TRANSACTIONS ON ELECTRICAL AND ELECTRONIC ENGINEERING
*IEEJ Trans* 2007; **1**: 84–93
Published online in Wiley InterScience (www.interscience.wiley.com). DOI:10.1002/tee.20101

**Paper**

# Development and Evaluation of a Certificate Validation System in Mobile Environments

Katsuyuki Umezawa,[*,**a] Member
Seiichi Susaki,[*] Non-member
Satoru Tezuka,[*] Non-member
Shigeichi Hirasawa,[**] Non-member

We have developed a public key certificate validation system considering the restrictions peculiar to the mobile environment, such as processing the speed and memory capacity of a cellular-phone terminal, and the network transmission speed. In this paper we derive a theoretical formula showing the performance of a validity check of the public key certificate of the conventional system and of the proposed system, and compare and examine a theoretical value in a mobile environment. Moreover, we evaluate the actual measurement that uses the server and cellular-phone terminal that we developed. We show that our proposed system based on the certificate validation server (CVS) system is better than the conventional system from the viewpoint of processing speed and transmission speed. © 2007 Institute of Electrical Engineers of Japan. Published by John Wiley & Sons, Inc.

**Keywords:** public key certificate, validity check, *CRL, OCSP, CVS, certificate validation system*

*Received 23 February 2006; Revised 4 August 2006*

## 1. Introduction

Generally, it is indispensable to verify a certificate strictly to confirm the validity of the communication partner by using public key infrastructure (PKI) technology. But it is difficult for a cellular-phone terminal to execute a complex calculation such as the validity check of the certificate.

A strict verification such as the validity check of the server certificate, cannot be done by the cellular-phone terminal till now. We have developed a new public key certificate validation system for the mobile environment taking in considering factors peculiar to the mobile environment, such as the processing speed of a cellular-phone terminal, its memory capacity, and the network transmission speed.

In a previous study, we performed our analysis from the viewpoint of the amount of communication of the total system [1]. When a server does a complex calculation such as the verification of the certificate at the location of a cellular-phone terminal, it is thought that the entire performance is decided by the transmission rate between the cellular-phone terminal and the server, and the calculation speed of the cellular-phone terminal and the server. We derive the theoretical formula for verification of the public key certificate, showing the performance including the processing time and network transmission time of the conventional system and the proposed system. These theoretical formulas apply not only to the mobile environment but also to the general Internet environment. We compare and examine a theoretical value in a mobile environment from the viewpoint of the ratio at the calculation speed and the ratio of the transmission rate. In addition, we evaluate the actual measurement of the proposed system based on the certificate validation server (CVS). In conclusion, we show that our proposed system is superior to other systems from both the theoretical and experimental viewpoints for a range of useful parameters.

Below, we describe the validity check system of the present certificate in Section 2 and the outline of the proposed system in Section 3. We derive the theoretical

[a] Correspondence to: Katsuyuki Umezawa.
E-mail: katsuyuki.umezawa.ue@hitachi.com
[*] Hitachi, Ltd. Systems Development Laboratory Hitachi System Plaza Shinkawasaki, 890, Kashimada, Saiwai-ku, Kawasaki-shi, Kanagawa, 212-8569
[**] Graduate School of Science & Engineering, Waseda University 3-4-1, Okubo, Shinjuku-ku, Tokyo 169-8555

formula for the average verification time required for one authentication in Section 4. In Section 5, we evaluate the theoretical formula derived in the preceding section by applying the parameter to a mobile environment. Finally, we offer our conclusions in Section 6.

## 2. Conventional Systems

We must execute 'the validity check of the public key certificate' for checking whether the public key certificate in the certification path (The certification path means the chain of certificates from the certificate of root CA to the certificate of the end entity.) is not revoked. (In addition, we must execute 'the construction of the certification path' and 'the verification of the certification path' in order to verify the public key certificate.) There are the Certificate Revocation List (CRL) system [2,3], the Online Certificate Status Protocol (OCSP) system [4], the CVS (CVS) system [5,6], etc. (There is SCVP system [7]; however, we exclude it from this evaluation because it is a draft version.) in 'the method of the validity check of the public key certificate.' The outline is shown below.

**2.1. CRL system** The CRL is the list of the serial numbers of the invalidated certificates, and it is published and managed by the Certification Authority (CA) in general. In case the verifier wants to confirm the validity of a certain certificate, the verifier acquires the CRL from the repository of the CA that published the certificate, and the verifier judges by checking whether the serial number of the certificate is indicated in the CRL. The CRL is usually issued at a constant cycle. On issue, the serial number of the certificate that has lapsed is added to the CRL. In addition, the serial number of the certificate that exceeds the validity term is excluded from the CRL. There are the completeness CRL system and the $\delta$-CRL system in CRL systems. (There are other systems, such as the partition CRL system that exhibit and divide the revocation information for the plural CRL, the indirect CRL system, the certificate revocation tree (CRT) system, etc.) In the completeness CRL system, we use the CRL that includes the numbers of all certificates that are within the validity term and have been invalidated at the time of publication. In the $\delta$-CRL system, we use the CRL that includes the same information as the completeness CRL, called the base-CRL, at a comparatively long time interval, and we use the CRL whose publication interval is shorter than the base-CRL, called the $\delta$-CRL. The $\delta$-CRL includes only the numbers of the certificates that are within the validity term and have been newly invalidated after publication of the base-CRL.

**2.2. OCSP system** The OCSP system asks the validity of the certificate online to the server called the 'OCSP Responder'. If the verifier sends the information on the certificate (ID of the certificate, etc.) as a request message, one of three answers will be given: validation (Good), invalidation (Revoked), or unknown (Unknown), as the response.

**2.3. CVS system** There are some problems in which the burden on the side of a certificate verifier is large in the CRL and OCSP systems because the certificate verifier has to construct the certification path and verify the certificate. One system that can reduce this burden is the CVS system. The CVS system is one that substitutes for the original certificate verifier that constructs and verifies the certification path, and confirms the validity of all the certificates in the certification path. If the verifier sends the certificate sets as the object of the verification and the trustworthy certificate of the CA to the server, the result of having checked the justification of the certificate for verification will be answered.

