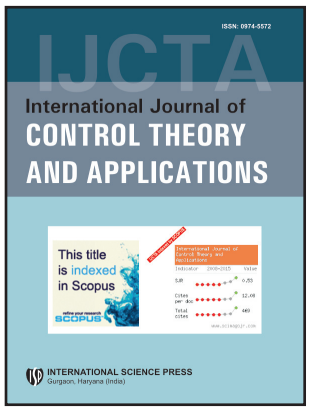

International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 9 • Number 43 • 2016

An Analysis of Trust Models of Public Key Infrastructure

Soshi Hamaugchi[a], Toshiyuki Kinoshita[b] and Satoru Tezuka[c]

[a]*School of Computer Science, Tokyo University of Technology, Tokyo, Japan. Email: soshi.hamaguchi@gmail.com*
[b]*Ph.D. School of Computer Science, Tokyo University of Technology, Tokyo, Japan. Email: Kinoshi@stf.teu.ac.jp*
[c]*Ph.D. Graduate School of Media and Governance, Keio University, Kanagawa, Japan. Email: Tezuka@sfc.keio.ac.jp*

Abstract: This paper presents a comparative study of five trust models, ETSI certification, WebTrust for CA, the US Federal PKI, EU eIDAS regulation and Japanese e-signature Act. We first explained each of trust models before the comparison. Similarities and differences were identified by comparing these five trust models which have different assurance level. We also derived principles of designing a new trust model by analysing the identified similarities and differences.

Keyword: PKI, Trust Model, Assessment, eIDAS, ETSI, WebTrust for CA, FPKI,

1. INTRODUCTION

Businesses and societies are increasingly global and are more and more based on electronic transactions. To establish trust between two or more entity in certain circumstances is very important. The US psychologist Denise Rousseu introduced the widely held definition on "trust" as *"a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another"* [1]. Required positive expectations to reach the state of trust may differ from application by application such as making online payment, signing on his/her e-mail and signing business contract. To enhance the trust upon such situations, several trust models have been established such as eIDAS regulation, ETSI certification, WebTrust for CA and the US Federal PKI.

This paper organizes existing trust models in order to find out the similarities and differences between them and analyses these findings in order to derive fundamental structural requirements for such trust models.

2. RELATED WORKS

Mark Sel compared the trust models of ICAO's global PKI Directory, the EU eIDAS regulation, the US FICAM model and Bitcoin's Blockchain and clarified similarities and differences between these trust models [2]. Mark Sel also introduced key concepts and terminology for trust model. This paper is going to analyse the trust model

for PKI and not only compare the trust models but also try to find the requirement for a trust model to achieve required certain assurance level.

Our previous study identified differences between ETSI certification and WebTrust for CA from both scheme and technical requirement point of view, and examined the possibility of reuse of certification result [3]. This paper rather compares the trust models for different assurance levels to analyse the similarities and differences among various trust models.

3. ETSI CERTIFICATION

Both ETSI and WebTrust for CAs are well known to major browser vendors and CAs issuing SSL certificate because these two models are adopted by trusted rootCA program of major browser vendors such as google, Mozilla and Microsoft [4]. SSL certificate is electronic certificate for organization managing web server and enable secure connection between browser and web server. When a SSL certificate is issued by a CA under trusted rootCA program and the SSL certificate is securely installed, closed-padlock will be shown as a symbol for secure connection like Figure 1.

