PGP Introduction and Keysigning

Joel Jaeggli For SSE AFNOG 2011

Rational

- We've talked about public key crypt in the context of web server certs.
- We talking about it in the context of encryption systems.
- Now it's time to do something with it.
- We're going to generate identities, validate and sign them.
- You can take them home with you, they can allow you communicate securily with your friends and colleagues.
- You'll form part of a web of trust with your AFNOG colleagues which you can further extend by signing the keys of your friends and colleagues.

Get software (some useful examples)

- Windows
 - http://www.gpg4win.org/download.html
 - Install, run kleopatra, create new openpgp keypair
 - Enigmail (thunderbird)
- Ubuntu
 - https://help.ubuntu.com/community/GnuPrivacyGuardHowto
- Mac
 - http://www.gpgtools.org/installer/index.html
- Generic
 - http://www.gnupg.org/download/index.en.html

Create a key (example is command-line GPG)

- gpg --gen-key
- Select DSA and el gamal (you can read some rather long screes on the internet about which is better)
- 2048 bit key size
- Does not expire or 20y are reasonable depending on whether you want a safety net for expiration or not.
- Real name
- Email address
- Comment
- Password

Uploading the key for the keysigning

- gpg –list
- Once you find the key-id
- Do gpg –export -a keyid to generate the ascii armor version of your public key.
- Go to http://biglumber.com/x/web?keyring=1203
- Paste in your ascii armored key

How a PGP-signing party works

- Everyone uploads their public keys...
- Keyfile is downloaded and distributed.
- A participant presents an identity document satisfactory to the other participants (government issued photo-id for example)
- And reads out-loud their keyfinger print
- Other participants sign the validated key having verified the key fingerprint.

000	Nagios Core	×	Console -> Devices -> × ([🗋 AfNOG 2011 – SS-E – D 🗙	Scnn who cell phones - 🛪	wphttp://www.washingtor ×	🕒 NfSen 🛛 🛪	🗋 View keyring	×	New Tab	×	Ð	
← → C	biglumber.com	ı/x/web	?keyring=1203								\$	0 -	2

View Keyring

- Event: afnog ws sse keysigning event
 Date: June 2 05, 2011
- Keyring name: afnog ws sse keysigning event keyring
 You may add keys to this keyring.

Download this keyring

Total entries: 2

You are the owner of this keyring. [Edit keyring settings]

View keyring as others see it

Visible?	Date uploaded	Fingerprint Key type / Key size Creation date / Expiration date	UIDs	Image
Y	20110601 08:00 EDT [remove from keyring]	<u>5C6E0104BAF040B05BD3C38BF00035ABB67F56B2</u> DSA / 1024 2003-08-11 / None	• Joel Jaeggli (08112003-alternate to pgp 5 keypair) <i><joelja "at"="" dot="" twin="" uoregon.edu=""></joelja></i>	
Z	20110601 07:54 EDT [remove from keyring]	BEDA1F529F0769A2B1CF336781BDD3C40E1F9B79 DSA / 1024 1999-09-23 / None	 Phil Regnauld (private) <pr "at"="" dot="" eu="" org=""></pr> Phil Regnauld (home address) <regnauld "at"="" dot="" org="" starbsd=""></regnauld> 	
Make char	nges			
Paste an a	scii-armored file below co	ontaining the key(s) you wish to add to the keyring.		

