IK2206 – Internet Security and Privacy
GPG Lab Notes

STEP1 – Getting started
This document was created during the GPG lab. Most commands that were used during the lab are documented in the following sections.

GPG Handbook: http://www.gnupg.org/gph/en/manual.html
GPG Cheat List: http://irtfweb.ifa.hawaii.edu/~lockhart/gpg/gpg-cs.html

STEP2
gpg --import <gpgfile.gpg>

gpg --list-key

gpg --edit-key Pehrs@kth.se
trust -> 4 (fully) -> quit

gpg --check-sigs 9DB307EA

gpg --check-sigs 6972F18A
-> 5 Beglaubigungen wegen fehlenden Schl³sseln nicht gepr³ft

gpg --delete-key 6972F18A

STEP3
gpg --gen-key
-> RSA/RSA -> 2048bit -> galliker@kth.se
-> Passwort: abcdefg12345678

STEP4
gpg --armor --export galliker@kth.se

STEP5
gpg --edit-key galliker@kth.se
-> adduid -> Thomas Galliker -> thomas.galliker@stud.hslu.ch -> save

pub 2048R/754E52A2 created: 2011-11-07 expires: 2012-02-05 usage: SC
trust: ultimate validity: ultimate
sub 2048R/3AB4C316 created: 2011-11-07 expires: 2012-02-05 usage: E
[ultimate] (1). Thomas Galliker (HSLU Identity) <thomas.galliker@stud.hslu.ch>
[ultimate] (2) Thomas Galliker (IK2206) <galliker@kth.se>

STEP6

gpg --output galliker.gpg --armor --export galliker@kth.se
gpg --import chmo.gpg
gpg --edit-key chmo
trust -> 4 -> quit
sign -> y -> y -> save
(Note: "gpg --sign-key chmo" would work the same way)
(Note: The signature status changes from "unknown" to "full)

gpg --import galliker_signed.gpg
gpg: key 754E52A2: "Thomas Galliker (HSLU Identity) <thomas.galliker@stud.hslu.ch>" 2 new signatures
gpg: Total number processed: 1
gpg: new signatures: 2
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 1 signed: 1 trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: depth: 1 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 1f, 0u
gpg: next trustdb check due at 2012-02-02

gpg --import C:\Users\Thomas\Dropbox\KTH_IK2206\course_material\gpg_lab\keys\galliker_signed_with_course_key.gpg
gpg: key 754E52A2: "Thomas Galliker (HSLU Identity) <thomas.galliker@stud.hslu.ch>" 1 new signature
gpg: Total number processed: 1
gpg: new signatures: 1
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 1 signed: 1 trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: depth: 1 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 1f, 0u
gpg: next trustdb check due at 2012-02-02

--edit-key galliker
[...]
gpg> check
uid Thomas Galliker (HSLU Identity) <thomas.galliker@stud.hslu.ch>
sig!3 754E52A2 2011-11-07 [self-signature]
sig! 4A4C222E 2011-11-07 Christoph Moser (ik2206) <christoph.moser@stud
uid Thomas Galliker (IK2206) <galliker@kth.se>
sig!3 754E52A2 2011-11-07 [self-signature]
sig! 4A4C222E 2011-11-07 Christoph Moser (ik2206) <christoph.moser@stud
sig! 9DB307EA 2011-11-07 Internet Security and Privacy (IK2206) <gpg-bo

STEP7

Note: A key must be "signed" and "trusted" to get rid of the warning below. Use following command:

gpg --verify "..\signed_messages_partX.gpg"
gpg: Signature made 11/07/11 18:41:35 W. Europe Standard Time using DSA key ID 9DB307EA
gpg: Good signature from "Internet Security and Privacy (IK2206) <gpg-both@netsec.xen.ssvl.kth.se>"
gpg: aka "Internet Security and Privacy (IK2206) <gpg@netsec.xen.ssvl.kth.se>"
gpg: aka "Internet Security and Privacy (IK2206) <gpg-key@netsec.xen.ssvl.kth.se>"
gpg: aka "Internet Security and Privacy (IK2206) <gpg-sign@netsec.xen.ssvl.kth.se>"
gpg: aka "Internet Security and Privacy (IK2206) <gpg-crypt@netsec.xen.ssvl.kth.se>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 34C2 57EB 4DEA EA93 3D3E 13B0 BB24 3E2A 9DB3 07EA

Note: Sending back all lines with good signatures:
gpg --clearsign signed_messages_goodlines.txt

STEP8

gpg --output encrypted_messages_part1.txt --decrypt encrypted_messages_part1.gpg

gpg -r galliker@kth.se -r gpg --output encrypted.gpg -a --encrypt "encrypted_message_goodlines.txt"

STEP9

gpg --output s&e_messages_part1.txt --decrypt s&e_messages_part1.gpg

gpg -a -r galliker@kth.se -r gpg --output signed_and_encrypted_messages.gpg --sign --encrypt

s&e_messages_goodlines.txt

STEP11

gpg2 --output galliker.pdf.sig --detach-sig galliker.pdf