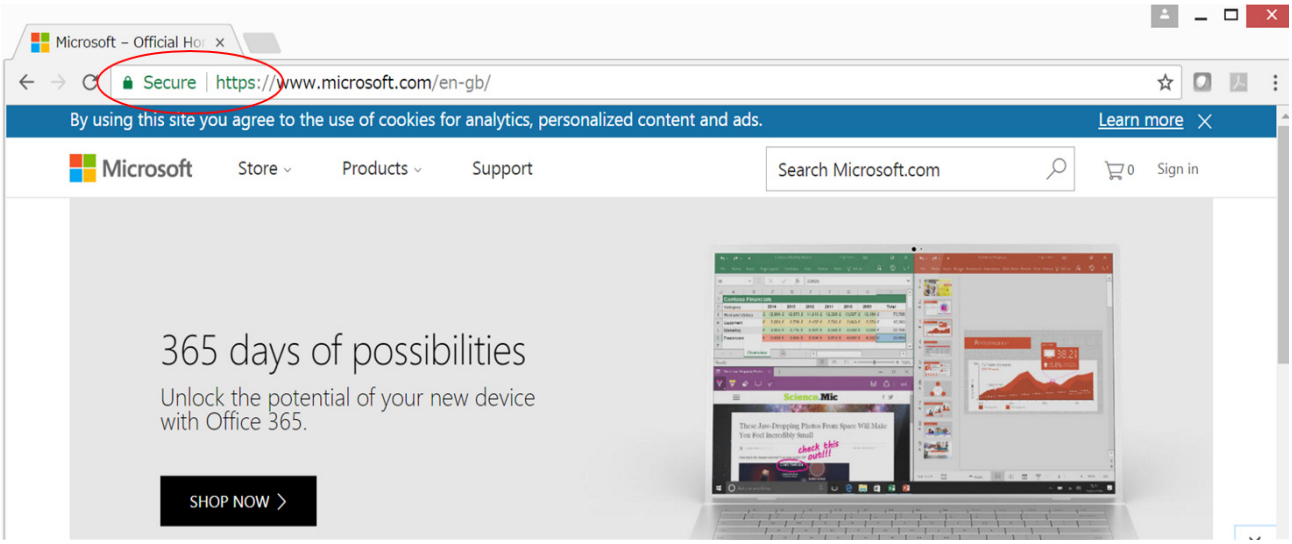

Figure 1: Indication of validation result of SSL Certificate on google chrome

Certification in accordance with ETSI standards are performed by certification bodies which are accredited by national accreditation bodies. Harmonization of accreditation processes among accreditation bodies is ensured by European Co-operation for Accreditation. Below Figure 2 shows the trust model of ETSI Certification for the trust rootCA program.

ETSI standards are developed by ETSI experts from industries and all requirements from CA/B Forum are included in the latest standards [5][6][7]. Therefore, conformance to the requirements described in ETSI standards can demonstrate that the CA fulfils the required assurance level in order to be trusted by browser vendors and their users. Inclusion to the trusted rootCA program is typical use case of ETSI certification but application is not limited to this.

4. WEBTRUST

WebTrust for CAs is another well known scheme for CAs and browser vendors as described in the previous chapter. Assessments of Web Trust for CAs are performed by independent accountant firms which are recognized

by AICPA/CICA. Trust model for WebTrust is very simillar and comparable to ETSI certification model excpet for the absense of harmonization body due to the fact that the AICPA/CICA is the only one accreditation body for this scheme.

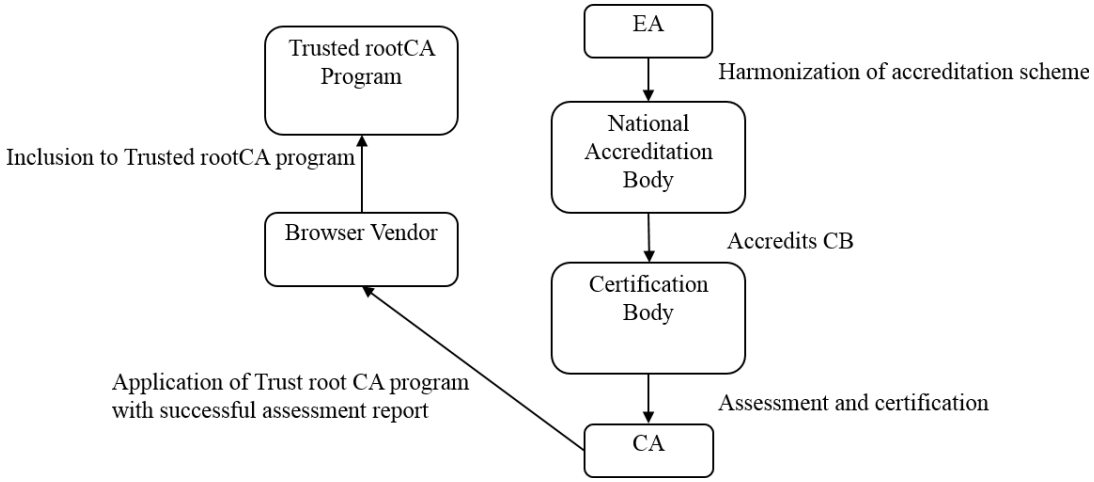

Figure 2: A trust model of ETSI Certification for root CA program

Figure 3 below shows the trust model of WebTrust for CAs program. Also application to trsuted rootCA program is not a part of WebTrust program, this is a very typical application.

