

100 procent veilige telefonie

CRYPTOGRAFIE Een Duits bedrijf brengt een systeem op de markt dat een telefoongesprek zo versleutelt dat afluisteren onmogelijk wordt. Het werkt ook voor mobieltjes.

Sybe Rispens

Berlijn - Het Duitse electronicabedrijf Rohde&Schwarz heeft twee weken geleden in München op de Systemhandelsbeurs voor elektronica een systeem geïntroduceerd waarmee telefoongesprekken, faxen en dataverkeer cryptografisch kunnen worden versleuteld. Het systeem, TopSec genoemd, bestaat uit diverse apparaten waarmee het afluisteren van telefoongesprekken of het versturen van faxen binnen het ISDN-telefoonnetwerk onmogelijk wordt. Een bijpassende mobiele telefoon maakt het zelfs mogelijk om onderweg er zeker van te zijn dat gesprekken niet door derden kunnen worden afgeluisterd.

De TopSec GSM-telefoon is wereldwijd de allereerste mobiele telefoon die niet afgetapt kan worden. De cryptografische module is, in nauwe samenwerking met Siemens, ingebouwd in een bestaande Siemens S35i-telefoon. De ontwikkeltijd bedroeg twee jaar. De versleuteling in de cryptografische module is een combinatie van een asymmetrisch en een symmetrisch logaritme. Bij het asymmetrische deel gaat het om een 1024-bit Diffie-Hellman encryptie, die ook veel op internet wordt gebruikt.

De Diffie-Hellman methode schrijft voor dat beide gesprekspartners elk een eigen privé-digitale sleutel gebruiken, waarna er volgens een vast protocol een publieke sleutel wordt uitgewisseld, waarmee alleen

de geautoriseerde ontvanger de versleutelde boodschap weer kan openmaken. De publieke sleutel heeft 10^{38} mogelijkheden en wordt na ieder gesprek weer gewist. Bovenop de asymmetrische versleuteling heeft Rohde en Schwarz nog een symmetrische versleuteling gelegd van 128 bit. Met deze versleuteling is het mogelijk om verschillende ontvangers tot één gebruikersgroep te definiëren. Alles bij elkaar is de versleuteling zeer kraakvast: 1000 Pentium-processoren zouden 10 miljoen jaar nodig hebben om een deel van de mogelijke sleutels te kunnen uitproberen. Er zit geen 'verborgen achterdeur' in het systeem en het kan dus absoluut niet worden afgeluisterd.

Het gebruik van de cryptografische mobiele telefoon is eenvoudig. De beller hoeft alleen maar op het knopje 'Crypto' te drukken en alles gaat daarna automatisch: het modem in de S35i wordt ingeschakeld, legt een verbinding met een TopSec ontvanger, en in de volgende vijftien seconden wordt de publieke sleutel tussen de twee apparaten uitgewisseld. Zodra het gesprek is beëindigd, wordt de publieke sleutel vernietigd. De TopSec cryptografische apparatuur komt in een politiek gevoelige tijd op de markt. Rohde & Schwarz levert daarom uitsluitend via de Berlijnse afdeling 'Sicherheit in Informationstechnik' aan bedrijven, banken en overheid. De TopSec mobiele telefoon 3200 Euro. ■