1. INLEIDING

De Philips Secure Telephone Set is een standaard telefoontoestel met een geïntegreerde high-grade digitale crypto-eenheid.

Met dit toestel is het mogelijk - naar keuze - een beveiligde of niet-beveiligde (normale) verbinding op te bouwen via het openbare telefoonnet.

Het toestel kent de volgende full-duplex communicatie-modes:

- niet-vercijferde spraak (normale verbinding);
- vercijferde spraak;
- vercijferde data (conform V.24/RS232-C).

De Secure Telephone Set is voorzien van een Key Card Reader.
Gebruik van het toestel als vercijferapparaat is alleen mogelijk nadat hierin een geldigee Personal Key Card (smart card [1]) is aangebracht en vervolgens de bijbehorende geldige Identificatie-code is ingetoetst.

De Secure Telephone Set is bestemd voor 'desktop'-gebruik.

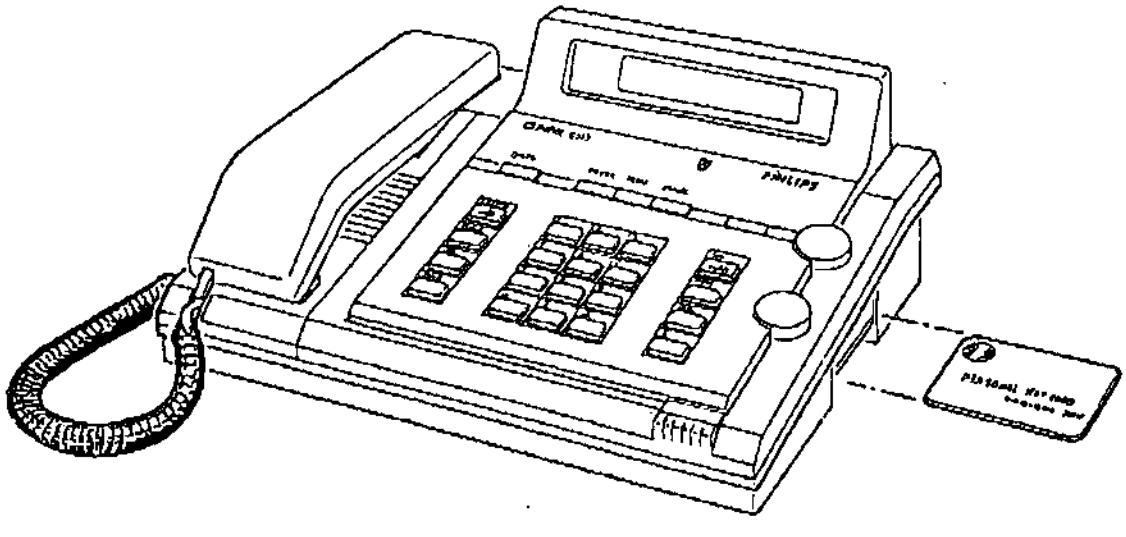


Fig. 1: Philips Secure Telephone Set PNVX

[1] Innovatron S.A. Licence

2. SPECIFICATIES

2.1 Cryptografische specificatie

2.1.1 Vercijfering/ontcijfering

• Principe	Stream cipher met niet-lineaire mixer voor waarborgen van data integriteit
• Sleutellengte	128 bits
• Mogelijk aantal verschillende sleutels	$> 10^{38}$
• Cycluslengte	> 1.000.000 jaar
• Algoritme	Ontwerp Philips Crypto B.V.

2.1.2 Key management

• Key management systeem	Matrix-systeem voor unieke paren end-to-end sleutels
• Max. grootte gebruikersgroep	K4: ± 100.000 gebruikers K3: K3A ± 128 gebruikers; K3B ± 170 gebruikers
• Sleutelopslag	Vercijferd op separate Key Card
• Sleutelselectie	Automatisch Generatie van random sleutel voor elk gesprek (Session key)
• Gebruikers-authorisatie check	Door: 1) Verificatie ingevoerde Identificatie-code 2) Verificatie Key Card
• Peer entity authenticatie	Tijdens de sleutelselectie wordt wederzijds nagegaan of de andere partij inderdaad degene is voor wie hij/zij zich uitgeeft

2.1.3 Synchronisatie

• Methode	Door middel van een random opgewekte berichtensleutel
• Lengte berichtensleutel	Max. 88 bits

2.1.4 Zeroize

• Actief wissen van sleutels	Via Master- of Crypto-installatie menu of door een interactieve 2-knops bediening

