

ELECTRONIC SIGNATURE AS A PART OF INFORMATION SOCIETY INFRASTRUCTURE

*Legal and Technological situation in Finland, the Republic of
Croatia and the Czech Republic*

Juhani Paavilainen, Suzana Stojakovic - Celustka, Dagmar Brechlerova

Abstract: This study describes and compares the use of Electronic Signature, Certificate Authorities, Public Key Infrastructure and Government to Citizen (G2C) and Citizen to Government (C2G) services in three European countries: Finland, the Czech Republic and the Republic of Croatia. These countries have built their own Information Society Infrastructure where public IT security issues were mostly based on Public Key Infrastructure. The Legislation is regularly coordinated with the one of the European Union and it very slightly differs between the countries. G2C and C2G services are under construction.

Key words: Electronic Signature, Certificate Authority, PKI

1. INTRODUCTION

The beginning of the 21st century is characterized by the massive growth of electronic communication. Important part of IT implementation at the moment is electronic government (G2C, C2G). New technologies have as well brought considerable IT security risks. This required suitable technologies like electronic signature and Public Key Infrastructure (PKI) to be established as a form of managing and mitigating these risks. Technology itself proved to be insufficient for adequate administration of IT security issues and the need for 'legal infrastructure' was set.

Finland is a Scandinavian country with one of the best economy ratings in the world and is a member of the EU. Czech Republic is Eastern European

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: [10.1007/978-0-387-35691-4_52](https://doi.org/10.1007/978-0-387-35691-4_52)

D. Gritzalis et al. (eds.), *Security and Privacy in the Age of Uncertainty*

© IFIP International Federation for Information Processing 2003

country, and is currently undergoing candidacy for the EU membership. Republic of Croatia is Southern European country, one of the youngest in Europe. It started building democracy after a severe war. This study will compare current legal and technological situation of PKI in the context of information society situation among the three countries. Well known inadequacies of conventional PKI and its implementation are not taken into consideration. [18].

2. INTERNET USE STATISTICS

The use of Internet in Finland is quite widespread. In 1999 it was one of the most computerized countries in the world [15]. About 60 % of the population had computers at home, at work or in schools and around 44% used Internet constantly. In 2001 more than 90% of enterprises used Internet [16] [17]. In Finland there are about 65 Internet Service Providers (ISPs) [1]. The use of Internet in Czech Republic started in 1991. It became more common after 1996. In proportion 15 % of connections are done from home, 16% from libraries and 52% from work places. In Czech Republic there are many ISPs.

The use of Internet in Croatia started in 1992. It was mostly used in academic purposes. Currently there are about 200 000 Internet users and 9 ISPs.

	Czech Republic	Finland	Republic of Croatia	EU Average [21] [22]
Area (Km ²)	78866	337030	56542	
Population (millions)	10,3	5,2	4,4	375
GPD (\$/capita) (2001)	14400	25800	8300	22500
Fixed telephone connections (Per 100 persons) 2001, 1)1997	38	55 ¹⁾	39	46
Mobile phones (Per 100 persons) 2001, 2) 1997	53	57 ²⁾	30	40
Internet users (% of population) (2000)	11	44	5	19
Number of Government Web-Sites (2000/2002)	83/168	198/198	60/75	
ISP Providers (in 2000)	More than 300	65	9	

Table 1. A summary of characterizations [1] [21] [22].

3. ELECTRONIC SIGNATURE SITUATION AND RELATED SERVICES

Electronic signature is well known application of PKI, therefore it is not described in more detail. In the following sections terms such as certificates, certificate providers, electronic signatures, advanced electronic signatures and other PKI related terms are used as they are defined in EU Directive 1999/93. [4]. The definitions are given in those cases where used terms differ.

3.1. Certificates and Certificate Service Providers

In the late 1990s Finland reformed and harmonized its laws according to EU legal regulations. Five new laws relating to information security and electronic administration were passed in 1999 (Acts 565, 723, 760, 1318, 189). This was a sign that the administration was trying to accommodate the recent advances in Internet use. A new identification card with electronic ID was issued by police in 1999. A person who wanted the new FINEID (Finnish Electronic Identity) card could use with (secret key is in the card) or without electronic identification. Thus the Finnish government defined that Finnish governmental PKI is grounded on the use of smart card based authentication. This means that a card reader is needed for on-line use. In the future, identification will be done from a mobile device such as a cellular phone equipped with a special chip. Currently the FINEID card cannot be used as a social security card and is more like an ID and travel document without general public administration use.

