Electronic Preprint for Journal of Information Processing Vol.20 No.3

Regular Paper

Quantifying Cost Structure of Campus PKI Based on Estimation and Actual Measurement

Shigeaki Tanimoto[1,a)] Masahiko Yokoi[2] Hiroyuki Sato[3] Atsushi Kanai[4]

Received: September 9, 2011, Accepted: February 3, 2012

Abstract: A ubiquitous ICT environment has rapidly developed through cloud computing, becoming very convenient to use. However, the threats of computer viruses, unauthorized accesses, attacks on servers, etc. have emerged. These threats also occur in the academic environment. Thus, a public key infrastructure (PKI) construction for achieving a safe and secure university ICT environment is desired. The University PKI project is underway at the National Institute of Informatics, and common specifications, such as supply specifications for a campus PKI and certificate policy/certification practice statement guidelines, have been proposed. However, PKIs are still rarely deployed. They generally have a high cost structure, and this has become one of the issues in their spread and promotion. This study quantitatively clarifies the cost structure of a PKI through estimation and actual measurement. This clarification will contribute to the increased use and advancement of a campus PKI.

Keywords: PKI, work breakdown structure, cost structure, work simulation

1. Introduction

A ubiquitous ICT environment has rapidly developed through cloud computing, becoming very convenient to use. However, the threats of computer viruses, unauthorized accesses, attacks on servers, etc. have emerged. These threats also occur in the academic environment. Thus, a public key infrastructure (PKI) construction is desired for achieving a safe and secure university ICT environment. However, since extensive knowledge and operation know-how regarding authentication technology are needed for this PKI construction and operation, installation is difficult. With the aim of easing PKI installation in an academic organization, the University PKI (UPKI) project is underway at the National Institute of Informatics. Common specifications, such as supply specifications for a campus PKI and certificate policy/certification practice statement (CP/CPS) guidelines, have been proposed [1], [2]. However, PKIs are still rarely deployed. Many elements are required in a PKI construction in order to guarantee high security, e.g., a *System*, the *PKI operation*, and a *Facility*. Thus, a PKI has a high cost structure.

This work quantitatively clarifies the cost structure of a PKI through an estimation method and an actual measurement method. First, to calculate the cost of the PKI by using estimation, the PKI was specifically subdivided into a work breakdown structure (WBS) [3], which is a typical method of estimation. Furthermore, a work simulation was performed for every work package, i.e., subdivision unit, and the cost structure of the PKI could then be clarified. Next, to actually measure the cost, a certificate authority was built, and the cost (man hours) of actual PKI operation was calculated for the prototype. By using these results, executive officers can easily decide whether to introduce a PKI. This ease contributes to the spread and promotion of PKIs.

Section 2 reviews the target of UPKI: the campus PKI model. In Section 3, the issues preventing the spread and promotion of the campus PKI are described, and the necessity of quantitatively clarifying the cost structure of a PKI is also detailed. In Section 4, a combination of estimation and actual measurement methods as a typical quantification method is used for software development, and the cost structure of the campus PKI is quantitatively clarified. Section 5 discusses related research, and Section 6 shows a future problem and concludes the paper.

2. Campus PKI

The outline of a campus PKI is described here. As mentioned, the UPKI project (**Fig. 1** (1)) is being conducted at the National Institute of Informatics. The UPKI consists of three-layer architecture from the viewpoint of cooperation with the existing PKI [3].

(1) Open domain PKI: This is the authentication infrastructure for end users outside the university, such as those disclosing a paper or giving a guest lecture at the university.

(2) Campus PKI: This is the authentication infrastructure limited for users in the university, such as students, school staff, etc. Accordingly, a university can develop and provide various unique applications for purposes such as student records management and electronic approval of staff [3], [4], [5], [6].

[1] Faculty of Social Systems Science, Chiba Institute of Technology, Narashino, Chiba 275–0016, Japan

[2] CIO department, NTT Communications, Chiyoda, Tokyo 100–8019, Japan

[3] Information Technology Center, The University of Tokyo, Bunkyo, Tokyo 113–8658, Japan

[4] Faculty of Science and Engineering, Hosei University, Koganei, Tokyo 184–8584, Japan

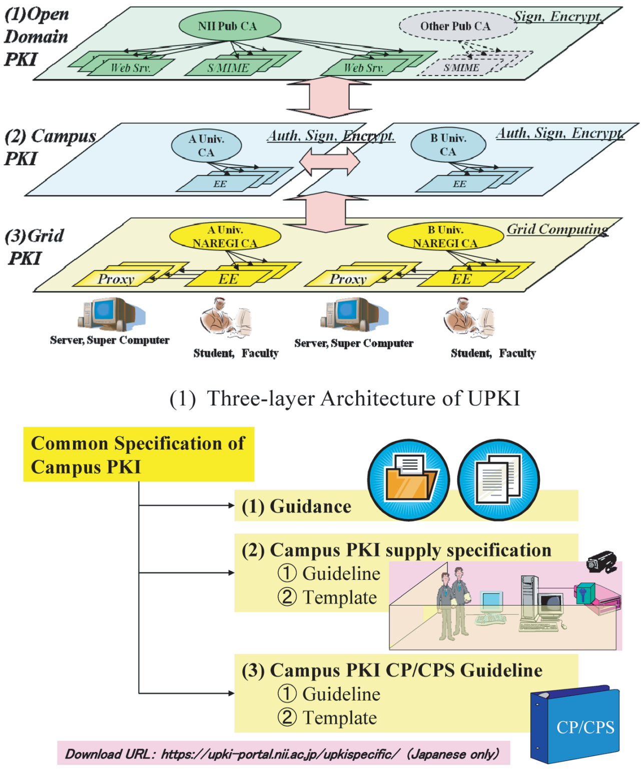
[a)] shigeaki.tanimoto@it-chiba.ac.jp

(3) Grid PKI: This is the authentication infrastructure used in a grid computing environment. The end entity issues the proxy certificate that transfers authority, and the grid PKI provides the structure for authentication using this certificate.