2.2 Elektrische specificatie

2.2.1 Elektrische signalen

• Lijnaansluiting	Conform de Nederlandse PTT-eisen, vastgelegd in T10 - T11
• Kiesinformatie-signalen	Via de programma-functie van het toestel (menu) in te stellen op kiespuls of TDK (toon-druktoets-keuze)
• Lijnsignalen tijdens crypto-bedrijf	- 2400 bits/s full duplex vlgs. CCITT - V.22bis
• Aansluiting data-terminal	- Conform EIA - RS232-C/ CCITT - V.24 - Data-rate: 2400 bits/s synchroon ≤ 600 bits/s asynchroon
• Monitor-aansluiting (recorder)	Analoog telefoonsignaal: - output: 150 mV (onbelast) bij 50 mV-eff, 800 Hz op microfoon-ingang van de hoorn - impedantie: 150 Ω
• Analoog-digitaal-omzetting	- Middels een LPC-10 vocoder - Data-rate: 2400 bits/s - Verstaanbaarheid ≥ 82 % DRT (back-to-back) vlgs. IZF 1982-13 (Testrapport IZF 1990-C8)
• Luidspreker-signaal	- Weksignaal: volume met potentiometer regelbaar van max. tot - 20 dB - Spraaksignaal-volume: max 200 mW, met potentiometer regelbaar tot - 20 dB - Waarschuwings-signalen: bij omschakelen van "PLAIN" naar "CRYPTO" en vice versa bij omschakelen van "VOICE" naar "DATA" en vice versa bij een foutieve bedienings-handeling.

■ Data/voice-switch

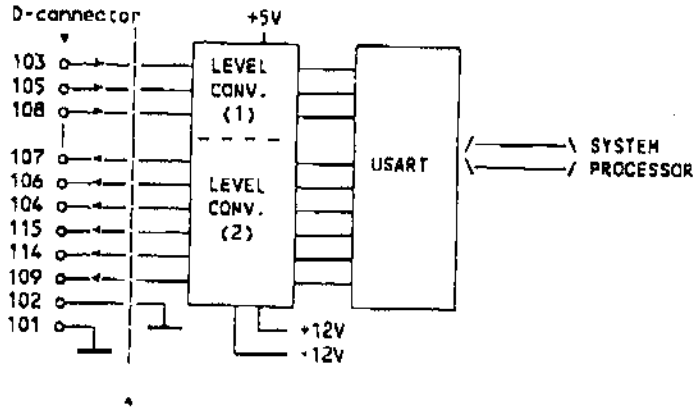
De firmware bepaalt welke van de beide bronnen, nl. vocoder of data-aansluiting, wordt vrijgegeven. De data vanuit de vrijgegeven bron wordt voor verwerking aan de crypto unit overgedragen.

■ RS232-C-/V.24 interface

Dit circuit (zie fig. 6) verzorgt de interfacing tussen de terminal-aansluiting en het bus systeem (signalen en niveaus zijn conform CCITT V.24/V.28).

De input-signalen worden geconverteerd naar HCMOS-niveau door level-converter 1 (receiver).
De output-signalen worden geconverteerd naar het juiste niveau door level-converter 2 (driver).

De interface tussen de level-converters enerzijds en de System Processor anderzijds wordt gevormd door een USART.



cct	pin	betekenis
103	2	Data Input (TxD)
105	4	Request To Send (RTS)
108	20	Data Terminal Ready
107	6	Data Set Ready
106	5	Clear To Send
104	3	Data Output (RxD)
115	17	Receive Clock
114	15	Transmit Clock
109	8	Received line signal detect
102	7	Digital Ground (on PCB)
101	1	Protection Ground (case)

DTE - DCE
(PC) (PNVX)

Fig. 6: RS232-C/CCITT V.24 interface

■ Key-Card-interface

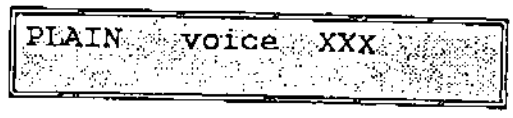
De Key Card interface zorgt voor de aanwezigheids-detectie van de Personal Key Card en maakt het uitwisselen van Identificatie-code en sleutel-informatie met die Personal Key Card mogelijk. De Personal Key Card kan zo de juistheid van de door de gebruiker ingetoetste Identificatie-code controleren.

6.1 Start vanuit een plain of crypto spraak verbinding

Een crypto data verbinding kan vanuit een plain of crypto spraak verbinding worden opgebouwd. Beide abonnees kunnen het initiatief nemen om over te gaan naar een crypto data verbinding.

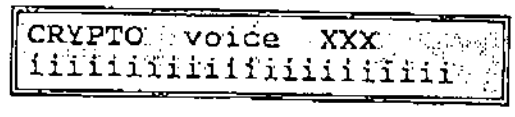
Opmerking:
Het data-apparaat van beide abonnees moet aangesloten en gereed zijn om te ontvangen/zenden.

