LAW ENFORCEMENT AND DATA RETENTION IN THE LIGHT OF AN ANONYMISATION SERVICES

by

STEFAN KÖPSELL[*] & PETR ŠVENDA[**]

The recently introduced legislation on data retention to aid prosecuting cyber-related crime in Europe also affects the achievable security of systems for anonymous communication on the Internet. We have analysed the newly arising risks associated with the process of accessing and storage of the retained data and propose a secure logging system, which utilizes cryptographic smart cards, trusted timestamping servers and distributed storage. A practical implementation of the proposed scheme was performed for the AN.ON anonymity service, but the scheme can be used for other services affected by data retention legislation. We also discuss the practical experience from process of response to legal authorities' requests both before and after the data retention directive was implemented. Moreover we give a general description of the legal obligations and the information about usefulness of the retained data is also provided. Derived from these obligations we give arguments reflecting challenges and obstacles for a secure and privacy respecting implementation of data retention.

KEYWORDS

Anonymity service, data retention, secure logging

1. INTRODUCTION

The legislation on data retention affects—at least in some countries (e.g., Germany) — systems for anonymous communication on the Internet such as AN.ON [BeFK00] or TOR [DiMS04]. As a provider of one such anomity service, we like to report on the impact of this legislation on the system, newly arisen risks associated with the legal compliance and our experience

[*] TU Dresden, Germany. E-mail: sk13@inf.tu-dresden.de

[**] Faculty of Informatics, Masaryk University, Brno. E-mail: svenda@fi.muni.cz

with answering law enforcement requests for (possibly) retained information. Additionally, we will briefly present technical means how to legally comply, minimize these risks at the same time and discuss usability of the retained data for criminal prosecution.

The directive 2006/24/EC (data retention directive) "on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communication networks", passed by the European parliament on March 15th, 2006, sets the legal framework of data retention for the European Union member states. According to the directive, the member states have to "bring into force the laws, regulations and administrative provisions necessary to comply with this directive by no later than 15 September 2007". The goal of the directive is to strengthen the success of law enforcement in the area of Internet-related crime and, more general, whenever electronic communication is involved. The motivation for the directive was that the data about past communication relations is already unavailable when it comes to a trial after weeks or months, in which evidence from the communication relations could be helpful. Data on communication relations can provide information about the person who accessed a specific website or who called a specific telephone, for instance. Germany has reacted to the data retention directive and adapted several laws [TKG07]. With respect to anonymity services on the Internet, the changes of the Telecommunications Act are most significant [TKG04]. This act defines in detail what kind of data had to be stored for various types of communications providers, including telecommunications companies like fixed-line or mobile phone providers and Internet service providers (ISPs). The act defined a retention period of six months. It anticipated services like anonymity services, which are in the first place contradictory to the law enforcement goals. In order to prevent any information gap, the Telecommunications Act declared in §113a 'Retention of Data':

> *'(6) Those, who provide telecommunication services and thereby alter data which have to be stored according to this law, have to store the original data and the new data as well as the time of the alteration.'*[1]

[1] Note that the quotations of the Telecommunications Act is an unofficial translation of the official law text in German. The authors are not aware of any official translation of the current version of the Telecommunications Act. The former version (of 22 June 2004) is available in English at: <http://www.bmwi.de/BMWi/Redaktion/PDF/Gesetz/telekommunkationsgesetz-en>.

Note that the commentary to this section issued by the legislator confirmed that this section was especially introduced because of anonymisation services. We want to emphasize that to the best of our knowledge this is a speciality of the German data retention law which we could not find in any other European data retention law.