000	Sent —	- nagasaki (295 messages)		\ominus
		V	Q	
Get Mail	Delete Junk Reply Reply All Forward New Message Note	To Do		Search
MAILBOXES	• • To Sul	bject	Date Sent	
Trhey	Patrick J Okui Re	e: did v4 transit get particularly crappy?	Yesterday	3:04 AM
	teemu.savolainen@nokia.com fy:	<pre>vi the ietf mailman seems to be getting bounces</pre>	Yesterday	4:30 AM
Mobileme	<teemu.savolainen@nokia.com> <teemu.savolainen@no… re<="" td=""><td>e: fyi the ietf mailman seems to be getting boun</td><td>Yesterday</td><td>5:44 AM</td></teemu.savolainen@no…></teemu.savolainen@nokia.com>	e: fyi the ietf mailman seems to be getting boun	Yesterday	5:44 AM
agasaki 924	Livingood, Jason Re	e: very private: whitelisting-implications	Yesterday	6:40 AM
Gmail (2893)	Phil Regnauld Re	e: Evening session proposal for tonight: virtualiza	Yesterday	6:40 AM
🔻 📩 Drafts	eric clark Re	e: Deploying IPv6 globally	Yesterday	8:54 AM
🦾 MobileMe	Jens Kuehlers Re	e: nokia/microsoft	Yesterday	10:45 AM 🕥
nagasaki 🛛 🔁 🔤	Alexa Morris Re	e: NANOG transition update	Yesterday	11:10 AM
Gmail	John Kemp te	est	Today	2:11 AM 🔻
▼ 🖾 Sent		0		
🖅 MobileMe	The message has been encrypted with OpenPGP.			Decrypt
🛷 nagasaki	Cublects test			0
妃 Gmail	Subject: test			
► Trash	Date: June 1 2011 2:11:37 AM PDT			
	To: John Kemp			
* RSS				
Apple Hot News	BEGIN PGP MESSAGE			
▼ ON MY MAC	Version: GnuPG v1.4.11 (Darwin)			
Recovered Messag				
MOBILEME	nu10Abuau/C8mGypEAT+02M2mFHCW0158WE80T8KnDDEKT]VC/V9 fDvvS1E15KkApbyEC006X4XbC5vveRoUX8HN4pv2eS1akv0n04Xb	91VKJDVCNKIGW 91VKJDVCNKIGW		
lunk	0+8IETlBhshfAhi0oHIoCXRDm8XHKys2HmDQX7ZixFcx6rk11xMy	vXzVRWAzo1VsD		
	AHX0QfzqyUi0VLS3BRkZ3M2RiyWIK1DW1FB39Uzuh/o853zcmWsv	vygXZOucZm2bY		U
NAGASAKI	bqMBT0grw+mPq5w9IfKkhdGEwIox5v6wHpDxo6mr3NL8C58R/yYw	Wfh6JtGp4+r0P		
Archives	3h0jtf0ime4asd0hS9op8K+JhUjcWeYKZsynNLpGJAf/Y1pZPmE1	LJCgIVINHHVLJ		
duplicates (1934)	9272E42AC/100102EX21X8X89J05V1FgL01+5n11W61D2nJPqD00 EPaDPCESuaav7UFFw807TNiFPo1ARSvriEIt1/+F/Go1070Twws8	cigcomzaapxyx 8uSvalzeoW9Ln		
MAIL ACTIVITY	Ha2Z0IVPJ+Dehu0x1VGa/wPV7jAscXGgHx+T6w80hE0wxdZXPmLv	v6mf88vX8mQ2D		
	S2Uz93bwV0Bx8wIagGpFx906YnKZaZ0crnD/jAhxAKASvw8c8b7w	w99N82BoWhhU2		
	4Uw80UR0Gex/Komzwwo25zJmrIR4n8rFyZCG+gjkQHR2Dr1Zw1+p	pze0Zoe7E1vt+		
	pIUEDgN6HX/mKUB/khAP/3FUkbCX0qoQpbu8trzqb6x/3Sv2Ghfu	uQkIAxf+BwFwy		
	<pre>yLpoknzJy/3wLbEr363Zg53yLbtX/mU29HrCAwqL1WV0PcgKZ5t3 cCpi1VbdD510PCoK0/6wb7Cz/CcA2cXcEuMowf/ToMcov0v6KVC0V</pre>			
	W21Yck0VSfFolluVTV80TSPaExw5ni/tR0iMKVx1+aVSXVvSVCr1	agyeXUX r8DwPh		
	kePTux/Vat04gaza+Jz2BhhtSxSvJ4HGV0fEXor64iec7vemz0Mf	fza6Jc41+tibi		A
+ 🔻 🌣 -	E05Jny/sN3ckdJTi/OTPaUQKhjlEDVR9D/K/dnkwt3b/EGNDRhok	KhE02diMlai5+		*
NAGASAKI Archives duplicates 1934 MAIL ACTIVITY + •	bqMBT0grw+mPq5w9IfKkhdGEwIox5v6wHpDxo6mr3NL8C58R/yYM 3h0jtf0ime4asd0hS9op8K+JhUjcWeYKZsynNLpGJAf/Y1pZPmE1 g27ZE4ZAc/16VtM2ExZiK8X09JU5v1FgL0l+5nfiw6ID2njPqDoc EPaDPCESuaav7UFFw8Q7TNjFPp1ARSyrjEItl/+E/Gol07QIwwx8 Ha2Z0IVPJ+Dehu0x1VGa/wPV7jAscXGgHx+T6w80hE0wxdZXPmLv S2U293bwV0Bx8wIagGpFx906YnKZaZ0crnD/jAhxAKASvw8c8b7w 4Uw80UR0Gex/Komzwwo25zJmrIR4n8rFyZCG+gjkQHR2Dr1zw1+p pIUEDgN6HX/mKUB/khAP/3FUkbCX0qoQpbu8trzqb6x/3Sv2Ghft yLpoKhZJy/3wC6Er3G3zgS3yIbtX7mU29HrcAwqIIWVoPcgKZ5t3 SGniJYbdD5L0PGeK0/6wbZCz/CrA3cXCFuWawf+IpWcx0v6KVS0V W21Yck0V5fFoUuVTV8QTSPaExw5ni/tRQiMKVx1+qYSXVvSYCrJg kePTux/Vqt04qaza+Jz2BhhtSxSvJ4HGV0FEXor64jec7vemz0Mf E05Jny/sN3ckd1Ti/0TPaUQKhjLEDVR9D/K/dnkwt3b/E0NDRhok	VyAcoccine Wfh6JtGp4+r0P LJcgIVINhHVLJ cIgcOmzaapxyx 8uSyqlzeoW9Ln v6mf88vX8mQ2D w99N82BoWhhU2 pze0Zoe7E1vt+ uQkIAxf+BwFwy 34/3KZw/IeNrh VEtgBXIaeAS0v g0xeXOXr8DwPh fzg6Jc41+tjbj KhE02diMlai5+		

Send Chat Attach Address Fonts Colors Save As Draft	Photo Browser Show Station
To: John Kemp	
Cc:	
Subject: private communications	
OpenPGP: ☑ Signed Uoel Jaeegli <joel.jaeggli@nokia.com></joel.jaeggli@nokia.com>	C Encrypted Keys
attack at dawn	