Evaluating Certificate Status Information Mechanisms

John Iliadis, Diomidis Spinellis,
Sokratis Katsikas
Dept. of Information & Communication
Systems, University of the Aegean,
GR-83 200 Karlovasi, Greece
{jiliad,dspin,ska}@aegean.gr

Dimitris Gritzalis
Dept. of Informatics, Athens
University of Economics &
Business, 76 Patission St.,
GR-10434 Athens, Greece
dgrit@aueb.gr

Bart Preneel
Dept. of Electrical Engineering,
Katholieke Universiteit Leuven,
K. Mercierlaan 94, Heverlee,
B-3001 Belgium
bart.preneel@esat.kuleuven.ac.be

ABSTRACT

A wide spectrum of certificate revocation mechanisms is currently in use. A number of them have been proposed by standardisation bodies, while some others have originated from academic or private institutions. What is still missing is a systematic and robust framework for the sound evaluation of these mechanisms. We present a mechanism-neutral framework for the evaluation of mechanisms, which collect, process and distribute certificate status information. A detailed demonstration of its exploitation is also provided. The demonstration is mainly based on the evaluation of Certificate Revocation Lists, as well as of the Online Certificate Status Protocol.

Keywords

Certificate, Certificate Revocation, Certificate Status, Certificate Revocation List, Evaluation Framework.

1. INTRODUCTION

The deployment of Public Key Infrastructures, as an e-commerce and e-business enabling technology, has been extensively studied. A number of value added services for PKIs have been investigated, as well, resulting in a large set of security services that can be used in order to meet the needs emerging in the electronic world. What has not been extensively and methodically studied is the mechanism (or mechanisms) used by PKIs for revoking the issued certificates and disseminating the respective revocation information.

In this paper, we present an agnostic framework for the evaluation of mechanisms, which collect, process and distribute information pertinent to the validity of a certificate (Certificate Status Information — CSI). With `agnostic' we mean that our evaluation mechanism strives to avoid unnecessary biases. We realise that there is always a tension between criteria which purely differentiate between mechanisms (and which do not result in a judgement) and criteria which are included based on our judgement of what such a CSI system should provide.

The evaluation framework comprises of a set of qualitative and quantitative evaluation criteria, which can be applied to any CSI mechanism. We use this model as a tool to identify in a methodical way the potential problems in the mechanisms. Our evaluation framework splits the evaluation process into three main domains, namely management, performance and security.

Management of revocation mechanisms includes the way these mechanisms operate, the way information processing is being performed, the participating entities, and the respective timeframe.

Performance of revocation mechanisms refers to the efficiency characteristics of those mechanisms. These characteristics include the timeliness of the mechanism, the freshness of the information it delivers, the scalability and adjustability of the mechanism, and the capability to immediately generate information on the status of a certificate (emergency certificate status information).

The security aspect of revocation mechanisms covers issues related to protecting the operation of the mechanisms themselves, as well as of the information they produce. Certificate status information has to be protected while generated, communicated, and stored.

While designing the evaluation framework, we took into consideration the requirements and restrictions imposed on the use of these mechanisms by the modus operandi required by the European Directive on a Community Framework for Electronic Signatures [6], the EESSI Expert Team Report [15] and the NIST PKI study [3, 16]. The framework can be used to evaluate CSI mechanisms that are operated by a Certification Service Provider (CSP) which issues "qualified certificates" [6, 15]. Certificates are considered to be "qualified" [6] if they meet the requirements set forth in Annex I of [6] and are provided by a Certification Service Provider meeting the requirements laid out in Annex II of [6]. We have also considered the draft or final requirements and recommendations contained in [11, 5, 1, 8, 17, 14, 9].

We demonstrate the application of our framework by evaluating Certificate Revocation Lists [11, 8], and the Online Certificate Status Protocol [14].

This paper is organised as follows: In section 2 we present the agnostic evaluation framework for CSI mechanisms itself. In section 3 we describe two representative CSI mechanisms and evaluate them based on the framework presented in section 2. Finally, section 4 contains our concluding remarks.

CCS'00, Athens, Greece.
Copyright 2000 ACM 1-58113-203-4/00/0011…$5.00.

2. EVALUATION FRAMEWORK

The recently published Electronic Signature Directive (Annex II of [6]) requires "the operation of a prompt and secure directory and a secure and immediate revocation service". Furthermore, the Directive requires that the authenticity and validity of the certificate required at the time of signature verification are reliably verified, and that the result of verification and the signatory's identity are correctly displayed. The [6] also requires that the date and time when a certificate is issued or revoked must be determined precisely.

