Financial Responsibility Issues Discussion

CA-Browser Forum
June 19, 2006
Mountain View, CA

June 12, 2006

To: Forum Members
From: Kirk Hall, GeoTrust

At our last meeting in Scottsdale, we discussed five related issues concerning financial responsibility for CAs who want to issue Extended Validation certs (Sections 9.1 through 9.11 of our Minimum Requirements document): CA financial stability, liability, insurance, disclosure, and implementation/enforcement. I have again included the portions of RFC 3647 relating to a CA's financial responsibility as Exhibit C for reference purposes (note: these sections are numbered 4.9.1 through 4.9.9, but correspond to our sections).

> **Recommendation: Adopt the insurance requirements in concept as shown in Exhibit A. Once we have agreed conceptually on liability and insurance requirements, we can adopt conforming changes to Sections 9.2, 9.4, 9.8, 9.10, and 9.11 of our Minimum Requirements document (see Exhibit B).**

Discussion

Issue 1: Financial Stability

The consensus from these discussions was that it would be too difficult to attempt to impose requirements concerning CA financial stability (positive net worth, going concern) because some CAs are not audited and do not disclose their financials, and WebTrust auditors in the US would be prohibited from also conducting a financial audit of an Extended Validation cert. It also appears that we can address financial responsibility issues in another way, namely insurance.

Issue 2: Liability

On the issue of Extended Validation CA liability, we discussed (a) to whom Extended Validation CAs should be liable – the possibilities included subscribers, relying parties, and the browsers and other applications who display or rely on an EV cert's Extended Validation status, and well as (b) for what Extended Validation CAs should be liable – the possibilities included liability for failure to follow the EV vetting guidelines, or for stating an incorrect identity in the EV cert (i.e., a warranty that the issuing CA has stated the *correct* identity information in the EV cert).

After further thought, our recommendation for EV certs is that the issuing CA should be liable (at least to the extent of the required EV CA insurance coverage discussed below) to *all* the parties who would potentially be injured by incorrect issuance of an EV cert, or the issuance to an imposter or fraudster – namely, *liability should extend to subscribers, relying parties, and browsers and other applications that use and display EV certs* – and that the issuing CA be liable not just for failing to follow its stated vetting steps, *but should be liable for issuing an EV cert with false or incorrect identity information* – meaning there would be liability for the issuing EV CA for issuing an EV cert to an imposter or fraudulent party. (Of course, the claimant would still have to show that the EV cert with false or incorrect identity information actually caused harm, and the dollar amount of the damages, to collect anything.)

Why have we reached this conclusion? *Because EV certs are ultimately about strongly confirming business identity in a highly reliable way that can be relied on by the public.* There's no reason to waste our time on the EV certs requirements process otherwise – if we as issuing CAs aren't willing to stand behind our EV certificates, why should anyone else use or rely on them?

Any current CA who doesn't want to take on this potential liability (which will require, for the first time, that CAs truly become serious about strongly confirming business identity in a highly reliable way) will not have to issue EV certs – and so those CAs can continue to issue their current certs via their current processes, without taking on liability as to the EV cert holder's ultimate identity and nothing will change. But that should not prevent other CAs from issuing EV certs and taking on liability (within insurance limits) for actual business identity, thereby creating something truly new and useful in Extended Validation certificates.

Issue 3: Insurance

It appears the best way to provide for financial responsibility would be through an insurance requirement for Extended Validation CAs (which would apply to their Extended Validation certs only, not other products). This approach has already been adopted by the Mortgage Brokers Association's SISAC organization (Secure Identity Services Accreditation Corporation). See links:

http://www.sisac.org/SISAC/documents/SISACCertPolicyReqsDocv14.pdf

http://www.sisac.org/doc_lib.asp

I spoke at length with R.J. Schlecht, SISAC's director, about these insurance requirements. He said SISAC adopted stronger CA requirements than WebTrust, including the insurance requirements shown in the links above, because the Mortgage Brokers Association was not satisfied with the identity vetting done by CAs today, and wanted something stronger. He noted that one company has already qualified (VeriSign), and that GeoTrust was part way through the process. One difference between SISAC insurance requirements and our recommendation for EV cert insurance requirements is what is being insured against – SISAC only requires the issuing CA to insure against failure to follow vetting steps. We are recommending insurance against issuance of an EV cert with false or incorrect identity for the reasons stated above.

On the insurance issue, he said no difficulties had been encountered to date. The insurance requirement was drafted to reflect the risks that would have to be covered by the CA, without trying to name the exact type of insurance that a CA should buy (as coverage may vary from carrier to carrier). In general, Mr. Schlecht said that errors &

omissions coverage (E&O) would likely be the right insurance for this risk, *but that a conforming CA would have to be certain to specifically list and describe the Extended Validation certs and potential liabilities to subscribers, relying parties, and browsers and other applications that use and display the EV cert identity information* in order to make certain there would be adequate coverage.

