Ballot 121 – EVGL Insurance Requirements

The EV Guidelines Working Group is considering updating the EV Guidelines in a number of areas. Kirk Hall of Trend Micro hereby makes the following motion, and Moudrick Dadashov from Skaitmeninio sertifikavimo centras (SSC) and Richard Wang from WoSign have endorsed it.

This ballot is to amend the current EV Guidelines (EVGL) Sec. 8.4 requirements as stated below. The reasons in favor of the Ballot are stated after the proposed amendments.

Motion begins:

Amend EV Guideline Section 8.4 to read as follows:

> **EV Guideline Section 8.4 - Insurance**
>
> Each CA SHALL maintain ~~the following~~ insurance related to ~~their~~ **its** respective performance and obligations under these Guidelines **in accordance with the the minimum insurance requirements (if any) as are applicable to the CA under the law of its jurisdiction of incorporation or registration.** ~~:~~
>
> > ~~(A) Commercial General Liability insurance (occurrence form) with policy limits of at least two million US dollars in coverage; and~~
> >
> > ~~(B) Professional Liability/Errors and Omissions insurance, with policy limits of at least five million US dollars in coverage, and including coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.~~
>
> ~~Such insurance MUST be with a company rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies each of the members of which are so rated).~~
>
> ~~A CA MAY self-insure for liabilities that arise from such party's performance and obligations under these Guidelines provided that it has at least five hundred million US dollars in liquid assets based on audited financial statements in the past twelve months, and a quick ratio (ratio of liquid assets to current liabilities) of not less than 1.0.~~

Motion Ends

The reasons for this proposed amendment are as follows:

- The insurance requirements were created basically out of thin air during initial drafting of the EVGL, without any particular analysis of claims against CAs, usefulness of insurance, availability of appropriate insurance, or necessary insurance levels. The main purpose of an insurance requirement in the EVGL was to impress the public with the responsibility of CAs who issue EV certificates. However, as noted below, these reasons aren't really justified by the facts.

- The types and amounts of insurance required under EVGL 8.4 are North America-centric, and are not easily available in other world regions (or not available at all). Insurance for damages "arising out of infringement of the proprietary rights of any third party" are generally not available in many professional liability/errors and omissions policies. The requirement is arguably unfair to CAs outside North America.

- The types of insurance required under EVGL 8.4 are not designed to provide relief or compensation to injured customers or the public who rely on EV certs issued by a CA. Both types of insurance are intended primarily to protect the issuing CA, not injured claimants, and the insurers will try to avoid or defeat all claims from claimants. The policies typically include defense costs within the policy limits, so an insurance policy might be entirely consumed by defense costs to protect the issuing CA, with nothing left to pay claims to claimants.

- Commercial General Liability insurance doesn't really help customers or relying parties who claim injury from a bad cert – these policies are more designed to protect the CA from things like people falling on a slippery floor in the CA's offices, etc. Likewise, professional liability/E&O coverage will only pay after defending the CA if a judgment is likely or rendered, and the insurer may try to avoid coverage if the issuing CA has done some bad things. For example, Diginotar's insurer has denied all coverage because Diginotar hid its breach and failed to report the problem for several weeks, compounding the damages and violating its obligations to the insurers – so the insurance was worthless. These policies also do not cover contract claims from customers (e.g., a claim of breach of contract by the CA such as failure to issue a proper cert).

- Some have suggested that even if the current insurance requirements don't actually protect the public or customers, they are nevertheless useful as a "show of seriousness" by a CA. If that is a worthwhile objective, we may as well require other irrelevant things instead like proof of auto insurance or a minimum office space size – none of these qualifications are really relevant to whether a CA operates competently and in compliance with requirements. Instead, we rely mostly on (1) annual performance audits, and (2) browser root programs (and consequences of failure) to confirm competence and compliance.

- VeriSign's previous general counsel for ten years has said VeriSign never faced a claim for damages from any certs during that time. In most cases, bad certs are simply revoked and possibly reissued.

- Even though there have been virtually no claims against issuing CAs, buying the minimum insurance can be expensive for smaller CAs. There is typically a minimum premium of $25,000 or more per year with a significant deductible, even though the CA will likely never have a covered claim. That's a waste of money.

- In the Diginotar case, apparently claims were made against the company's insurers (perhaps from investors for loss of value of the company when it was shut down). In any case, Diginotar's insurer denied all coverage for the claims based on Diginotar's bad acts and breach of its obligations to the insurer. There would be no possibly insurance coverage for customers or relying parties, so the insurance was of no value.

- Some countries have their own minimum insurance requirements for companies incorporated or registered in their jurisdiction, while many do not. The CA/Browser Forum should defer to these decisions by the governing jurisdictions and require compliance with local standards – or just delete Section 8.4 entirely, as every CA must already comply with applicable laws.

- Finally, under current EVGL Sec. 8.4, large companies like Trend Micro get to opt out of the insurance requirements because they meet the stated financial requirements. This is arguably an unfair advantage for large companies over small ones.

The review period for this ballot shall commence at 2200 UTC on Wednesday, 23 April 2014, and will close at 2200 UTC on Wednesday, 30 April 2014. Unless the motion is withdrawn during the review period, the voting period will start immediately thereafter and will close at 2200 UTC on Wednesday, 7 May 2014. Votes must be cast by posting an on-list reply to this thread.

A vote in favor of the motion must indicate a clear 'yes' in the response. A vote against must indicate a clear 'no' in the response. A vote to abstain must indicate a clear 'abstain' in the response. Unclear responses will not be counted. The latest vote received from any representative of a voting member before the close of the voting period will be counted. Voting members are listed here: https://cabforum.org/members/

In order for the motion to be adopted, two thirds or more of the votes cast by members in the CA category and greater than 50% of the votes cast by members in the browser category must be in favor. Also, at least six members must participate in the ballot, either by voting in favor, voting against, or abstaining.