USABILITY OF SAFETICA OUTPUTS IN CRIMINAL CASES AS ELECTRONIC EVIDENCE

www.safetica.com

safetica®

I CONTENTS

THE MOST IMPORTANT INFORMATION

- Ensure compliance with local laws and regulations in order to collect information about employees in a legal way.
- Control and monitor access to information.
- Document the process of collecting information and the security measures taken.
- Ensure the security of information: confidentiality, authenticity, integrity, and non-repudiation.

PREFACE

Increasingly more criminal cases today involve electronic evidence in some way. The Safetica wants to protect the company's goals and assets by control and monitoring. However, in case some security incident actually happens in the company, it is necessary to reveal and convict the offenders. There are many laws and regulations concerning electronic evidence worldwide. Therefore, there are some requirements that Safetica logs must fulfill in order to be accepted as proof. The specific laws according to the territories of their relevance are discussed in separate subchapters of this text. There are also countries with no legislative background for electronic evidence – if no information is provided to a specific country, the courts concern these cases individually.

It is noteworthy, that there is one model law that applies to the admissibility of electronic evidence in many states worldwide. This is relevant to all UNCITRAL states [16] that enacted the UNCITRAL Model Law on Electronic Commerce (1996) as part of their local law. This model law *"...served as a basis of electronic contracting legislation in a wide range of different jurisdictions, including Australia, Bahrain, Bermuda, Canada, Columbia, Dominican Republic, Dubai, France, Hong Kong, Ireland, Mexico, Philippines, Singapore, Slovenia, the United Kingdom and the United States."* [1]. The impact of this law on electronic evidence is that the Article 9 states:

> *"(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:*
>
> *(a) on the sole ground that it is a data message; or,*
>
> *(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.*
>
> *(2) Information in the form of a data message shall be given due evidential weight. (...)"* [1].

These facts ensure that the electronic evidence is dealt with as traditional evidence in court cases. The UNECTRA official website provides the information, which countries adopted this model law [16].

There are also some common criteria that can be observed from laws of many countries. In the first place, the evidence needs to be legal, in other words it needs to be collected in compliance with local laws. Secondly, the good documentation done in the process of collecting can increase the weight of evidence in court. The good practice in court cases worldwide also indicates that some measures should be taken even when collecting information the legal way: that the confidentiality, authenticity, integrity, and non-repudiation of such data are ensured.

The **confidentiality** can often be achieved by encryption. Safetica logs are stored in encrypted form automatically when using the Small installation and, when using Standard installation, the encryption can be set in MS SQL by the system administrator.

The **authenticity** of data is a difficult issue, mainly to prove it in court cases. Unfortunately, this principle is often discussed in courts – the adversary can challenge the authenticity of the data, stating that anyone with access could have altered it. This risk can be reduced by providing access to such data to as few people as possible; by checking and maintaining their professional background and trustworthiness; and by establishing monitoring over such data, with the supervision of preferably only one trustworthy person.

There are few concepts that can be used to ensure the **integrity** of data. The one approach to this principle is to store the data (by means of single log entries) with their hash values.[1] The other option is to *"(...) store logs on WORM (write once, read many) drives such as CD-R/DVD-R or storage devices such as EMC's Centera. (...) (this ensures) that tampering of logs can be detected or prevented."*[2]. It is also possible to use digital signatures (they are discussed in the next paragraph).

Digital signatures, in addition to integrity, also provide **non-repudiation**. They can be used in a similar way as hash values – by signing each log entry. Unlike hashes, it is also necessary to store cryptographic keys, ensure the trustworthiness of the certificate service provider (the trusted party), and also ensure the integrity of the signed content and certificate. It is also possible to sign each log entry with multiple signatures.

Please note that the use of digital signatures and similar technologies can be regulated by law.

I NORTH AMERICA

According to the UNECTRA official website [16], *The UNECTRA Model law 1996 was enacted by the following countries: Canada, Dominican Republic, Guatemala, Mexico, and the United States.*

The United States laws

The use of electronic evidence in the US is regulated mainly by the Federal Rules of Electronic Evidence [3], Electronic Communications Privacy Act (ECPA[2]), and the court decisions in relevant cases. Firstly, in order for electronic evidence to be accepted, its original storage, collection, processing, and presentation are considered [4]. Collection and processing of the evidence depends on criminal investigators, its presentation in most cases is arranged by the attorney and/or expert witness (in these cases the Daubert's test [5] may be applied for an expert to decide on their respective expertise), so basically the only thing that can be done before some security incident happens is to ensure the security of protected data (in our case, the logs and statistics of Safetica software). This was further discussed in the Preface of this document.