Finally, the last major requirement of [6] that relates to CSI mechanisms is that the use of these mechanisms must be in accordance with data protection legislation, and respect the privacy of individuals.

The identified requirements fall in three main categories: *performance*, *management* and *security*. These requirements are, in fact, criteria that can be used both for evaluating existing CSI mechanisms, as well as for designing new ones. From this point and on these requirements will be called CSI Evaluation Criteria, or criteria for short.

2.1 Management

2.1.1 Feedback

Feedback is mostly a matter of user interface of the PKI-aware applications or devices that handle CSI on behalf of the dependent entity, and not a matter of the CSI mechanisms themselves. Dependent entities must receive information regarding the intermediate results of the operation of the CSI mechanism and the final output it produces (status of the certificate), in accordance with Annex II of [6]. This feedback must indicate at least the following information:

1. The CSI location information that has been found by the mechanism, which relates to the certificate the dependent entity attempts to validate. This information could be a URI [12],
2. if the CSI location has been successfully contacted,
3. if CSI has been retrieved,
4. if the validity (integrity and authenticity) of the retrieved CSI can be verified. Also, if this verification can be based (directly or indirectly) on information the dependent entity has declared as trusted (e.g. CA certificates stored locally), or if other, possibly untrusted, information is also needed (e.g. more CA certificates which cannot be validated based on the existing set of trusted CA certificates),
5. if the CSI that was retrieved corresponds to the certificate the dependent entity wishes to validate,
6. the status of the certificate the dependent entity wishes to validate.

If the CSI mechanism can provide the dependent entity with the information above, either at the beginning or in whole the end of the execution of the CSI mechanism, or in fragments while the mechanism is operating, then the feedback criterion is met.

2.1.2 Transparency

The majority of PKI dependent entities are bound to lack information security awareness and training. Therefore, locating the CSI repository (CSI location function) and verifying that the CSI contained in that repository is the one the dependent entity is looking for (CSI validation function), must be an automated procedure that requires no human intervention. The intervention of the user should be restricted, if possible, to requesting a validity check on a specified certificate.

If CRLs or Delta-CRLs are used, the added communication burden for disseminating certificates to dependent entities consists of the number of bytes needed for the *cRLDistributionPoints* X.509v3 certificate extension, which points to a valid URI where the specific CRL can be downloaded from. For Distribution Point CRLs based on reason for revocation, one URI should be included for every revocation reason. For the other types of Distribution Point CRLs, a single URI suffices.

If OCSP is used, a certificate should include the AuthorityInfoAccess extension which points to the location of the authority that provides OCSP service for the specific certificate. The communication burden for this case equals to the number of bytes needed to include the AuthorityInfoAccess extension.

2.1.3 Delegation of revocation.

The dependent entity could trust an authority, other than the CA, for generating the CSI. "CSI generation" in this context means signing CSI in order to protect its integrity and authenticity.

It could be either another CA or another authority that operates only as a Revocation Authority (RevA) and not as a Certification Authority. Moreover, it could be an authority, using a separate, distinct CA-issued key for signing the CSI or it could be a distinct authority, local to the dependent entity, that is trusted by this entity.

In any case, the dependent entity must be able to verify the status of the keys used by that authority, based on certificates or other information it already considers to be trusted, before trusting and using CSI from that authority.

2.1.4 Delegation of the CSI dissemination

The CA may delegate CSI dissemination to another authority. This second authority may need to be trusted by the dependent entities or not, depending on the mechanics of the CSI dissemination.

The dependent entity has to be able to verify the authenticity and integrity of CSI it retrieves from that authority. If CSI delivered to the dependent entity is contained in a CA-signed field, then the repository (e.g. Directory) used by the CSI dissemination authority need not be trusted. However, if CSI delivered to the dependent entity is not contained in such a field, then the authority that disseminates CSI must sign the CSI before delivering it to the dependent entity and the dependent entity must be able to validate the respective certificates. However, even if CSI is contained in a CA-signed field, the authority that disseminates CSI may behave maliciously, withholding fresh CSI from the dependent entity. Every CSI mechanism uses a different method to allow the dependent entity verify that the CSI it received is the most fresh one (e.g. bounded revocation in CRLs, whitelists in CRS [13].

The communication cost $s(t)$ (in time units) of distributing CSI using a CRL to one authority grows linearly with the size of the CSI at time t. When n authorities/repositories must receive this CSI, the communication cost equals n times the cost to distribute the CSI to one authority, i.e., the communication cost for n authorities/repositories equals $n \cdot s(t)$ time units.

