"France struggles to implement world's first Trusted Third Party infrastructure with key escrow"

Samuel Cadogan, Journaliste
E-Business- http://ebusiness.org/ Paris/Lyon/Genenve;

19, Boulevard de Sébastopol
75001 Paris
Tel: 01.42.33.61.87,
Fax: 01.42.33.61.88
E-mail:sc@ebusiness.org

27 bis cours d'Herbouville
69004 Lyon
Tel: 04.78.27.72.13
Fax: 04.72.07.89.51
E-mail: cadogan@calva.net

Samuel Cadogan is a French journalist of Irish extraction specializing in new electronic commerce business applications and technologies. He presently works for the independent French newsletter (e)-business, that he helped launch in March '96. He is also a regular contributor to other French and Anglo-Saxon IT publications.

Abstract

Unique in the western world for it's blanket ban on the use of strong encryption,France also became in February '98 the first country to official institute a scheme of Trusted Third Parties with Key Escrow. However such an implementation has been far from plain sailing. It is also in contradiction with the choices made by it's European partners, most notably Germany. And finally it thwarts the emergence of a pan-european security industry as well as the creation of a secure and interoperable Internet infrastructure.

France's uncompromising stance on encryption reflects, perhaps, in it's purest form, this country's present inability and unwillingness to adapt to and face off the challenges posed by digital globalisation. Before analysing and detailing the context in greater depth it is important to bear one fact in mind: any use, whatsoever, of encryption over the Internet and on French territory, with key length above 40 bits, is completly outlawed...unless used in conjunction with a key escrow mechanism. The consequences of such a draconian policy are dramatic. Not only are French companies, run, on the whole, by civil civil servants renowned for their unflinching "cartesian" thinking, thus even more reluctant to embrace an open public network such as the Internet. But, perhaps even more alarmingly, France'sblanket ban on encryption is diametrically opposed to the approach adopted by it's European partners. The contrast is particularly blatant with the the liberalism "en vigueur" over the Rhine in Germany. This is all the more galling, at a time when, as the 21st centurty dawns, these two countries are supposed to be the driving force paving the way to European economic integration and political unity.

To start with, it is usefull to understand the legislative backdrop. Back in 1990, when data exchanged on Internet was but a mere trickle, the French governement, under the premiership of the socialist Michel Rocard, accomplished a first milestone. In effect article 28 of the law no. 90-1170 on the "Régulation des Telecommunications" [1] voted on the 29th of December abolished, for the first time, the classication of encryption as a "weapon of war" ("arme de guerre"). However, it wasn't until the 26th of July 1996, just as the Internet was beginning to rear it's head in France, that a further amendment (Article 17) contained in the final bill no.96-659 on "Réglementation des Telecommunications" [2] was voted by the new right wing administration of Alain Juppé. In effect this officially instituted the mechanism of Trusted Third Party with Key Escrow. In other words any "liberalisation of encryption" was inextricably tied to the emergence of a nationwide infrastructure of Trusted Third Parties, with Key Escrow. The problem being that no

commercial entity was willing to take on the cost and complexity of administering key escrow centers. As Thierry Autret, a consultant at Atos (491,8 million Euro in revenues) [3], one of France's largest computer services companies, pointed it out "To be financially viable the creation of a key escrow system by the French State would entail creating a new tax for each individual French citizen wishing to use strong encryption to protect his private data !"

A potentially highly unpopular decision at a time when the press has been revealing how ex-French president François Mitterrand wantonly abused of wire tapping to listen in on the telephone conversations of journalists, film stars and other unsuspecting members of the public. A classic case of Catch 22. To illustrate further the technical difficulties, let's take the example a key escrow mechanism used with a symmetric encryption algorithm such as Diffie-Helman. In effect, it would mean every single French citizen, bar none, having to transmit to these centers each randomly generated key for each session every time a secure communication channel was established.

