From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: Michael Markowitz <markowitz@infoseccorp.com>, Mike Ounsworth <mike.ounsworth@entrust.com>, pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates
Date: Friday, October 28, 2022 02:21:01 PM ET
Attachments: smime.p7m

FWIW, I concur with Michael M. His points and refutations appears quite clear and correct to me.

--

V/R,

Uri

> **From:** 'Michael Markowitz' via pqc-forum
> **Reply-To:** Michael Markowitz
> **Date:** Friday, October 28, 2022 at 14:14
> **To:** Mike Ounsworth , "pqc-forum@list.nist.gov"
> **Subject:** [pqc-forum] RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates
>
> Hi, Mike.
>
> >I think this will be my last email on this thread because yeah, we're well into a holy war.
>
> So we do agree on something!
>
> >I will say that you're being very high on criticism, and very low on any concrete details or examples.
>
> To summarize, my "details," now relisted in what might be regarded as declining order of importance (but still rather poorly described), are:
>
> ·ephemerality of required hacks to certificate creation/parsing, path discovery/ chain validation

- complexity of required modifications to revocation mechanisms (are there any that make sense? See below.)
- baroque complications to security policy handling, and likely protocol interoperability standards
- waste of communications bandwidth
- increased attack surfaces
- development/maintenance or ISARA code licensing costs

(I've removed lack of IETF support, *not* because I agree that it involves a circular argument, but because I just heard the subject is once again under debate in lamps; more on that below.)

>Again, I'm not trying to convince you to use any specific form of PQ migration mechanism. I'm just to argue that there are use cases for them.

And I'm trying to refute the efficacy of catalyst-based use case solutions. Our positions are pretty clear.

>Ok, let me expand. A server serves a Catalyst cert. If the client (and for that matter maybe even the protocol carrying it) is completely legacy and does not understand PQ or Catalyst, then it will treat it as a legacy cert and everything works. If the client does, then the PQC will be used.

You'll have to explain how legacy certs accomplish the same because I don't get it.

>It seems like, in order to support parallel PKIs, you'll need protocols to have some kind of "I support parallel PKIs" upgrade flag. Some protocols may already have mechanisms flexible enough to accomplish this as they are (CMS SignedData comes to mind), but many do not. Needing to change dozens or hundreds of protocols to support parallel PKI and their upgrade flags sounds to me like *way* more work and risk than doing it at the X.509 or signature algorithm layer.

Speaking generically, since you haven't suggested a particular protocol to analyze, one might counter by saying that servers generally serve certificates in response to stimuli (requests) and the context of the request is generally sufficient for the responder to decide whether the requestor is asking for an RSA, ECC, or QS key. To turn this around… try hitting a website with your RSA cert selected in Firefox as the default for *client auth*,

then hit it again with your ECDSA cert selected… does the server care? Do I need a catalyst hybrid cert carrying both the RSA and ECDSA keys for this transparency?

>Disagree. Consider for example PIV smartcards. I am not a deep expert here, but I have been told that supporting a composite signature algorithm would be a relatively trivial firmware change. Supporting a Catalyst certificate (esp. if it creates one composite signature) is also a fairly trivial change. But supporting two certificates and producing two independent signatures is basically a re-build of the whole firmware and communication architecture.

I really was under the impression that PIV cards *already* carry two certificates… one for signing and one for encryption. No? And if they have two – handily injected by the issuing software upon initialization – they can certainly have four… four single SPK certs being not much larger, but certainly more flexible, than two catalyst certs.

> development/maintenance [costs]

I find it amusing that you think one change to X.509 is more work than changes to dozens or hundreds of protocols to both handle multiple certificates and to handle the upgrade / backwards compatibility case.

“one change to X.509?” You don’t think any modification to RFC 5280 will be required (for example)? Thought experiment: you’ve deployed your catalyst certs; you learn the apocalypse will arrive tomorrow, so you’ve got to deprecate, if you haven’t already, all RSA signature keys; whoops, that means you have to either revoke ***all*** certs and start over, or you must have carefully modified RFC 5280 to be able to kill off just the RSA extensions. This is just a sample of the ripple effect the use of “previously non-standard” catalyst certs will have on your standards infrastructure. Can’t imagine why this is simply glossed over in ISARA propaganda (cited below).