In Finland there are several Certificate Service Providers (CSP) but only the Finnish Population Register Centre is accredited. This is provided for in the Finnish laws 507/1993, 1318/1999 829/1999. CSPs in Finland do not have any hierarchical structure. The basic idea, under current legislation, is that certificate service provision is pure business. Every company that fulfils all the requirements for an accredited service provider can be such a provider. Thus, CSPs satisfy Finnish laws and also business laws.

In the Czech Republic the mode of action is quite similar to Finland. The PKI system is not hierarchical. The Electronic Signature Act of the Czech Republic (Act. 227/2000) [3] also defines requirements of CSPs [2]. This act differs slightly from the EU directive [3] and only use as a qualified certificate is under this Act. The Electronic Signature Act was amended in 2002 [6]. There are several CSPs in the Czech Republic but most of them are in business fields. Only one CSP is currently accredited. Certificates and keys issued by this CSP are only accepted by public administration

authorities [3]. The qualified certificate from this accredited provider (with or without smart card) is expensive for ordinary people.

In Croatia public infrastructure is undergoing major development. Like other European countries Croatia is also constructing laws closer to EU legislation. PKI systems are in use, but mostly in the business field, i.e. banks and financial organizations. These systems are internal business systems and cannot be used in public transactions. Every system has its own certificate provider and is not officially accredited. The law on electronic signature was passed at the beginning of 2002 and its definitions of certificates and signatures are very similar to the EU directive [4][7][8][9][10]. The root certificate is in the possession of Ministry of Economy which is also the Bridge Certification Authority. It intrinsically defines the hierarchical structure of PKI. The first CSP is Croatian Financial Agency (FINA). Other possible providers are not yet known.

3.2. Accepted certificates in public administration

In Finland accepted certificates have been prescribed by the law "Act on Electronic Services in Administration" [13]. Every public authority has to give the opportunity for electronic transactions (under predefined conditions) and an accredited certificate must be accepted. In principle all public authorities are ready for G2C/C2G services regarding the law but technically the situation is not the same. Only a few public authorities offer services where certificates can be used.

The current situation in Finland is that the Act on Electronic Signature is still undergoing preparation. Current certificates can be divided to certificates and qualified certificates, which are officially accredited. Practically this is FINEID. In the draft legislation 197/2001 qualified certificate is defined as "a civil certificate" and every Finnish citizen will have one [14]. This creates the possibility for new G2C and C2G services.

According to the Czech Republic Act [3]: "In the area of organs of public authority, only advanced electronic signatures and qualified certificates issued by an accredited certification-service-provider may be used." Currently there is only one accredited CSP. In Croatia there is not yet exact definition what certifications are accepted by public authorities.

3.3. Existing G2C and C2G services

The Finnish government has been committed to information society and G2C and C2G services, but the information society is not yet in full swing. Nowadays there are more than twenty services which are using accredited certificates, but only 13 000 FINEID cards are in use. To improve the current

situation the state has started several pilot projects where certificates have been used. One was the FEIDHE project (Electronic Identification in Finnish Higher Education) [11]. The purpose was to investigate and to plan possibilities for implementing a smart card based electronic identification system in institutions of higher education. One goal was to make a full scale PKI system and it was first in the world on this scale and with technology. Another was a project named Satakunta Macro Pilot where a new electronic social security card was introduced [12]. There were many technical problems in these projects caused by actors, vendors, problems in software and technical interfaces. Nevertheless, these projects demonstrated that electronic ID card and certificates can be used in public services but the infrastructure as a whole, established procedures and service processes are not ready for this.

In the Czech Republic there is only one public administrative application that currently uses advanced electronic signatures and qualified certificates [3]. This application is for social support, but only 3 people have used it because the required confirmation had to be also on paper. However, the new Ministry of Informatics has great new plans for the novel use of electronic signature in all public administration

Because laws and regulations have only recently been passed and legislative infrastructure has just been built in Croatia, the new services do not yet exist. The current PKI practice in Croatia after the Electronic Signature Act and its Regulations has not much changed from the practice before this act. Intensive efforts are in progress to make the proposed PKI work as soon as possible.