This paper focuses on a campus PKI, which is the core of the UPKI project. The National Institute of Informatics has decided on UPKI common specifications [2], [7] from the viewpoint of spreading and promoting campus PKIs. The UPKI common specifications offer guidelines on the factors that make introducing a campus PKI easy. These guidelines cover supply specifications and CPs/CPSs [2], [7].

3. Main Issues in Spread and Promotion of Campus PKI

There are two main issues to consider in the spread of a campus PKI. One is that there are few killer applications from the user viewpoint. The other is that a PKI has a high cost structure from the provider viewpoint [8], [9].



(1) Three-layer Architecture of UPKI

(2) Common Specifications of Campus PKI

Fig. 1 Position of campus PKI in UPKI.

3.1 Few Killer Applications in PKI

For a system to become widespread in use, the presence of a killer application is generally needed. A killer application would be indispensable for advancing the spread of PKIs, but one is not currently available. Wireless LANs, an online journal, and single sign-on (SSO) are used in present PKI authentication. Furthermore, Secure/Multipurpose Internet Mail Extensions (S/MIME) are used for the digital signature or encryption. However, these are not considered killer applications.

3.2 High Cost Structure of PKI

A PKI is generally composed of three elements: a *System*, the *PKI operation*, and a *Facility* (**Fig. 2** (1)). Each of these elements includes various factors adding to the cost, such as identification and authentication, compliance audits and other assessments, tamper-proof equipment, and fireproofing/waterproofing of the facility (Fig. 2 (2)). All these cost factors mean that the overall high cost of the PKI is inevitable.

3.3 Quantification of Cost Structure

As shown in Fig. 2, a PKI qualitatively has a high-cost architecture, but the cost structure has not yet been quantitatively examined in detail. This work quantitatively investigates the high cost structure of a PKI, which is a direct factor in the occurrence of PKI installation and is a problem in the spread and promotion of a campus PKI.

4. Analysis of PKI Cost Structure

First, the preconditions for analyzing a cost structure are described. Next, to analyze the cost structure quantitatively, the results of having subdivided the cost structure of a PKI with the WBS method [10] are presented. Furthermore, for detailed analysis, a business flow is modeled for every work package derived with the WBS method, and the cost structure of the PKI is clarified.

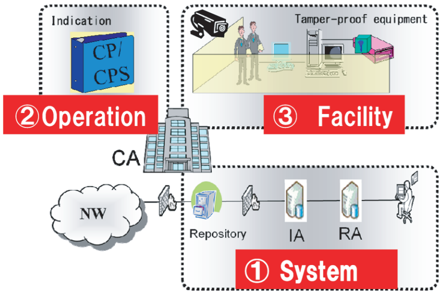
4.1 Preconditions

4.1.1 Target of Cost Estimation

The cost structure of a PKI is generally divided roughly into equipment cost and labor costs. Since equipment cost is already well known, this work focuses only on labor costs.

4.1.2 Method for Estimating PKI Labor Cost

The general analytical methods for expressing the PKI labor cost structure quantitatively are shown in **Table 1**. For estimation



CA: Certificate Authority, RA: Registration Authority, IA: Issuing Authority

Element	Main Cost Factors	
(1) System	RA	Issuing Registration, Revocation Registration, Inspection, Key Pair Generation
	IA	Certificate Issuing, Certificate Revocation, Repository
(2) Operation	CP/ CPS	Identification and Authentication, Certificate, CRL, and OCSP Profiles, Compliance Audit and Other Assessments
(3) Facility	Tamper-proof equipment, Fire prevention / Waterproofing function, Surveillance cameras	

Fig. 2 Three elements of PKI and main cost factors.

of the cost structure, the integrating method was used; the guessing method could not be used because no previous calculations of the PKI labor cost structure exist. For actual measurement, since operation based on CP/CPS is needed for a standard actual measurement, a simple evaluation of the operation of a prototype PKI was done.

Thus, the labor cost structure of a campus PKI was quantitatively clarified using the integrating method and actual measurement of the operation of a prototype PKI.

4.2 Analysis Results of Integrating Method

4.2.1 Subdivision by WBS Method

Quantitative clarification of the labor cost structure of a campus PKI was conducted based on the UPKI common specifications. That is, based on these specifications, the cost structure of the PKI was subdivided into work packages (WPs), the minimum unit in a WBS. Some of the subdivisions are shown in **Fig. 3**. First, the cost structure of the PKI was divided into the costs of the registration authority and the issuing authority (Level 1). These were then subdivided hierarchically until a WP, i.e., the minimum unit of the WBS (Level 3 or 4), was obtained. The purpose of creating WPs is to make functional units. That is, as Fig. 3 shows, we decided to consider some of these processes, such as Key Pair Generation Work (1.2.2.4) and Identity Validation Work (1.2.2.2), as work packages.

The results of subdividing the PKI cost structure by using the WBS method are shown in Appendixes A and B. These results were verified in terms of their comprehensibility and validity by using the Campus PKI supply specification guidelines (Fig. 1 (2)). The results shown in both Appendixes were classified according to the type of certificate authority (issuance or registration), the PKI cost element, and the PKI phase. The results are shown in **Table 2**. For the classification by the PKI phase, each WP was classified according to the initial cost (cost required only at the time of initial installation) and running cost (cost incurred during operation of the PKI).

As shown in Table 2, the operation cost structure of the PKI consists of a total of 84 WPs. The total numbers of WPs for the registration authority and for the issuance authority do not differ greatly. Moreover, the results of classification by the PKI cost

Table 1 General analytical method of PKI labor cost structure.

Analytical method		Description
Estimation method	Guessing method	Guess the cost structure from a past similar example.
	Integrating method	Cost structure is subdivided by WBS, and then man hours are calculated for every work package, i.e., subdivision unit. Finally, cost structure is computed by integrating the man hours of each work package.
Actual measurement method		Prototype PKI is actually operated, and the man hours related to the operation are calculated.

