EUROPEAN UNION
THE COUNCIL

Brussels, 14 January 1998

5246/98

LIMITE

ENFOPOL 5

NOTE

from : Netherlands delegation

to : Police Cooperation Group

No. prev. doc. : 11075/1/97 ENFOPOL 196 REV 1

Subject : **Cryptography law and regulations**
- **replies to questionnaire 9766/97 ENFOPOL 167 on Trusted Third Parties (TTPs)**

The replies to the questionnaire on Trusted Third Parties, up till now twelve member states responded, are presented in the annexed matrix. From this matrix the following draft conclusions could be derived:

1. General cryptography policy.

1.1. There is, except for two member states, no general policy regarding the use of cryptography by members of the public and companies.

1.2. In most of the member states however a policy is being developed or under consideration.

1.3. Except for two member states there are no regulations regarding the use of cryptography by members of the public and companies.

1.4. Generally spoken, except for one member state, there are no requirements set for the cryptography or the regulations concerning cryptography rom a crime detection and state security viewpoint.

2. Use of TTP services.

2.1. Only three member states replied that the development of a TTP structure in the market sector is or was encouraged by the government.

2.2. Four member states replied that the use of TTP services is considered for either the Certification of Electronic Transactions Services, providers of cryptographic services, certification services or private companies and internet providers.

2.3. In four member states TTPs are operating.

2.4. No experience, so far, has been gained of these TTPs from a crime detection and state security viewpoint.

2.5. Except for three member states, where the requirements set for TTPs from a crime detection or state security viewpoint is under discussion, the general response was that no requirements were set.

3. Key recovery.

3.1. Except for one country where it is under discussion and three other member states where there is a certain qualification to put forward a request, the majority of the replies showed that crime detection services are not authorised to oblige members of the public or companies to surrender the keys of encrypted messages.

3.2. In five member states such obligations are however being considered or developed.

3.3. The replies of six member states to the questionnaire, showed that in three countries crime detection services are not authorised to oblige members of the public or companies to decode encrypted messages.

3.4. In the replies of eight member states it was found that this also applies to the suspect.

3.5. In eight member states state security services are not authorised to oblige members of the public or companies to surrender the keys of encrypted messages to crime detection or state security services.

3.6. In six member states this is being considered.

3.7. In seven member states state security services are not authorised to oblige members of the public or companies to decode encrypted messages.

Further Action.

Before taking the work forward, the Netherlands delegation invites the Police Co-operation Working Group to agree on the abovementioned draft-conclusions and underline that "recommendations" in the field of TTPs could be necessary.

ENFOPOL 196 REV 1
Cryptography law and regulations
** Replies to questionnaire on Trusted Third Parties (TTPs)*

		SP	UK	DENM	LUX	SW	IT	NETH	FR	GREECE	IRELAND
1.	General cryptography policy										
1.1	Does your country have a general policy regarding the use of cryptography by members of the public and companies?	yes regarding companies	no	no	no	no	no	no	yes members of the public & companies	no	no
1.2	If not, is such a policy being developed?	yes regarding members of the public	yes regarding companies Interd. disc.	yes, for members of the public & companies	under discussion	yes. for members of the public & companies	no	under discussion		no	no
1.3	In a general sense, are there regulations regarding the use of cryptography by members of the public and companies?	yes, for members of the public & companies	no	no	no	no	no	no, apart from export regulations	yes, for members of the pubi & companies in telecom regulations	no	no
1.4	Are requirements set for the cryptography or the regulations concerning cryptography from a crime detection and state security viewpoint?	no	no	no	(yes)	no	(yes)	no	yes	no	no
2.	**Use of TTP services**										
2.1	Is or was the development of a TTP structure in the market sector encouraged by the government?	yes	Government policy is under consi-deration	yes	no	no	no	consultant investigates government & market needs	yes	yes	no
2.2	If so, for which category of TTPs is this considered?	for certification of electronic transaction services	providers of crypthogr. services	for certificat. authorities				no		private companies & internet providers	

		SP	UK	DENM	LUX	SW	IT	NETH	FR	GREECE	IRELAND
2.3	Are TTPs operating in your country?	no, but under consideration	yes	yes	no	no		yes, e.g. keymail	no	yes	no
2.4	Which services are provided by those TTPs?	certification key recovery confident. data integrity authentication	pilot certification projects	pilot certification projects				pilot certification projects	key recovery	acces & support services in the Internet field	
2.5	Has experience been gained of these TTPs from a crime detection and state security viewpoint?	no	no	no	no			no	no	no	no
2.6	Are or were requirements set for TTPs from a crime detection or state security viewpoint?	no	discussion	discussion	no	discussion		no	no	no requirem. laid down	no
2.7 & 2.8	If so, which requirements are set for TTPs from a crime detection and state security viewpoint? Which requirements are under discussion?	the articles 49 & 52 (Bill of Telecomm.)	licensing TTPS	certificates for confident. under discussion				see enfopol 196 REV 1			
2.9	Which governmental authorities are responsable for development and policy forming concerning TTPs?	Inform. techn. superior council	Interdepart.	ministry of research	minister of state & minister of communic.	ministry of foreign affairs		ministry of Transport in co-operation with ministry of Economic Aff.	prime minister office		
3.	Key recovery										
3.1	Are crime detection services authorised to oblige members of the public or companies to surrender the keys of encrypted messages (possibly via third parties) to crime detection or state security services?	under discussion	police in certain circumst.	no	no	no	no	yes, agencies are qualified to request	yes, agenc. are qualified to request	no	no
3.2	Are such obligations being considered or developed?	yes	yes	no	no	yes		yes	yes	no	no

		SP	UK	DENM	LUX	SW	IT	NETH	FR	GREECE	IRELAND
3.3	Are crime detection services authorised to oblige members of the public or companies to decode encrypted messages (deliver as plain text)?	under discussion	court may order	no	no	crime detection services	no	no	yes	no	no
3.4	Do the obligations mentioned above also apply to the suspect?	under discussion	no	no	no	no	no	no	yes	no	no
3.5	Are state security services authorised to oblige members of the public or companies to surrender the keys of encrypted messages (possibly via third parties) to crime detection or state security services?	under discussion	no	no	no	no	no	no	yes	no	no
3.6	Are such obligations being considered or developed?	yes for stored data & data traffic	yes	no	under consideration	yes for stored data & data traffic		yes, considered for stored data & data traffic	yes	no	no
3.7	Are state security services authorised to oblige members of the public or companies to decode encrypted messages (deliver as plain text)?	under discussion	no	no	no	security services authorised	no	no	yes	no	no

The replies of Germany and Austria are, for the moment, negative. Internal discussions have not been finalised yet.