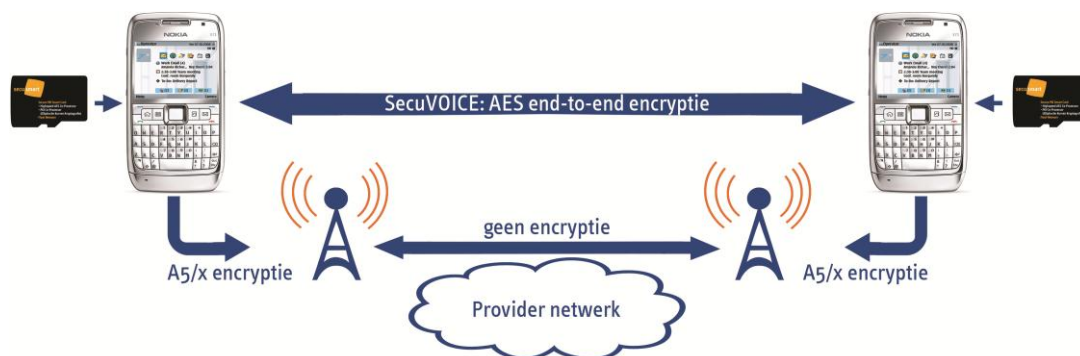


1 SecuVOICE van Fox-IT

Fox-IT biedt een unieke oplossing voor het beveiligen van zowel telefoongesprekken als SMS met de mobiele telefoon. SecuVOICE combineert gebruiksgemak met de benodigde veiligheid.

SecuVOICE werkt op basis van een Secusmart Security Card (microSD-smartcard), die gesprekken tussen twee mobiele telefoons, alsmede SMS, volledig end-to-end versleutelt. Deze kaart bevat naast 4 GB flash geheugen ook een cryptochip die alle gesprekken en SMS'jes versleutelt. Vertrouwelijke data kan de Secusmart Security Card nooit zomaar verlaten. Als gevolg van deze versleuteling, zijn gesprekken niet door derden af te luisteren. Het 4 GB flash geheugen bestaat uit 2 GB vrij geheugen beschikbaar voor alle telefoonapplicaties en 2 GB geheugen, die hardwarematig versleuteld is en alleen toegankelijk is door gebruik van de smartcard (cryptografisch deel van de Secusmart Security Card).

Hiermee zijn alle contacten en sms'jes veilig opgeslagen en niet toegankelijk voor anderen. In een later stadium kan ook e-mail hier veilig opgeslagen worden.



SecuVOICE is beschikbaar voor de laatste serie toestellen van Nokia. Na invoer van de Secusmart Security Card in het microSD slot van de telefoon installeert de applicatie automatisch. Door vervolgens een gesprek te voeren via SecuVOICE ben je ervan verzekerd dat er niemand meeluistert en dat je daadwerkelijk spreekt met de gewenste persoon en niet met iemand die zich uitgeeft voor een ander. Er kan gekozen worden tussen een privé kaart of een kaart waarbij de naam van uw organisatie wordt geregistreerd en opgenomen in het certificaat. Bij een privé kaart wordt het telefoonnummer of de naam (indien bekend) van de beller getoond. Indien het domein (organisatienaam) ook is opgenomen in het certificaat wordt deze naam ook getoond op het display. Gebruikers kunnen kiezen uit een gewoon of een versleuteld gesprek. Voor het laatste is één druk op de knop voldoende. Uiteraard dienen beide personen een Secusmart Security Card te hebben. Daarnaast kunnen ze hun mobiele telefoon ook normaal blijven gebruiken.

Toegang tot de Secusmart Security Card is beveiligd met een pincode. Dit product maakt verder gebruik van de hardware van de telefoon. Niet alleen wordt de spraak versleuteld door de hardware cryptochip op de Secusmart Security Card, maar wordt de spraak ook gecompriemd door de hardware chip in de telefoon. Dit heeft zowel voor de geluidskwaliteit, de vertraging en de totale spreektijd met een (volle) batterij grote voordelen. Dankzij de intuïtieve gebruikersinterface en spraakkwaliteit, voelt een gesprek via SecuVOICE aan als een regulier gesprek en vormt bovendien geen extra belasting op de energieconsumptie van het toestel.