Table 2 WBS subdivision of PKI labor cost (unit: number of WPs).

	Element	Number of WPs		Subtotal
		Initial Cost	*Running Cost*	
Registration Authority	*System*	15	0	15
	Operation	2	23	25
	Facility	5	0	5
Issuing Authority	*System*	18	0	18
	Operation	1	13	14
	Facility	7	0	7
Total		48	36	84

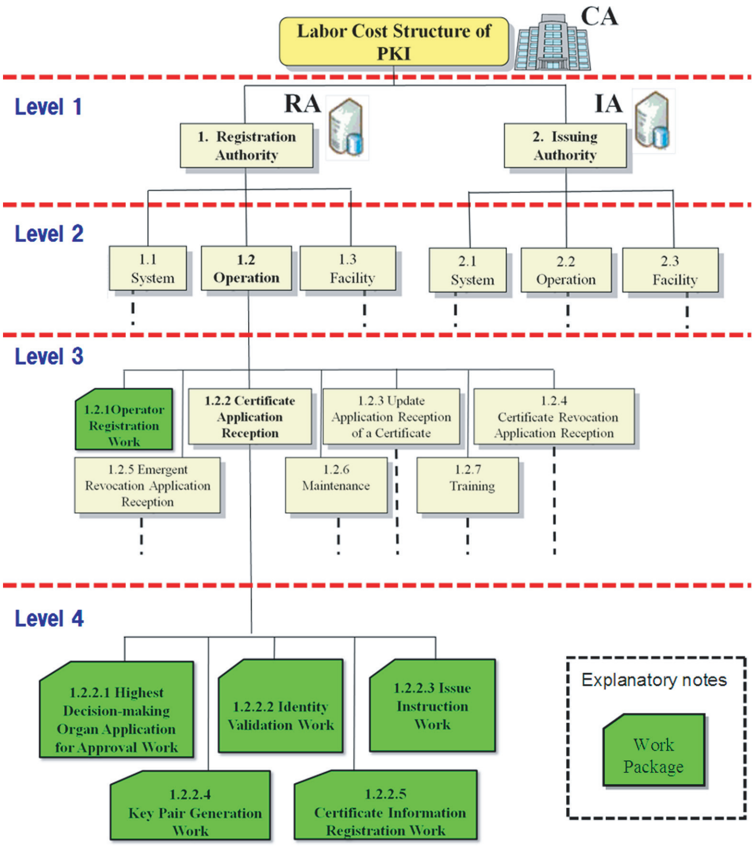

Labor Cost Structure of PKI
CA
Level 1
RA
IA
1. Registration Authority
2. Issuing Authority
Level 2
1.1 System
1.2 Operation
1.3 Facility
2.1 System
2.2 Operation
2.3 Facility
Level 3
1.2.1Operator Registration Work
1.2.2 Certificate Application Reception
1.2.3 Update Application Reception of a Certificate
1.2.4 Certificate Revocation Application Reception
1.2.5 Emergent Revocation Application Reception
1.2.6 Maintenance
1.2.7 Training
Level 4
1.2.2.1 Highest Decision-making Organ Application for Approval Work
1.2.2.2 Identity Validation Work
1.2.2.3 Issue Instruction Work
1.2.2.4 Key Pair Generation Work
1.2.2.5 Certificate Information Registration Work
Explanatory notes
Work Package

Fig. 3 Example WBS of PKI labor cost structure.

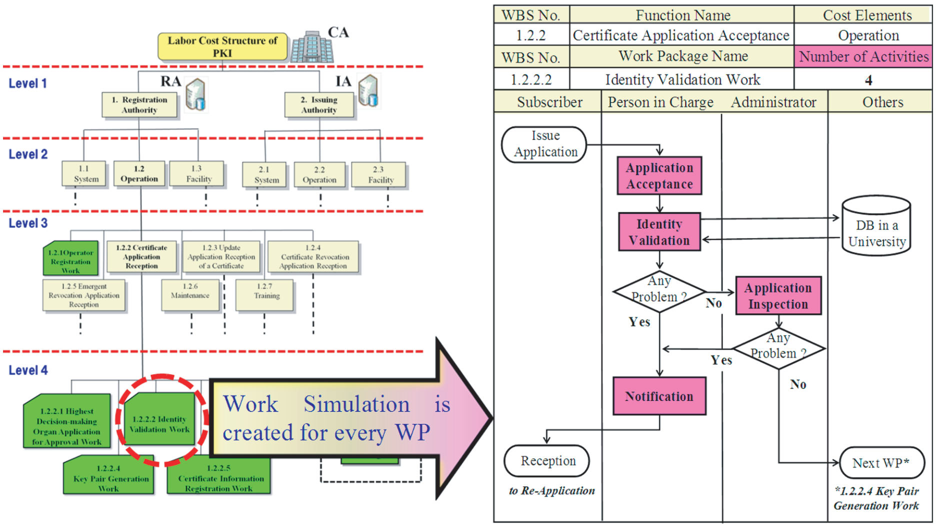

Labor Cost Structure of PKI
CA
Level 1
RA
IA
1. Registration Authority
2. Issuing Authority
Level 2
1.1 System
1.2 Operation
1.3 Facility
2.1 System
2.2 Operation
2.3 Facility
Level 3
1.2.1Operator Registration Work
1.2.2 Certificate Application Reception
1.2.3 Update Application Reception of a Certificate
1.2.4 Certificate Revocation Application Reception
1.2.5 Emergent Revocation Application Reception
1.2.6 Maintenance
1.2.7 Training
Level 4
1.2.2.1 Highest Decision-making Organ Application for Approval Work
1.2.2.2 Identity Validation Work
1.2.2.4 Key Pair Generation Work
1.2.2.5 Certificate Information Registration Work
Work Simulation is created for every WP
WBS No.
Function Name
Cost Elements
1.2.2
Certificate Application Acceptance
Operation
WBS No.
Work Package Name
Number of Activities
1.2.2.2
Identity Validation Work
4
Subscriber
Person in Charge
Administrator
Others
Issue Application
Application Acceptance
Identity Validation
DB in a University
Any Problem ?
No
Yes
Application Inspection
Any Problem ?
Yes
No
Notification
Reception
to Re-Application
Next WP*
*1.2.2.4 Key Pair Generation Work

Fig. 4 Example of work simulation of registration authority work.

