

The Right to Encryption

Ministry of Research and Information Technology

IT- Security Council

PRESS RELEASE

11th June 1996

The right to encryption

The Government's Information Technology Security Council recommends that no limitations on the right of the individual to encrypt electronic communications should be introduced. In consequence, the Council has recommended that the authorities should not be granted the opportunity - through a court order - to intercept any communication encrypted by means of the citizen's card, which is soon to be introduced. This statement was issued by the Chairman of the Security Council, Professor Mads Bryde Andersen LLD after Monday's meeting of the Council.

As part of the work involved in a review of the Danish IT security policy in general, the IT Security Council has been dealing with the presentation of the central problem to do with encryption - that is to say, the coding technique, which is able to prevent unauthorised persons gaining access to electronic information. A unanimous IT Security Council has reached the above conclusion on encryption, though the Council's three members from the Ministries of Commerce, Justice and Research and Information Technology have expressed reservations on the grounds that the Government has not yet committed itself.

It is only in one particular area that the IT Security Council proposes an intervention in the right to encryption, reveals Mads Bryde Andersen: Telecommunications companies, which introduce encryption as an integral part of their services, for instance in connection with ordinary telephony, shall be able - through a court order - to decrypt, i.e. decode, a communication. "In this way, the obligation which telecommunications companies are currently under to contribute to intercepting in connection with police investigations into serious crime is carried a step further", Mads Bryde Andersen emphasises and adds, "The proposal does not, however, place any limitations on the communicating parties' opportunities for personally encrypting communications. But the rule will enjoin the telecommunications companies to provide the opportunities for intercepting in pursuance of a court order, so that those problems

that have been evident within the GSM network can be avoided".

Encryption is an essential security element in electronic communication, for example in connection with home-banking on the Internet and public self-service systems as well as with electronic trading and money transfer between business enterprises.

The spread of encryption has, however, created problems for the authorities, since encryption normally precludes the police from intercepting in the course of crime investigations. Only in the event that the police are ensured access to keys used in encryption, for instance by the keys being stored in a central register to which the police has access, can encrypted communications be intercepted.

In consequence, all over the world authorities have raised the question of whether the right to make use of encryption ought to be subject to restrictions so that the police force and intelligence staff can continue to have the possibility of carrying out legal intercepting.

In most countries there is free access to the utilisation of encryption, though a few countries are insisting on restrictions in the opportunities for utilising encryption. In France, encryption is prohibited in principle, while in the USA attempts have been made to introduce a voluntary national encryption standard, which will provide the authorities with the opportunities for breaking the encryption.

"In the question of encryption, we are in the position of trying to balance two fundamentally different interests in a community founded on the rule of law, i.e. the individual's interest in safe and inviolable communication as opposed to the considerations of legitimate opportunities for intelligence investigation", points out Mads Bryde Andersen and continues, "The decisive factors in the Council's adoption of a position have been partly that any prohibition against or radical regulation of encryption at the present time is in reality an illusion, since anyone can quite easily find and use the tools for efficient encryption via Internet".

For further information:

IT Security Council Chairman: Professor Mads Bryde Andersen LL.D,
tel: +45 35 323133 or mobile tel: 4048 0925, Internet:

PRIVATE HREF="mailto:lawmads@pc.ibt.dk" MACROBUTTON
HtmlResAnchor lawmads@pc.ibt.dk .

Appendix:

IT Security Council terms of reference and composition

IT SECURITY COUNCIL

1. Terms of reference

The IT Security Council shall offer the government and the Ministry of Research the highest quality of specialist advice within the field of IT security and shall attempt to advance a qualified public debate on IT security. IT security shall contribute to the formulation of an overall Danish security policy for the utilisation of IT and telecommunications.

The Council shall point out the human and social risks and interests, to which modern information technology gives rise. The Council shall also present its recommendations on how best these risks can be countered and how conflicting interests in the field of IT security can be offset.

Furthermore, the IT Security Council shall formulate a plan for the means by which data can be optimally protected against a breach of confidence, for example through the use of electronic signatures and encryption.