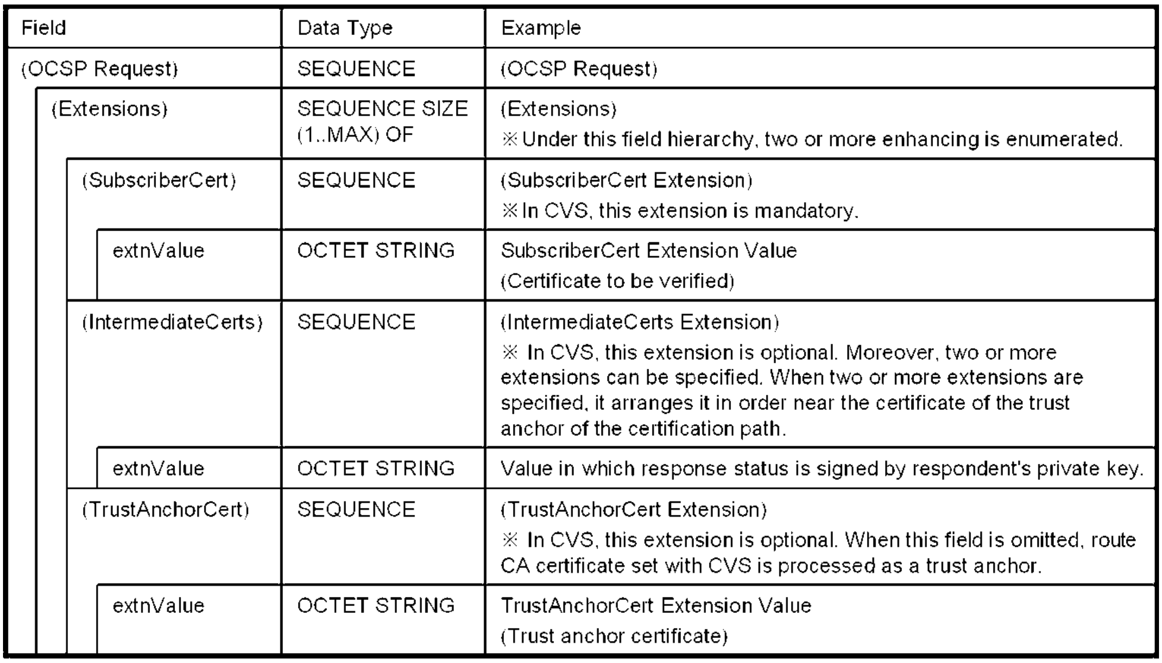
## 3. Proposal for certificate validation system for mobile network

**3.1. Approach for mobile network** In a mobile environment, it is assumed that two or more mobile operators set up a CA and issue certificates to a cellular-phone and official service provider. Therefore, a mechanism is necessary where by in the certificates that are issued by two or more CAs of the mobile operator can be verified mutually. The verification method is provided in Ref. 3. However, it is difficult for a cellular-phone terminal to implement a method such as the construction of the certification path, the verification of the certification subscription, and the validity check using the CRL.

A certificate validation server that does a complex verification of the certificate in place of the original verifier (a cellular-phone terminal) is needed from the above-mentioned viewpoint in a mobile environment. The amount of the communication for the validity check of the certificate is the number of bits of request and response. Therefore, it is most important to reduce the request and response size as much as possible.

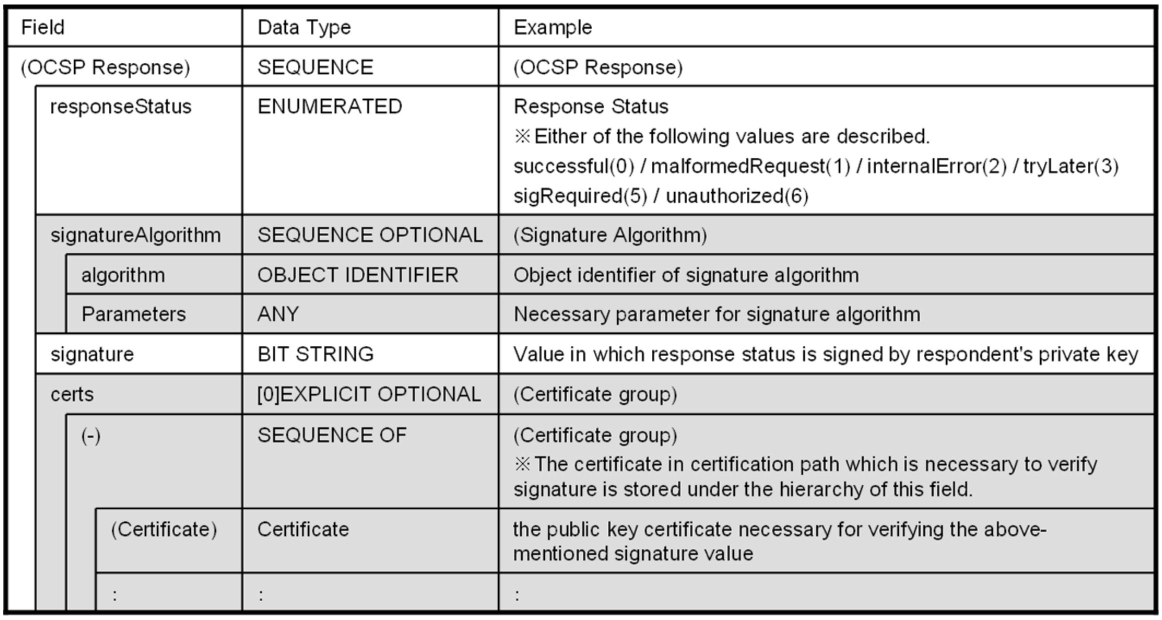
**3.2. Certificate validation request and response formats for the mobile network** We examine a suitable method for a mobile environment. We define the certificate validation request and the response format for a mobile environment that omit tedious data to reduce the size as much as possible. Table 1 shows the request message that the verifier transmits to the CVS. Table 2 shows the response message with which the CVS replies to the verifier. The hatched items in Table 2 can be omitted by the policy of the CVS server.