After these new laws came into force 1st of January 2008 several complains against these new regulations were presented to the German constitutional court. On 11th of March 2008 a first preliminary decision[2] of the German constitutional court sets restrictions with respect to the access of law enforcement agencies to the retained data. In order to get access to retained data, the court demands the investigated crime has to be a "serious crime" listened within a catalogue of crimes[3]. But the court did *not* forbid the data retention in general and required the data to be retained at least until the final decision of the court. The preliminary decision was prolonged (and slightly extended) three times: on 1st of September 2008[4], 28th of October 2008[5] and 15th of October 2009[6]. The final decision of the court was announced on the 2nd of March 2010[7]. At first, the court declared the implementation of data retention to be unconstitutional. Data retention had to be stopped immediately and all retained data so far had to be deleted. Secondly, the court decided that data retention is *not* unconstitutional in principle. The court further explained that a new law has to be very specific about the necessary conditions under which law enforcement agencies could get access to the retained data. Moreover the court demands concrete procedures which ensure a secure storage of and access to the retained data.

To summaries, there is currently no data retention in place in Germany. But on the other hand the pressure from all sides to the minister of justice to issue new data retention laws is very high. This is especially true at the very moment due to the ongoing terror alarm in Germany (December 2010).

---

2 1 BvR 256/08, 11. March 2008, <http://www.bverfg.de/entscheidungen/rs20080311_1bvr025608.html>; German Federal Law Gazette 2008, Part I, Nr. 13, Bonn, 10. April 2008, page 659.

3 This catalogue is given in §100a(2) of the German Code of Criminal Procedure.

4 German Federal Law Gazette 2008, Part I, Nr. 41, Bonn, 23. September 2008, page 1850.

5 German Federal Law Gazette 2008, Part I, Nr. 53, Bonn, 27. November 2008, pages 2239–2240.

6 1 BvR 256/08, 15. October 2009, <http://www.vorratsdatenspeicherung.de/images/vb_bverfg_beschluss_2009-10-15_1-bvr-256-08.pdf>; German Federal Law Gazette 2009, Part I, Nr. 73, Bonn, 11. November 2009, page 3704.

7 1 BvR 256/08, 2. March 2010, <http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html>; German Federal Law Gazette 2010, Part I, Nr. 11, Bonn, 17. March 2010, page 272.

Therefore we expect new data retention laws coming into the force within the next few months.

1.1. LEGAL AND OPERATIONAL REQUIREMENTS ON LOGGING OF RETAINED DATA

In this section, we summarize the requirements for the retained data and the logging procedures. These are general requirements applicable to any service which needs to be compliant with the EC data retention directive. They can be divided into legal obligations (R1–R4) and the operational needs (R5). Moreover, they can be classified as functional requirements (R1; what the system should *do*) and non-functional requirements (R2–R5; how the system should *be*).

R1: Logged data has to include all statutory categories of data. Article 5 of the data retention directive describes what types of services have to retain which data categories. National implementations of the directive could extend this. This functional requirement basically states that some meaningful data has to be logged and that logging of (e.g.) random data would not be sufficient.

R2: Logged data have to be deleted after a specific period of time. This means that logged records cannot be accessed outside a given data retention period. In the following text we use the term "outdated" to describe a property of a given item (cryptographic key, log entry etc.) to which the access should be prevented because the related retention period already expired.

R3: Logged data need to be accessible, so that requests from law enforcement agencies can be answered without undue delay.

R4: Logged data have to be secure, so that no access to the logged data by unauthorised person is possible. This requirement covers confidentiality as well as integrity of the logged records. Note that in our case the integrity means that the operator can detect if the logged data have been altered—it is not necessary that the operator proves something to the third party.

R5: The cost of logging has to be reasonable. It includes the monetary costs (e.g. initial necessary investments, operational costs) but also the degradation of the overall performance of the system as well as the organisational overhead.

1.2. INTRODUCTION TO THE AN.ON SYSTEM

We are operating an anonymity service called AN.ON, which is based on Mixes. A Mix [Chau81] is a server which forwards messages thereby ensuring that an outsider (e.g. an eavesdropper) cannot link incoming and outgoing messages. This is accomplished by a combination of several (cryptographic) mechanisms. In order to enhance the trustworthiness of the anonymity system, several Mixes are chained together. The sender of a given message can only be deanonymised if all Mixes along the path of his message reveal the linkage between the appropriate incoming and outgoing messages. Therefore, the use of multiple Mixes offers protection against dishonest Mix operators.