2 Interoperabiliteit & Open Standaarden

Het kabinet lanceerde in samenwerking met het ICTU een actieplan "Open in Verbinding" opgericht. Dit plan werd eind 2007 unaniem aangenomen door de Tweede Kamer en stelt dat bij ICT-verbouw of nieuwbouw het gebruik van open standaarden verplicht is ("pas toe of leg uit"-beleid). Ook de EU eist een meer uniforme aanpak en integratie van open standaarden binnen ICT projecten (European Interoperability Framework). Heel recent is er ook een brochure "Sturen op Open Standaarden" uitgebracht van het Forum Standaardisatie (onderdeel van Logius, MinBzK), die een handreiking biedt voor het gebruik van open standaarden binnen overheidsorganisaties.

Vele producten op de markt gebruiken nog proprietary protocollen voor het veilig communiceren. Deze producten zijn enkel geschikt voor "veilige" communicatie tussen toestellen met dezelfde oplossing. SecuVOICE is het eerste product die aanstuurt op het gebruik van open standaarden voor veilige communicatie tussen mobiele telefoons. SecuVOICE ondersteunt de open SNS standaard (Sichere Netzübergreifende Sprachkommunikation). SNS is dé open civiele standaard voor end-to-end versleutelde netwerk- en leverancier onafhankelijke spraak (en SMS) communicatie. Deze open standaard is ontwikkeld door de BSI, Secusmart, Rohde & Schwartz en T-Systems en maakt het mogelijk veilig te bellen/sms-en tussen oplossingen van verschillende leveranciers.

SNS ondersteunt zowel een verplichte als een leverancier afhankelijke modus en is compleet netwerk en drager onafhankelijk. SNS biedt ondersteuning voor PSTN, GSM, Tetra en satellietnetwerken voor carriers zoals; CSD, ISDN, 3G/WLAN (VoIP).

Zowel Rohde-Schwartz (TopSec) en Secusmart (SecuVOICE) ondersteunen op dit moment de SNS standaard en geslaagde interoperabiliteitstesten hebben bewezen dat het zeer eenvoudig is om een veilig gesprek op te zetten tussen producten van verschillende leveranciers, zolang zij maar dezelfde standaard ondersteunen.