The Council manifests itself through statements, which either are presented on its own initiative or on request from the Danish Government and/or the Ministry of Research.

2. Composition

Chairman of the Council

Ä à

˘

’Öú. òó+,Æ0 ¿ H P h p \ x

ê ‰ - Kommunedata I/S \ 1

- TheRighttoencryption
Word

Microsoft

Document MSWordDoc Word.Document.6
h ẽ + ≥ Ÿ 0 İ ê ò Π f < \ Ë

Microsoft
t Ä ®

¥
¿ Ã ‘ < %o %o - The Right to encryption - »F -
Keld Poulsen - @ - I <META HTTP-EQUIV="Content-Type"
CONTENT="text/html; charset=ISO-8859-1"> fC - Track 1
Poul ñ ò ô Ê ? ~ 3 Cîĩîĩ 3ï y

Keld Poulsen&C:\Dokumenter\noglecenter\RSA_fsk.doc

Layne Kaplan5C:\My Documents\RSA'97\Day 2\Track 1 Poulsen
word.doc^ Ué ~ ~ ' ~ `:

AutoOpen AUTOOPEN @HP LaserJet

4 \\Server\hp4m HPPCL5MS HP LaserJet 4 HP LaserJet

4 ^ @ g X X @MSUDNHPLaserJet

4 %o ; d HPLaserJet4 ^ @ g

X X @MSUDNHPLaserJet

4 %o ; d Ä ~ P P - C ê Times New Roman

ê Symbol

&ê Arial 5ê Courier New " @à - h MK ÜGL Ü

É 1)" ã The Right to encryption H<META HTTP-
EQUIV="Content-Type" CONTENT="text/html; charset=ISO-8859-1">

Keld Poulsen

It is only in one particular area that the IT Security Council proposes an intervention in the right to encryption, reveals Mads Bryde Andersen: Telecommunications companies, which introduce encryption as an integral part of their services, for instance in connection with ordinary telephony, shall be able - through a court

order - to decrypt, i.e. decode, a communication. "In this way, the obligation which telecommunications companies are currently under to contribute to intercepting in connection with police investigations into serious crime is carried a step further", Mads Bryde Andersen emphasises and adds, "The proposal does not, however, place any limitations on the communicating parties' opportunities for personally encrypting communications. But the rule will enjoin the telecommunications companies to provide the opportunities for intercepting in pursuance of a court order, so that those problems that have been evident within the GSM network can be avoided".

Encryption is an essential security element in electronic communication, for example in connection with home-banking on the Internet and public self-service systems as well as with electronic trading and money transfer between business enterprises.

The spread of encryption has, however, created problems for the authorities, since encryption normally precludes the police from intercepting in the course of crime investigations. Only in the event that the police are ensured access to keys used in encryption, for instance by the keys being stored in a central register to which the police has access, can encrypted communications be intercepted.

In consequence, all over the world authorities have raised the question of whether the right to make use of encryption ought to be subject to restrictions so that the police force and intelligence staff can continue to have the

≤ h Ë Ë ÷\ ≤\

[illegible]

V W ñ ó ò ö Â ~ · . T m Ê Á È Í
. ? @ E O â ü † ∂) / Ä Ü Δ ÷ ◇ Ó 4 p
◦ ˇ - ÷-
`˙áA°iŮi°ŤÊÊ%°,°Ůıff°,Ê,,Ê//ÿÿÿ
UÅc ^b VÅ c UÅ UÅ\$ uD 🍏-
a c CÅ uD CÅ uD 2 ≥ ¥ μ Â · / X\ ° ë

u ^

ã
1 ... T n E P â † Σ -
> Δ ◇ Ô 5 e ú Í # R p ϕ Í 0 c è Ê °
¿! ~ ¿! ~ ¿!M Ú ¿!Ä Ì ¿!∞ Ì ¿!🍏 Ì ¿!🍏 Ì ¿!P Ì
¿!🍏 Ì ¿!🍏 Ì
¿!🍏 Ì ¿!🍏 Ì ¿!🍏 Ì ¿!🍏 Ì ¿!🍏 Ì Ì Ì Ì Ì Ì Ì Ì Ì Ì Ì Ì Ì Ì Ì Ì Ì Ì
Ì Ì Ì Ì Ì Ì Ì Ì Ì << << ! << *Ê D é —
+--°°°°°°°°°
 <<*K
`Ò~ Normal,P a \$ @ \$