Table I. Request data format



| Field | Data Type | Example |
|---|---|---|
| (OCSP Request) | SEQUENCE | (OCSP Request) |
| (Extensions) | SEQUENCE SIZE (1..MAX) OF | (Extensions)<br>※Under this field hierarchy, two or more enhancing is enumerated. |
| (SubscriberCert) | SEQUENCE | (SubscriberCert Extension)<br>※In CVS, this extension is mandatory. |
| extnValue | OCTET STRING | SubscriberCert Extension Value<br>(Certificate to be verified) |
| (IntermediateCerts) | SEQUENCE | (IntermediateCerts Extension)<br>※ In CVS, this extension is optional. Moreover, two or more extensions can be specified. When two or more extensions are specified, it arranges it in order near the certificate of the trust anchor of the certification path. |
| extnValue | OCTET STRING | Value in which response status is signed by respondent's private key. |
| (TrustAnchorCert) | SEQUENCE | (TrustAnchorCert Extension)<br>※ In CVS, this extension is optional. When this field is omitted, route CA certificate set with CVS is processed as a trust anchor. |
| extnValue | OCTET STRING | TrustAnchorCert Extension Value<br>(Trust anchor certificate) |

Table II. Response data format



| Field | Data Type | Example |
|---|---|---|
| (OCSP Response) | SEQUENCE | (OCSP Response) |
| responseStatus | ENUMERATED | Response Status<br>※Either of the following values are described.<br>successful(0) / malformedRequest(1) / internalError(2) / tryLater(3)<br>sigRequired(5) / unauthorized(6) |
| signatureAlgorithm | SEQUENCE OPTIONAL | (Signature Algorithm) |
| algorithm | OBJECT IDENTIFIER | Object identifier of signature algorithm |
| Parameters | ANY | Necessary parameter for signature algorithm |
| signature | BIT STRING | Value in which response status is signed by respondent's private key |
| certs | [0]EXPLICIT OPTIONAL | (Certificate group) |
| (-) | SEQUENCE OF | (Certificate group)<br>※The certificate in certification path which is necessary to verify signature is stored under the hierarchy of this field. |
| (Certificate) | Certificate | the public key certificate necessary for verifying the above-mentioned signature value |
| : | : | : |

**3.3. Validation request protocol for mobile network** We adopted the POST method [8] of the HTTP protocol supported by many current cellular-phone terminals as a validation request protocol.

**3.4. Configuration element of the certificate validation system** We developed the prototype of the following three components.

- CVS
- Validation module on the service provider side
- Validation module on the cellular-phone terminal side

With respect to the CVS, we developed a function for constructing the certification path necessary to verify the certificates that two or more CAs issued, a function to verify certification path by the method of reference [3] at the location of the cellular-phone terminal, and a function to execute access to a good many of CAs as a proxy and to check the validity of all certificates that constitute a certification path.

With respect to the validation module on the service provider side, we developed a function to verify signature and for access to CVS. For the model in which two or more mobile operators independently set up a CA and a CVS, respectively, it is necessary to distribute each certificate received from the cellular-phone terminal to the CVS of each mobile operator appropriately. Therefore, we also developed a function to distribute each certificate appropriately in the verification module on the service provider side.

With respect to the validation module on the cellular-phone terminal side, it is necessary to consider the restrictions peculiar to a mobile system, such as processing speed, memory capacity, transmission rate, communication stability, power resource, etc. We developed a verification module that can be executed on a low-performance cellular-phone terminal. Concretely, as shown in Section 3.2, we defined the minimum information necessary for verifying the certificate as the CVS verification request format for mobile environment, and we developed the function for accessing the CVS using this format.

**3.5. Proposed system configuration** Fig. 1 shows the system configuration when the mobile operator sets up the CVS, and the cellular-phone terminal verifies service provider's certificate. Here, the mobile operator issues the certificate and CRL to the cellular-phone terminal, and the service provider CA issues the certificate and CRL to the service provider. When the cellular-phone terminal verifies the service provider's certificate, the cellular-phone terminal receives the service provider's certificate, and transmits in from the validation module (CVS client) in the cellular-phone terminal to the CVS of the mobile operator. CVS demands CRL from the service provider's CA repository and verifies the certificate. (We explained the procedure at the server authentication here. On the contrary, at the client authentication, the service provider will verify the certificate that the cellular-phone terminal presented.)

The operation screen of the validation module in the cellular-phone terminal is shown in Fig. 2. When the server authentication of the SSL protocol is done, this module is built into a browser request for validation to CVS.

## 4. The Average Total Time of the Certificate Verification

In this section, we evaluate the average verification time (communication time + calculation time) required in case a certain Entity carries out a one-time certificate verification.

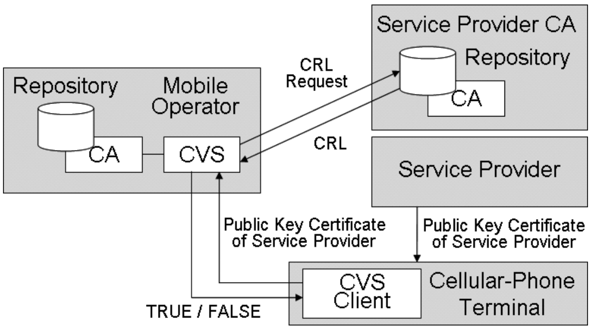
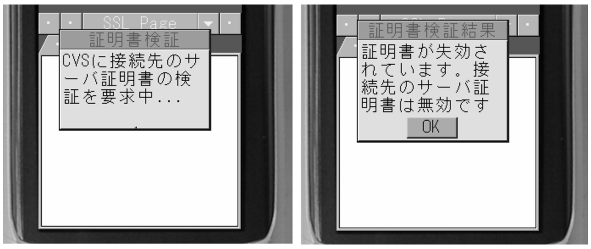


Fig. 1 Outline of system configuration



CVSに接続先のサーバ証明書の検証を要求中...

