Juan C. Dela Cruz (ABC Bank) <juan.delacruz@yahoo.com>" 2048-bit DSA key, ID BC5CC263, created 2012-02-08.</juan.delacruz@yahoo.com>	Enter passphrase of compliance officer, then
Passphrase	click Ok .
<u>OK</u> <u>C</u> ancel	

	Summary:
ck	Signed user IDs: Anti-Money Laundering Council (AMLC Institutional Key Pair) <amlc@bsp.gov.ph></amlc@bsp.gov.ph>
inish.	Selected secret certificate: Juan C. Dela Cruz (ABC Bank) <juan.delacruz@yahoo.com></juan.delacruz@yahoo.com>
	Certification successful.

7. Backup Procedure

Make sure to do this procedure to ensure that you will not perform all the steps enumerated above in the event that your public key has been corrupted.

nport Certificates Ex	port Certificates	C Redisplay	Stop Operation	Look	up Certificates on	Server	
d:					My Certific	ates	•
My Certificates	Trusted Cer	tificates	Other Certificat	es			
Name	E-Mail	Valid Fro	om Valid U	ntil	Details	Key-ID	-
		042 02 00	r		OnonDCD	BC5CC262	
Juan C juai	n.delacru 2	012-02-08			openror	DCJCC203	

Open Kleopatra.

From My Certificates tab, click the name of the key owner (Compliance Officer).

kg	New Certificate	Ctrl+N		ø				
*	Lookup Certificates on Server	Ctrl+Shift+I	n l	ookup Certificates o	n Server			
-	Import Certificates	Ctrl+l				Му	Certificates	
3	Export Certificates	Ctrl+E	cates					
1	Export Secret Keys.	Ctrl+Shift+E		Valid From	Valid Until	Details	Key-ID	
-	Export Certificates to Server		g	2010-01-12		OpenPGP	117B9F65	
	Sign/Encrypt Files Create Checksum Files							
0	Verify Checksum Files	CHANN						
_	Cluse	GUITVY						
•								

From the menu bar, click **File** then select **Export Certificates.**

anize 👻 New folder		= • 🔞		
Documents Name	Date modified	Туре		
Music	_			
Pictures	No items match your search.			
Videos				
=				
Computer				
Local Disk (C:)				
, RLYN (G:)				
Drive H (\\nasug				
IMAGAPPS (\\na				
CIs (\\legaspi\CS 👻 🔺	III d	*		
File <u>n</u> ame: back_up_publickey.asc	-	-		
		i		

ect the ectory ere you nt to save backup /our olic key B), by ault name is ır gerprint. u have option to nge the name) k Save.

- - X 👩 Kleopatra File View Certificates Tools Settings Window Help C 6% 0 Import Certificates Export Certificates Redisplay Stop Operation Lookup Certificates on Server On My Find: My Certificates -Certificates My Certificates Trusted Certificates Other Certificates * tab, click the Name E-Mail Valid From Valid Until Details Key-ID name of the Juan C. ... juan.delacru... 2012-02-08 OpenPGP BC5CC263 key owner (Compliance Officer).

A	New Certificate Ctrl+N Lookup Certificates on Server Ctrl+Shift+I		n	Kookup Certificates o	n Server			
aga,	Import Certificates	Ctrl+I					My Certificates	
	Evnot Cartification	CtduE	cate	S				×
	Export Certificates	CIII+E		Valid From	Valid Until	Detail	ls Key-ID	
1	Export Contification to Server	Ctd+Shift+E	g	2010-01-12		OpenPGF	0 117B9F65	
	Export Certificates to Server	endicates to Server		2004-10-11		OpenPGF	4D0BDEE5	
R.	Decrypt/Verify Files							
	Sign/Encrypt Files							
	Create Checksum Files							
	Verify Checksum Files		ι.					
	Close	Ctrl+W						
3								

From the menu bar, click File then select Export Secret Keys.

Export Secret Certificate	2	×
Please select export options for <rpdelapena@amlc.gov.ph> (4D0</rpdelapena@amlc.gov.ph>	JUAN DELA CRUZ)BDEE5):	Select the directory where you
Output file:		want to save the
ASCII armor		backup of your privat key (USB) b clicking the diskette
	<u>O</u> K <u>C</u> ancel	icon.