When a CRL is distributed over p Distribution Point CRLs, and $spi(t)$ denotes the time needed to deliver CRL partition pi based on the CRL produced at time t, then the total time needed to transport all CRL partitions equals to the sum of all $spi(t)$'s, making the communication cost equal to $s(t)$ time units.

The time needed to ship the Delta-CRL equals $s(t+l)-s(t)$, being the difference in the time needed to send the new CRL and the time needed to distribute the BaseCRL. When n authorities/repositories must receive the new Delta-CRL, the communication cost equals $n\cdot(s(t+l)-s(t))$ time units. However, if the authorities/repositories do not already have the BaseCRL, the communication cost becomes $n\cdot s(t+l)$ time units.

In a system with n OCSP service providers, the communication cost of CSI dissemination equals that of the first case: $n\cdot s(t)$ time units.

2.1.5 Delegation of the certificate path validation

We consider delegation of the certificate path validation from the dependent entity to another entity. The dependent entity should be provided with the means to review and verify the results of the validation process (Annex II of [6]). In addition to that, the entity that performs the certificate path validation should be trusted by the dependent entity.

The validation of a certificate path takes as input the certificate to be validated, a number of other certificates the dependent entity trusts, and CSI regarding these certificates. The output is status information regarding the certificate to be validated.

In some CSI mechanisms one proceeds as follows to assert the validity of a certificate: the dependent entity retrieves CSI regarding the certificate to be validated and uses as input the other certificates, the retrieved CSI and the certificate in question. Other CSI mechanisms can perform the certificate path validation on behalf of the dependent entity. This dependent entity uploads the certificate to be validated and the other certificates (or appropriate values that cryptographically identify in a unique way these certificates), to the authority that has access to CSI; this authority will then validate the certificate in question on behalf of the dependent entity. Next the authority communicates the validity check result to the dependent entity. The dependent entity has to be able to verify the integrity and authenticity of the result returned by the CSI mechanism, using appropriate cryptographic validation mechanisms.

2.1.6 Referral capability

If the CSI location function leads the dependent entity to a CSI location that does not contain the requested CSI (the CSI may be less fresh than requested, or it may not contain information regarding the specific certificate to be validated), CSI mechanisms could support the capability to refer the dependent entity to another CSI location in order to retrieve the requested CSI.

2.1.7 Revocation Reasons

When validating the path, the certificate path validation function could consider the reasons for the revocation of a specific certificate contained in a certificate path. Depending on the revocation reason, the validation function may output different results. The semantics of revocation reasons and the logic the validation function uses in order to include this information, while validating a certificate path, is a matter of policy.

If the certificate path validation function occurs locally to the dependent entity, then the dependent entity must be able to set the policy for using revocation reasons in the validation function. If the certificate path validation function is delegated to another authority then the inclusion of revocation reasons in the logic of certificate path validation is a matter of the policy used by that authority. The dependent entity must be aware of that policy. Alternatively, the dependent entity could communicate its own policy regarding revocation reasons to the authority who performs the validation.

2.1.8 Notification of revocation or suspension

A subscriber, whose certificate is being revoked or suspended should be notified; it might be necessary to inform other entities as well (mentioned as a possible policy requirement in [5]).

Notification should not be an absolute requirement and should not be integrated in the CSI mechanisms themselves, because failure to locate appropriate contact information for the certificate owner, the dependent entity or any other entities could lead to disruption of the CSI mechanism. This procedure must be implemented outside the CSI mechanism itself, but temporally linked to the generation or storage function of the CSI mechanism.

2.2 Performance

2.2.1 Timeliness of CSI

Dependent entities should be able to locate and receive CSI in a timely fashion, to allow them to use such information in authenticating entities or verifying the signatures of entities. This feature, along with the Emergency CSI capability criterion, satisfies the requirement for an "immediate revocation service" contained in Annex II of the [6].

Timeliness concerns the amount of time between the generation of CSI from the appropriate authority until this CSI becomes available (this does not include the actual dissemination of CSI to dependent entities, but only its availability) to the dependent entities. Timeliness of CSI increases when this amount of time decreases.

2.2.2 Freshness of CSI

This criterion concerns the maximum period of time between the most recent CSI generation, regarding a specific certificate, and a request for the CSI regarding that certificate. In the following paragraphs, we present quantitative metrics that can be used to estimate the timeliness and freshness of CSI.