証明書が失効されています。接続先のサーバ証明書は無効です

Fig. 2 Mobile browser with certificate verification module

**4.1. The definition of models** We define the model of the validity check of the certificate first. Figure 3 is the model by the ($\delta$-)CRL system given in Ref. 9. Figures 4 and 5 are models that use the OCSP system between the validation authority (VA) of the certificate and the Entity. Figure 4 is the model that the Entity asks a plural VA for the validity check of the certificate individually, and Figure 5 is the model that carries out the validity check of the all certificate paths by one inquiry. Figure 6 shows the model that uses the CVS system between the VA and the Entity.

**4.2. The average verification time** The verifier need not acquire the CRL after the second time if the verifier acquires the CRL once, because the CRL is usually published by the CA for the verifier periodically, as we showed in section 2.1. Thus the necessity for acquisition time of the CRL is based on the probability

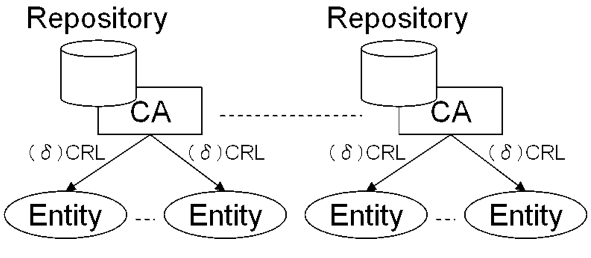


Fig. 3 ($\delta$-)CRL model

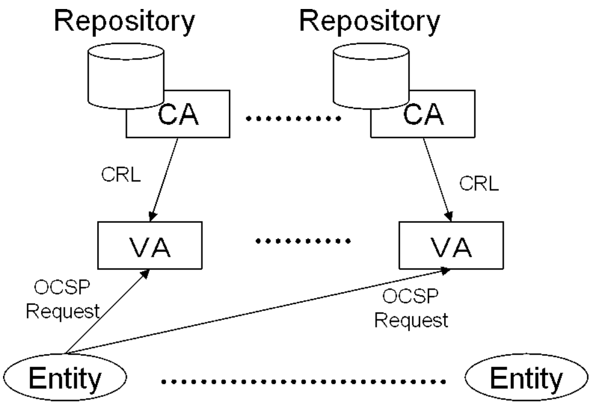


Fig. 4 OCSP model 1

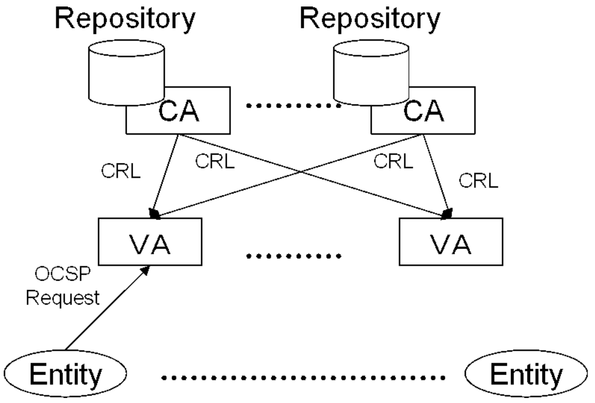


Fig. 5 OCSP model 2

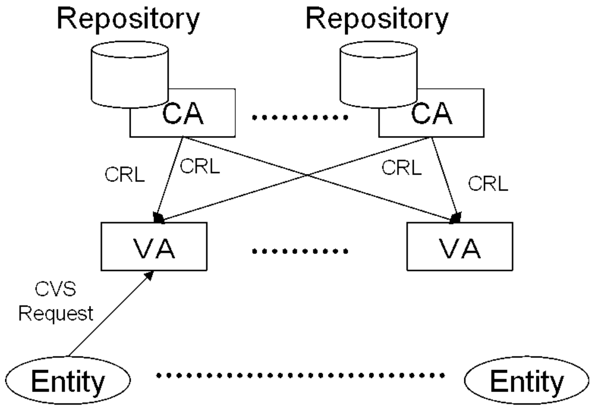


Fig. 6 CVS model

of the event of certificate verification having occurred, and therefore we need to calculate the acquisition time of the CRL by its average value. Suppose that we take the average of acquisition time of the CRL as $C_x$, the calculation time required for verification of the certificate at the cellular-phone terminal and the server as $M_x$, and the requirement time of a validity check as $R_x$. Hence the average verification time $T_x$ is:

$$T_x = C_x + M_x + R_x \tag{1}$$

However, $x$ expresses the model. We calculate $C_x$, $M_x$, and $R_x$ for every model in the following section.

**4.3. The probability of performing the certificate verification** First, we calculate the probability of the event of the certificate verification before calculating $C_x$. In general, the probability distributions of occurrence times $X$ of the event occurred is on average $\lambda$ times a certain time interval based on the Poisson distribution $P(X) = \lambda^X \cdot e^{\lambda}/X!$. (Reference [9] assumes same Poisson distribution.)

Suppose that we interpret the authentication frequency (Because the verification happens at each authentication, it can be paraphrased as the verification frequency.) as $q$[time/day number] and the number of the CA as $k$[number] from reference [9], the mean of the number by which a certain verifier certifies the Entity belonging to a certain CA between the time interval $T$ (day) is $qT/k$ (time). Thus it is considered as the number that a certain Entity certifies that the Entity belongs to a certain CA based on the Poisson distribution: $\lambda = \frac{qT}{k}$. Therefore the probability $p_{e}{}^{T}_{X\geq 1}$ that the Entity is certified one or more times between the time intervals $T$ in the Entity is:

$$p_{e}{}^{T}_{X\geq 1} = 1 - e^{-\frac{qT}{k}} \tag{2}$$

Next, we calculate the probability of occurrence of the authentication in the VA. The authentication in the VA refers to the process based on the validity check that is required from the Entity. Suppose that we interpret $X$ and $X'$: $X$ is the number of occurrences of an event in plural groups and $X'$ is the number of occurrences of the event that totals $X$. When the probability distribution in Poisson, the probability distribution of X′, also a Poisson, is known. Suppose that we interpret $N$ as the number of the Entity, and $N_v$ as the number of the VA, then the authentication frequency is $q' = \frac{q \cdot N}{N_v}$ in the VA. The VA verifies that the Entity belongs to $k/N_v$ CAs in OCSP model 1, and $k$ CAs in OCSP model 2 and the CVS model; then, the mean of the numbers that the VA verifies the Entity belongs to the CA during the time interval $T$ once: the first is $qT/k \times N$ times, the second is $qT/k \times \frac{N}{N_v}$ times. Therefore, the probability that the VA verifies the Entity one or more times during the time interval $T$ is represented by the following formulae when we suppose that we interpret the probability for $p'{}_{v}{}^{T}_{X\geq 1}$ in the OCSP model 1 and $p_{v}{}^{T}_{X\geq 1}$ in the OCSP model 2 and the CVS model.