Table 3 Analysis results of labor cost structure of PKI.

	Element	Number of WPs		Number of Activities	
		Initial Cost	*Running Cost*	*Initial Cost*	*Running Cost*
Registration Authority	*System*	15	0	51	0
	Operation	2	23	10	108
	Facility	5	0	19	0
Issuing Authority	*System*	18	0	78	0
	Operation	1	13	4	53
	Facility	7	0	35	0
Total		48	36	197	161

element showed that the number of WPs in the respective *System* and *Operation* elements of the two authorities were the same. Furthermore, there is no remarkable difference between the two authorities in their respective initial costs and running costs.

Overall, there was no significant difference between the results of classifying the authorities, PKI cost element, and PKI phase according to the number of WPs.

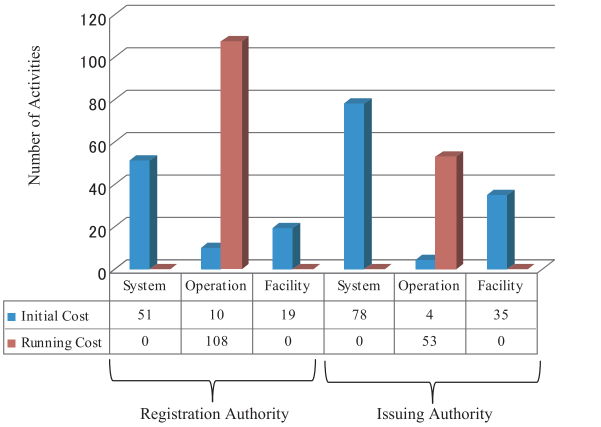
4.2.2 PKI Labor Cost Structure based on Work Simulation

Since no significant factor was found in the analysis of the PKI labor cost structure by using the WBS method, as described in Section 4.2.1, a more detailed analysis was then carried out. As mentioned, the labor cost of the PKI was found to be a total of 84 WPs. For a more detailed analysis of the PKI labor cost, a work simulation was performed for these WPs.

As an example, the results of analyzing the labor cost structure for Identity Validation Work (1.2.2.2), which is one of the registration authority's WPs, are shown in **Fig. 4**. The cost details are clarified based on these results. The cost unit is the number of activities. Here, an activity is one processing unit, i.e., shaded areas in Fig. 4. Four activities are shown in the figure.

The analysis results of the labor cost structure are shown in **Table 3**. A comparison of the initial cost and running cost in the registration authority and in the issuing authority, based on the results in Table 3, is shown in **Fig. 5**. The running cost of the registration authority was found to be the highest.

Next, the results in Table 3 were rearranged according to the PKI elements: the *System*, *PKI operation*, and *Facility*. The results are shown in **Table 4**, and a comparison is shown in **Fig. 6**. As mentioned above, in the labor cost structure of the PKI, a little over 50% of costs was consumed by the operation element.

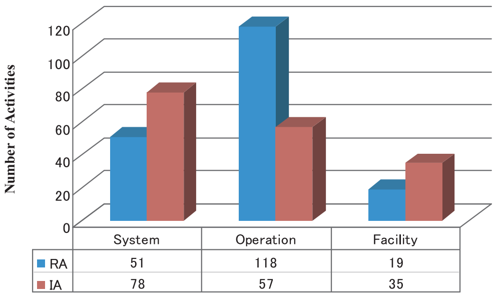


	System	Operation	Facility	System	Operation	Facility
🟦 Initial Cost	51	10	19	78	4	35
🟥 Running Cost	0	108	0	0	53	0

Fig. 5 Analysis results of labor cost structure of PKI (PKI labor cost structure in registration authority and in issuing authority).

Table 4 Cost structure by PKI element (unit: number of activities).

	System	Operation	Facility	Subtotal
Registration Authority	51	118	19	188
Issuing Authority	78	57	35	170
Total	129	175	54	358



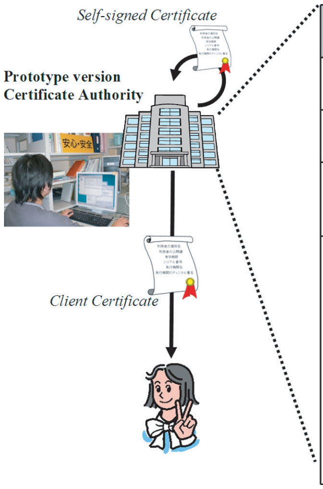
	System	Operation	Facility
🟦 RA	51	118	19
🟥 IA	78	57	35

Fig. 6 Labor cost structure by PKI element.

4.3 Actual Measurement Results of Prototype Operation

4.3.1 Actual Measurement Method

For comparison, the labor cost structure of a certificate authority should be actually measured. However, since complete operation of a certificate authority has not yet been measured, partial



Elements	Contents
OS	• Windows Server 2008
Software	• EasyCert, which is free software ➢RA and IA function are provided
Certificate Authority Configuration	• Self assignment certificate authority
Client Certificate Profile	C: Japan O: CIT OU: PM CN: S. Tanimoto EMAIL: ***@it-chiba.ac.jp Validity: 2011/12/12 Public key encryption: RSA Key length: 512bit Hash function: SHA-1 Certificate version: v3

Fig. 7 Principal configurations of prototype certificate authority.