The metric that estimates the cost of having a CRL, issued at time t, and posted to n repositories, equals $n\cdot s(t)$, where $s(t)$ equals the time needed to distribute the CSI to one repository. Assume that it takes $d\cdot s(t)$ time units to forward the same CSI to the dependent entities. The freshness requirement of k time units must be larger than $n\cdot s(t)+d\cdot s(t)=(n+d)\cdot s(t)$, and the CRL must be updated at least every $k-(n+d)\cdot s(t)$ time units.

A similar metric can be given for the cost (in time) to distribute a Distribution Point CRL coming from the appropriate authority to the dependent entities; the freshness requirement of k time units must now be larger than $(d+1)\cdot s(t)$, and the Distribution Point CRL must be issued at least every $k-(d+1)\cdot s(t)$ time units.

For a Delta-CRL that is issued at time $t+l$, the time needed to have the Delta-CRLs distributed among n repositories is given by $n\cdot(s(t+l)-s(t))$, and it takes $d\cdot(s(t+l)-s(t))$ time units to send the CSI to the dependent entities. Therefore, the timeliness metric equals $k-((n+d)\cdot(s(t+l)-s(t)))$. This means that a Delta-CRL must be issued at least every $k-((n+d)\cdot(s(t+l)-s(t)))$ time units.

For OCSP, the timeliness metric is given by $k-n\cdot s(t)$: it takes $n\cdot s(t)$ time units to update the CSI of the OCSP service providers, and the dependent entities retrieve their CSI on-line from the OCSP service providers.

2.2.3 Bounded revocation

There should be an upper time limit for new, fresh CSI to be produced and made available (this does not include the actual dissemination of CSI to dependent entities, but only its availability). Dependent entities should reject CSI they receive, if the "date of fresher CSI generation" is in the past and not in the future.

There could be another requirement concerning the time of issuance of CSI, that restricts the placement of CSI issuance in time even more. We call this *time-complete* revocation. In time-complete revocation, CSI is generated in specific moments in time, neither sooner nor later.

2.2.4 Emergency CSI capability

This requirement concerns the ability of the CSI authority to generate CSI and make it available, immediately after receiving a valid revocation request. However, this does not include the immediate dissemination of this CSI to dependent entities, but only the immediate generation of CSI. This feature, along with the timeliness criterion, satisfies the requirement for an "immediate revocation service" in Annex II of the [6].

2.2.5 Scalability

When the number of the authorities and users (e.g. CAs, RevAs, dependent entities, certificate holders) increases, new obstacles in the operation of the CSI mechanism should not emerge.

2.2.6 Adjustability

The dependent entities (or the CA and the CSI authorities) should be able to adjust the location or validation function operation, in order to create a balance between performance and protection, depending on the requirements and the risk assessment in each case. Ideally, the dependent entity should be able to adjust the location or validation function, since it is the dependent entity that takes the risk by accepting this balance between performance and protection.

2.3 Security

The CSI mechanism features presented in this section meet the requirement (Annex II of [6]) for a "secure directory" and a "secure revocation service".

2.3.1 CSI disseminator authentication

The dependent entities must verify the origin of the CSI they receive. If authentication is not used, a malicious entity pretending to be a trusted CSI dissemination entity could disseminate to the dependent entities false CSI that appears to be valid.

2.3.2 CSI integrity

The integrity of the CSI must be verified, when it is stored in the CSI repository, while it is transferred to the dependent entities and when it is stored in the dependent entities' local repository. Such verification must be possible to preclude that a malicious entity can modify either the stored CSI or the CSI while in transit. If this happens, the dependent entity may not realise that the received CSI is old, partial, or invalid in any way.

2.3.3 CA compromise

There should be a mechanism for the dependent entities to know whether a CA has been compromised. This mechanism should also foresee a mechanism to recover from a CA compromise. The effects of a CA key being compromised should be minimised.

2.3.4 RevA compromise

There should be a mechanism for the dependent entities to know whether the authority that revokes certificates (RevA) has been compromised. This mechanism must not be the same as the one used by the dependent entities in order to receive the CSI on certificates that belong to entities other than the RevA.

2.3.5 Contained functionality

If RevA is compromised, it should not be possible for the entities that gained control of the RevA to issue new certificates.

2.3.6 Availability

The CSI dissemination mechanism has to be resilient against unreliable networks, Denial Of Service (DoS) attacks, etc.

3. EVALUATION OF CSI MECHANISMS

In this section we apply our evaluation framework to Certificate Revocation Lists [11, 8] and the Online Certificate Status Protocol [14].