Toestel in plain spraak mode;
XXX = LSP of HFR

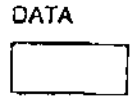


of

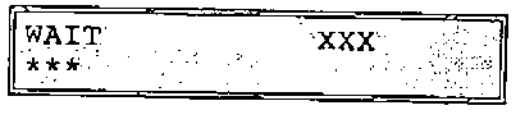
Toestel in crypto spraak mode;
i..i = identiteit van de gesprekspartner



Druk toets DATA
(Eén van de beide abonnees)



Begin van crypto data synchronisatie;
Wacht op de melding "CRYPTO data"



Akoestisch signaal geeft aan dat het toestel overschakelt naar de crypto data mode

Toestel in crypto data mode

Opmerking:
De hoorn heeft in de crypto data mode geen functie en mag tijdens de data communicatie op de haak gelegd worden.

6.2 Terug naar een crypto spraak verbinding

Het initiatief om vanuit een crypto data verbinding terug te gaan naar een crypto spraak verbinding kan door beide abonnees genomen worden.

Toestel in crypto data mode;
i..i = identiteit van de gesprekspartner

Indien nodig, neem de hoorn van de haak
(Geldt voor beide abonnees)

Opmerking:
Indien de gesprekspartner de hoorn op de haak laat liggen, dan zal na indrukken van de toets CRYPTO de verbinding verbroken worden !

Druk toets CRYPTO
(Eén van beide abonnees)

Begin van crypto spraak synchronisatie;
Wacht op de melding "CRYPTO voice"

Akoestisch signaal geeft aan dat het toestel overschakelt naar de crypto spraak mode

Toestel in crypto spraak mode;
i..i = identiteit van de gesprekspartner

6.3 Terug naar een plain spraak verbinding

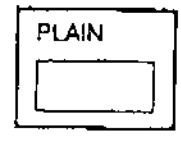
Het initiatief om vanuit een crypto data verbinding terug te gaan naar een plain spraak verbinding kan door beide abonnees genomen worden.

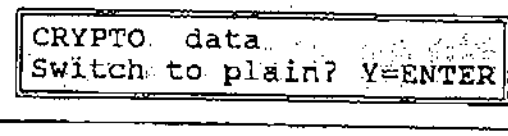
Toestel in crypto data mode;
i..i = identiteit van de gesprekspartner

Indien nodig, neem de hoorn van de haak
(Geldt voor beide abonnees)

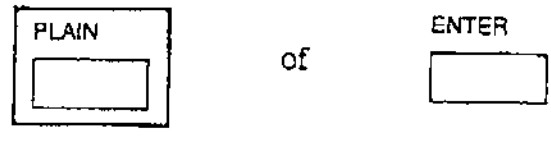
Opmerking:
Indien de gesprekspartner de hoorn op de haak laat liggen, dan zal na indrukken van de toetsen PLAIN en PLAIN/ENTER de verbinding verbroken worden !

Druk toets PLAIN
(Eén van beide abonnees)





Wilt u werkelijk terug naar een plain spraak verbinding, dan:
Druk toets PLAIN of ENTER
(binnen 10 seconden)

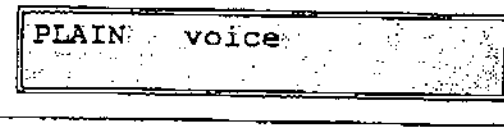


Zo niet:
Druk willekeurige andere toets

In de display van de gesprekspartner verschijnt "Press PLAIN !". Deze dient nu ook toets PLAIN in te drukken.

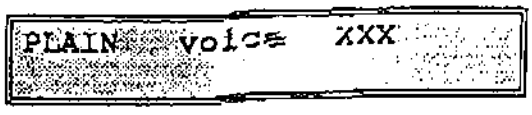
Akoestisch signaal geeft aan dat het toestel overschakelt naar de plain spraak mode

Toestel in plain spraak mode



7.1 Memo-functie

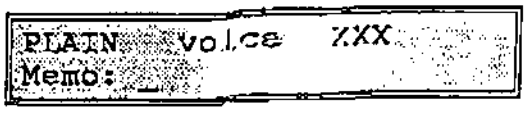
Indien u tijdens een plain spraak verbinding een nummer moet onthouden, b.v. het volgende telefoonnummer dat u wilt gaan kiezen, dan kunt u dit nummer m.b.v de memo-functie opslaan in het toestel.



Toestel in plain spraak mode;
XXX = LSP of HFR

ENTER

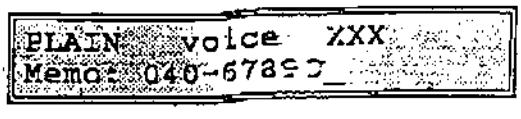
Om de memo-functie te activeren
Druk toets ENTER



Memo-functie is actief
Toets gewenste telefoonnummer in, b.v. 040-67890

Druk toets MUTE wanneer een pauze (streepje in display) gewenst is tussen b.v. kengetal en abonneenummer

De ingevoerde cijfers kunnen worden gewist met toets ←—



ENTER

Om de memo-functie te beëindigen
Druk toets ENTER

Na het beëindigen van het gesprek kunt u de hoorn van de haak nemen en op toets DIAL drukken om het opgeslagen nummer direct te kiezen (zie paragraaf 5.2).