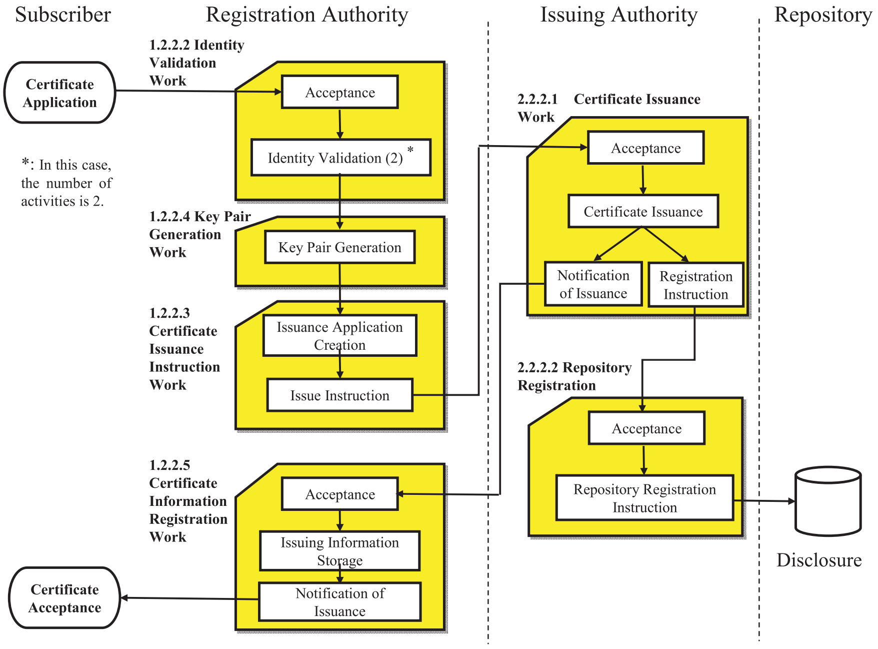

Subscriber
Registration Authority
Issuing Authority
Repository
Certificate Application
1.2.2.2 Identity Validation Work
Acceptance
Identity Validation (2) *
*: In this case, the number of activities is 2.
1.2.2.4 Key Pair Generation Work
Key Pair Generation
1.2.2.3 Certificate Issuance Instruction Work
Issuance Application Creation
Issue Instruction
1.2.2.5 Certificate Information Registration Work
Acceptance
Issuing Information Storage
Notification of Issuance
Certificate Acceptance
2.2.2.1 Certificate Issuance Work
Acceptance
Certificate Issuance
Notification of Issuance
Registration Instruction
2.2.2.2 Repository Registration
Acceptance
Repository Registration Instruction
Disclosure

Fig. 8 Actual measurement flows: certificate issuing flow.

actual measurement of operation by a prototype was performed. By using the results from the integrating method (Section 4.2) and actual measurement, the labor cost of the PKI was clarified quantitatively, and the trends were visualized. The principal configurations of a prototype certificate authority are shown in **Fig. 7**.

EasyCert [11], which is free software for the operation of a certificate authority as shown in Fig. 7, was used. Actual measurement was performed for only the following work in the operation of the prototype certificate authority:

(a) Certificate issuance man hours: man hours for issuing one certificate

(b) Certificate revocation man hours: man hours for invalidating one certificate

The certificate issuing flow and the certificate revocation flow that were measured are shown in **Figs. 8** and **9** respectively. Actual work was done as shown in these figures and the man hours were calculated. The results quantitatively clarified the concrete cost structure of operation of a prototype PKI through EasyCert.

4.3.2 Actual Measurement Results

The man hours after an application from a user was received until a certificate was issued or invalidated was actually measured for the EasyCert-built certificate authority.

(a) Actual Measurement Results for Certificate Issuance Application

The man-hour rate in certificate issuance application based on operation of the prototype is shown in **Fig. 10**. As can be seen, the highest man-hour rate was for Identity Validation Work (Fig. 8; 1.2.2.2). In a certificate authority, verification work such as by a meeting (face to face), by a student identification card, etc. is generally needed to verify an applicant. In this paper, a simple verification method was considered for the prototype operation. Concretely, the personal identification of an applicant was verified by viewing a student identification card. However, as shown in Fig. 10, even with this simplified work, Identity Validation Work had the highest man-hour rate.

(b) Actual Measurement Results for Certificate Revocation Application

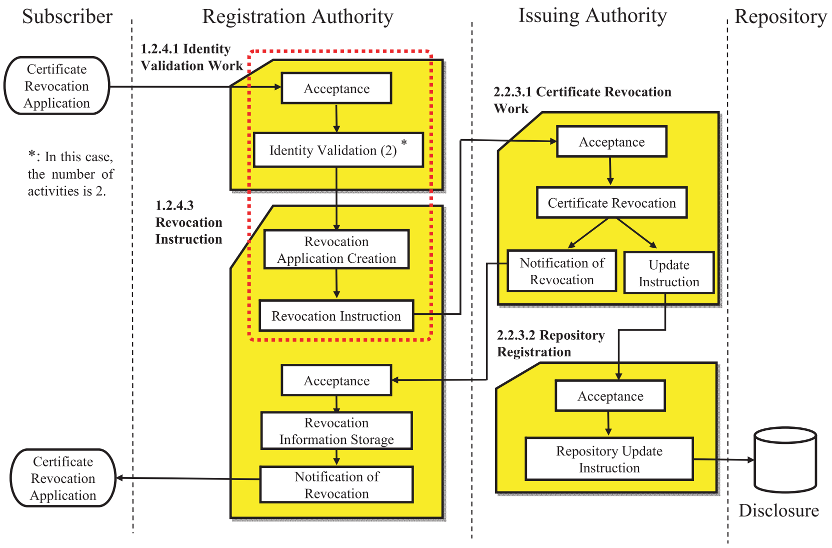

Subscriber
Registration Authority
Issuing Authority
Repository
Certificate Revocation Application
*: In this case, the number of activities is 2.
1.2.4.1 Identity Validation Work
Acceptance
Identity Validation (2) *
1.2.4.3 Revocation Instruction
Revocation Application Creation
Revocation Instruction
Acceptance
Revocation Information Storage
Notification of Revocation
Certificate Revocation Application
2.2.3.1 Certificate Revocation Work
Acceptance
Certificate Revocation
Notification of Revocation
Update Instruction
2.2.3.2 Repository Registration
Acceptance
Repository Update Instruction
Disclosure

Fig. 9 Actual measurement flows: certificate revocation flow.