Interoperabiliteit tussen leveranciers

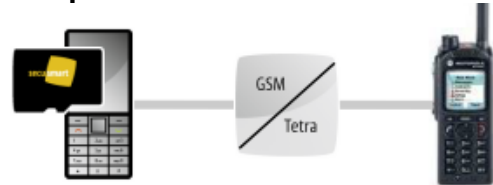


secuVOICE met crypto telefonie/gateways van derden



SecuGATE met gateways van derden

Interoperabiliteit tussen netwerken

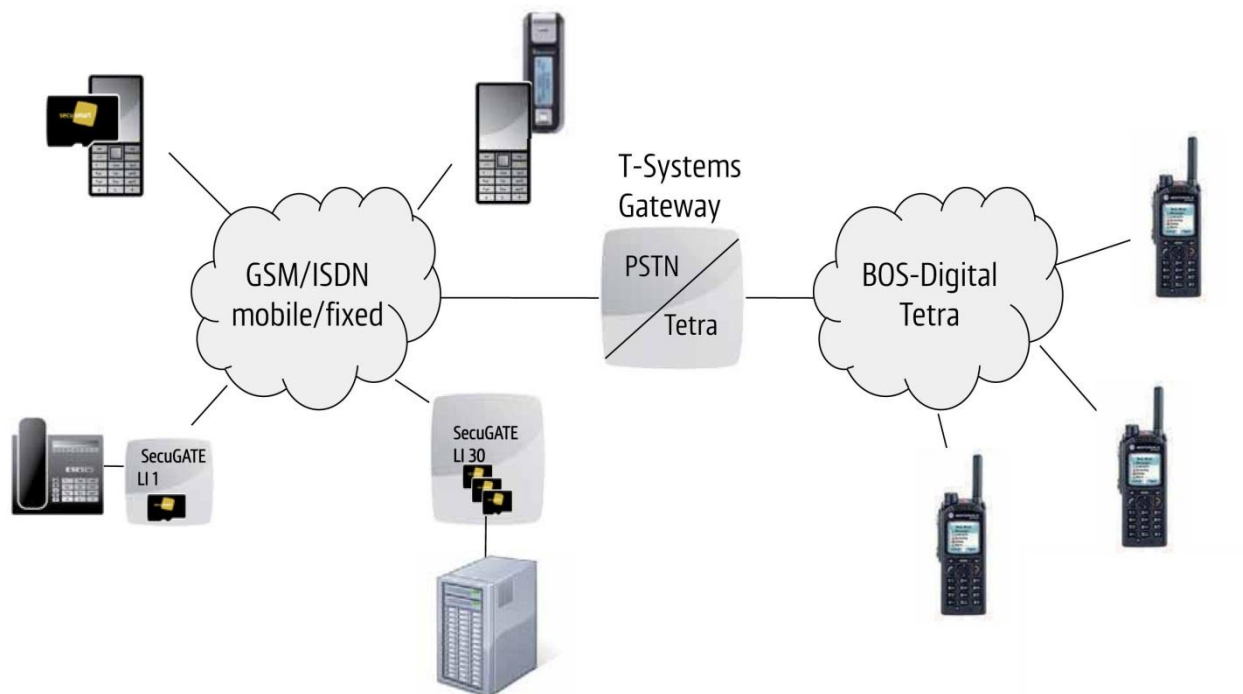


secuVOICE i.c.m. Tetra



3 SecuVOICE en C2000 (Tetra)

Uitbreiding van het C2000 netwerk bij calamiteiten is mogelijk door C2000 portofoons een veilige verbinding op te zetten met mobiele telefoons uitgerust met SecuVOICE. De open SNS standaard is gebaseerd op de BOS-chip (Behörden und Organisationen mit Sicherheitsaufgabe) van de BSI en volgt daarmee de communicatiestandaard in het digitale BOS-netwerk (Tetra). De veilige ontsluiting van het portofoonnetwerk van Tetra met het GSM netwerk (SecuVOICE) en het vaste netwerk (SecuGATE) is daarmee relatief simpel te implementeren, zonder de noodzaak van extra gateways om proprietary oplossingen te koppelen met een Tetra netwerk. Alle producten zoals SecuVOICE, SecuGATE en de Tetra-portofoons ondersteunen dezelfde Tetra-spraakcodec alsook dezelfde cryptografie (BOS). In Duitsland maken politiediensten op dit moment al gebruik van de veilige koppeling en communicatie tussen portofoons in het Tetra-netwerk en mobiele en vaste telefoons met SecuVOICE.



Volledige SNS implementatie in Duitsland



4 De voordelen van SecuVOICE

4.1 Hoog gebruikersgemak

Het gebruik van eigen mobiele telefoons die SecuVOICE ondersteunen is mogelijk en maakt daarmee de aanschaf van nieuwe telefoons overbodig. Na het invoeren van de Secusmart Security Card in het microSD-slot van een standaard mobiele telefoon installeert SecuVOICE zich automatisch op de telefoon. Het opnemen of opzetten van een veilig gesprek is daarna net zo eenvoudig als een gewoon gesprek. Naast het veilig bellen en sms-en kan de telefoon ook als normale mobiele telefoon gebruikt worden. Het installeren van eigen applicaties, zoals navigatie en het voeren van een gebruikelijk gsm-gesprek is vanzelfsprekend nog steeds mogelijk.

4.2 Hoge kwaliteit

Het unieke van SecuVOICE is dat het volledig gebruik maakt van de beschikbare resources op de mobiele telefoon. Zo maakt het gebruik van de dezelfde hardware waarmee standaard gsm-gesprekken gecodeerd worden. De hardware van de Secusmart Security Card versleutelt daarna deze gecodeerde spraak. Dit betekent dat SecuVOICE dezelfde geluidskwaliteit heeft als een gewoon telefoongesprek zonder een extra belasting te vormen voor de telefoon en de energieconsumptie van de telefoon.

