From: Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
To: Mike Ounsworth <mike.ounsworth@entrust.com>, Michael Markowitz <markowitz@infoseccorp.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: Thursday, October 27, 2022 04:54:55 PM ET
Attachments: smime.p7m

> how we (more or less) successfully transitioned from RSA to ECC.

> As far as I can tell, RSA signature are still the majority of public TLS certs on the internet. RSA key transport is still (within rounding) 100% of S/MIME encryption certificates.
>
> NSA's Suite B 2015 dropped ECC as mandatory to implement due to lack of adoption.

I think (though perhaps I should've let NSA speak for itself) that the main reason ECC was dropped as mandatory in 2015 was that they did not want to force a "big transition" twice – and they were already planning for the Post-Quantum change. I'm pretty sure that if not for the PQC effort, ECC would still be in CNSA.

> So sure, TLS key exchange and Signal protocol went to ECC, but are we forgetting about all the rest of the stuff that makes up "the internet" that still uses RSA? With the PQ migration we can't afford to simply ignore the difficult cases. I can't see how having additional migration tools available is a bad thing. (nobody is forcing you personally to use them).

The one concern I'd have with the above is, in one word – interoperability. The more tools you have, the less likely they are to interoperate, IMHO.

> **From:** 'Michael Markowitz' via pqc-forum
> **Sent:** October 27, 2022 12:17 PM
> **To:** Philip Lafrance ; pqc-forum@list.nist.gov
> **Subject:** [EXTERNAL] [pqc-forum] RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates
>
> WARNING: This email originated outside of Entrust.
> DO NOT CLICK links or attachments unless you trust the sender and know the content is safe.
>
> Philip Lafrance wrote (entire message quoted at end):

> *ISARA has dedicated four patents relating to crypto-agile hybrid certificates to the public. It is ISARA's belief that crypto-agile approaches will be crucial for migrating industries and ecosystems to quantum-safe cryptography, and that dedicating these patents to the public will make it easier for organizations to begin their migrations now. ISARA has made this strategic decision to positively impact the overall quantum-safe industry and accelerate migration planning efforts.*

I suppose this action is to be commended. Unfortunately, I'm convinced that the "technology" described in these patents could have a severe *negative* impact on the industry, and would *severely impede* the worldwide quantum safe migration effort. I urge everyone considering the adoption of this nonsense to take a step back, disregard the hype, and remember how we (more or less) successfully transitioned from RSA to ECC. Did that require hybrid certificates? Thank your lucky stars (or favorite deity) that it did not.

Rather than repeat the argument against these patents that I've presented elsewhere (more than once), let me simply recall some history.

Hybrid certificates of the type proposed by ISARA (their "Catalyst Methodology") were introduced -- probably not for the first time -- by Lin, Harn, and Laih in [1]. This draft died, for very good reasons, on its *first* Sept. 2001 iteration, almost 15 years before the application for US9660978 [2] (which does not cite it as prior art). [Homework assignment: compute the impact of this proposal on current and future relying applications; compare with the independent PKI approach we successfully applied in the RSA -> ECC transition.]

The latest attempt to foist this detrimental technology on the IETF failed miserably after just two iterations ([3]).

Why did it succeed within ISO X.509-02 ([4])? Could it be that the chair of the responsible ETSI technical WG feeding advice ([5]) into ITU-T/SG17 and ISO/IEC JTC1/SC27/WG2 is an ISARA shill? Just follow the money!

Is it not suspicious that no mention is made of US Patent #10841295, filed 10/31/2018 and issued 9/24/2019, nor of the dozens (hundreds?) of other possibly relevant patents held by ISARA and its cronies? In a round 2 comment on classic McEliece posted to this forum on June 2, 2019 [6], Dan Bernstein <djb@cr.yp.to> wrote:

> "*I recommend that researchers avoid collaborating with ISARA, and avoid allowing ISARA people to review paper submissions.*"

I don't know whether Dan's view on this subject has changed over the past 3+ years, but he certainly had a strong argument for this statement at the time. I personally have seen no reason not to wholeheartedly agree with his sentiments now.

Sincerely hoping that people – Jim Goodman, I'm thinking of you! -- are not taken in by trolls with bad patents and that this virus is nipped in the bud,

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

[1] "Multiple-Public-Key (MPK) Certificate Format," https://datatracker.ietf.org/doc/draft-lin-mpk-app/

[2] "Using a digital certificate with multiple cryptosystems," https://patents.google.com/patent/US9660978B1/en

[3] "Multiple Public-Key Algorithm X.509 Certificates," draft-truskovsky-lamps-pq-hybrid-x509-01

[4] Recommendation ITU-T X.509 | ISO/IEC 9594-8 , 10/2019

[5] ETSI GR QSC 001 V1.1.1 (2016-07)

[6] Classic-McEliece-round2-official-comment," https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjdo7jY1YD7AhVtAjQIHREABuIQFnoECBkQAQ&url=https%3A%2F%2Fcsrc.nist.gov%2FCSRC%2Fmedia%2FProjects%2Fpost-quantum-cryptography%2Fdocuments%2Fround-2%2Fofficial-comments%2FClassic-McEliece-round2-official-comment.pdf&usg=AOvVaw3RvS_lq907FRf1sTh42V3x

From:pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** Philip Lafrance
Sent: Thursday, October 27, 2022 9:13 AM
To:pqc-forum@list.nist.gov
Subject: [pqc-forum] ISARA Dedicates Four Hybrid Certificate Patents to the Public

Greetings all,

This e-mail is to bring to your attention a recent announcement by ISARA.

ISARA has dedicated four patents relating to crypto-agile hybrid certificates to the public. It is ISARA's belief that crypto-agile approaches will be crucial for migrating industries and ecosystems to quantum-safe cryptography, and that dedicating these patents to the public will make it easier for organizations to begin their migrations now. ISARA has made this strategic decision to positively impact the overall quantum-safe industry and accelerate migration planning efforts.

Crypto-Agile Patents Dedicated to the Public:

- US9660978

- US9794249

- WO2018027300

- JP6644894

For further details, please see the full press release: https://www.isara.com/company/newsroom/isara-dedicates-four-hybrid-certificate-patents-to-the-public.html

Best regards,

Philip Lafrance

--

Philip Lafrance, CISSP | Standards Manager
Mobile: +1.226.750.2439

www.isara.com · 560 Westmount Road North, Waterloo, Ontario N2L 0A9 CANADA

--
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/DS7PR12MB5983FCB499A6BA7A738D92BEAA339%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/CH0PR11MB5739C3D30FA47A910AA89F549F339%40CH0PR11MB5739.namprd11.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/8C87857D-CCDD-40A6-9F67-1805AC05E39C%40ll.mit.edu.