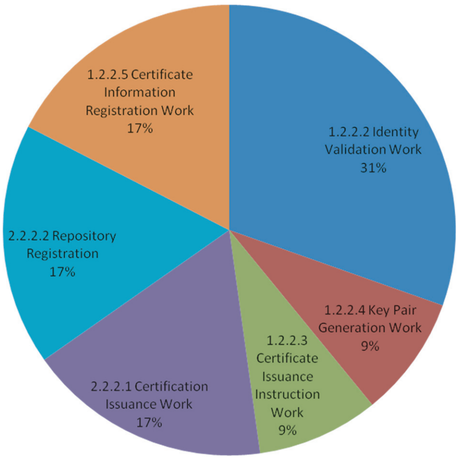


Fig. 10 Man-hour rates for certificate issuance application.

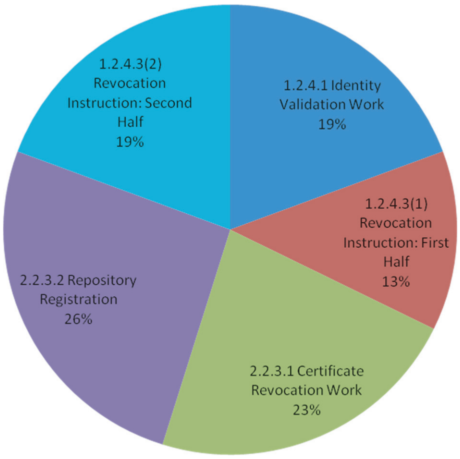


Fig. 11 Man-hour rates for certificate revocation application.

The measured man-hour rate in certificate revocation application is shown in **Fig. 11**. As can be seen, the rate for personal identification (1.2.4.1 Identity Validation Work, 1.2.4.3 (1) Revocation Instruction; dashed red box in Fig. 9) was high.

Overall, in the actual measurement results for the operation of the prototype, the certificate issuing application and the revocation application work had high man-hour rates for the verification of personal identification.

4.4 Evaluation and consideration

4.4.1 Results of Integrating Method

The operation cost structure of the certificate authority was divided into 84 WPs (Section 4.2). There were 33, 39, and 12 WPs respectively for the *System*, *PKI operation*, and *Facility* elements of the PKI. The granularity of the structure was still rough from these results, so characteristic results were not seen. A work simulation was also performed for every WP unit obtained from applying the WBS method to the PKI, and the number of activities calculated for the whole certificate authority was 358. There were 129, 175, and 54 activities respectively for the *System*, *PKI operation*, and *Facility* elements of the PKI.

Although concrete man hours must still be calculated for more detailed results, important basic data for installing a PKI were obtained.

4.4.2 Actual Measurement Results for Operation of Prototype

The actual measurement results in Section 4.3 showed that the man-hour rate for confirmation processes, such as personal identification verification and the reason for a revocation, was high. Accordingly, the cost structure is considered to be dependent on the level of these confirmation processes. The level is related to the CP/CPS, which is an operation basis of PKIs.

This indicates that clarifying the relation between the CP/CPS and cost structure is important in the spread and promotion of PKIs. The prototype was actually measured, with the aim of visualizing the cost structure factor by quantifying the PKI labor cost. Accordingly, mapping the results of the integrating method and actual measurement is future work.

5. Related Work

5.1 Campus PKI

InCommon is a U.S. project related to the campus PKI [12]. InCommon issues client certificates for institutions of higher education. The Trans-European Research and Education Networking Association (TERENA) issues server certificates for academic organizations in Europe [13]. As these projects show, there is current activity in this field that will lead to cheap introduction of joint use of a PKI in academic organizations, which shows that our proposal has contributed to the promotion and spread of a campus PKI.

5.2 Cost Quantification Method

Estimation and actual measurement methods using a prototype are typical for estimating costs in software development [14], [15]. Though used for analyzing the upstream of software development, the function point method is used as a more detailed estimation method [16]. This research was not targeted at systems (software) but at operation costs in connection with PKI operation. Since application of the function point method based on data flow could not be applied, our proposed method was detailed by conducting a work simulation based on the common specifications of the UPKI.

5.3 Conventional Cost Analysis Results

The following studies also investigated the cost of a PKI, although the details of a method for analyzing cost structures were not sufficiently clarified [17]. In one study, cost analysis was introduced when using a PKI for a financial transaction [18]. However, the effectiveness of application of this analysis to the campus PKI is not known. In another study, analysis of the cost structure of a PKI was conducted with risk factor [19]. However, the risk of this analysis to the campus PKI is not known.

6. Conclusion

The problem of the high cost structure of a campus PKI affecting its spread and promotion was described. The labor cost structure of a PKI was quantitatively clarified by estimation using the integrating method and by actual measurement of the operation of a prototype PKI.

The results of both the estimation and actual measurement showed clearly that the operation cost is a dominant factor in PKI labor cost. However, the integrating method evaluated the number of activities in a work simulation, and the precision of this method is rough compared with the man-hours method usually used. Moreover, the actual measurement was of a prototype, and not all aspects of practical use (complete operation and facilities based on a CP/CPS) were covered. Although there is scope for improvement in this quantification method, the PKI labor cost can be quantitatively visualized. As a result, a decision about whether to install a PKI can be easily made, which is expected to contribute to the spread and promotion of a campus PKI.

As mentioned, the precision of a work simulation (subdivided into activities) by the integrating method needs to be improved. Real operation based on a CP/CPS and increased accuracy of the actual measurement data are required. By these improvements, mapping the results of the integrating method and the actual measurement method can be achieved, and a cost estimate closer to actuality can be obtained. Furthermore, this method could be applied to determine the cost factor of information security, not only for a PKI but in general. A method for visualizing the costs of a complex information security system could be established accordingly. This could also contribute to the advancement of information security at large.