>Also, the farther you get from core crypto code, the less expert you should assume your developers. Take a UI developer who’s been asked to encrypt credit card numbers in POST bodies; we should not assume that they are gonna know how to correctly combine two public keys into one operation.So I’m arguing that a CA saying *“I issued you two certificates, now go and do something clever with them”* should not be the default solution for the internet because I believe it is actively dangerous. Go take a look at the [x.509] tag on stackoverflow: and tell me that this is fine; that we can make this more complicated on end users and nothing is going to go wrong.

You might have a point, or… we could simply follow NSA recommendations: forego the hybrid crypto operations and only employ “pure” key derivation and signature schemes. (Flag this as a feeble attempt at humor as I wearily try to finish off this thread.)

>Doesn’t dedicating the patents to the public mean no more licensing costs? Isn’t that what this thread is about?

I’m no longer that naïve. Four patents have been abandoned; there are dozens more. Besides, you just said you wanted to simply drop in a library that performs cert creation/parsing. Absent any indication that ISARA is giving away their library, I have to ask from whence you expect that to come. Yes, you can try implementing it yourself, but can you do it in such a way as to avoid all the patents you haven’t yet read. (The situation is vaguely reminiscent of Certicom’s attempts to inject point compression into various ECC standards. Hmmm. Anyone remember MQV? ISC received an NSA sublicense for that. Didn’t do us much good, did it? If you don’t remember MQV, let me just say that Certicom featured prominently in the nearly 4 decade long Mobius/RIM/Certicom/Blackberry/ISARA progression. If you try to follow the money there, you’ll end up thoroughly disgusted.)

> ephemerality of required hacks to certificate parsing semantics, modifications to security policy handling

>I’m not sure why this is a CON: X.509 is meant to be extended and we extend it to cover weird corner cases all the time.

You’re arguing that hybridization is somehow less ephemeral if you do it in the TLS / javascript / database / whatever-else-uses-crypto code?

You miss my point… let’s return to our thought experiment and go just beyond the apocalypse. Are you going to carry forward dead RSA keys in every cert – assuming RFC 5280 bis somehow allows that -- or simply drop that extension and revert to simple QS certs? Of course, you’re going to drop the extension. Now everything reverts to the previous X.509 status quo; I don’t see an alternative. For me, this is one of the more compelling arguments against undertaking the expensive, ephemeral code and policy mods I’ve tried to describe.

> changes to protocol interoperability standards

>I think you have this in the wrong column: this is a PRO for Composite and Catalyst, and a CON for parallel PKIs.

Just stumbled across: https://www.isara.com/openssl/2.1/ISARA-Catalyst-Connector-MPKAC-Tutorial.html

Is there a reasonable treatment of certificate revocation there? All I see, admittedly at first glance, is a reference to the current RFC 5280. So is it all-or-nothing?

> lack of IETF support.

>This is a circular argument of *"you should stop working on this because it hasn't been worked on yet".* No IETF WGs have yet adopted drafts for any kind of PQ/Traditional authentication (signature) scheme.

In my first message I cited TWO attempts (drafts) to introduce catalyst or catalyst-like hybrid certs and pointed out that both rather quickly failed to advance due to lack of WG support. But now that lamps might be going for a third round, I guess we're tied on this issue for the time being.

You still haven't answered by core question: other than the handwavy *"why standardize 2 solutions when 1 will do?"*, why are you so violently against other people taking a different hybridization approach than you?Personally, I don't really care if you're planning to use Catalyst or not, nobody's asking you to. Why do you care so much whether me and my customers do?

I have addressed this point… also twice. The basic issue is interoperability. If you deploy hybrid catalyst certs and I stand up two independent PKI silos, our users really can't interoperate, can they? Are we just moving into separate bubbles?

Michael J. Markowitz, Ph.D.

VP R&D

1011 Lake St., Suite 425, Oak Park, IL 60301

Phone: 708-445-1704

Web: www.infoseccorp.com

Email: markowitz@infoseccorp.com

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/DS7PR12MB5983CE86F64991FA83E8F779AA329%40DS7PR12MB5983.namprd12.prod.outlook.com.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/3E7AFF0F-58C1-4B9A-8AAB-8C01D517D8B3%40ll.mit.edu.