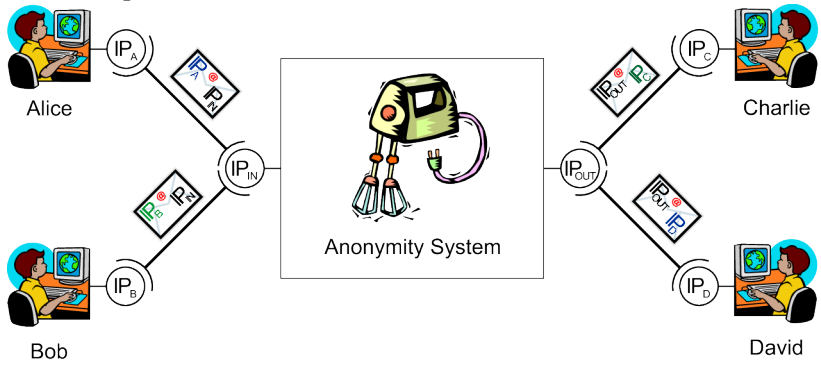


FIGURE 1: SIMPLIFIED "BLACK BOX" MODEL OF AN.ON: THE IP ADDRESSES OF THE SENDERS ARE EXCHANGED WITH THE IP ADDRESS OF THE ANONYMISATION SERVICE

In order to easy the explanations one can imagine our anonymisation service as a simple proxy which a user uses to hide its own IP-address, e.g. towards a web server (see Figure 1). In terms of sentence (6) of §113a of the Telecommunications Act the proxy, that is the anonymity service, replaces the IP-address of the user (IP_U) with its own IP-address (IP_{Out}).

An urging question is which data has to be logged by anonymity services such as AN.ON in order to comply with the data retention law. In §113a, the Telecommunications Act distinguishes several types of service and defines for each service the sort of data to be stored. The best match for AN.ON is 'Internet Service Provider' (ISP). According to the Telecommunications Act, an ISP has to log the IP address of a user, a unique identifier of the connection, and the period of time in which this assignment was valid.

In combination with sentence (6), this means that the anonymity service has to log the replacement of IP addresses only, but nothing more, particularly no 'identifiers' of higher layers, such as TCP-port numbers etc. Besides, consulted lawyers argue that only the replacement of source IP addresses (but not destination IP addresses) are allowed to be retained. They justify their assessment with sentence (8) of §113a: '…data about retrieved Internet pages must not be retained.' The lawyers also concluded that logging is allowed only for IP packet flows in upstream direction, that is only for packets from the user to the service, a web server for instance, but not for downstream packets.

Summarising, each retained log entry can be seen as a pair of IP-address and timestamp: (IP_U, t). As IP_{Out} of the proxy will be visible in suspicious requests, the law enforcement agencies ask questions in the form of: "Who was using IP-address IP_{Out} at time t_R". In order to answer such questions we need to search through our log files for all records with timestamps t_i for which: $t_R - \varepsilon \leq t_i \leq t_R + \varepsilon$. The need for the parameter ε reflects the fact that we cannot assume that all clocks of all servers creating log records are synchronised.

1.3. INCREASED RISKS FROM LEGAL COMPLIANCE

Standard secure logging mechanisms such as [MaTs09] protect the logged records sufficiently against unauthorized access (confidentiality), unauthorized modification (integrity) and in some cases attempt to ensure availability of records. But when applied to the needs of data retention logging on the logging entity side, newly arising risks remain unsolved as the attacker model has changed.

Potentially sensitive data are now present on logging entity side as a result of compliance with data retention legislation. The logging entity (Mix operator) can be forced to reveal, delete or modify this data—threats that did not exist before as there was no need to store such data in the first place. Specifically, threats related to the data retention period must be addressed and mitigated. Note that the risk for a user to be deanonymised, if the operators of the chosen anonymity servers behave *dishonestly*, exists before the introduction of data retention. But if the operators are *honest*, the attacker gains an additional advantage of mounting a successful attack on the anonymity of a given user with the help of retained data. Moreover, it is now possible for the attacker to start his attack *after the fact* (i.e. after the activity,

the attacker wants to deanonymise took place). This was not possible before, as the attacker had to log the anonymised and encrypted traffic at the time of this activity in order to analyse it later on.