$$p'{}_{v}{}^{T}_{X\geq 1} = 1 - e^{-\frac{qT}{k}\cdot N} \tag{3}$$

$$p_{v}{}^{T}_{X\geq 1} = 1 - e^{-\frac{qT}{k}\cdot\frac{N}{N_v}} \tag{4}$$

**4.4. Derivation of the average of the acquirement time of the CRL** The CRL is acquired between the CA and the Entity in the CRL model and the $\delta$-CRL model; in the other models, the CRL is acquired between the CA and the VA. (According to Ref. 9, suppose that we interpret that we can disregard the communication quantities required for the verification of the invalidation frequency of the CA certificate because the invalidation frequency of the CA certificate is small enough.) The probability that the verifier acquires the CRL within the publication interval $T_C$ is the probability that the verifier authenticates the Entity that belongs to a certain CA one or more times. Hence the average time $C_{CRL}$ that the verifier takes for an acquisition of the CRL in the CRL model is:

$$C_{CRL} = \frac{k \times pe_{X\geq 1}^{T_C} \times l_{CRL}}{T_C \times q \times s} \tag{5}$$

$l_{CRL}$ is the size of the CRL that a CA publishes once, and from Ref. 9:

$$l_{CRL} = \frac{N'pL}{k} \times l_{sn} + l_{sig}[bit] \tag{6}$$

Moreover, $q$ is the average number of times that the Entity is authenticated in a day, and $s$ is the communication speed (bit/sec) between the CA and the Entity.

The $\delta$-CRL model requires, in contrast, the times that acquire both base-CRL and $\delta$-CRL. Suppose the first is $C_{baseCRL}$ and the second is $C_{delta}$; then:

$$C_{deltaCRL} = C_{baseCRL} + C_{delta} \tag{7}$$

Suppose that we interpret the time interval in (5) is $T_B$, that is, the publication interval of the base-CRL. Then we adopt it to express $C_{baseCRL}$ that is the acquisition time of base-CRL to (8):

$$C_{baseCRL} = \frac{k \times pe_{X\geq 1}^{T_B} \times l_{baseCRL}}{T_B \times q \times s} \tag{8}$$

However, $l_{baseCRL}$ is the same as $l_{CRL}$ at (6). $C_{delta}$ is the acquisition time of $\delta$-CRL, therefore (9) averages $l_{delta}(n)$, that is, the size of $\delta$-CRL was published to the $n$th per day:

$$C_{delta} = \frac{k \times pe_{X\geq 1}^{T_C} \times \sum_{n=1}^{\frac{T_B}{T_C}-1} l_{delta}(n)}{T_B \times q \times s} \tag{9}$$

From Ref. 9, $l_{delta}(n)$ is:

$$l_{delta}(n) = \frac{N'pL}{k}\left\{1 - \left(1 - \frac{T_C}{L}\right)^n\right\} \cdot l_{sn} + l_{sig}$$

And other models acquire the CRL between the CA and the VA, and $C_x$ is the average time that is required for one acquisition of the CRL then:

$$C_{OCSP1} = \frac{\frac{k}{N_v} \times p'^{T_C}_{vX\geq 1} \times l_{CRL}}{T_C \times q' \times \beta s} \tag{10}$$

$$C_{CVS} = C_{OCSP2} = \frac{k \times p_{vX\geq 1}^{T_C} \times l_{CRL}}{T_C \times q' \times \beta s} \tag{11}$$

However, $\beta$ (In general, the assuming of $\beta \geq 1$ works out because the transmission rate of the back end network is higher than that of a mobile network.) is the amplification of the communication speed between the CA and the VA (back end) for the communication speed between the VA and the Entity (mobile network).

**4.5. Derivation of calculation time** Generally for the Entity that has acquired the certification process we have the following:

1. The construction of the certification path
2. The verification of the certification subscription
3. Generation of the requirement of the validity check of the certificate
4. The validity check using the CRL
5. The verification of the subscription that is the result of the validity check of the certificate

Every model has to calculate 1 and 2 of these calculation process $r-1$ times; however, there is a difference between the CVS model and the other models because while the VA calculates it in the CVS model, the Entity calculates it in the other models. Moreover, with respect to 3 and 5, the CRL model and the $\delta$-CRL model that make the validity check on line do not calculate them; however, OCSP model 1 must calculate them $r-1$ times, and the other models have to calculate them once. In addition, with respect to 4, the Entity calculates it in the CRL and $\delta$-CRL, but the VA calculates it in the other models. Hence, $M_x$($x$ is a model) that the verifier requires for the calculation time in a verification of the certificate is:

$$M_{CRL} = M_{deltaCRL} = (r-1)(M + M'') \tag{12}$$

$$M_{OCSP1} = (r-1)(M + \alpha M'' + M') \tag{13}$$

$$M_{OCSP2} = (r-1)(M + \alpha M'') + M' \tag{14}$$

$$M_{CVS} = (r-1)(\alpha M + \alpha M'') + M' \tag{15}$$

where:

$M$: The construction of the certification path and the verification time of the certification subscription in the Entity terminal (sec)

$M'$: Generation of the requirement of the verification of the certificate and the verification time of the subscription that is the result of the validity check of the certificate in the Entity terminal (sec)

$M''$: The validity check using the CRL in the Entity terminal (sec)

$r$: The length (CA rank +1) of the certificate path (rank)

$\alpha$: The ratio of the calculation speed of the VA server to the calculation speed of the Entity terminal ($0 < \alpha < 1$)

These calculations use time multiplied by $r - 1$ because we suppose that we interpret the certificate of the root CA that has been verified by some systems and the Entity as the trust anchor that has been trusted.