Acknowledgments The authors thank Mr. Tsuyoshi Takamoto, Mr. Toshihiko Moriya and Mr. Satoru Kurosaki of Chiba Institute of Technology for their help evaluating a work simulation and actual measurement.

References

[1] National Institute of Informatics: UPKI project (in Japanese), available from ⟨https://upki-portal.nii.ac.jp/⟩.

[2] National Institute of Informatics: UPKI common specifications (in Japanese), available from ⟨https://upki-portal.nii.ac.jp/docs/upkispecific⟩.

[3] Shimaoka, M. et al.: Design of Architecture for University PKI, *IEICE Trans. B*, Vol.J94-B, No.10, pp.1246–1260 (2011), (in Japanese).

[4] Iida, K. et al.: Construction and Operation of Campus-Wide Authentication and Authorization System, *IEICE*, Vol.J92-B, No.10 (2009), (in Japanese).

[5] Akiyama, T. et al.: Campus-wide IT Authentication Infrastructure Development in Osaka University, *IPSJ*, Vol.49, No.3 (2008), (in Japanese).

[6] Information Technology Center, The University of Tokyo (in Japanese), available from ⟨http://www.pki.itc.u-tokyo.ac.jp/⟩.

[7] Tanimoto, S. et al.: Campus PKI Common Specifications for University Authentication Cooperation, *IEICE Trans. B*, Vol.J94-B, No.10, pp.1383–1388 (2011), (in Japanese).

[8] Tanimoto, S. et al.: Managing PKI Deployment and Operation Based on Assurance Levels and Cost Structure, *Proc. 5th International Conference on Project Management* (2010).

[9] Tanimoto, S. et al.: Quantifying Cost Structure of Campus PKI, *The 5th Workshop on Middleware Architecture in the Internet* (*MidArch 2011*), *The 11th IEEE/IPSJ International Symposium on Applications and the Internet*, Munich, Germany, pp.315–320 (July 2011).

[10] PM Standards Committee: A Guide to the Project Management Body of Knowledge, available from ⟨http://www.unipi.gr/akad_tmhm/biom_dioik_tech/files/pmbok.pdf⟩.

[11] EasyCert, available from ⟨http://www-ailab.elcom.nitech.ac.jp/security/easycert/index.html⟩.

[12] InCommon, available from ⟨http://www.incommon.org/⟩.

[13] The Trans-European Research and Education Networking Association (TERENA), available from ⟨http://www.terena.org/⟩.

[14] Tausworthe, R.C.: The work breakdown structure in software project management, *Journal of Systems and Software*, Vol.1, pp.181–186 (1979–1980).

[15] Boehm, B. et al.: Software development cost estimation approaches—A survey, *Analysis of Software Engineering*, Vol.10, No.1-4, pp.177–205 (2000).

[16] Symons, C.R.: Function Point Analysis: Difficulties and Improvements, *IEEE Trans. Software Engineering*, Vol.14, No.1 (Jan. 1988).

[17] Dr. Berkovits, S. et al.: Public Key Infrastructure Study, *MITRE* (1994).

[18] Platis, A.N. et al.: A Probabilistic Model for Evaluating the Operational Cost of PKI-based Financial Transactions, *EuroPKI 2004*, pp.149–159 (2004).

[19] Argyroudis, P. et al.: Comparing the Costs of Public Key Authentication Infrastructures, *Proc. 1st Workshop on the Economics of Securing the Information Infrastructure* (*WESII'06*), p.10, Washington DC, USA (Oct. 2006).

Appendix

A.1 Detailed Results of WBS Division of PKI Cost Structure (Total: 84 WPs)

A.1.1 Registration Authorities (Subtotal: 45 WPs)

Authority（Level 1）	Element（Level 2）	Level 3 or Work Package	Level 4 or Work Package	Work Package (Level 5)
1. Registration Authority (Subtotal: 45WPs)	1.1 System (Subtotal: 15WPs)	1.1.1 Software (4WPs)	1.1.1.1 Registration Authority Server	1.1.1.1.1 RA Server Soft Installation
				1.1.1.1.2 RA Server Data Installation
			1.1.1.2 Registration Authority Terminal	1.1.1.2.1 RA Terminal Soft Installation
				1.1.1.2.2 RA Terminal Data Installation
			1.1.1.3 Certificate Store Media Soft Installation	
		1.1.2 Hardware (5WPs)	1.1.2.1 Server Hardware Installation	
			1.1.2.2 Terminal Hardware Installation for Registration	
			1.1.2.3 Certificate Storing-medium Hardware Installation	
			1.1.2.4 IC Card Reader Hardware Installation	
			1.1.2.5 IC Card Printer Hardware Installation	
		1.1.3 Database (5WPs)	1.1.3.1 Registration Authority Database	1.1.3.1.1 User's Information Database
				1.1.3.1.2 Operator Information Database
				1.1.3.1.3 Administrative Database
			1.1.3.2 Within the Campus Database	1.1.3.2.1 School Staff Database
				1.1.3.2.2 Student Database
	1.2 Operation (Subtotal: 25WPs)	1.2.1 Operator Information Registration		
		1.2.2 Certificate Application Acceptance (5WPs)	1.2.2.1 Highest Decision-making Organ Application for Approval	
			1.2.2.2 Identity Validation	
			1.2.2.3 Certificate Issuance Instruction	
			1.2.2.4 Key Pair Generation	
			1.2.2.5 Certificate Information Registration Work	
		1.2.3 Certificate Update Application Acceptance (5WPs)	1.2.3.1 Highest Decision-making Organ Application for Approval	
			1.2.3.2 Identity Validation	
			1.2.3.3 Issue Indication	
			1.2.3.4 Key Pair Generation	
			1.2.3.5 Certificate Information Registration work	
		1.2.4 Certificate Revoke Application Acceptance (3WPs)	1.2.4.1 Identity Validation	
			1.2.4.2 Authenticity Verification Work	
			1.2.4.3 Certificate Revocation	
		1.2.5 Urgent Revoke Application Acceptance (2WPs)	1.2.5.1 Identity Validation	
			1.2.5.2 Revocation Instruction	
		1.2.6 Maintenance (7WPs)	1.2.6.1 Manual Preparation (Maintenance)	
			1.2.6.2 Entering Leaving (Maintenance)	
			1.2.6.3 Regular Backup	
			1.2.6.4 Inspection	
			1.2.6.5 Log Function	
			1.2.6.6 Archive	
			1.2.6.7 Backup outside Facilities	
		1.2.7 Education (2WPs)	1.2.7.1 Training before Work	
			1.2.7.2 Extraordinary Training	
	1.3 Facility (Subtotal: 5WPs)	1.3.1 Room (2WPs)	1.3.1.1 Authentication Equipment Room (Installation)	
			1.3.1.2 Terminal Equipment Room for Registration (Installation)	
		1.3.2 Others Equipment (3WPs)	1.3.2.1 IC Card (Storage Place Installation)	
			1.3.2.2 A Physical Key (Storage Place Installation)	
			1.3.2.3 Monitoring Camera (Installation)	