Moreover the key escrow centers would have to establish and log the identity of the users as well as the individual session. Hardly surprising then that the last missing piece the legislative jigsaw, know as the "décrets d'application", were only published two years later in February '98. In French law, these "décrets (no. 98-101 et 98-102)" [4] , were necessary to define the conditions under which the Trusted Third Parites would be designated and how they would operate. Upon their publication in the "Journal Officiel" most of the press here gave the annoucement a knee jerk rapturous welcome. However, on closer inspection they resolved very little. Whilst, it appeared that electronic signatures technologies (without use of encryption) were now free of use as was the transmission of an encrypted "password", (but not the number a credit card number (!)), there was still no indication how these Trusted Third Parties, with key escrow would operate. The conditions for being at all elligible were however defined. In essence, it was necessary to be a French company with at least four staff permanently on site that were veted by the Ministry of Defense.

This last detail points to the real power behind the throne: a shadowy organisation called the "Service Central de la Sécurité des Systèmes d'Information"(SCSSI). Retreated in it's bunker on the "rue du Docteur Zamenhof" in the southern suburbs of Paris, it is presided over by the Général Jean-Louis Desvignes and is an emanation of the "Secrétariat Général de la Défense Nationale" (SGDN). It is in theory only answerable to the Prime Ministers' Office. Some politicians, such as Christian Pierret, actual Minister of Industry, were foolhardy enough to promise, on repeated occasions, that 56 bit key would be free of use. But the Général, drapped in the cloak of the French Jacobin State, insisted at InfoSec'97 in Paris that this would only happen over his dead body. The publication of the "decret" in February '98, making compulsory escrow mechanisms for any encryption above 40 Bit,
was therefore a clear victory for the General. Fully aware however that this stalemate could not go on forever, the General was furiously spearheading behind the scenes all through '97, a whacky implementation a key escrow architecture based on the now infamous "Royal Holloway Protocol" [5]. For memory's sake, this scheme was also supported for a short time and then rejected by the British Authorities (GCHQ Protocol).

It in effect implied the creation of pairs of "Trusted Third Parties" who would ensure the tranmission of user B's key to user A. Deployed on a national scale, let alone internationaly, the complexity of such an archictecture is mind boggling. Undeterred, the General enlisted on his crusade France's Sagem SA. (2,5 billion Euro in revenues) [6] and another major French company (whose identity has not been revealed). But the fact that this year's "decret" (see above) failed to describe the mechanism of key escrow to be used showed that something was amiss. In fact, Sagem's, as well as it's partner, implementation of the "Royal Holloway" scheme predictiably had had to be abandonned as unworkable. Besides the losses incurred in the developement costs, Sagem no longer had any commercialy viable encryption solution on the domestic market!

It is safe then to assume that the publication of the "décret" in February '98, with the covert support of the French press, can be seen esentialy as a stalling manoeuvre. Because in the meantime, the Général Jean-Louis Desvignes had began working with another French company, just as closely tied to the French Ministry of Defense, CS-Telecom (a business unit of the Compagnie des Signaux - 484 million Euro in turnover) [7] . Their lead crypto developper has confirmed that they are presently working hard on a next generation implementation of the "Royal Holloway" Scheme integrating smart card and PKI. As they say, if you don't succeed try and try again... Even with a meagre penetration of 2.5% of Internet use in France some companies have felt the urge to jump the gun. However on each occasion their permission to use strong encryption has had to be conditionned to the SCSSI himself acting as a Trusted Third Party

with key Escrow ! This was the case for example, for the first fully fledged French Web banking site, openned in november '97 by the "Crédit Commercial de France" (CCF) [8] .