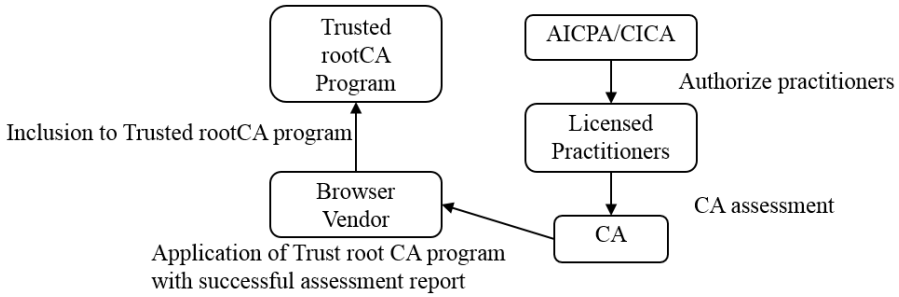

Figure 3: A trust model of WebTrust for root CA program

Likewise ETSI standards, audit criteria of WebTrust CAs include all defined requirements from CA/B Forum [8][9]. Therefore, conformance to WebTrust for CAs can also demonstrate that the CA fulfils the required assurance level in order to be trusted by browser vendors and their users.

5. eIDAS

eIDAS regulation was adopted in EU in July 2014 and the legal framework for trust services were established across Europe [10].

Trust model of eIDAS and previous trusted rootCA program are so called Trust list model but is still very similar to previous two models. Conformity assessment of eIDAS is performed by Conformity Assessment Body accredited by National Accreditation Body and, like ETSI certification, harmonization of accreditation processes among accreditation bodies is ensured by European Co-operation for Accreditation [11]. Below Figure 4 shows typical trust model of eIDAS. Successful assessment report is sent to Trust service Status Notification Body from Conformity Assessment Body and Trust Service Status list will be updated and CA is listed as qualified trust service provider.

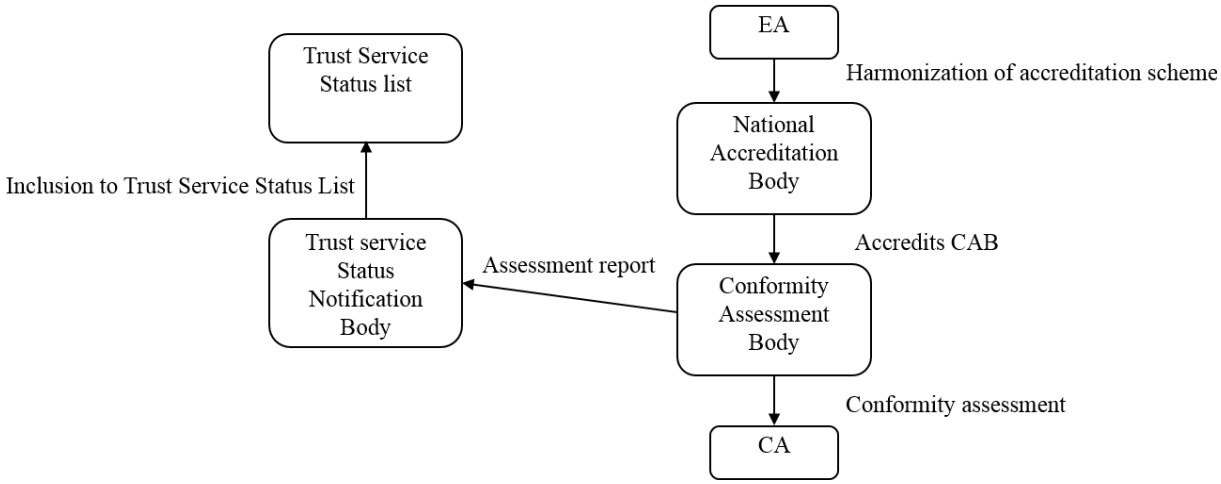

Figure 4: A trust model of eIDAS

Role of Trust Service Status list is a trust anchor for relying parties. For example, person who received electronicaly signed document can check with this Trust Service Status list if the certificate used for the e-signature is issued by one of the qualified trust service providers.

