Дијаграм за STS протколот

Значење на ознаките во дијаграмот:

g- Произволен 512 битен број кој го генерира иницијаторот на комуникацијата.

p- Произволен 512 битен прост број кој го генерира иницијаторот на комуникацијата.

x- произволен број на првиот корисник.

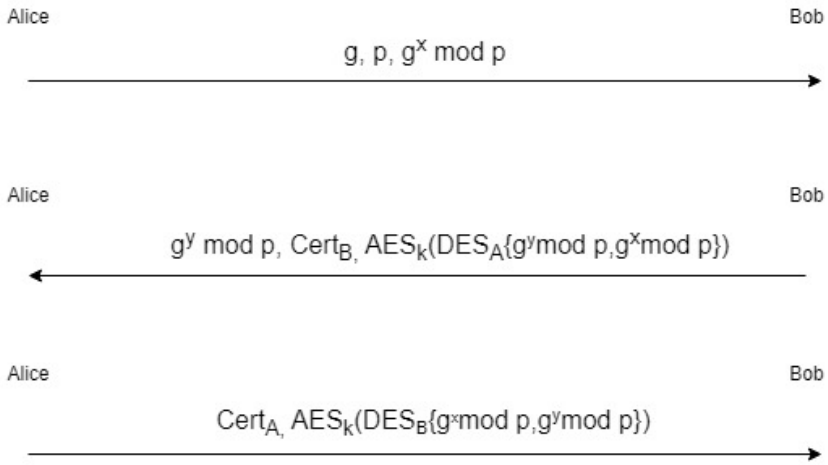
y- произволен број на вториот корисник.

$Cert_U$ -Сертификат генериран од страна на U – корисникот.

$AES_{K=}(a)$ – Енкрипција на a со AES алгоритамот и со симетричниот клуч K.

{a} – Хеширање на a.

$DES_U(a)$ – Потпишување на a со тајниот клуч на U – корисникот со помош на DES алгоритамот.



Како овој протокол заштитува од Man-In-The-Middle напад:

STS протоколот користи сертификати кои се дигитално потпишани користејќи приватен клуч (енкриптирани со асиметричен алгоритам за енкрипција) од страна на авторот на сертификатот и може да се отклучи (декриптира) само со јавниот клуч на авторот на сертификатот. Дигиталниот потпис на сертификатот всушност ја енкриптира хешираната вредност на податоците во сертификатот како што се g, p, име на авторот и јавниот клуч од авторот. Овие податоци се спојуваат и се хешираат за потоа хешираната вредност да се енкриптира со приватниот клуч на авторот. Целокупниот сертификат се испраќа до вториот корисник кој потоа го автентицира со тоа

што ги зема сите податоци од сертификатот и ги хешира. Ги отклучува потпишаните хеширани податоци со помош на јавниот клуч кој е сместен во сертификатот и потоа ги споредува вредностите на декриптираниот хеш и хешот што самиот корисник го пресметува. Доколку се исти тоа значи дека сертификатот е валиден и дека корисникот е тој што тврди дека е. Доколку има трето лице кое сака неовластено да се вклучи во комуникацијата, да прислушкува и да манипулира со податоците, тоа лице нема да може да го лажира сертификатот бидејќи не го знае тајниот клуч со кој е потпишан тој сертификат и со тоа неговиот обид за man-in-the-middle напад е неуспешен.