Fortunately, US court practise indicates that the digital evidence is as trustworthy as paper evidence and the probability of their alteration is not often discussed. For example, in the case U.S. v. Bonallo, the court stated: *"The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness."* [6]

There are also other laws, dealing mainly with digital signatures: *Digital Signature and Electronic Authentication Law and Electronic Signatures in Global and National Commerce Act*. Nevertheless, these laws do not contain restrict regulations when using digital signatures in this context.

[1] More specifically as a pair *P=(a, h(a))* where *a* represents a log entry and *h(a)* the hash value of a using the hash function *h(x)*. Elements of this pair should be strongly bound together.

[2] For additional information, see Safetica and ECPA, a Regulatory Compliance document by Safetica.

Canada

The most important law in Canada concerning electronic documents is the Personal Information Protection and Electronic Documents Act (PIPEDA[3]) [7]. The Canada Evidence Act also involves electronic evidence [8]. The trustworthiness of electronic documents as proof, according to PIPEDA, is achieved mainly by electronic signatures [7, 36] with timestamps or similar technology, so that it can be verified that from a specified time, an electronic document has not been altered. The electronic document is then considered *Original*. [7, 42]

There are also other requirements that need to be considered before using Safetica logs as evidence in a court. *"Any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be."* [8, 31.1] The Canada Evidence Act also provides additional information for electronic documents admissibility in court. According to the best evidence rule for electronic documents [8, 31.2], their integrity must be proven. Furthermore, when using digital signatures for their protection, *"(...) (a) the association of secure electronic signatures with persons; and (b) the integrity of information contained in electronic documents signed with secure electronic signatures."* [8, 31.4] must be taken into consideration.

I THE EUROPE

European Union – common criteria for all countries

There is no specific procedure in the European countries for the obtaining, analysis, and presentation of e-evidence. Nevertheless, there are three main aspects of electronic evidence that should sustain in order to be admissible by courts.

"The principles that affect electronic evidence are basically the respect for data protection standards and the respect for the secrecy of communications and for the right of freedom of expression." [9]

There are initiatives that indicate that in the following years there could be a European directive concerning digital evidence, containing the requirements for admissibility in courts.

The comparative case study [9] provides much information about the meaning of electronic evidence in member states. The local laws of some countries contain some references on electronic evidence, but these are mainly definitions of electronic evidence (meaning that the electronic evidence can be used in court), and not regulations. The case study indicates that, nowadays (because of no legal background or European framework), electronic evidence is ruled by the analogical requirements as traditional evidence, with more difficult sustaining in courts. This applies to all member states. Because of that, it is required to provide a level of security to Safetica logs in order to prove that they were not compromised. This was further discussed in the Preface of this document.

Czech Republic

Electronic evidence is not regulated by law in the Czech Republic yet. Nevertheless, there has been a court case, dealing with monitoring in the workplace: *"The judgment is precisely the case where the employer argued that the employee violated the work order and he cancelled the employment contract. The employer sustained his statement with the record of a telephonic conversation of the employee. The employee sued his former employer: he argued that the cancellation of the employment contract was not valid and he won the court case. Among other things, the court judged the question of the evidence provided by the employer – the record of the telephonic conversation,*

[3] For additional information, see Safetica and PIPEDA, a Regulatory Compliance document by Safetica.

which was collected without the permission or knowledge of any party. (...) This evidence was not accepted by the court." Transl. author. [10]

This indicates the general requirements of evidence to be collected in a legal way. The other general requirements for the evidence can be applied to increase its credibility – but they are not enforced by law.

I ASIA

According to the UNECTRA official website [16], The UNECTRA Model law 1996 was enacted by the following countries: Vietnam.

Japan

Electronic evidence is considered as traditional evidence in Japan [11]. The Criminal Procedure Act of Japan is an applicable law, which allows the use of electronic evidence in courts. The legality of collected evidence must be ensured (as discussed previously in this text) and, again, when the Safetica logs are stored in a secure way, their admissibility is easier.

Malaysia

In Malaysia, there is the Electronic Commerce Act 2006 [12] that defines electronic data and information, and provides them the same value as traditional information. This applies also to electronic evidence.

India

India enacted, in 2000, The Information Technology Act. This act provides electronic documents the same level of admissibility as for traditional documents.

I THE MIDDLE EAST

According to the UNECTRA official website [16], The UNECTRA Model law 1996 was enacted by the following countries: Bahrain, Iran, Jordan, Pakistan, Qatar, and United Arab Emirates.

Pakistan

"In Pakistan, it is allowed to use any modern devices through which evidence can be presented in court. Under the Electronic Transactions Ordinance, 2002, electronic evidence via emails etc. has also been made admissible as evidence in court." [13]

Saudi Arabia

In Saudi Arabia, there exists an applicable Electronic Transactions Protection Law [14]. It states: *"Electronic transactions, records and signatures shall have full effect and their validity and enforceability may not be contested (...)"* Therefore, the situation in Saudi Arabia is similar to those countries that enacted the UNECTRA Model law.

