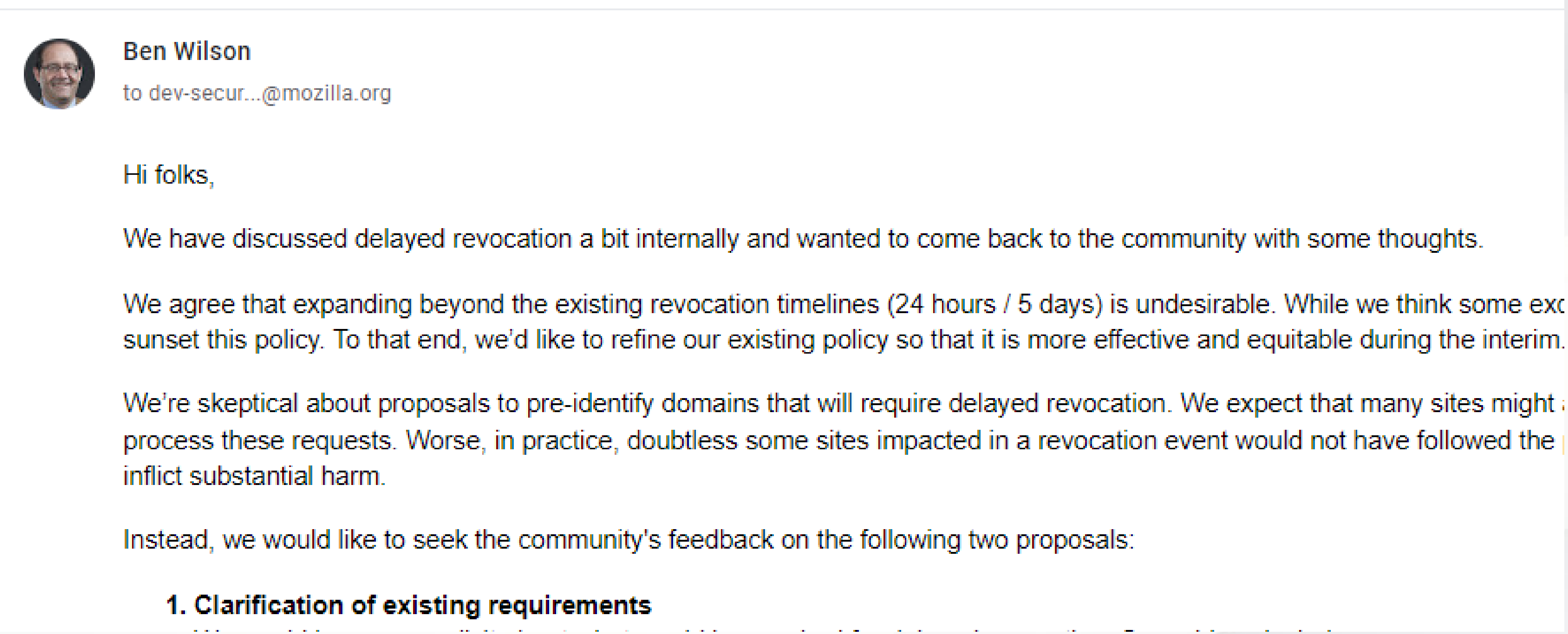
The privilege of being a public CA

Let’s talk about delayed revocation

- Delrev = delayed revocation bug
- Deliberate = choice by CA
  - Versus accidental delrev = software or process error unforeseen in good faith
- 9/20/24 snapshot
  - 70 open Bugzilla bugs
  - 22 delayed revocation
  - 20 deliberate delrev (29%), one accidental, and one meta-bug
- Nearly one third of ALL open bugs are for deliberately delayed revocation

Mozilla delivers a smackdown



Ben Wilson

to dev-secur...@mozilla.org

Hi folks,

We have discussed delayed revocation a bit internally and wanted to come back to the community with some thoughts.