We discussed appropriate coverage limits. SISAC requires $10,000,000 in insurance coverage for high level certs issued by a CA. He said that an aggregate limit per Extended Validation certificate (total damages from all claims from a single bad cert) were appropriate so the issuing CA would not be wiped out, and believed a limit of $100,000 per claim/$100,000 aggregate all claims arising from or relating to issuance of a single certificate or group of certificates from a single vetting process would be reasonable in the market. If the CA outsources some of all of the RA function, the insurance must cover the outsourced activities (or the RA must show proof of the same insurance coverage that covers its activities for Extended Validation certs). Extended Validation CAs should also provide an "easy access" claims process, as is the case for CAs who seek SISAC accreditation.

Protecting the public from bad Extended Validation certs containing false or incorrect identity information is very important, and can be accomplished fairly easily by agreeing to these insurance requirements. See specific insurance requirements recommendations at Exhibit A.

4. Disclosure

In line with the principles of WebTrust, CPs, and CPSs, we should require that Extended Validation CAs fully disclose the liability they are assuming as well as the insurance they are maintaining in their CPS for Extended Validation certs. We also should consider requiring a short-form, simple language disclosure concerning liability and insurance for Extended Validation certs that must be given prominent display on an Extended Validation CA's web site, perhaps on the "order" page for Extended Validation certs (right now, finding a CPS is hard enough, let alone locating the liability and insurance provisions).

5. Implementation and Enforcement

Finally, whatever requirements are adopted should have to be included in an Extended Validation CA's relevant CPS, and be audited annually, either as a Supplemental Audit performed by the CA's WebTrust auditor, or eventually incorporated directly in the WebTrust audit itself.

> **Further Action Required:** *Once the CA-Browser Forum has decided on appropriate liability and insurance requirements for Extended Validation certs, we will need to make conforming changes to Sections 9.2, 9.4, 9.8, 9.10, and 9.11 of our Minimum Requirements document for review and adoption at the next meeting.*

Exhibit A – EV Certificate Insurance Requirements

[Recommendation to CA-Browser Forum]

The CA must maintain indemnity insurance coverage (e.g. "errors and omissions," "cyber coverage," "network computer liability," "professional liability," or other similar coverage) for Extended Validation Certificates obtained from an insurance company rated __[ratings to be specified]__ or better by international ratings organizations. "Self-insurance," asset pledges, and bonding will not be allowed as a substitute for these insurance requirements, but insurance provided by a bona fide captive insurer is acceptable.

Such coverage must be an occurrence basis in an annual aggregate coverage amount of not less than $10 million with respect to the issuance of Extended Validation Certificates, with per claim coverage of not less than $100,000 per claim/$100,000 all claims arising from or relating to issuance of a single Extended Validation certificate or group of certificates from a single Extended Validation vetting process.

Such coverage must cover damage claims presented by:

> (1) subscribers who obtain Extended Validation certificates,
>
> (2) relying parties who rely on an Extended Validation certificate in a communication or transaction with the business or site that has obtained the cert, and
>
> (3) browsers and other applications that use and display Extended Validation certificates to relying parties and other users,

when a misidentification results at the time of issuance and the Extended Validation certificate contains false or incorrect identity information about the business that obtained the certificate.

Evidence of insurance must be presented as part of the process of obtaining approval from the browsers of an Extended Validation OID to be used in connection with Extended Validation certs, and proof of insurance must be established by means of an annual supplemental audit provided by a WebTrust for CAs approved auditor. Failure to maintain adequate insurance must result in revocation of the CA's ability to issue Extended Validation certificates, withdrawal of approval of the CA's Extended Validation OIDs, and a change in status of all Extended Validation certificates issued by the CA and still outstanding from Extended Validation status to non-Extended Validation status.

Certificates of insurance must be requested from the carrier by a CA and delivered to all browsers or other applications upon request prior to Extended Validation OID or other Extended Validation status approval, and such certificates must identify the browser or other application as additional insureds thereunder and must include certified copies of endorsements along with a provision that coverages afforded must not be canceled without 60 days prior written notice to the browser or other application.

The CA must specify an "easy access" system for those claiming entitlement to coverage for claims under such insurance policy. Any claim resulting from a failure to follow required I&A procedures must be paid by the CA within a very short time, not to exceed three (3) months, or allow the claimant to seek coverage directly from the CA's insurer.

Exhibit B - Draft Sections 9.1 to 9.11 to Minimum Requirements Document

[June 19, 2006]

9. Other Business and Legal Matters

9.1 Fees

No stipulation.