4. CONCLUSIONS

Finland was one of the first countries to produce electronic identity and related services. The first release of a national electronic identification card and related services was more or less unsuccessful. Therefore, Finland is now losing its position as a leading country in the information society. Czech Republic and Croatia started a little later with their own information societies, but have caught up with Finland and other European countries. The gap between these countries is becoming smaller all the time [20]. Even though technological and legal infrastructures in the information society differ, the practical situation is almost the same. Main obstacles for practical use of electronic signature and PKI are: the certificates are too expensive for ordinary people; the advantages of their use are not clearly explained to public; the use of Internet is not so widespread or is too expensive; the required forms are still complicated and there is no suitable knowledge about

proper use of PKI and electronic signatures. As the situation in Finland shows, it seems to be a long way from building legal and technological infrastructure for the general use of G2C and C2G services. Countries which have started later, can learn from existing mistakes and failures and avoid wasting their resources.

REFERENCES

- [1] The World fact Book 2002, <http://www.cia.gov/cia/publications/factbook/index.html>
- [2] Brechlerová D. "IT and Law – The Situation in the Czech republic". In *Security and Control of IT in Society –II*, IFIP, p.173-181, 2001.
- [3] Electronic Signature Act http://www.uoou.cz/eng/227_2000.php3
- [4] EU Directive 1999/93, Community framework for electronic signatures, Official Journal L 013, 19/01/2000 p. 0012-0020.
- [5] Hobley Christopher. Just numbers, Numbers on Internet use, electronic commerce, IT and related figures for the European Community. January 2001, Published by the European Commission's Electronic Commerce Team
- [6] Novel proposal for Czech Republic Electronic Signature law, www.uoou.cz/Z-226-2002.pdf, only Czech
- [7] Croatian Electronic Signature Act, NN No. 10, 30.01. 2002, (in Croatian),
- [8] Croatian Regulation about Evidence of Providers of Certification Services for Electronic Signatures, NN No. 54, 15.05.2002., (in Croatian)
- [9] Regulation about Measures and Actions of Use and Protection of Electronic Signature, Advanced Electronic Signature, Equipment for Making Electronic Signature and [Croatian Act 5] Advanced Electronic Signature and Systems for Certification and Obligatory Insurance of Providers of Qualified Certificates, NN No. 54, 15.05.2002., (in Croatian)
- [10] Regulation about Technical Rules and Conditions of Connection of Systems for Certification of Electronic Signatures, NN No. 89, 25.07.2002., (in Croatian)
- [11] FEIDHE project report, <https://hstya.funet.fi/>
- [12] Report of Satakunta macro project (<http://www.makropilotti.fi/english/>)
- [13] Finnish Act 1318/1999, Act of Electronic Service in the Administration, Also in English:
- [14] HE 197/2001, Finnish Government's proposal for new Electronic Signature law.
- [15] Internet Metrics: using Host and domain counts to Map the Internet. The International Journal on Knowledge Infrastructure Development, Management and Regulation Volume 24, No. 6/7 (July/August 2000), <http://www.tpeditor.com/contents/2000/zoook.htm>
- [16] Internet and eCom in enterprises in 2002 Tilastokeskus. (in Finnish)
- [17] Nordic Information Society Statistics 2002, Nordic Council of Ministers, Yliopistopaino, Helsinki 2002 , ISBN 952-467-109-3
- [18] Roger Clark, "The Fundamental inadequacies of Conventional Public Key Infrastructure". In Proc. Conf. ECIS. 2001 June; Bled Slovenia.
- [19] Anzinger Gunnar. Governments on the WWW, www.gksoft.com/govt/en/world.html
- [20] European Economy. Directorate-general for Economic and Financial Affairs, Supplement B, Business and Consumer Surveys results, No 12, December 2000.
- [21] Straubhaar Thomas. Migration Policies and EU Enlargement, East-West Migration: Will It Be a Problem?. Intereconomics, July/August 2001. P 167-170.