40791 / EU XX. GP

EUROPÄISCHE UNION
DER RAT

Brüssel, den 27. November 1997 (09.12)
(OR.en)

12787/97

LIMITE

ENFOPOL 229

AUFZEICHNUNG

der britischen Delegation

für die Gruppe "Polizeiliche Zusammenarbeit"

Nr. Vordokument: 6005/97 ENFOPOL 12, ABl. Nr. C 329 vom 4.11.1996, S. 1

Betr.: **Überwachung des Fernmeldeverkehrs**
- Internationale Anforderungen für den rechtmäßigen Zugriff auf Kryptographiedienste

Diese Anforderungen

- unterliegen nationalem Recht und sollten gemäß den geltenden nationalen Prinzipien ausgelegt werden,

- gelten für die Anbieter von Kryptographiediensten,

- erstrecken sich nicht auf den ursprünglichen rechtmäßigen Zugriff auf die verschlüsselten Daten, der mit den unterschiedlichsten Methoden hergestellt werden kann; andere Anforderungen - wie z.B. die internationalen Benutzeranforderungen (IUR) für die rechtmäßige Überwachung des Fernmeldeverkehrs [1] - sind anwendbar.

Anforderungen

1. **Einholung von Dienstinformationen** Auf der Grundlage einer rechtmäßigen Anfrage und bei einer gegebenen Kennung der Zielperson oder anderer Informationen zur Zielperson bzw. verschlüsselter Daten mit diesbezüglichen Informationen ist den Strafverfolgungsbehörden folgendes zur Verfügung zu stellen: (1) Detaillierte Angaben zur Zielperson, einschließlich der Dienstnummer, (2) Informationen, die die von der Zielperson genutzten Kryptographiedienste umfassend identifizieren und (3) die technischen Parameter der Kryptographiemethode.

(1) im Amtsblatt Nr. C 329 vom 4.11.1996, S. 1 veröffentlicht.

Entschlüsselung, Rechtzeitigkeit und Verfügbarkeit: Die Strafverfolgungsbehörden benötigen so rasch wie möglich (in dringenden Fällen innerhalb weniger Stunden oder Minuten) Zugriff auf die entschlüsselte Nachricht. Dies kann im Wege der Bereitstellung des Schlüsselmaterials und aller notwendigen Informationen zur Entschlüsselung der Daten oder durch Bereitstellung der Daten in Klarform geschehen. Die EDV-technischen und operativen Bemühungen, die eine Strafverfolgungsbehörde für die Erlangung der entschlüsselten Botschaft aufwenden muß, sollten sich auf ein Minimum beschränken, damit die Effizienz, Wirtschaftlichkeit und Zeitnähe der Operation sichergestellt ist.

2.2. Der Zugriff auf die entschlüsselte Nachricht im Sinne von Nummer 2.1 muß für diejenigen Verschlüsselungssysteme möglich sein, die sowohl für den nationalen als auch den internationalen Betrieb geeignet sind.

3.1. **Sicherheit und Integrität:** Für die Strafverfolgungsbehörden ist es wichtig, daß der Entschlüsselungsvorgang so konzipiert und durchgeführt wird, daß eine unbefugte oder unsachgemäße Verwendung ausgeschlossen ist und Informationen mit Bezug auf den Vorgang geschützt sind.

3.2. Wird Schlüsselmaterial zur Verfügung gestellt, so hat dies in elektronischer Form oder in einer anderen vereinbarten Form unter Verwendung eines sicheren Übermittlungswegs zu geschehen. Letzterer muß geschützt werden, um die Authentizität, die Integrität und die Vertraulichkeit solchen Materials sicherzustellen und um zu gewährleisten, daß es auf akzeptable Weise bereitgestellt wird.

3.3. Das Schlüsselmaterial oder die Daten in Klarform dürfen nur der in der Anordnung genannten Behörde übermittelt werden.

3.4. Die Strafverfolgungsbehörden müssen sich darauf verlassen können, daß die Anbieter von Kryptographiediensten der Zielperson oder etwaigen Dritten (1) die Zielperson, die Gegenstand der Anordnung ist, (2) den Umstand, daß Schlüsselmaterial oder Daten in Klarform geliefert worden sind und (3) Informationen über die Art der Durchführung der Operation nicht offenlegen.

4. **Überprüfung:** Nach Maßgabe des nationalen Rechts können Anbieter verpflichtet werden, ordnungsgemäß geschützte Aufzeichnungen über die Bereitstellung von Schlüsselmaterial und Daten zu führen.