A CRL consists of a signed list containing timestamped pointers to revoked certificates. The certificate identifier used in this list is the unique serial number assigned to the certificate by the Certification Authority (CSP). There are two major variations in the use of CRLs: CRLs with Distribution Points (DP CRLs) and Delta-CRLs [11, 8].

Distribution Points provide the means to partition a CRL. The CRL partitions can be created either by assigning ranges of certificate serial numbers to different CRL partitions, or by creating CRL partitions that contain certificates that were revoked because of a specific revocation reason (e.g. a CRL containing only the certificates that were revoked because of change in the affiliation of the certificate holder).

Delta-CRLs reduce the necessary resources for the communication of CSI to dependent entities and for the processing of CSI by these entities. Delta-CRLs can be used in order to communicate incremental CSI, thus reducing the communication or processing resources needed by CRLs or CRLs with Distribution Points.

The Online Certificate Status Protocol (OCSP) [14] is a protocol proposed by the IETF PKIX Working Group that allows dependent entities to query for CSI in a more timely fashion than CRLs. These queries are performed online. OCSP can also be used in conjunction with CRLs, as it provides an extension that can be used as a pointer to a CRL, in case more timely CSI is unavailable at a certain point of time.

Certain evaluation criteria are accompanied by quantitative metrics, which can, in turn, be used in order to investigate possible enhancements to the CSI mechanisms we examine. The notation that will be used for providing quantitative metrics is explained in Table 1.

Table 1 Notation of quantitative metrics

t	linearly increasing event timescale
s(t)	cost of distributing CSI
spi(t)	cost of distributing CRL partition *pi* to the appropriate authority or repository
n	number of authorities or repositories that must receive the generated CSI
d	number of dependent entities seeking CSI
k	freshness requirement (in time units)

3.1 Management

3.1.1 Feedback

We believe that it is necessary to provide the dependent entity with feedback information. An assertion regarding the status of a certificate will be interpreted differently by the dependent entity, depending on the information that led to this assertion and the local policy. Existing standardisation efforts, which are related to the CSI mechanisms we examine, do not include suggestions for the user interface of such applications or devices.

It is also necessary to define a simple way to convey this information to the dependent entity, because of the complexity of the information as well as of the possible lack of understanding of nontrivial security and cryptography issues by the dependent entity. Standardisation efforts related to the mechanisms we examine should include high-level requirements for a user interface that provided such information to the dependent entities. This would result in an even higher level of user awareness of the CSI mechanisms. Finally, this information could be provided to the dependent entity at no substantial cost for the CSI mechanism.

3.1.2 Transparency

Although this is an important feature of CSI mechanisms and does not introduce an important additional communication cost, it is not, as of today, a matter of common practice among commercial or non-commercial CAs. The fact that standardisation efforts regarding the CSI location and retrieval information in the certificates are ongoing could be a reason for that.

3.1.3 Delegation of revocation.

OCSP does not support delegation of revocation, because OCSP does not include a specific mechanism for generating CSI. It uses the CSI generated by the CA, retrieving it possibly from a database indicated by the CA, in order to construct the CSI to be sent to the dependent entities.

CRL, DP CRL and Delta-CRL support that feature. The CA can designate a distinct authority (or a unit of the CA itself, distinct to the certificate-issuing unit) to issue CRLs, DP CRLs and Delta-CRLs. The CA has to issue a certificate for that authority, which must contain the cRLSign key usage attribute.

3.1.4 Delegation of the CSI dissemination

Delegation of CRL, DP CRL, and Delta-CRL dissemination can be performed since this CSI is contained in a field signed by the CA. However, since the authority that disseminates CSI and the respective repository may not be trusted, there has to be a specific policy for the issuance of CRLs, DP CRLs and Delta-CRLs. Such a policy must ensure that the CRL provided by the CSI disseminating authority is always the one that corresponds to the needs of the dependent entities at the specific moment in time when the CSI query is performed. Furthermore, the aforementioned policy must ensure that dependent entities have the ability to understand whether the CSI disseminating authority is withholding a specific CRL, DP CRL, or Delta-CRL from them.

OCSP supports two levels of CSI dissemination delegation:

1. At the first level, the authority (CA Designated Responder [14]) that disseminates CSI (OCSP signed Responses) must have a certificate issued by the CA for that purpose.
2. At the second level, the authority that disseminates CSI can be a third, distinct authority (Trusted Responder [14]) whose public key is trusted by the dependent entity.

Partitioning the CSI space and assigning the responsibility of disseminating the CSI partitions to a number of authorities could decrease communication costs, incurred by CSI dissemination.