4.3 Positieve feedback

Het NBV (Nationaal Bureau voor Verbindingsbeveiliging en onderdeel van de AIVD) heeft in 2010 een quick scan uitgevoerd van verschillende "veilig bellen" producten. Verschillende overheidsorganisaties hebben deelgenomen aan deze uitgebreide test. In het opgestelde rapport kwam SecuVOICE als één van de best geteste producten naar voren en bevestigde daarmee niet alleen het veiligheidsniveau, maar ook het hoge gebruikersgemak en kwaliteit van het product.

Uit de NBV nieuwsbrief van juni 2010:

Quick Scan veilig bellen afgerond

De Quick Scan naar veilig-bellen-applicaties op mobiele telefoontoestellen is afgerond. Het resultaat is gepubliceerd in een rapport. Het NBV wil zowel de veilig-bellen-oplossingen van de firma's Sectra en van Secusmart onderwerpen aan een evaluatie voor het niveau Departementaal Vertrouwelijk. De Sectra Phantom II werkt met Windows Mobile als platform en de Secuvoice met Symbian als platform.

4.4 GSM versus VOIP

De huidige versie SecuVOICE werkt over het GSM/CSD netwerk. Dit is een oplossing die het probleem van het onveilige GSM verkeer echt oplost. CSD heeft een bredere wereldwijde dekking dan een VoIP oplossing. Aanpassingen aan de eigen infrastructuur of het provider netwerk zijn niet nodig. Een veilig gesprek opzetten via het CSD kanaal is zeer eenvoudig, door zoals gewoonlijk naar het standaard 06-nummer van de andere persoon te bellen, zonder de noodzaak van tussenliggende servers of extra aanschaf van licenties en daarmee gemoede onderhoudskosten. Daarnaast is de kwaliteit van CSD, net als bij GSM, gegarandeerd. Veilig bellen via het CSD kanaal heeft een vertraging rond de 1 seconde en ligt daarmee een fractie hoger dan VoIP. Dit wordt doorgaans niet als hinderlijk ervaren.

Medio 2011 komt Secusmart ook met een VoIP oplossing voor in eerste instantie de BlackBerry en Nokia. Later volgen ook meerdere platformen, zoals Android. Deze oplossingen hebben als voordeel dat de vertraging kleiner is en meer bandbreedte ter beschikking hebben voor een nog beter geluidskwaliteit. Daarbij komt wel dat het noodzakelijk is om een licentie voor de tussenliggende SIP-server af te nemen. Alternatief is om deze in eigen beheer te nemen. De telefoons dienen verder continu een 3G/UMTS/GPRS of WIFI verbinding te hebben om een gesprek te kunnen opzetten. Door de veel beperktere dekking van



3G, zowel binnen als buiten, kan dit problemen geven. Daarbij moet er op gelet worden dat men vaak hogere kosten maakt voor bellen via VoIP in zowel binnen- als buitenland. Verder is de kwaliteit van de verbinding niet - net als bij GSM - gegarandeerd.

4.5 Lage Total Cost of Ownership (TCO) en beheerkosten

Voor het versleuteld bellen over het GSM/CSD netwerk is het niet nodig extra (centrale) services te draaien voor het opzetten van een gesprek. Een gesprek via CSD wordt direct gerouteerd over het provider netwerk, ongeacht de locatie. Het beheer van een tussenliggende SIP (bij VoIP oplossingen) of management server is niet noodzakelijk. Voor het opzetten van een gesprek is alleen een telefoon met een Secusmart Security Card nodig. Indien een telefoon beschadigt of defect is en een nieuwe telefoon noodzakelijk is, is het plaatsen van de microSD smartcard in de nieuwe telefoon voldoende en werkt meteen. Tussenkost van de ICT-afdeling is niet noodzakelijk. Kortom deze oplossing is zeer vriendelijk in gebruik voor zowel de gebruiker als de organisatie met nauwelijks beheerlasten, incidenten wat resulteert in een zeer lage TCO.

4.6 Veilig

Naast het voeren van veilige gesprekken alsmede het versturen van veilige SMSjes, zijn alle contacten en SMSjes op het toestel veilig opgeslagen op de Secusmart Security Card. SecuVOICE identificeert de gebruiker niet aan de hand van het telefoonnummer, maar aan de hand van een unieke fingerprint, opgeslagen op het certificaat. Op deze manier is er een effectieve maatregel tegen misbruik van 'gespoofde' telefoonnummers. Indien dezelfde persoon belt met een ander telefoonnummer, omdat deze van SIM is veranderd, wordt dit netjes weergegeven tijdens het bellen. Verder blijft er geen spoor op de telefoon achter na het verwijderen van de microSD-smartcard.