By the Trust Service Status list, qualified trust service provider can prove that their service is legally effective.

6. FPKI

In contrast to the Trust List models, the US federal PKI is a bridge CA model. Centre of this trust model is Federal Bridge CA. Federal Bridge CA acts as a Trust Hub for disparate PKI domains. Policy mapping is performed by Federal Policy Management Authority and Federal Bridge CA cross-certifies with CA which fulfils the requirements of applicable NIST standards and guidelines of FPKI [12][13]. Below Figure 5 shows the trust model of FPKI.

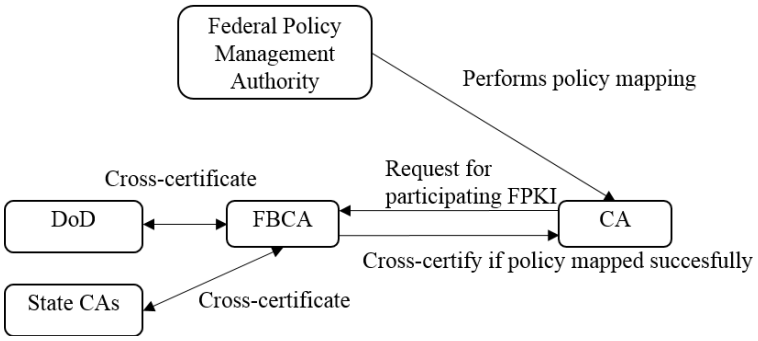

Figure 5: A trust model of FPKI

Cross-certification with Federal Bridge CA can demonstrate that the CA operation and its security level is equivalent to what the US governments requires for their PKI system.

Certification policy of each CAs are mapped to leve1 of assurance 1 to 4 described in NIST SP 800-63.

7. JAPANESE E-SIGNATURE ACT

Japanese e-Signature Act sets a legal framework for e-signature in Japan. Figure 6 describes a trust model of Japanese e-signature Act.

Figure 6: A trust model of Japanese e-Signature Act

Competent Ministers, Minister of Internal Affairs and Communications, Minister of Justice and Minister of Economy, Trade Industry, designated an investigative organization which investigates the conformance of applied certification business. Accreditation status to the applied certification business is granted by Competent Minster when successful investigation is received from the designated investigative organization.

Electronic signature based on the certificate issued by accredited certification business is regarded as legal effective signature.

8. COMPARISON OF DIFFERENT MODELS

The comparison among five trust models is presented in the below Table 1.

A. Similarities

Following similarities are analysed.

- NAB, CB, CAB are involved in all of the trust models compared.
- Existence of supporting technical standards.

Trusted third party is fundamental for all of trust models studied in this paper. The role of the trusted third party is to check the CAs conformance to the agreed requirements for all of stakeholders (e.g. users, applicants and relying parties, etc.).

Supporting technical standards are not only providing detailed technical requirements for applicant CA, but also providing transparency of entire model and technical interoperability within the domain of the model.

B. Differences

Major differences are observed by the reason of different assurance level to be achieved and necessity of harmonization body. Both ETSI certification and WebTrust are to provide technical compliance to the requirements agreed by industry and not for legal admissibility even though compliance to ETSI standards or WebTrust may have massive meaning in jurisdiction. Thus No. legal background and governor exist in these two models. On the other hand, eIDAS and Japanese e-signature act are for providing legal value on trust service although the scope of Japanese e-signature act is limited to e-signature. For these two models, law and governor are necessary so that whole trust chain of the model is ensured by the law or governor.

Harmonization body for ETSI certification and eIDAS is required because both models cover multiple accreditation bodies.