We agree that expanding beyond the existing revocation timelines (24 hours / 5 days) is undesirable. While we think some exc
sunset this policy. To that end, we'd like to refine our existing policy so that it is more effective and equitable during the interim.

We're skeptical about proposals to pre-identify domains that will require delayed revocation. We expect that many sites might
process these requests. Worse, in practice, doubtless some sites impacted in a revocation event would not have followed the
inflict substantial harm.

Instead, we would like to seek the community's feedback on the following two proposals:

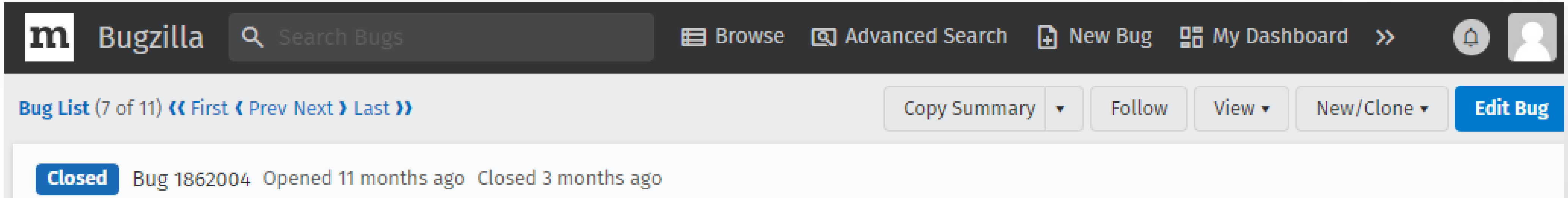
1. **Clarification of existing requirements**

SECTIGO®

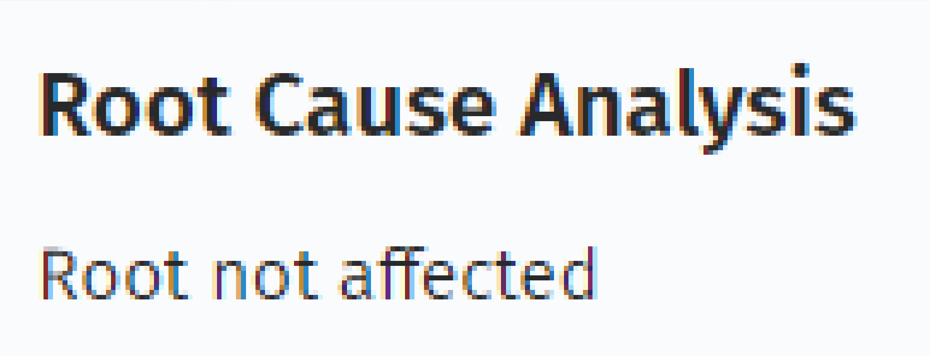
Delrev is just an example

- Delrev
- Refrev (refused revocation)
- Failure to lint
- Failure to report
- Failure to answer questions, correct previous errors, or learn from other CAs

Is this what we want?



Closed Bug 1862004 Opened 11 months ago Closed 3 months ago



Root Cause Analysis

Root not affected

Is this what we want?

- CAs who act like their corporate owners trump the WebPKI
- CAs who act like their local governments trump the WebPKI
- CAs who do the minimum they can get away with
- CAs who choose Subscriber convenience over compliance
- CAs who hide and misdirect and trick the community
- CAs who don’t know the basic rules for being a CA
- CAs who make self-serving, intellectually dishonest arguments
- CAs who resist CABF changes for the good of the community because of their own inconvenience

Why do we have these things?

- A rule requiring linting
- A rule requiring CAs to support automation
- A rule dictating the maximum time to respond to a certificate report
- A rule dictating the maximum time to respond to a Bugzilla question
- A rule requiring that CAs find root causes for incidents and take action items to rectify them

What do we want to be?

If you liked this conversation…

ROOT CAUSES

A PKI & Security Podcast

Available on these streaming services

Spotify

iHeart RADIO

STITCHER

iTunes

SOUNDCLOUD

Thank you very much!

https://www.sectigo.com/