The same procedure applied to the Certification Authority created by the banking and "high-tech" consortium e-Comm [9] for the French implementation of Visa's and Mastercard's payment protocol SET. This also goes for the Dassault Electronic's (133 million Euro) [10] and Lagardère's Group's (9,9 billion Euro) Matranet's [11] respective IP VPN encryption architectures, known respectively as "Dedicace" and "M-Tunnel/M-Wall". As the General Jean-Louis Desvignes remarked himself at last week's InfoSec'98 [12] the only use of strong encryption allowed without key escrow is for GSM mobile telephones and Pay TV decoders ! But paradoxically, the General was being here economical with the truth. Because on 13th of May of this year his services had allowed a relativly unknown French computer services company called Neurocom SA [13] (the designated integrator for the CCF) to commercialise a java online banking security architecture using a 128 bit algorithm ("NetSecure Web Applet"). No key escrow would be required, but for this company only!!! The explanation lies in the fact that the advent of the Single European Currency combined with many Web sites of European banks (outside France) openly boasting, as a marketing argument, of using strong encryption with their customers the pressure had grown too strong on French politicians. Nonetheless Neurocom had to hand over it's source code and ensure that it's algorithms could not be used for any interpersonnal communication. Not forgetting that this decision gave Neurocom a near monopolistic grip on the French market. So much for market forces !

Although the unravelling of the present franco-french stalemate may be impossible the predict, the consequences on Europe are all too clear. As the number two economic power in the European Union with a GDP of $1,393 billion dollars France plays a pivotal role in any pan-european economic initiative. Therefore, the consequences of it's virtual ban on encryption are above all economic. Firstly, it prevents the creation of a truly secure and interoperable pan-european Internet infrastructure. For example it is difficult to imagine at all autonomous industry wide cost cutting extranets gaining ground in Europe, along the lines of the "Certification Authority Interoperability pilot" launched in June by the Internet Council of the "National Automated Clearing House Association" (NACHA) with five major US banks, or even the "Automated Network Exchange" presently being tested by Ford Motor Corp, General Motors Corp and Chrysler Corp with their respective suppliers. Secondly, it thwarts the emergence of security companies with a true pan-european foothold. As the Danish Minister for IT Jan Trojborg pleaded on April the 23rd at the "European expert hearing on Digital Signatures and Encryption" [14] "Europe must seize it's chance to unify it's encryption policies to allow the creation of powerfull international crypto champions". Indeed companies such as Germany's Brokat [15] and Utimaco [16] or Siemens' Irish spin-off SSE Lmtd [17], although incredibly dynamic, cannot yet take full advantage from an integrated and unified European market.

But, For France the supreme irony is that its stance on encryption plays right into the hands of the emerging american security behemoths (Security Dynamics Technologies Inc., Network Associates Inc, etc.) as they continue their feverish consolidation and aquisition raids on their own domestic market. And showing how much he hold European security and econmic interests closely to his heart the General Jean-Louis Desvignes, in an unrepentant statement two week ago, went so far as to admit that "should they (The American administration) lift their restrictions on the export of strong encryption nobody will no longer be able to control anything anymore".

[1] Loi no. 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications
www.adminet.com/jo/PTTX9000123L.html

[2] Loi n° 96-659 du 26 juillet 1996 de réglementation des télécommunication
www.telecom.gouv.fr/francais/activ/telecom/reglemen.htm

[3] www.atos-group.com/

[4] décret n° 98-101 du 24 février 1998 www.telecom.gouv.fr/francais/activ/telecom/deccrypto1.htm décret n° 98-102 du 24 février 1998 www.telecom.gouv.fr/francais/activ/telecom/deccrypto2.htm

[5] The Royal Holloway TTP-based key escrow scheme (PostScript)
ftp://ftp.dcs.rhbnc.ac.uk/pub/Chris.Mitchell/istr_a2.ps A Supplementary Analysis of the Royal Holloway TTP-based Key Escrow Scheme Ben Laurie (ben@algroup.co.uk) 16 Nov 1996 www.algroup.co.uk/crypto/rh.html

[6] www.sagem.com/

[7] www.cie-signaux.fr/ www.cstelecom.com/

[8] www.bancopc.ccf.fr/

[9] e-comm.fr/

[10] www.dassault-elec.com/

[11] www.matranet.com/

[12] www.clusif.asso.fr/infosec/congres.htm

[13] www.neurocom.com/

[14] www.fsk.dk/fsk/div/hearing/

[15] www.brokat.com/

[16] www.utimaco.com/

[17] wwww.sse.ie/