Heading 1,H1 UÅc, \$ @ \$

Heading 2,H2 UÅc * @ *

Heading 3,H3 🍏 < UÅ] & @ &

Heading 4,H4 🍏 < UÅ(@ (

Heading 5,H5 🍏 < UÅc (\@ (

Heading 6,H6 \ 🍏 < UÅc " A`Ú~° " Default Paragraph Font
 ,O
 Address < < VÅ& ,O & Blockquote h h < <
 ,Oç CITE VÅ ,Oç! CODE\] c : ,O 2: Definition
 Compact,DL COMPACT h ò< < . ,O B . Definition
 List,DL – 0~< < \$,Oç Q \$ Definition Term,DT\] c ,Oç a
 Definition,DFN VÅc , ,O ,
 Directory,DIR h @
 Ä ,Oç Å
 Emphasis,EM VÅ6 ,O 6 Horizontal
 Rule,HR İ~ &È 'È (È)È / ,Oç °
 Hypertext,A ^ b ,Oç ±

Keyboard,KBD] ^ c b 0@ ¬ b List Bullet,UL F

– ò_ε

$$4\tilde{}$$

$$-\partial_c$$

b 1@ “b List Number,OL F

4 \sim h .

X₆O X MenuF-

– ∂_6

4~ h ΣΣΣΣΣΣΣΣΣΣ \,O Ú\ PRE WIDE @
ıN1ª % / ° ^ Ú Ì
Ë „ fi / ' – À
Δ#¬&Ω)Π, \] c ^ ,O ^ Preformatted,PRE : -1ª %)
`ı\ Ä
‡ @ † `-,! %Ä(‡+ \] c " ,OÖ~ "
RestartList ! Ú~ ,Oç !
Sample,SAMP] " ,Oç 1 " Strikethrough,STRIKE WÅ ,Oç A
Strong,STRONG UÅ ,Oç Q
Typewriter,TT \] c ,Oç a