9.2 Financial Responsibility

[This section must be conformed to whatever insurance requirements we agree to.]

9.3 Other assets

No stipulation.

9.4 Insurance or warranty coverage for end-entities

[This section must be conformed to whatever insurance requirements we agree to.]

9.5 Confidentiality of business information

9.5.1 Scope of confidential information

No stipulation.

9.5.2 Information not within the scope of confidential information

No stipulation.

9.5.3 Responsibility to protect confidential information

No stipulation.

9.6 Privacy of personal information

9.6.1 Privacy plan

No stipulation.

9.6.2 Information treated as private

No stipulation.

9.6.3 Information not deemed private

No stipulation.

9.6.4 Responsibility to protect private information

No stipulation.

9.6.5 Notice and consent to use private information

No stipulation.

9.6.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.6.7 Other information disclosure circumstances

No stipulation.

9.7 Intellectual property rights

Copyright - ? Patent claims – not applicable.

9.8 Representations and warranties

9.8.1 CA representations and warranties

[This section must be conformed to whatever insurance requirements we agree to.]

I can't find a suitable section for this …

The ***CA*** SHALL include by reference these requirements in all contracts with arms-length subordinate CAs, RAs, hosting services, etc.. The ***CA*** SHALL enforce the terms of such a contract.

9.8.2 RA representations and warranties

[This section must be conformed to whatever insurance requirements we agree to.]

9.8.3 Subscriber representations and warranties

[This section must be conformed to whatever insurance requirements we agree to.]

The ***CA's*** subscriber agreement MUST require the signer to provide complete and accurate identifying information.

9.8.4 Relying party representations and warranties

No stipulation.

9.8.5 Representations and warranties of other participants

No stipulation.

9.9 Disclaimers of warranties

[This section must be conformed to whatever insurance requirements we agree to.]

9.10 Limitations of liability

[This section must be conformed to whatever insurance requirements we agree to.]

The ***CA*** MAY place limits on the extent of the liability that it assumes.

9.11 Indemnities

[This section must be conformed to whatever insurance requirements we agree to.]

Exhibit C - RFC 3647 Excerpts

RFC 3647 - Internet X.509 Public Key Infrastructure – Nov. 2003

The provisions of RFC 3647 -- X.509 PKI CP and CPS Framework relating to a CA's financial responsibility and insurance are found at Section 4.9. *Note: We have numbered this as **Section 9** of our Requirements document*.

4.9. Other Business and Legal Matters

This component covers general business and legal matters. Sections 9.1 and 9.2 of the framework discuss the business issues of fees to be charged for various services and the financial responsibility of participants to maintain resources for ongoing operations and for paying judgments or settlements in response to claims asserted against them. The remaining sections are generally concerned with legal topics.

Starting with Section 9.3 of the framework, the ordering of topics is the same as or similar to the ordering of topics in a typical software licensing agreement or other technology agreement. Consequently, this framework may not only be used for CPs and CPSs, but also associated PKI-related agreements, especially subscriber agreements, and relying party agreements. This ordering is intended help lawyers review CPs, CPSs, and other documents adhering to this framework.

With respect to many of the legal subcomponents within this component, a CP or CPS drafter may choose to include in the document terms and conditions that apply directly to subscribers or relying parties. For instance, a CP or CPS may set forth limitations of liability that apply to subscribers and relying parties. The inclusion of terms and conditions is likely to be appropriate where the CP or CPS is itself a contract or part of a contract.

In other cases, however, the CP or CPS is not a contract or part of a contract; instead, it is configured so that its terms and conditions are applied to the parties by separate documents, which may include associated agreements, such as subscriber or relying party agreements. In that event, a CP drafter may write a CP so as to require that certain legal terms and conditions appear (or not appear) in such associated agreements. For example, a CP might include a subcomponent stating that a certain limitation of liability term must appear in a CA's subscriber and relying party agreements. Another example is a CP that contains a subcomponent prohibiting the use of a subscriber or relying party agreement containing a limitation upon CA liability inconsistent with the provisions of the CP. A CPS drafter may use legal subcomponents to disclose that certain terms and conditions appear in associated subscriber, relying party, or other agreements in use by the CA. A CPS might explain, for instance, that the CA writing it uses an associated subscriber or relying party agreement that applies a particular provision for limiting liability.

4.9.1. Fees

This subcomponent contains any applicable provisions regarding fees charged by CAs, repositories, or RAs, such as:

* Certificate issuance or renewal fees;

* Certificate access fees;

* Revocation or status information access fees;

* Fees for other services such as providing access to the relevant CP or CPS; and

* Refund policy.