I SOUTH AMERICA

According to the UNECTRA official website [16], The UNECTRA Model law 1996 was enacted by the following countries: Colombia, Ecuador, Panama, Paraguay, and Venezuela.

Bolivia

The Law on Records, Electronic Signatures, and e-commerce (2007) [15] is an applicable law in Bolivia. Similar to other laws, it states that electronic documents have the same effect as traditional documents. Again, it can be applied in electronic evidence, so it is possible to use Safetica logs as electronic evidence in courts.

I SUMMARY

There are no strict rules for electronic evidence to be accepted in courts. On the other hand, the court cases, changes to legislations, international agreements, and recommendations indicate that there are some measures that should be taken in order to increase the weight of the electronic evidence collected, when it comes to a security incident. The electronic evidence should be trustworthy. To achieve this feature, everything that can provide high information value about the system (mainly the logs of Safetica) should be explicitly protected with respect to confidentiality, authenticity, integrity, and non-repudiation.

The logs and another Safetica outputs, such as summaries or screenshots, should, therefore, be backed up regularly; encrypted; their integrity should be ensured, for example by hashes and they should be stored on a medium such as a DVD; their physical protection and the protection of the backups should be ensured; non-repudiation of them should be achieved using digital signatures; access to them should be restricted and monitored; and everything related to their protection should be documented properly. The digital evidence stored in this way achieves a greater degree of credibility.

The evidence must be collected in a legal way. This means that all relevant laws and regulations must me complied with before using Safetica and its outputs as evidence. The Safetica produces, for a better understanding of the legal requirements, the Regulatory compliance documents for legislatures worldwide.

I BIBLIOGRAPHY

[1] Information and Communication Technology Policy and Legal Issues for Central Asia: Guide for ICT Policymakers [online]. Available at: <http://vi.unctad.org/digital-library/?task=dl_doc&doc_name=99-ict>

[2] *Information and Communication Technology Policy and Legal Issues for Central Asia: Guide for ICT Policymakers* [online]. Available at: <http://vi.unctad.org/digital-library/?task=dl_doc&doc_name=99-ict>

[3] ZHEN, J.: *Steps for preserving the integrity of log data* [online]. c2005. Available at: <http://features.techworld.com/networking/1964/steps-for-preserving-the-integrity-of-log-data/>

[4] *Federal Rules of Evidence* [online]. c2010. Last revision November 27th 2011. Available at: <http://www.law.cornell.edu/rules/fre/>

[5] RYAN, D. J., SHPANTZER, G.: *Legal Aspects of Digital Forensics* [online]. c2006. Last revision September 8th 2007. Available at: <http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf>

[6] DAUGHERTY, H. M.: *Daubert Test – Further Readings* [online]. Last revision March 9th 2010. Available at: <http://law.jrank.org/pages/5962/Daubert-Test.html>

[7] *Searching and Seizing Computers and Obtaining Electronic Evidence Manual* [online]. c2009. Last revision December 10th 2011. Available at: <http://www.cybercrime.gov/ssmanual/05ssma.html>

[8] *Personal Information Protection and Electronic Documents Act* [online]. Available at: <http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf>

[9] *Canada Evidence Act* [online]. Available at: <http://laws.justice.gc.ca/PDF/C-5.pdf>

[10] INSA, F.: *The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—Results of a European Study* [online]. c2007. Journal of Digital Forensic Practice, 1:4, 285-289. Available at: <http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/libro_aeec_en.pdf>

[11] BRABEC, F.: *Telefony zaměstnanců jsou soukromé* [online]. c2000. Available at: <http://mobil.idnes.cz/telefony-zamestnancu-jsou-soukrome-d7m-/mob_tech.aspx?c=A000221_0009486_mob_prakticky>

[12] *Issues Concerning the Investigation of Corporate Crime* [online]. c2008. Last revision November 14th 2010. Available at: <http://www.unafei.or.jp/english/pdf/RS_No76/No76_13RC_Group2.pdf>

[13] *ELECTRONIC COMMERCE ACT 1996* [online]. Available at: <http://www.wipo.int/wipolex/en/text.jsp?file_id=201798>

[14] SABOOHI, M.: *COLLECTING DIGITAL EVIDENCE OF CYBER CRIME* [online]. c2006. Last revision August 24th 2007. Available at: <http://www.supremecourt.gov.pk/ijc/Articles/10/2.pdf>

[15] *Electronic Transactions Protection Law* [online]. Available at: <http://www.wipo.int/wipolex/en/text.jsp?file_id=197970>

[16] *Law on Records, Electronic Signatures and e-commerce* [online]. Available at: <http://www.wipo.int/wipolex/en/text.jsp?file_id=252933>

[17] Status 1996 - UNCITRAL Model Law on Electronic Commerce [online]. Available at: <http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html>

Prague | Czech Republic | August 10, 2012