**4.6. Derivation of requirement time of validity check** The time of the validity check can be derived by the communication time and the data size of the requirement of the validity check in each system. The time of the validity check is 0 in the CRL model and $\delta$-CRL model because those models do not conduct the validity check online. (The judgment times required strictly for ID of the certificate for object verification are contained in their own CRL.) The numbers of certificates that should check validity is $r - 1$ in the OCSP model 1 and OCSP model 2, and $r$ in the CVS model. In the OCSP model 1, it is necessary to send $r$ requests. In the OCSP model 2 and the CVS model, two or more requests can be settled in one request. Then the numbers of bits is $(r-1)(D_{sn}+D_{sig})$ in the OCSP model 1, $(r-1)D_{sn}+D_{sig}$ in the OCSP model 2, and $rD'_{sn}+D'_{sig}$ in the CVS model. Hence, $R_x$ that the verifier requires for the requirement time of the validity check in a verification of the certification is: (Although the answer times of a result are taken strictly, the size is excluded because it is small.)

$$R_{CRL} = R_{deltaCRL} = 0 \tag{16}$$

$$R_{OCSP1} = \frac{(r-1)(D_{sn}+D_{sig})}{s} \tag{17}$$

$$R_{OCSP2} = \frac{(r-1)D_{sn}+D_{sig}}{s} \tag{18}$$

$$R_{CVS} = \frac{rD'_{sn}+D'_{sig}}{s} \tag{19}$$

where

$D_{sn}$: The number of bits per item of the OCSP request (a certificate ID etc.) (bit)

$D_{sig}$: The number of bits of the constant element that is not based on the number of items of the OCSP request (bit)

$D'_{sn}$: The number of bits per item of the CVS request (a certificate etc.) (bit)

$D'_{sig}$: The number of bits of the constant element that is not based on the number of items of the CVS request (bit)

$s$: The communication speed between the VA and the Entity (mobile network) (bit/sec)

## 5. Comparison when Mobile Environment Parameters are Applied

We assume the parameters of a mobile environment as shown in Table 3 for evaluating the average of the certificate verification time. These parameters are not very different from the parameter used in the current state of mobile service in Japan.

Because average verification time $T_x$ ($x$ is a model) is $T_x = C_x + M_x + R_x$ from (1), the parameters in Table 3 are substituted into the theoretical formula derived in the preceding Section [(2)–(19)], and the average verification time of each model is as follows. (The publication interval of the base-CRL $T_B$ of (8) and (9) was calculated by the numeric calculation (all searches) according to Ref. 9. $T_B = 28$ becomes the best in the parameters in Table 3.)

$$T_{CRL} = \frac{42636.13}{s} + 4M \tag{20}$$

$$T_{deltaCRL} = \frac{23470.36}{s} + 4M \tag{21}$$

$$T_{OCSP1} = \frac{0.0084}{\beta s} + \frac{1408}{s} + (2\alpha+4)M \tag{22}$$

$$T_{OCSP2} = \frac{0.0842}{\beta s} + \frac{1336}{s} + (2\alpha+3)M \tag{23}$$

$$T_{CVS} = \frac{0.0842}{\beta s} + \frac{19456}{s} + (4\alpha+1)M \tag{24}$$

We calculated them as $M' = M$, $M'' = M$, and $q = 30$.

Moreover, we show the average of the verification time in Figs. 7, 8, and 9 when $\alpha = 0.1$. That means the transaction speed of the server is 10 times the transaction speed of the terminal, and $\beta = 100$ means the communication speed between CA and VA is 100 times the communication speed of the mobile network. From Figs. 7, 8, and 9, it does not depend on the calculation time of the terminal, and we can see that the CVS system verification time is shorter than that of the CRL and $\delta$-CRL systems.

Moreover, we note the value of the intersection $M$ of $T_{OCSP1}$,$T_{OCSP2}$, and $T_{CVS}$ for Table 4 in Figs. 7, 8, and 9.

Table III. The Parameters for Evaluation

| Item | Parameter |
|---|---|
| The numbers of the Entity (the verification): $N$[number] | 87 000 000 |
| The numbers of the object: $N'$[number] | 3 000 000 |
| The frequency of the invalidation occurrence: $p$[time/day] | 0.1/365 |
| The validity term of the certificate: $L$[day] | 365 |
| The occurrence interval of the completeness CRL and $\delta$-CRL: $T_C$[day] | 1 |
| The size per particular of CRL: $l_{sn}$[bit] | 72 |
| The size of the constant element that is not based on the CRL: $l_{sig}$[bit] | 728 |
| The numbers of the CA: $k$[number] | 500 |
| The numbers of the VA: $N_v$[number] | 10 |
| The numbers of bits per particular of the OCSP requirement (a certificate ID, etc.): $D_{sn}$[bit] | 632 |
| The numbers of bits of the constant element that is not based on plural particulars of the OCSP requirement: $D_{sig}$[bit] | 72 |
| The numbers of bits per particular of the CVS requirement (a certificate etc.): $D'_{sn}$[bit] | 6,464 |
| The numbers of bits of the constant element that is not based on plural particulars of the CVS requirement: $D'_{sig}$[bit] | 64 |

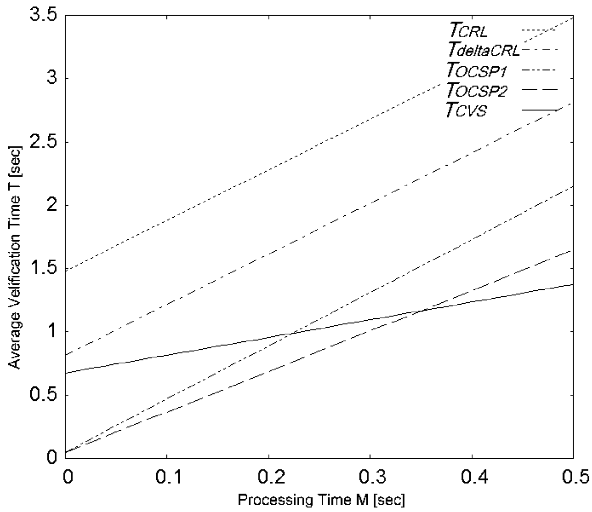


Fig. 7 The average of the verification time in each system when the transaction speed is $s = 28.8k$[bit/sec]