Variable,VAR VÅ] c * Ÿ O * z-Bottom of Form ' & c
Ÿ Oç Å z-HTML Tag] ^ b c (Ÿ O (z-Top of
Form) (c ééÍÁΠ æÀæŸfiœ ΣŸçÆ⁻†°†°øçÆ¶İΒÆ√Ô,
ÎÆøΣΣΠçÆÃÔ†Î°†ÈçÆ«†Î·†Î´ÁÔÍÁ†√Ôİ·Æ√
ÿ·ÍÆ⁻Á·°~çÆ,,·Á·Ô·È·,,çÆ,,·ÁÆÎ[~]
ÁÎ°æÃâ√Ôİ·İ™İ°æÃâ·Ô·°~İİÁä√œ«ŸİÊ ã,èé
àİÈX ã,ééàİç£§ÁàÈÃ†Á⁻ÊÍÃâ√Ôİ·İ™ÇÈ ãàÍÁÇÕ·
~/....,·İÔ,İÃâ·Ô·°~†âÉ,ééèÁÑÕ·~/.»Á,İÍÁ
âfœÂÎ™ÇÈÀ ã%ÅÆÕ·,,Ô·ÁÍÁ,Á~Æú%âŸfiÔÍΩ°
ðàÍÁÑÃİ·~·Ô·,ÇÈà ãÃâfÔÂÎ™âİÁÑÃİ·~·
·Ô·,Ç,ôéèÃæÃ⁻ÁİÁÑÃİ·~·Ô·,Ã,ôéèÃãf·Î†
ÇÃÑÃİ·~·Ô·,â,èèİÁÑÃİ·~·Ô·,Ç,ôéèÃãf·
Î†Ç,ééÍÃâfÔÂÎ™ÇÈà ãÃã%ıİ†àİÈ» ã%ÊÕ·,,Ô·
ÁÍÁ,Á~ú%âŸfiÔÍΩ°ðúÃâfœÂÎ™âİà»Á†Á⁻ÊóİÁç
Î·É,ééèÃäÔÂ⁻ÁİİİİİÁÇÕ·~/....,·İÔ,İç£§ÁàÈ
Ã†Á⁻ÊÍ·Ãâ√ÔİŸÁ·™ÇÃâ√Ôİ·İ™â%âŸœ°·İ·Î†İ·
ÃâÀ†İ·~·ÇÈM ãÃâ√ÔİŸÁ·™Ãİ·ÃÃâ†İ·~·É,ééè
İ·âÈL Ãâ√ÔİŸÁ·™ú%Å...,·İÔ,Ÿœ°·İ·Î†ú,èéÍ·İİ
à»Ã†Á⁻Êóİ·ÃÃâ†İ·~·Ç,ééèÃâ·Ô·°~Ç,èéÍ·ÃÃâ
†İ·~·É,ééèÃâ·Ô·°~ÇÃçİ·İİİİİÁÑÕ·~/.»Á,
İİç£§ÁàÈÃ†Á⁻ÊÍ·°Ãçİ,ÈİÈ/éÍ·∞Ãçİ,Èİ·Ãá·
İ»·,,Ô·ÇÃçİ,È⁻ÊéÍ·ÃÃá·İ»·,,Ô·Ã,èèè§ÃàÈÃ†Á⁻
⁻ÊÍ·Ãâ√ÔİŸÁ·™ÇÃâ√Ôİ·İ™â%âŸœ°·İ·Î†İ·ÃÜ√
Ôİ·İ™ÇÈ´ ãàâ%âŸœ°·İ·Î†İ·ÃÃá·İ»·,,Ô·É,èé
èÈ/èèÇÈ´ ãàú⁻ÊéÇ,èéÍ·ÃÃâ†İ·~·ÇÈM ãÃâ√ÔİŸÁ·
™Ãİ·ÃÃâ†İ·~·É,ééèİ·âÈL Ãâ√ÔİŸÁ·™úÃÜ√Ôİ
/·İ™ú,èéÍ·âÈ/éÍ·İİ·İàÈÃ†Á⁻ÊóİİİİİÃæÃ⁻Áİç£
§ÃàÈÃ†Á⁻ÊÍÃàfÔ·ÔÂ™Ç%ÅÆÆÆÆÆÆÆÆÆÆÆÆÆÆÆÆÆİÁ
ç,,İ™Ç%≤ æÀæŸfiœ ΣŸçÆÆ⁻†°†°øçÆÆ¶İΒÆÆ√Ô,ÎÆÆøΣ
ΣΠçÆÆÃÔ†Î°†ÈçÆÆ«†Î·†Î´ÁÔÍÁç,,~™ÇÃà%Ô·ÔÂ™
ãÁç,,İ™İÃâ≈Î≈Ô†Ô†ãÁç,,~™ú,ééàÍÃà≈Î≈Ã·ÃãÁç,,~
™ú,Ãéú,ÑéàÍÃÑ...Î†≈Ô†Ô†ãÁç,,İ™ú,Ãéú,ÃéàÍÃà≈
Î≈Ã·ÃãÁç,,~™ú,Ãéú,ééàÍÃÑ...Î†≈Ô†Ô†ãÁç√İ™ú,
Ãéú,£éàÍÃà≈Î≈Ã·ÃãÁç√~™úÈç ãÁç,,~™ú,İéàİİİİİÃÑ
...Î†≈Ô†Ô†ãÃÃÔ,™úÃà%,,,ÔÊúÃã~ÔÂ·°àÍÃãÃ
Ô,ø™ÇÃãÃÔ,™İ≠ÃàÈÃ·°†ÈÇ,èé™Ãà%,,,ÔÊİ·ÃãÃÔ
,ø™Ç%èÆãÃãÃÔ,ø™İ·ΠÃãÃÔ,ø™İ·Ãà°†ÈÈ°ãÃã~ÔÂ
·°àİ®ÃàÈÃ·