The use of Distribution Point CRLs reduces the communication cost to distribute the CRL information from the CA to the repositories. A combined solution wherein Delta-CRLs are used to update Distribution Point CRLs reduces the communication cost even further.

When the number of revoked certificates in a system does not grow significantly over time, Delta-CRLs are the best choice.

The ideal situation involves a hybrid system, in which OCSP is used whenever it is possible to post online CSI queries, and where Delta-CRLs are used in the other case.

3.1.5 Delegation of the certificate path validation

CRL, DP CRL, and Delta-CRL do not support delegation of the certificate path validation function.

OCSP partially supports delegation of the certificate path validation function. Extensions to the supported delegation have recently been proposed [2]. Delegation of the certificate path validation function requires the availability of a large set of trust-related information (e.g. CA certificates, CRL or CSI in other formats) to the OCSP service provider. The aggregation of this kind of information could incur communication, maintenance or other costs.

3.1.6 Referral capability

The referral capability relates to transparency. OCSP partially supports this capability, through the *serviceLocator* request extension. If the OCSP service provider does not have CSI concerning the certificate the dependent entity enquires, it may refer the dependent entity to another CSI provider. Location information for that CSI provider is contained in the OCSP Response extension *serviceLocator*.

CRL, DP CRL and Delta-CRL do not inherently support the referral capability. If an LDAPv3 [4] Directory is used as the CRL repository, the CSI provider can refer the dependent entity to other CSI providers by using LDAP referrals [4].

3.1.7 Revocation Reasons

All the mechanisms we examine can disseminate information to the dependent entity on the reasons for the revocation of a certificate (*CRLReason* extension [8, 14]). However, the use of those reasons as input information in a certificate path validation function has to be studied further [7, 10]. These reasons should be used in the process of certificate path validation only if they can provide results that are complete, repeatable, and compliant with the policy of the dependent entity and the policy of the authority which executes the certificate path validation function. These requirements are currently not met by the mechanisms we examine.

3.1.8 Notification of revocation or suspension

The CSI mechanisms we examine do not provide this kind of functionality. This functionality must not be integrated to the CSI mechanism; it should only be temporally bound to the CSI generation or storage.

3.2 Performance

3.2.1 Timeliness of CSI

The metrics presented in the respective part of section 2 can be used in order to evaluate the use of the CSI mechanisms we examine, either on their own or their joint use, in specific communities of certificates users (certificate holders and dependent entities). The initial number of certificate holders, dependent entities, CAs, CSI providers and CSI requests has to be estimated. The rate of growth of those has to be estimated as well, over time or over specific time periods. Using the aforementioned data, we could evaluate the use of the mechanisms we examine for a specific community of certificates users.

3.2.2 Freshness of CSI

The freshness property of CSI for CAs in Europe depends on legal requirements ([6] and national laws). A freshness value that meets these requirements should be agreed upon, through the use of certain mechanisms (see previous section on timeliness). Less fresh CSI should also be available, offering other advantages.

3.2.3 Bounded revocation

CRL, DP CRL, Delta-CRL and OCSP support bounded revocation with the use of the *nextUpdate* CRL and Response extensions respectively. These CSI mechanisms could also support time-complete revocation. This is a matter of policy.

3.2.4 Emergency CSI capability

All the mechanisms we examine support this capability. Immediate generation of CSI, though, does not include necessarily immediate CSI dissemination.

A CSI authority that uses one (or more) of the mechanisms we present can generate CSI immediately after receiving an authorised revocation request. However, this CSI will not be made available to the dependent entities immediately, with the exception of OCSP. If the OCSP service locator retrieves CSI directly from the repository, where the CSI authority stores it, then CSI will also be made available to the dependent entities immediately.

3.2.5 Scalability

For CRLs and OCSP, the communication cost in time units varies linearly with the size of CSI. This is also the case when the number of authorities or CSI repositories varies.

For Distribution Point CRLs, the communication cost in time units varies linearly with the size of CSI, and this is independent of the number of partitions.

The communication cost (in time units) of Delta-CRLs grows linearly with the number of authorities or CSI repositories. This cost grows also linearly with the differences between the BaseCRL and a DeltaCRL.

The timeliness metrics depend highly on the characteristics of the communications medium, the bandwidth, and the propagation delay of the communications channel between the CA and the repositories, and of the communications channel between the repositories and the dependent entities. For the CSI mechanisms we examine, the timeliness metric decreases when the CSI size increases, and when the number of repositories grows.

