1 Laboration i säker e-post

Table of Contents

Betygsnivåer. VG: klara alla frågor som ställts tillräckligt bra. G: Fråga 1.2e felaktig eller ej behandlad.

1.1 Inledning

Vi ska i denna laboration lära oss att hantera kryptering och digitala signaturer.

Du måste använda en säker e-postklient. Det finns en lista på säkra e-mailklienter här: http://www.bretschneidernet.de/tips/secmua.html.

PGP/MIME är den ursprungliga standarden för säker e-post. Den öppnades upp och blev standardiserad och under namnet OpenPGP: http://www.openpgp.org/.

En fri variant av OpenPGP är GNU Privacy Guard (GnuPG eller GPG) https://www.gnupg.org/. I Windows är det lättast att använda "GnuPG For Windows" som finns här: http://www.gpg4win.org. OpenPGP och GnuPG är kompatibla med varandra.

Mozilla Thunderbird: https://www.mozilla.org/en-US/thunderbird/ och OpenPGP/GnuPG via ett AddOn som heter EnigMail: http://www.enigmail.net/home/index.php är ett bra, gratis och väldokumenterat val som som jag kan **rekommendera** i labben.

Det går även bra att använda en kompatibel webbläsare och vissa webbmail-tjänster tillsammans med Mailvelope: https://www.mailvelope.com/ för att få säker e-post. Denna lösning kan vara bra om man inte vill installera program på sin dator. Ett addon/extension måste dock installeras i webbläsaren.

Som exempel i laborationen för att visa tekniken har jag använt The Bat! (https://www.ritlabs.com/en/products/thebat/) som är ett bra alternativ till Outlook Express och Windows Mail m.fl. The Bat! Home eller Professional Edition kan användas gratis i 30 dagar och svenskt språkstöd finns.

Du bör använda den e-postklient som du tror du kan få att fungera med säker e-post **(OpenPGP/GPG är den standard jag stöder)**. Min publika nyckel finns här: http://users.du.se/~hjo/cs/ik1080/lab/lab1_saker_e-post/ i filen: **GPG_pubkey_hjo.du.asc.**