4.7 Verlies of diefstal

De Secusmart Security Card is beveiligd met een pincode, waardoor bij verlies of diefstal de risico's tot een minimum beperkt blijven. Na het 5x invullen van de verkeerde pincode, blokkeert de kaart zichzelf en is daarna onbruikbaar. (Activeren kan daarna alleen met de geleverde PUK code.) Daarbovenop is het aan te bevelen om een toestel in de basis te voorzien van de nodige security maatregelen, zoals het automatisch locken, versleuteling van de data op het toestel, of remote wipen van overige "niet SecuVOICE" gerelateerde gegevens.

4.8 SNS

SNS is de enige standaard die specifiek ontwikkelt is voor een veilige communicatie tussen mobiele telefoons en geschikt is voor implementatie op een mobiele telefoon. Het is mogelijk om met SecuVOICE veilig te bellen met producten van andere fabrikanten (zoals Rohde-Schwarz), mits zij ook deze standaard ondersteunen.

4.9 Goedkeuringen

SecuVOICE is uniek door naast een Common Criteria EAL5+ certificering ook als enig product een goedkeuring te hebben in Duitsland voor gebruik tot het niveau NfD (Verschlussache-Nur für Dienstgebrauch), vergelijkbaar met Departementaal Vertrouwelijk. De Nederlandse goedkeuring is in april 2011 ontvangen.

4.10 Volwassenheid

SecuVOICE is al enkele jaren op de markt verkrijgbaar en wordt al lange tijd geleverd aan klanten, waaronder een aantal grote ministeries in Duitsland. Het product is een kant-en-klaar product die zich al enige jaren heeft bewezen, wat ook blijkt uit de recent uitgevoerde NBV quick scan.

4.11 Grote klantenkring

Vooral in Duitsland heeft SecuVOICE een grote groep gebruikers, waaronder de federale overheid. Zij hebben op dit moment enkele duizenden gebruikers van SecuVOICE en is daarmee de de-facto standaard binnen de Duitse overheid. Naast Duitsland wordt SecuVOICE uitvoerig gebruikt in Nederland en andere Europese landen.



5 Ondersteunde toestellen



6210



6220



E51



E63



E66



E71



E75



N78



N79



N81



N82



N85



N86



N95



N97



5228



E90



5230



5230 Nuron





5235



5250



5530



5800



C6-00



N97



N97 Mini



5730

Een actueel overzicht van meest recent ondersteunde toestellen staat op:
<http://www.secusmart.com/en/secusuite/mobile-telephones/mobiletelephones1.html>