Note that an OCSP service provider may be vulnerable to DoS attacks due to the fact that it has to authenticate every OCSP response, which is time consuming.

3.2.6 Adjustability

None of the mechanisms we examine supports adjustability of the protection level offered by the CSI mechanisms. The freshness and timeliness of the available CSI is not adjustable. However, the CA policy could provide more than one level of protection, by requiring more than one, separate instances of the CSI mechanism. Every instance could provide CSI with different characteristics, as far as timeliness and freshness is concerned.

3.3 Security

Features discussed in this section are the ones that would have to be met to comply with the European Directive (Annex II of [6]). These features mainly address those requirements contained in the European Directive, which concern the “secure directory” and the “secure revocation service”.

3.3.1 CSI disseminator authentication

All the CSI mechanisms we examine meet this criterion. CSI disseminator authentication in CRL, DP CRL, and Delta-CRL is achieved through the verification of the digital signature in the respective revocation lists. OCSP Responses are also signed, thus OCSP also meets this criterion.

3.3.2 CSI integrity

The integrity of CSI, while in transit or while stored at the dependent entities' local storage, is protected through the digital signatures of the CSI authority. This applies to all the mechanisms we examine (see also CSI dissemination authentication, previous section).

3.3.3 CA compromise

None of the mechanisms we examine meet this criterion. If the CA is compromised, the entity who gained control of the respective CA keys is able to revoke certificates or issue new ones at will, until the CA compromise information reaches the dependent entities through an Authority Revocation List (ARL) or another, possibly out-of-band mechanism (e.g. in case the CA private key is no longer available to the CA personnel and it is only available to the entity who illegally gained control over it).

3.3.4 RevA compromise

OCSP does not provide for delegation of certificate revocation; thus the authority that revokes certificates is the CA itself. In this case, dependent entities will be informed of a possible CA compromise through an ARL. The same applies for the other CSI mechanisms we examine (CRL, DP CRL, and Delta-CRL).

3.3.5 Contained functionality

If the authority that disseminates CSI is a Trusted Responder, a CA Designated Responder [14], or a CA (CSI is distributed in CRL, DP CRL, or Delta-CRL and the CA uses a separate CA key to sign CSI), then the compromise of the keys used by these authorities do not enable the entities who gained control of these keys to issue new certificates. However, previously revoked or suspended certificates can be made valid again.

If the authority that disseminates CSI is a CA, and it uses the CA certificate signing key in order to sign CRL, DP CRL or Delta-CRL as well, then a compromise of that authority (that is, the CA) will enable the entity who gained control of the respective keys to revoke certificates and issue new ones at will.

3.3.6 Availability

There are no mechanisms in CRLs [11, 8] to protect the availability of CSI. If LDAP Directories are used as CSI repositories, LDAPv3 [4] replication and referral mechanisms could be used in order to increase the availability of CSI.

The OCSP *serviceLocator* extension and the mirroring of the CSI repositories used by OCSP in order to generate CSI from, could increase the availability of CSI provided by OCSP.

4. CONCLUSION

The evaluation framework we presented can be used by the research community for further research on CSI mechanisms, either improving the existing or developing new ones. This framework can also be used by the industry; until now, high-level PKI requirements were compared against specific CSI mechanisms based on empirical methods or ad hoc research while our framework can be used by PKI implementers and policy makers to select the CSI mechanism or mechanisms that will be used in a PKI, depending on the underlying, high-level requirements.

We evaluated CRLs and OCSP, using our evaluation framework, and we defined quantitative metrics for estimating the timeliness, freshness and scalability of these mechanisms. The criterion of adjustability is not met by any of the mechanisms, therefore freshness and other metrics are not adjustable by the entities who take the risk of trusting CSI.

Furthermore, none of these mechanisms meets the feedback criterion, which we believe is crucial for the efficient operation of CSI mechanisms. Although the mechanisms we examined support the inclusion of revocation reason information in CSI, they do not process this information within their certificate path validation functions. There are still issues to resolve [7], before this is feasible. Moreover, revocation notification is not inherently supported by any mechanism, though external notification procedures could well be synchronised with the CSI mechanisms. The same applies for the referral capability of CSI mechanisms.

The consequences of having the CSI authority key compromised are in some cases contained while the consequences of having the CA key are not; if the CSP signing key is compromised, certificates can be issued and revoked at will by the entity who gained control of this key.

All the mechanisms we present support delegation of CSI dissemination, bounded revocation, CSI disseminator authentication and CSI integrity protection. These are well-supported features of the mechanisms. The mechanisms also meet the transparency criterion; however the respective features of the mechanisms have not been widely used by the industry.