A.1.2 Issuing Authorities (Subtotal: 39 WPs)

Authority（Level 1）	Element（Level 2）	Level 3 or Work Package	Level 4 or Work Package	Work Package (Level 5)
2. Issuing Authority (Subtotal: 39WPs)	**2.1 System (Subtotal: 18WPs)**	2.1.1 Software (8WPs)	2.1.1.1 Issuing Authority Server	2.1.1.1.1 IA Server Soft Installation
				2.1.1.1.2 IA Server Data Installation
			2.1.1.2 Issuing Authority Terminal	2.1.1.2.1 Terminal Soft Installation for Issuance
				2.1.1.2.2 Terminal Data Installation for Issuance
			2.1.1.3 Issuing Authority Terminal for Revoke	2.1.1.3.1 Terminal Soft Installation for Revoke
				2.1.1.3.2 Terminal Data Installation for Revoke
			2.1.1.4 Issuing Authority Terminal for Repository	2.1.1.4.1 Terminal Soft Installation for Repository Registration
				2.1.1.4.2 Terminal Data Installation for Repository Registratio r
		2.1.2 Hardware (6WPs)	2.1.2.1 Server Hardware Installation	
			2.1.2.2 Terminal Hardware Installation for Issuance	
			2.1.2.3 Terminal Hardware Installation for Lapse	
			2.1.2.4 Terminal Hard Installation for Repository Registration	
			2.1.2.5 IC Card Reader Hardware Installation	
			2.1.2.6 IC Card Printer Hardware Installation	
		2.1.3 Database (4WPs)	2.1.3.1 Issuing Information Database	2.1.3.1.1 Issuing Information Database
				2.1.3.1.2 Operator Information Database
			2.1.3.2 Within the Campus Database	2.1.3.2.1 Database for Teachers
				2.1.3.2.2 Database for Students
	2.2 Operation (Subtotal: 14WPs)	2.2.1 Operation Procedure Creation		
		2.2.2 Certificate Application Acceptance (2WPs)	2.2.2.1 Certificate Issuance Work	
			2.2.2.2 Repository Registration and Disclosure	
		2.2.3 Certificate Revoke Application Acceptance (2WPs)	2.2.3.1 Certificate Revocation	
			2.2.3.2 Repository Registration	
		2.2.4 Maintenance (7WPs)	2.2.4.1 Manual Preparation	
			2.2.4.2 Inspection Log	
			2.2.4.3 Vulnerable Evaluation	
			2.2.4.4 Routine Inspection	
			2.2.4.5 Inspection	
			2.2.4.6 Archive	
			2.2.4.7 Backup outside Facilities	
		2.2.5 Education (2WPs)	2.2.5.1 Work Training	
			2.2.5.2 Systems Operation Training	
	2.3 Facility (Subtotal: 7WPs)	2.3.1 Room (3WPs)	2.3.1.1 Issuance Authorities Equipment Room	
			2.3.1.2 Terminal Equipment Room for Issuance	
			2.3.1.3 Terminal Equipment Room for Lapse	
		2.3.2 Others Equipment (4WPs)	2.3.2.1 Management of Log by IC Card	
			2.3.2.2 Physical Key	
			2.3.2.3 Monitoring Camera	
			2.3.2.4 Biometrics Equipment	

Shigeaki Tanimoto graduated from University of Tokushima, Japan where he received his B.E., M.E. and Dr. E. degrees in 1982, 1984 and 1997, respectively. He joined NTT Laboratories from 1984 to 2009, and he is currently Professor at Chiba Institute Technology. His research interests include information security management, network security service and internet service. He is a member of IPSJ, IEICE and IEEE.

Masahiko Yokoi is currently Senior Manager of CIO department at NTT Communications, planning and executing company-wide IT governance on a global level. He is integrating and developing the whole global IT system for more than 40 NTT Com group companies worldwide. From 1999 to 2011, he was Project Manager for IT system development at NTT Com, introduced security platforms and applications using PKI and smartcard for public sector. He greatly contributed to standardizing authentication platform, SSO security platform, and PKI for Japanese national universities. He holds PMP, CISSP.

Hiroyuki Sato is Associate Professor at the University of Tokyo. He received his B.Sc., M.Sc. and Ph.D. from the University of Tokyo in 1985, 1987, 1990, respectively. He is majoring Computer Science and Information Security.

Atsushi Kanai received his B.S., M.S. and Ph.D. degrees from Tohoku University in 1980, 1982 and 2002, respectively. Since 1982, he had worked at NTT Laboratories. He is currently Professor of Applied Informatics at Faculty of Science and Engineering, Hosei University. His research interests include software design methodology, Web service technologies, information network and information security. He is a member of IEICE and IEEE.