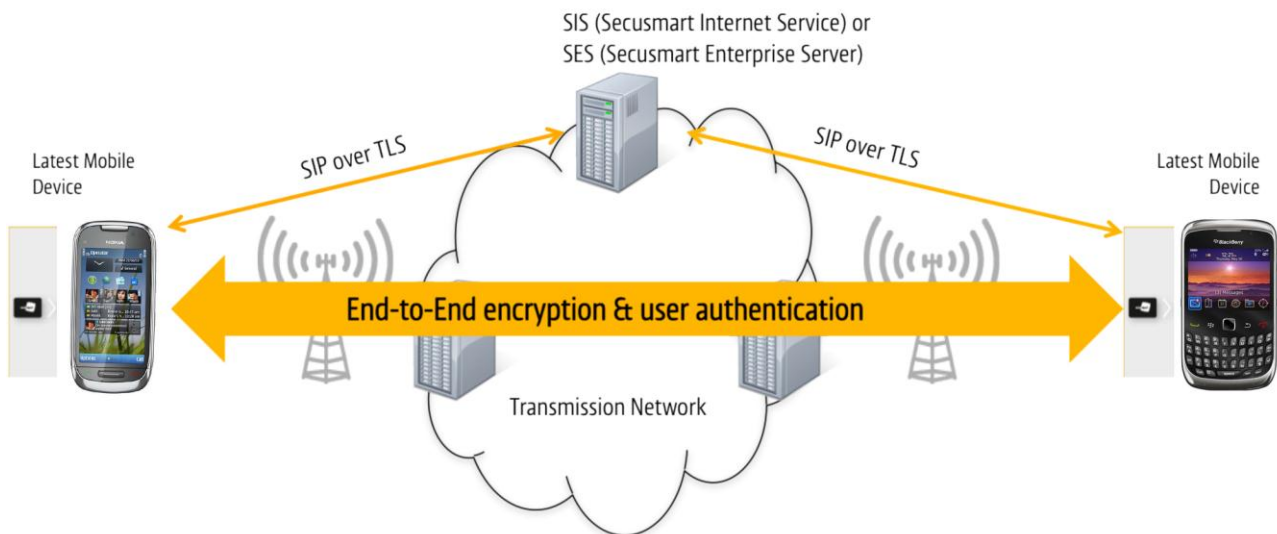


6 SecuVOICE VoIP / BlackBerry

SecuVOICE voor BlackBerry werd op de CeBIT 2011 gelanceerd en zal naar verwachting medio dit jaar op de markt verschijnen. Dit product zal ondersteuning krijgen van SNS in combinatie met VoIP. Tevens zal rond die tijd SecuVOICE voor Nokia ondersteuning krijgen voor VoIP. Beide oplossingen bieden dezelfde beveiliging voor spraak en SMS als de huidige SecuVOICE SNS oplossing via GSM. Het hart van de beveiliging vormt de Secusmart Security Card. Met ondersteuning van VoIP voor zowel Nokia als BlackBerry is het mogelijk een veilig gesprek tussen beide telefoons op te zetten. Ondersteuning van VoIP betekent wel dat een SIP server noodzakelijk is voor het opzetten van een beveiligd gesprek. Dit kan een standaard SIP server zijn, maar ook een speciale SecuVOICE SIP-server met extra beveiligingsmaatregelen. De server kan zowel centraal als binnen de organisatie gehost worden.

Belangrijkste eigenschappen

- High Security End-to-End versleuteling van telefoongesprekken op de laatste smartphone modellen;
- Geheime sleutel verlaat nooit de beveiligde hardware (Secusmart Security Card);
- Future-proof door IP gebaseerde communicatie;
- Netwerk onafhankelijk (WLAN, HSPA, UMTS);
- Ondersteuning voor RIM BlackBerry;
- Compatible met een breed scala van mobile apparaten van diverse producenten;
- Zeer goede geluidskwaliteit;
- Voorbereid op goedkeuring door de autoriteiten;
- Makkelijk te installeren en te gebruiken.