Additional new risks arise from the fact that the logged data is not only stored, but also used for law enforcement. Assume the attacker modifying the logged data so that an innocuous user of the anonymity service becomes suspicious when modified retained data are used in criminal investigation. For an operator of an anonymisation server, the new risk is that an attacker may force him to modify the logged data in such a way or in other way which hides the criminal activities of the attacker. Thus a suitable logging scheme should not only protect the users of the anonymity service but also its operators.

2. THE PROPOSED SCHEME FOR SECURE LOGGING

This paper abstracts from the unnecessary technical details of the scheme we proposed in [KS09] and focuses on the impact and usability of the scheme from the perspective of law enforcement. Here, we will summarize only the most important conceptual properties to demonstrate, that data retention logging can be efficiently implemented in a secure way which also mitigates the risks of anonymity service operators.

The logged data has to be stored encrypted and integrity protected (cf. requirement R4). The encryption ensures that the content of the logged data can not be revealed without the knowledge of the secret key. The advantage of encrypting the logged data is that the data can be protected using available (probably insecure) backup mechanisms. Note that because of this backup, it is in generally not possible to (provably) delete the retained data. So the "deletion" has to be accomplished by cryptographic means (e.g., by destruction of a decryption key[8]).

Confidentiality and integrity of the retained records can be achieved by either symmetric or asymmetric encryption. Asymmetric encryption has the advantage that no secret key needs to be stored on the logging server but suffers from poor performance compared to the symmetric encryption. We utilize a hybrid encryption scheme where the symmetric encryption is used

[8] Deletion of a single decryption key, which is not part of any backup, is much easier compared to ensuring that every backup copy of a given log file is deleted. This is especially true if the backup in place is not under full control of the operator of the anonymisation server itself.

for the log entries itself. The corresponding symmetric key k_Y is stored within the log file using asymmetric encryption.

The private key is stored on a trusted device (e.g., smart card) with ability to control the access to the private key thus also to retained data. As result, an access to outdated log files (cf. requirement R2) is prevented and the risk that the operator is forced by the attacker to decrypt outdated log files is mitigated. Therefore, an important property of the access control to the private key implemented by the trusted device is, that it not only depends on proper authorisation (e.g. password of the operator) but also *on the current time*. The idea is, that the trusted device denies decryption of a symmetric key (used to unlock access to log records) if the related log file is already outdated (outside the data retention period). If the smart card is used as trusted device, reliable time can be obtained from trusted time servers via the TSP protocol [RFC3136].

For the protection of log file integrity, we need to prevent/detect modification of a log entry, copying of a log entry to another position within a log file or to a different log file, truncation of the log file and completely replacing a whole log file by a forged one. Integrity of a single log entry can be verified through Message Authentication Code (MAC) as usual defence. In order to prevent the deletion of a legitimate log file and creation of a completely forged one we utilise a combination a multiple mechanisms: digital signatures, distribution of integrity checksums and trusted timestamping.

The "digital signature" mechanism basically means that the logging server digitally signs the log files. The "distribution" mechanism means that every artefact (e.g. signature test keys) involved in the integrity verification process are distributed in a way so that it is hard for the attacker to manipulate all copies simultaneously. One way to achieve this is to utilise censorship resistant P2P-networks such as FreeNet [CSWH00] or Free Heaven [DiFM00]. The "trusted timestamping" mechanism means that every artefact mentioned above is time stamped by multiple external trusted timestamping services.