Table 1
Comparison among 5 models

	ETSI Certification	*WebTrust*	*eIDAS*	*FPKI*	*Japanese e-Signature Act*
Law	N/A	N/A	eIDAS regulation	E-Government Act of 2002	Act on Electronic Signatures and Certification Business
Objective	Technical Interoperability and trusted third party assessment	Technical Interoperability and trusted third party assessment	Legal recognition of trust services,	Identity management and trust across organizational, operational, physical and network boundaries.	To promote the distribution of e-document through ensuring the smooth use of e-Signatures.
Governor	N/A	N/A	EU Committee	CIO Council	Ministry of Economy, Trade and Industry. Ministry of Internal Affairs and Communications. Ministry of Justice.
Harmonization Body	EA	N/A	EA	N/A	N/A
Accreditation Body	National Accreditation Bodies	AICPA/CIPA	Member states	FPKI Policy Authority	Ministry of Economy, Trade and Industry. Ministry of Internal Affairs and Communications. Ministry of Justice.
Certification Body	CB accredited by NAB	Licensed Practitioners	Supervisory Body	FPKI Policy Authority	Same as above
Conformity Assessment Body	evaluation body	Same as above	Conformity Assessment Body	FPKI Cortication Policy Working Group	Designated Investigation Organization
Supporting Technical Standards	ETSI Standards	WebTrust Criteria	ETSI Standards, CEN Standards	NIST SPs, FIPS 201, FPKIPA Documents	Accreditation Criteria
Assurance to be achieved	Technical Compliance	Technical Compliance	Legal admissibility + Technical Compliance	Technical Compliance, Interoperability with Federal PKI system	Legal admissibility + Technical Compliance

Federal PKI is more complex, because at first FPKI was only federal-wide system and opened to the industry afterwards. FBCA is the bridge between the Federal PKI trust infrastructure and industries.

C. Basis of Designing a New Trust Model

As businesses and societies are increasingly global, mutual recognition and interoperability among nations, industries should always be considered when designing a new trust model. Similarities and differences found out in this study can be used to derive the basic requirements of a new trust model. Similarities among all trust models are, on the other word, common parts and these are the fundamentals to establish the trust. Trusted third party assessment, consists of accreditation body, certification body and conformity assessment body, is the essential for the trust model. Self-declaration may be adopted instead of trusted third party assessment, but assurance level to be achieved by such model is very limited.

Development or assignment of supporting technical standards is important as well because this will be a consensus between stakeholders regarding width and depth of the assessment requirement.

From differences, optional requirements for a trust model can be derived. Harmonization Body is required only when the trust model supports multiple accreditation body. Law and governor are required when the legal admissibility is assured by the trust model.

9. CONCLUSION

Upon designing a new trust model, interoperability and mutual recognition with other or existing trust model should be considered due to the rapid business and society globalization. However, the assurance level required for the trust model is differ from application by application and appropriate design, understanding and adoption of trust model are challenges also.

We compared and analysed five trust models and found out the similarities and differences among them. By analysing the different trust models, principle for designing a new trust model are identified and we believe these identified principle can contribute to design a new trust model which are interoperable and comparable to the existing models. Furthermore, this paper organized and explained five existing trust models. We hope our study will help to obtain appropriate understanding about the trust models, and proper adoption and application of the trust models.

REFERENCES

[1] Denise M. Rousseauo, “NOT SO DIFFERENT AFTER ALL: A CROSS-DICIPLINE VIEW OF TRUST”, Academy of Management Review 1998, Vol. 23 No. 3, 393-404.

[2] Marc Sel, “A Comparison of Trust Models”, ISSE 2015 pp 206-215.

[3] Soshi Hamaguchi, Toshiyuki Kinoshita and Satoru Tezuka, “Examination on Possibility on Reuse of Certification Result between Different Assessment Scheme for Certification Authority”, The 15th International Conference on Security and Management, Las Vegas Nevada, USA 2016.

[4] CA/Browser Forum, Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates, Version 1.4.2, January 2017.

[5] European Telecommunication Standards Institute, ETSI EN 319 401 V2.1.1, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers, February 2016.

[6] European Telecommunication Standards Institute, ETSI EN 319 411-1 V1.1.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements , February 2016.

[7] European Telecommunication Standards Institute, ETSI EN 319 411-2 V2.1.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, February 2016.

[8] CPA Canada, WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.4.5, April 2014.

[9] CPA Canada, WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.1, November 2016.

[10] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[11] European Union Agency for Network and Information Security, Guidelines on initiation of qualified trust services, final draft 0.7 September 2016.

[12] Federal PKI Management Authority, Federal PKI Trust Infrastructure Overview, V1.0 September 2015.

[13] Federal Public Key Infrastructure Policy Authority, Federal Public Key Infrastructure (FPKI) Concept of Operation (ConOps), Version 1.0.0, January 2012.