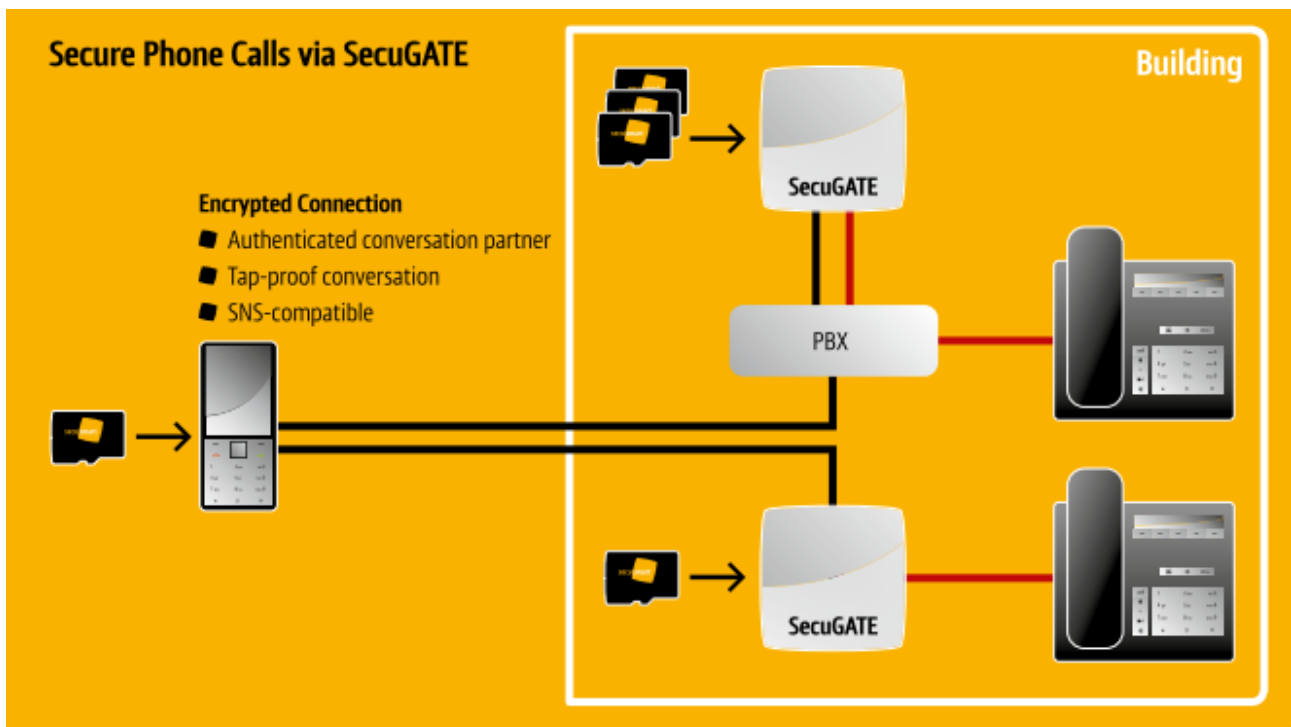


Wanneer de klant op het moment van beschikbaarheid van de huidige Nokia oplossing van SecuVOICE met ondersteuning voor GSM/CSD wenst over te gaan naar de aankomende BlackBerry/VoIP oplossing, kan Fox-IT hiervoor een upgrade uitvoeren. Om dit te realiseren is naast een manuele software upgrade op de Secusmart Security Card ook de aanschaf, dan wel een licentie van een SIP server noodzakelijk.



7 SecuGATE

Naast een oplossing voor veilige communicatie tussen mobiele telefoons levert Secusmart ook een oplossing voor veilige communicatie naar vaste, op dit moment alleen ISDN lijnen. De SecuGATE versleutelt direct de spraak op de vaste lijn, waarmee u in staat bent veilig te bellen tussen vaste lijnen maar ook van vast naar mobiel en vice versa. Een speciale telefoon is hierbij niet noodzakelijk. Het ontsluiten van 1 vaste telefoon is mogelijk met de SecuGATE LI 1 of 4 tegelijk (SecuGATE LI 4). Verder komt er een Enterprise versie beschikbaar van de SecuGATE, de LI 30. Deze kan tegelijkertijd 30 versleutelde verbindingen ontsluiten. De SecuGATE is direct verbonden aan de PBX centrale van de organisatie. Het is hiermee ook mogelijk groeps gesprekken op te zetten tussen meerdere gebruikers, vast of mobiel uitgerust met SecuVOICE, of producten die compatibel zijn met de SNS standaard. In een later stadium zal de SecuGATE naast ISDN ook VoIP ondersteunen.



8 Samenwerking Secusmart en secunet

In 2009 is een samenwerking aangekondigd tussen secunet Security Networks en Secusmart om kennis uit te wisselen en samen te werken voor toekomstige oplossingen. secunet staat bekend als leverancier van SINA VPN apparatuur voor het versleuteld versturen van data voor de niveaus Stg. Confidentieel en Stg. Geheim. Deze apparatuur wordt door Fox-IT aan de Nederlandse overheid geleverd ter bescherming van staatsgeheimen.

De samenwerking heeft tot nu toe een eerste prototype opgeleverd van een op IP/Sec gebaseerde VPN oplossing (IKE v.2, ESP). Aan de mobiele zijde is hiervoor ESP (Encapsulating Security Payload) beveiligd met de cryptografische eigenschappen van de Secusmart Security Card en aan de SINA zijde doormiddel van een MKK Card. Secusmart gebruikte voor deze opstelling de Nokia S60 met ingebouwde VPN en de SINA Box S van secunet.