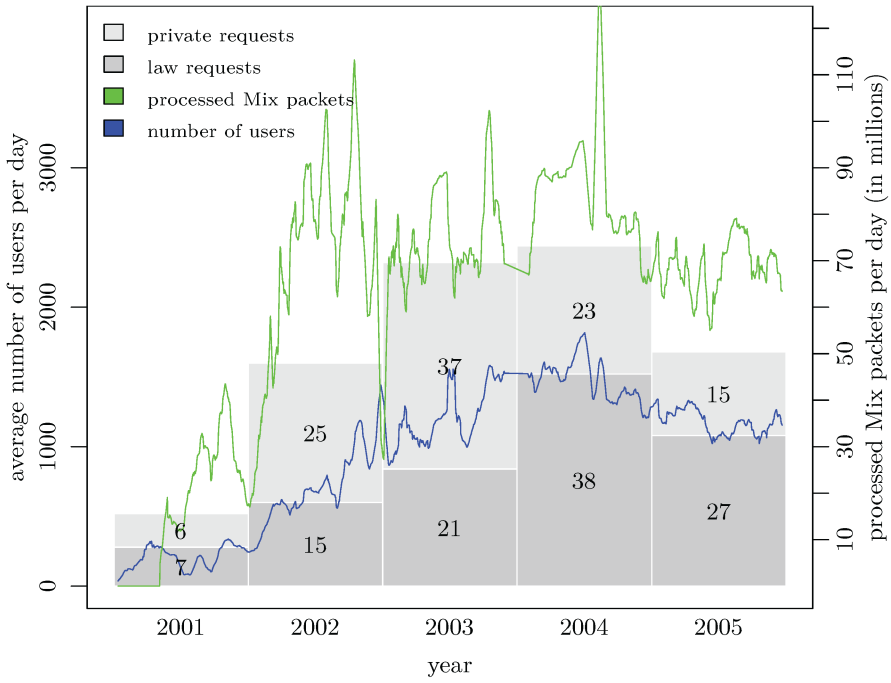
The practical implementation of the scheme was demonstrated with Java Card smart card as trusted device. Logging performance was demonstrated to be very good, as well as the searching performance for locating entries relevant to data retention request.

A demand for the practical implementation originates from the needs of the AN.ON anonymity service. But the proposed logging scheme can be used for other services affected by the data retention legislation as well. More generally, the scheme can be used for any logging service where the logged records should be accessible only for a limited time period or where knowledge of cryptographic secrets might lead to personal threats of the holder.

3. EXPERIENCE WITH ABUSE OF THE ANONYMISATION SERVICE AND WITH LAW ENFORCEMENT

AN.ON is available for the public since September 2000. Currently, we are offering our service both free of charge through volunteering Mix operators as well as commercial service through a spin-off company[9]. Since 2000 we observed a constantly growing number of users. At the moment we have roughly 6000 users online at the same time. We estimate that we have more than 50000 users who use our service on a regular base (see [BeBK08] for a description of an empirical study which leads to that number, although by the nature of our service we do not collect any identifying information usable for giving a precise number of users). Currently our service anonymises more than 800 million web requests per month leading to more than 20 TByte of transmitted data.

[9] <http://www.jondos.org/>



Year	total	law requests	private requests
2001	13	7	6
2002	40	15	25
2003	58	21	37
2004	61	38	23
2005	42	27	15
Sum	221	112	109

TABLE 1: OVERVIEW OF RECEIVED REQUESTS FROM LAW ENFORCEMENT AGENCIES AND PRIVATE PERSONS AND COMPANIES [ULD06] IN PERIOD 2001 – 2005. SINCE 2006, AROUND 2–4 REQUESTS FROM LAW ENFORCEMENT AGENCIES PER MONTH AND 3–6 PRIVATE REQUESTS ARE RECEIVED. THE DRAWING RELATES THE MISUSE TO THE USE OF THE ANONYMISATION SERVICE.