4.9.2. Financial Responsibility

This subcomponent contains requirements or disclosures relating to the resources available to CAs, RAs, and other participants providing certification services to support performance of their operational PKI responsibilities, and to remain solvent and pay damages in the event they are liable to pay a judgment or settlement in connection with a claim arising out of such operations. Such provisions include:

* A statement that the participant maintains a certain amount of insurance coverage for its liabilities to other participants;

* A statement that a participant has access to other resources to support operations and pay damages for potential liability, which may be couched in terms of a minimum level of assets necessary to operate and cover contingencies that might occur within a PKI, where examples include assets on the balance sheet of an organization, a surety bond, a letter of credit, and a right under an agreement to an indemnity under certain circumstances; and

* A statement that a participant has a program that offers first-party insurance or warranty protection to other participants in connection with their use of the PKI.

4.9.3. Confidentiality of Business Information

This subcomponent contains provisions relating to the treatment of confidential business information that participants may communicate to each other, such as business plans, sales information, trade secrets, and information received from a third party under a nondisclosure agreement. Specifically, this subcomponent addresses:

* The scope of what is considered confidential information,

* The types of information that are considered to be outside the scope of confidential information, and

* The responsibilities of participants that receive confidential information to secure it from compromise, and refrain from using it or disclosing it to third parties.

4.9.4. Privacy of Personal Information

This subcomponent relates to the protection that participants, particularly CAs, RAs, and repositories, may be required to afford to personally identifiable private information of certificate applicants, subscribers, and other participants. Specifically, this subcomponent addresses the following, to the extent pertinent under applicable law:

* The designation and disclosure of the applicable privacy plan that applies to a participant's activities, if required by applicable law or policy;

* Information that is or is not considered private within the PKI;

* Any responsibility of participants that receive private information to secure it, and refrain from using it and from disclosing it to third parties;

* Any requirements as to notices to, or consent from individuals regarding use or disclosure of private information; and

* Any circumstances under which a participant is entitled or required to disclose private information pursuant to judicial, administrative process in a private or governmental proceeding, or in any legal proceeding.

4.9.5. Intellectual Property Rights

This subcomponent addresses the intellectual property rights, such as copyright, patent, trademarks, or trade secrets, that certain participants may have or claim in a CP, CPS, certificates, names, and keys, or are the subject of a license to or from participants.

4.9.6. Representations and Warranties

This subcomponent can include representations and warranties of various entities that are being made pursuant to the CP or CPS. For example, a CPS that serves as a contract might contain a CA's warranty that information contained in the certificate is accurate. Alternatively, a CPS might contain a less extensive warranty to the effect that the information in the certificate is true to the best of the CA's knowledge after performing certain identity authentication procedures with due diligence. This subcomponent can also include requirements that representations and warranties appear in certain agreements, such as subscriber or relying party agreements. For instance, a CP may contain a requirement that all CAs utilize a subscriber agreement, and that a subscriber agreement must contain a warranty by the CA that information in the certificate is accurate. Participants that may make representations and warranties include CAs, RAs, subscribers, relying parties, and other participants.

4.9.7. Disclaimers of Warranties

This subcomponent can include disclaimers of express warranties that may otherwise be deemed to exist in an agreement, and disclaimers of implied warranties that may otherwise be imposed by applicable law, such as warranties of merchantability or fitness for a particular purpose. The CP or CPS may directly impose such disclaimers, or the CP or CPS may contain a requirement that disclaimers appear in associated agreements, such as subscriber or relying party agreements.

4.9.8. Limitations of Liability

This subcomponent can include limitations of liability in a CP or CPS or limitations that appear or must appear in an agreement associated with the CP or CPS, such as a subscriber or relying party agreement. These limitations may fall into one of two categories: limitations on the elements of damages recoverable and limitations on the amount of damages recoverable, also known as liability caps. Often, contracts contain clauses preventing the recovery of elements of damages such as incidental and consequential damages, and sometimes punitive damages. Frequently, contracts contain clauses that limit the possible recovery of one party or the other to an amount certain or to an amount corresponding to a benchmark, such as the amount a vendor was paid under the contract.

4.9.9. Indemnities

This subcomponent includes provisions by which one party makes a second party whole for losses or damage incurred by the second party, typically arising out of the first party's conduct. They may appear in a CP, CPS, or agreement. For example, a CP may require that subscriber agreements contain a term under which a subscriber is responsible for indemnifying a CA for losses the CA sustains arising out of a subscriber's fraudulent misrepresentations on the certificate application under which the CA issued the subscriber an inaccurate certificate. Similarly, a CPS may say that a CA uses a relying party agreement, under which relying parties are responsible for indemnifying a CA for losses the CA sustains arising out of use of a certificate without properly checking revocation information or use of a certificate for purposes beyond what the CA permits.