Delegation of certificate path validation is partially supported by OCSP, while delegation of revocation is only supported by CRLs. Finally, Emergency CSI generation is supported by all mechanisms. However, rendering available the CSI that was generated in an emergency situation would cause problems in the policy of a CSI authority, should this authority wish to support time-complete revocation.

We hope that our evaluation framework will provide aid to other researchers, while improving the existing CSI mechanisms or investigating new ones. We also hope that our evaluation of CRLs, DP CRLs, Delta-CRLs and OCSP will provide useful information to current PKI researchers and developers. In the future we plan to apply our framework after adding specific metric values to suggest improvements in existing schemes for wide scale deployment.

5. ACKNOWLEDGMENTS

The authors would like to thank the anonymous referees for their helpful comments. This work was partially funded by the European Commission (Directorate General III, contract #ETD/99/502536). Bart Preneel is a research associate, sponsored by the National Fund for Scientific Research, Flanders (Belgium).

6. REFERENCES

[1] Adams C., Farrell S., Internet X.509 Public Key Infrastructure Certificate Management Protocols, Request for Comments 2510, 1999 (available at http://www.ietf.org/rfc/rfc2510.txt).

[2] Hallam-Baker P., OCSP Extensions, IETF Internet Draft, September 1999.

[3] Berkovits S., Chokhani S., Furlong J. A., Geiter J. A., and Guild J. C., Public Key Infrastructure Study: Final Report. Produced by the MITRE Corporation for NIST, Apr. 1994.

[4] Chadwick D. W., Internet X.509 Public Key Infrastructure, Operational Protocols: LDAPv3 (Category: Standards Track), August 1999.

[5] Chokhani S., Ford W., Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, (Status: INFORMATIONAL) Request for Comments 2527, March 1999 (available at http://www.ietf.org/rfc/rfc2527.txt).

[6] Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures, 13 December 1999.

[7] Fox B., LaMacchia B., Certificate Revocation: Mechanics and Meaning, In *Proceedings of Financial Cryptography 98*, LNCS 1465, New - York, Springer - Verlag.

[8] Housley R., Ford W., Polk W., Solo D., Internet X.509 Public Key Infrastructure, Certificate and CRL Profile, IETF PKIX Working Group, Request for Comments 2459 (Category: Standards Track), January 1999 (available at http://www.ietf.org/rfc/rfc2459.txt).

[9] Housley R., Ford W., Polk W., Solo D., IETF PKIX Working Group, Internet X.509 Public Key Infrastructure, Certificate and CRL Profile, Internet Draft, October 1999 (available at http://www.ietf.org//internet-drafts/draft-ietf-pkix-new-part1-00.txt).

[10] Iliadis I., On the Dissemination of Certificate Status Information, MSc thesis, Department of Mathematics, Royal Holloway and Bedford New College, University of London, UK, 1999.

[11] ISO/IEC 9594-8 (1994), Open Systems Interconnection - The Directory: Authentication Framework.

[12] Berners-Lee T., Fielding R., Masinter L., Uniform Resource Identifiers (URI): Generic Syntax, (Draft Standard), August 1998 (available at http://www.ietf.org/rfc/rfc2396.txt).

[13] Micali S., Efficient Certificate Revocation, Technical Memo 542b, Laboratory for Computer Science, Massachusetts Institute of Technology, March 1996.

[14] Myers M., Ankney R., Malpani A., Galperin S., Adams C., Internet X.509 Public Key Infrastructure, Online Certificate Status Protocol, IETF PKIX Working Group, Request for Comments 2560 (Category: Standards Track), January 1999 (available at http://www.ietf.org/rfc/rfc2560.txt).

[15] Nilsson H, Van Eecke P., Medina M., Pinkas D., Pope N., European Electronic Signature Standardization Initiative, ICTSB, Final Report of the EESSI Expert Team, 20 July 1999.

[16] US National Institute of Standards and Technology, *A Public Key Infrastructure for US Government unclassified but sensitive applications*, September 1995.

[17] Santesson S., Polk W., Barzin P., Nystrom M., IETF PKIX Working Group, Internet X.509 Public Key Infrastructure, Qualified Certificates Profile, Internet Draft, February 2000 (available at http://www.ietf.org//internet-drafts/draft-ietf-pkix-qc-03.txt).

[18] ITU-T Rec. X.509 (1997) | ISO/IEC 9594-8 - Information Technology - Open Systems Interconnection - the Directory: Authentication Framework.