Unfortunately, also some misuse results from the operation of the anonymisation service. We learn about such misuse if we receive "request for information" from affected party. Such requests can be basically divide into two types: a) requests from private persons, organisations or companies (consecutively named "private requests") and b) requests from law enforce-

ment agencies ("law requests" for short). Table 1 gives an overview about the number of requests we received per year (from 2001 to 2005). Since 2006 we get around 2–4 requests from law enforcement agencies per month and 3–6 private requests. Note that we can only report about incidents which we get to know by some "requests for information". Clearly there is a number of unknown cases: law enforcement agencies told us, that they will not ask us any longer because they already know that they will not get any useful information if the anonymisation service was involved. Nevertheless we do not believe that the true amount of misuse would be extraordinary higher compared to the reported misuse. Otherwise we would expect much more "attention" of law enforcement agencies with respect to our anonymisation service.

Some of the private requests just want that we stop any of the reported abusive activities. We solve that by blocking the access to the reported web site from our anonymisation service. But all the requests from law enforcement agencies and most of the private requests ask for the person who uses a given IP-address – which is one of the IP-addresses of our anonymisation servers – at a given point in time. During the times when data retention was not an obligation we just responded that we do not have logged any data so that we can not provide any useful information. Such negative responses were accepted by nearly all law enforcement agencies and most of the private persons and companies without any further comments. Only a very few of the law enforcement agencies started some kind of "ethical discussion" but at the end accepted our explanations with respect to data protection and the related data protection laws, as operating an anonymisation service is completely legal in Germany.

Although we saw all kind of reasons for law requests during the last 10 years, the majority of the law requests were related to some kind of financial frauds especially credit card frauds or more generally spoken the identity frauds. Child pornography was the reason for the law requests only in three cases.

The reasons for private requests were mainly because of blaming of people (e.g. in chats, e-mails, blogs etc.) or "vandalism" i.e. activities which affect the functionality of a given web service e.g. by changing the content of a web site or manipulating the data stored in the underlying database system.

Note that most of the law requests deal with "ex tunc" incidents. Only few of them (less then 5) requested "ex nunc" observations (comparable to lawful interceptions known from the plain old telephone). The reason for that small number can be seen in the special situation in Germany which not only requires a court order but also the suspicion for a (serious) crime listened in a special catalogue. I.e. law enforcement agencies would not get such court order just for investigating a credit card fraud. Nevertheless to the best of our knowledge none of the observations leads to actually catching a criminal.

Summarising the said, one can conclude that our anonymisation service was and will be misused to some extend – but the amount of misuse is much smaller than usually expected by uninformed person.

4. DISCUSSION OF PRACTICAL USABILITY OF RETAINED DATA

Our anonymisation service basically exchanges the IP-addresses of its users with its own outgoing IP-address IP_{Out} (see Figure 1). Therefore answer to a typical law enforcement question: "Who uses IP-address IP_{Out} at time t? " with the help of the retained data will only reveal the IP-addresses of *all* users which were logged-in resp. active at time t, not a single one usually expected by law enforcement requester. In [BeBK08] we reported the results of an empirical study showing that such a request led to at least 400 different IP-addresses on our anonymisation servers used the most. Clearly, such amount of suspicious persons is not helpful for most if not all law enforcement investigations.

Additional we studied the case where the law enforcement agency (through some external knowledge) knows, that the same offender used the anonymisation service at multiple points in time ($t_1 ... t_x$). Therefore the law enforcement agency could request the sets of suspicious IP-addresses for all these points in time and afterwards calculate the intersection of these sets of suspicious IP-addresses, as the offenders IP-address has to be an element of that intersection.[10] Our study revealed that if two different points in time are chosen (same offender uses anonymity service twice), chances are very high that the intersection will contain more than 10 IP addresses. Even if the intersection is calculated for 10 different points in time the chance that the in-

[10] Note that assuming that the offender always has the same IP-address represents already the best case for the law enforcement agency.

tersection would reveal more than one suspicious IP-address is not negligible. This is especially true if the offender behaves intelligently and follows some rules which were explained in detail in [BeBK08].

From January 2009 until March 2010, i.e. the time data retention was lawful in Germany, we received around 10 written law requests which were related to retained data. Some of them had formal errors, e.g. referred to the wrong paragraphs etc. None of the received requests fulfils the requirement of showing a court order which in turn refers to one of the needed offences listened in the catalogue of offences. So there was no need to reveal any of the retained data,we answered accordingly and answer was accepted in all cases.