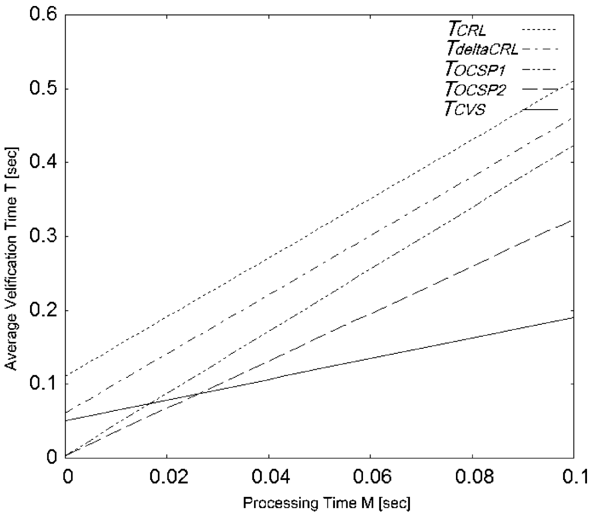


Fig. 8 The average of the verification time in each system when the transaction speed is $s = 384k$[bit/sec].

From Table 4, $T_{CRL}$ and $T_{OCSP2}$ cross at $M = 0.0262$ when the communication speed is $384k$(bit/sec), for instance; therefore, we can see that the average verification time is shorter than that of the other systems when the processing time of the terminal is longer than 26.22(ms).

We fixed $\alpha = 0.1$, that is, the ratio of the communication speed to the calculation time of the Entity terminal in Figs. 7, 8, and 9. However, we moved $\alpha$ to 0.5 in Fig. 10, and we made graphs showing the intersection of the average of the verification time in OCSP system 1, OCSP system 2, and the CVS system when the communication speed s is $384k$ (bit/sec) and $2.4M$ (bit/sec). The upside domains of each curve in Fig. 10 indicate the domains where the average of the verification time of CVS system is shorter than that of the other systems.

In the future, the processing speed ratio will not change much because the speed of the cellular-phone terminal and the server will increase. On the other hand, it is expected that the speed of mobile communication will also get faster and faster. Then, the advantageous range of the proposed system based on CVS will be extended because the curves in Fig. 10 will fall.

**5.1. Evaluation of actual measurement** We evaluated the capability for the server of the verification of the certification for a mobile environment using a cellular-phone terminal (BREW terminal) with CDMA 1x WIN standards and a computer. This computer used an Intel(R) Pentium(R) 4 processor (3.4GMHz), a 2GB

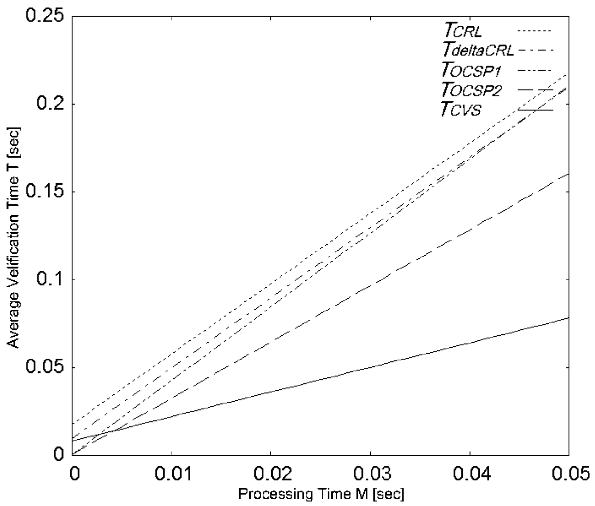


Fig. 9 The average of the verification time in each system when the transaction speed is $s = 2.4M$[bit/sec].

Table IV. The value of $M$ that is the intersection in Fig. 7, 8 and 9

| | $T_{OCSP1} - T_{CVS}$ | $T_{OCSP2} - T_{CVS}$ |
|---|---|---|
| 28.8k | $M = 0.2238$ | $M = 0.3495$ |
| 384k | $M = 0.0168$ | $M = 0.0262$ |
| 2.4M | $M = 0.0027$ | $M = 0.0042$ |

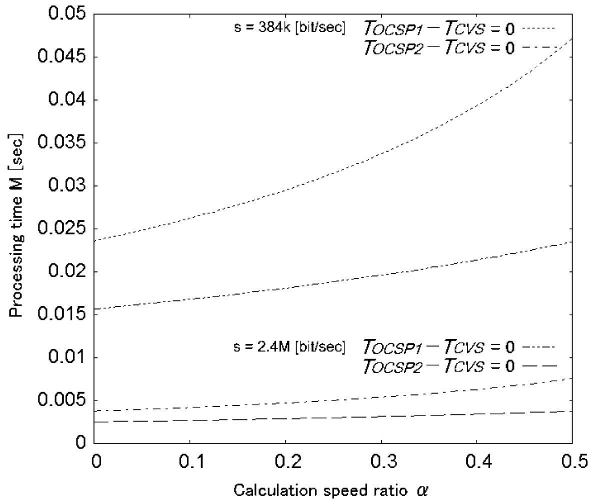


Fig. 10 The intersection of the average of the verification time in OCSP system 1, OCSP system 2, and the CVS system.

CPU memory, and the Windows(R) XP operation system. We show the actual measurement value that is 100 times the average time of the subscription generation in Table 5. We used $M = 0.01003$ and $\alpha = 0.16/10.03$ and the substitution of them for $T_{OCSP2} - T_{CVS} > 0$; then we calculate $s$; $s \geq 917933$. That means the CVS system is valid compared with the OCSP system when the communication speed is more than about 900k(bit/sec) in the mobile network.