Despite the written requests we also had some telephone calls from law enforcement agencies (again around 10) asking for the retained data. We explained that we need a court order which fulfils the requirements set by the constitutional court. But again none of the communicated cases was of the kind needed, i.e. was not able to get the necessary court order.

As a side remark we like to report on one of these telephone calls. Here a police man from the German Federal Criminal Office (BKA) asked about the general availability of retained data. We explained the necessity of the right court order, which in this case was not seen as a problem as explained by the police man. When we explained that we expect at least 400 IP-address as a result (based on our empirical study), the police man acknowledge that this amount of suspicious IP-addresses is not helpful for his investigations. We therefore explained the basic idea of the calculation of the intersection (as explained above). This approach was well understood by the police man. But even the envisaged much smaller set of suspicious IP-addresses (we told him, that he might get "a handful of IP-addresses") was not narrowed down enough. We were told that the police man in such case would afterwards not get the needed search warrants, i.e. a judge would not sign say five search warrants knowing that four of them targeting innocent citizens. Although we only had such experience once it might indicate that even a little uncertainty with respect to the correctness of the conclusions drawn from the retained data might render them useless for practical investigations.

Finally we want to report on case which is not directly related to a request for retained data but illuminates the usefulness of the retained data from a different perspective. In this case a German police man sent the usu-

al law request. The request was dated October 2010 requesting information with respect to some incident which happened May 2008. We checked back if really 2.5 years old information were requested. The simple answer was: "Yes. The request is based on an international letter of request originated from Portugal". Given that time frame and assuming that a request from some member state of the European Union should take less time compared to a request from some country outside of Europe it shows that for effective law enforcement the retained data needs to be stored at least say 5 years (with associated privacy risks on the other side) – if not forever (of course one could also try to optimise the organisational procedures but this is out of scope of this paper.)

5. CONCLUSIONS AND OUTLOOK

The compliance with the new data retention directive introduces not only benefits for the law enforcement agencies, but also additional risks for the users and operators of the communication service that need to be mitigated. We have proposed, implemented and start into the practical usage a secure logging service based on a combination of log file encryption, key recovery with smart cards and data retention period enforcement via trusted timestamping servers. The implementation is available for public use. An operator cannot be forced to reveal logged records outside the data retention period, because the period is enforced directly on the smart card with the help of trusted timestamping servers.

The log data of selected German AN.ON servers were protected with the proposed mechanism since 1st January 2009 until the 2nd of March 2010, when the German constitutional court decided to stop data retention.

A new data retention law will be introduced in Germany soon (with high probability). This new law will mandate secure storage and transmission of retained data according to the decision of the constitutional court. Although our implementation for storing retained data already fulfils these requirements, it can be foreseen that some official certification might be required. This would comprise the usage of certified hardware and software components.

One reason we assume this lays in the current version of the German Technical Guideline for the implementation of legal measures for surveillance of telecommunications and information requests for traffic data (TR

TKÜV)[11]. These regulations cover (in Part B) also the requirements for retained data transmission. Although at the moment legacy means (like telefax or data carrier) are still admissibly a transmission of the retained data according the ETSI specification TS 102 657 is envisaged. This kind of transmission would require the participation in a governmental virtual private network (VPN) which in turn requires certification of the participating entities and the usage of certified hardware. The biggest problem with these requirements is the high expenses making the volunteering operation of an anonymisation server infeasible.

Moreover additional legal obligations and responsibilities might appear soon. One of these obligations is already somehow into force – the obligation of a communication service provider to block the access to certain web sites on request of law enforcement agencies because of child pornography. We say "somehow into force" because on the one hand the law passed all the necessary steps and is therefore – from a theoretical point of view – in force. But on the other hand there exist official instructions which forbid the law enforcement agencies to actually request any blocking. (Some lawyers argue that this way of de facto repealing a law is unconstitutional, but such a discussion is out of scope of this paper.) Again chances are high that the consequences of this law will come into force soon and again this means expenses for the certified communication infrastructure necessary to get access to the list of web sites to be blocked.

Finally the Anti-Counterfeiting Trade Agreement (ACTA) might be ratified soon. Depending on the final regulations it might introduce liability of communication providers in case of copyright infringements. The misuse of AN.ON together with such kind of liability will led to an incalculable financial risk for Mix operators.

To summarise: when we started in 2000 with the deployment of our anonymisation service the main obstacle was the resource consumption of the servers in terms of computing power and bandwidth. Today one can rent the required resources for less than 100 EUR per month making the operation of an anonymisation server feasible for a small data protection association or even private person. But it turned out that the legal obligations today and especially the uncertainty with respect to liability are the main reasons for thwarting a broader deployment of our anonymisation service.

[11] <http://www.bundesnetzagentur.de/cae/servlet/contentblob/153316/publicationFile/6608/2010-04-27_TRTKUE6-0Englishpdf.pdf>

REFERENCES

[1] [BeBK08] Stefan Berthold, Rainer Böhme, Stefan Köpsell: *Data Retention and Anonymity Services*; Proc. The Future of Identity in the Information Society - Challenges for Privacy and Security, FIDIS/IFIP Internet Security & Privacy Fourth International Summer School, Springer, Boston, IFIP Advances in Information and Communication Technology, volume 298, 2009, 92–106.

[2] [BeFK00] Oliver Berthold, Hannes Federrath, Stefan Köpsell: *Web MIXes: A System for Anonymous and Unobservable Internet Access*; Proc. of Privacy Enhancing Technologies Workshop (PET 2000), Springer, Berlin / Heidelberg, LNCS 2009, July 2000, 115–129.

[3] [Chau81] David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24/2, 1981, 84–88.

[4] [CSWH00] Ian Clarke, Oskar Sandberg, Brandon Wiley, Theodore W. Hong: *Freenet: A Distributed Anonymous Information Storage and Retrieval System*; Proc. of the Workshop on Design Issues in Anonymity and Unobservability, Berkeley, CA, Springer, Berlin / Heidelberg, LNCS 2009, July 2000.

[5] [DiFM00] Roger Dingledine, Michael J. Freedman, David Molnar: *The Free Haven Project: Distributed Anonymous Storage Service*; Proc. of the Workshop on Design Issues in Anonymity and Unobservability, Berkeley, CA, Springer, Berlin / Heidelberg, LNCS 2009, July 2000.

[6] [DiMS04] Roger Dingledine, Nick Mathewson, Paul F. Syverson: *Tor: The Second-Generation Onion Router*; Proc. of the 13th USENIX Security Symposium, August 2004, 303–320.

[7] [KS09] Stefan Kopsell, Petr Švenda: *Secure logging of retained data for an anonymity service*; IFIP Advances in Information and Communication Technology, Vol. 320, pp. 284-298, 2009.

[8] [MaTs09] Di Ma, Gene Tsudik: *A new approach to secure logging*; ACM Transactions on Storage (TOS), vol. 5, issue 1, ACM, New York, March 2009.

[9] [RFC 3161] C. Adams, P. Cain, D. Pinkas, R. Zuccherato: *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*; August 2001, Proposed Standard, Available online: <http://www.rfc-editor.org/rfc/rfc3161.txt>

[10] [TKG07] Bundestag: *Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007*; Bundesgesetzblatt, Jahrgang 2007, Teil I, Nr. 70, December 2007, 3198–3211, ausgegeben zu Bonn.

[11] [TKG04] Bundestag: *Telekommunikationsgesetz vom 22. Juni 2004 (2007), BGBl. I S. 1190, zuletzt geändert durch Artikel 2 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198)*.

[12] [ULD06] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: *Abschlussbericht für das Projekt AN.ON – Juristische Arbeitspakete –*; Abschlussbericht des AN.ON Projektes, Förderkennzeichen 01 MS 917, 9. Oktober 2006.