Table V. The measurement value

| Transaction Contents | Time(ms) |
|---|---|
| Transaction in the cell-phone | 10.03 |
| Transaction in the server | 0.16 |

## 6. Conclusions and Future Work

We developed the public key certificate validation system in consideration of restrictions peculiar to the mobile environment. Furthermore, we derived the theoretical formula showing the performance of the validity check of the public key certificate of the conventional system and the proposed system, and compare the theoretical value in the mobile environment. Then we described the range that is suited for the CVS system in the mobile environment. As the conclusion of this paper, we show that the proposed system based on CVS is superior compared with the other systems from both theoretical and experimental viewpoints for a useful range of parameters.

In future, we hope to evaluate the performance by considering the load of the server.

## Acknowledgement

This research was done as a part of the consignment research ‘Research and Development of Infrastructure Technology of Mobile Security’ of the National Institute of Information and Communications Technology (NICT).

## About Trademarks

— Windows is a trademark of the Microsoft Corporation in the U.S. and/or other countries.
— Intel and Pentium are trademarks of the Intel Corporation and subsidiary companies in the U.S. and/or other countries.
— BREW is a trademark of QUALCOMM Incorporated.

## References

(1) Umezawa K, Takahashi A, Uchiyama H, Sakazaki H, Oikawa M, Susaki S, Hirasawa S. Development of Certificate Verification System for Mobile Services, IEICE Technical Report, Vol. 105, No. 311, IT2005-59 (2005–09) 2005; 49–54.

(2) *ITU-T Recommendation X.509. ISO/IEC 9594-8:2001: Information Technology—Open Systems Interconnection—The Directory: Public-key and Attribute Certificate Framework*, 2000.

(3) Housley R, Polk T, Ford W, Solo D. RFC 3280—Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, IETF, 2002.

(4) Myers M, Ankney R, Malpani A, Galperin S, Adams C. RFC 2560—X.509 Internet Public Key Infrastructure—Online Certificate Status Protocol—OCSP, IETF, 1999.

(5) Fujishiro T, Kaji T, Hane S, Kumagai Y, Tezuka S. Development of Certificate Validation Service, IEICE Transactions D-I Vol.J87-D-I No.8, 2004.

(6) Government PKI Interoperability Specification, 2003; http://www.gpki.go.jp/session/CompatibilitySpecifications.pdf.

(7) Fressman T, Housley R, Malpani A, Cooper D, Polk T. Simple Certificate Validation Protocol (SCVP), IETF, 2005.

(8) Fielding R, Gettys J, Mogul J, Frystyk H, Masinter L, Leach P, Berners-Lee T. RFC 2616—Hypertext Transfer Protocol—HTTP/1.1, IETF, 1999.

(9) Tanaka N, Iino Y. Volume of communications necessary for certificate revocation in PKI estimated based on probability theory. Information Processing Society of Japan (IPSJ) Journal 2004; **45(12)**:2824–2833.

(10) Umezawa K, Takahashi A, Uchiyama H, Sakazaki CH, Oikawa M, Susaki S, Hirasawa S. Development and evaluation of certificate verification system in mobile environment. Computer Security Symposium, Computer Security Group, Information Processing Society of Japan (IPSJ) Proceeding, 2005; 121–126.

(11) Umezawa K, Oikawa M, Susaki S, Hirasawa S. Evaluation of certificate verification method in mobile environment. Society of Information Theory and its Applications (SITA) Proceeding, 2005; 587–590.

**Katsuyuki Umezawa** (Member) was born in Saitama, Japan, on December 6, 1971. He received the B.E. and M.E. degrees in Industrial and Management Systems Engineering from Waseda University, Tokyo, Japan, in 1994 and 1996, respectively. In 1996, he joined Hitachi, Ltd., Systems Development Laboratory, Kanagawa, Japan. His research interests are distributed object systems, mobile security, and smart card security. He is a member of the Information Processing Society of Japan and a sutudent member of the Institute of Electrical Engineers of Japan.

**Seiichi Susaki** (Non-member) received the B.E. degree in Electorical and Computer Engineering from Yokohama National University, Kanagawa, Japan, in 1991 and the Dr. E. degree in Environment and Information Sciences from Graduate School of Yokohama National University, Kanagawa, Japan, in 2004. In 1996, he joined Hitachi, Ltd., Systems Development Laboratory, Kanagawa, Japan. His research interest is in information security systems. He is a member of the Information Processing Society of Japan. He received the 1996 Best Paper Award at the 52nd IPSJ National Convention, and the 2000 IPSJ Yamashita SIG Research Award.

**Satoru Tezuka** (Non-member) received the B.E. and the Dr. E. degrees in Science and Technology from Keio University, Kanagawa, Japan, in 1984 and 2000, respectively. In 1984, he joined Hitachi, Ltd., Micro-Electronics Development Laboratory, Kanagawa, Japan. At present he is with Hitachi, Ltd., Systems Development Laboratory, Kanagawa, Japan. His research interest is in Security Systems, especially the development of Electronic Certification Systems.

**Shigeichi Hirasawa** (Non-member) was born in Kobe, Japan, on October 2, 1938. He received the B.S. degree in mathematics and the B.E. degree in electrical communication engineering from Waseda University, Tokyo, Japan, in 1961 and 1963, respectively, and the Dr. E. degree in electrical communication engineering from Osaka University, Osaka, Japan, in 1975. From 1963 to 1981, he was with the Mitsubishi Electric Corporation, Hyogo, Japan. Since 1981, he has been a professor at the School of Science and Engineering, Waseda University, Tokyo, Japan. In 1979, he was a Visiting Scholar in the Computer Science Department at the University of California, Los Angeles (CSD, UCLA), CA. He was a Visiting Researcher at the Hungarian Academy of Science, Hungary, in 1985, and at the University of Trieste, Italy, in 1986. In 2002, he was also a Visiting Faculty at CSD, UCLA. From 1987 to 1989, he was the Chairman of the Technical Group on Information Theory of IEICE. He received the 1993 Achievement Award and the 1993 Kobayashi Memorial Achievement Award from IEICE. In 1996, he was the President of the Society of Information Theory and Its Applications (Soc. of ITA). His research interests are information theory and its applications, and information processing systems. He is an IEEE Fellow, an IEICE Fellow, and a member of Soc. of ITA, the Information Processing Society of Japan, and the Japan Industrial Management Association.