From: Philip Lafrance <philip.lafrance@isara.com> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: [pqc-forum] ISARA Dedicates Four Hybrid Certificate Patents to the Public
Date: Thursday, October 27, 2022 10:13:00 AM ET
Attachments: image001.jpg

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

From: Jim Goodman <jimg@crypto4a.com> via pqc-forum@list.nist.gov
To: Philip Lafrance <philip.lafrance@isara.com>, pqc-forum@list.nist.gov
Subject: RE: [pqc-forum] ISARA Dedicates Four Hybrid Certificate Patents to the Public
Date: Thursday, October 27, 2022 11:45:15 AM ET
Attachments: image001.jpg

Hi Philip,

Thanks for the note! This is great news as it gives us another tool to help with the unwieldy task of sorting out the migration path from classical to quantum-safe cryptographic systems.

We've found the ideas covered by these patents to be very useful in our migration efforts, so it's nice to hear that they can now be used by the community at large in a free and fair manner. Hopefully it will lead to hybrid certificate schemes being considered for various quantum-safe applications and uses cases.

Take care.

Jim

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** Philip Lafrance
Sent: October 27, 2022 10:13 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/D796A020-471C-4A64-AE17-6ACBED84686C%40isaracorp.com.

From: Michael Markowitz <markowitz@infoseccorp.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Philip Lafrance <philip.lafrance@isara.com>, pqc-forum@list.nist.gov
Subject: [pqc-forum] RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates
Date: Thursday, October 27, 2022 01:17:44 PM ET
Attachments: image002.png
image003.jpg

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

From: Jim Goodman <jimg@crypto4a.com> via pqc-forum@list.nist.gov
To: Michael Markowitz <markowitz@infoseccorp.com>, Philip Lafrance <philip.lafrance@isara.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 01:30:55 PM ET
Attachments: image001.png
image003.jpg

Hi Michael,

Your concerns are duly noted, and thanks for your concern but I'm still (mostly) in control of my own faculties (or so my wife tells me… ;->). All opinions are welcome, and the one of the many benefits of this forum is that everyone can express those opinions in an open fashion and make their own determinations as to what they wish to do based on those disclosures.

Take care.

Jim

From: 'Michael Markowitz' via pqc-forum <pqc-forum@list.nist.gov>
Sent: October 27, 2022 1:17 PM
To: Philip Lafrance <Philip.Lafrance@isara.com>; pqc-forum@list.nist.gov
Subject: [pqc-forum] RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates

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 *sev erely 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

Information Security CORPORATION

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.

From: Mike Ounsworth <mike.ounsworth@entrust.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Michael Markowitz <markowitz@infoseccorp.com>, Philip Lafrance <philip.lafrance@isara.com>, pqc-forum@list.nist.gov
Subject: [pqc-forum] RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates
Date: Thursday, October 27, 2022 02:01:37 PM ET
Attachments: image001.png
image002.jpg

At the risk of fanning the flame war, I'm not sure that this statement is true:

> 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.

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).

Mike Ounsworth

From: 'Michael Markowitz' via pqc-forum <pqc-forum@list.nist.gov>
Sent: October 27, 2022 12:17 PM
To: Philip Lafrance <Philip.Lafrance@isara.com>; 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.

Any email and files/attachments transmitted with it are confidential and are intended solely for the use of the individual or entity to whom they are addressed. If this message has been sent to you in error, you must not copy, distribute or disclose of the information it contains. Please notify Entrust immediately and delete the message from your system.

From: Michael Markowitz <markowitz@infoseccorp.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Mike Ounsworth <mike.ounsworth@entrust.com>, Philip Lafrance <philip.lafrance@isara.com>, pqc-forum@list.nist.gov
Subject: [pqc-forum] RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates
Date: Thursday, October 27, 2022 02:33:24 PM ET

Mike: Sorry, tt's hard to get tongue-in-cheek remarks across via email, but use of "more or less" was supposed to convey some sarcasm with respect to the success of the RSA -> ECC "transition." 😊

In any case, this is beside the point. What's important is to note that parallel, independent PKIs are the way to most efficiently accomplish the classical PKC -> QS PKC migration. The RSA -> ECC transition, whether or not you consider it successful, didn't fail because it was insufficiently "agile." And it should still be the model for how to carry off such a migration with minimal initial and residual impact on relying applications.

-mjm

From: Mike Ounsworth <Mike.Ounsworth@entrust.com>
Sent: Thursday, October 27, 2022 1:01 PM
To: Michael Markowitz <markowitz@infoseccorp.com>; Philip Lafrance <Philip.Lafrance@isara.com>; pqc-forum@list.nist.gov
Subject: RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates

At the risk of fanning the flame war, I'm not sure that this statement is true:

> 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.

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).

Mike Ounsworth

From: Mike Ounsworth <mike.ounsworth@entrust.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Michael Markowitz <markowitz@infoseccorp.com>, Philip Lafrance <philip.lafrance@isara.com>, pqc-forum@list.nist.gov
Subject: [pqc-forum] RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates
Date: Thursday, October 27, 2022 03:42:29 PM ET

Michael,

I think we're actually in (almost) full agreement. Organizations that can do a wholesale one-shot migration from RSA/ECC to PQ should absolutely just do that.

That leaves two cases:

1) Organizations that can't.

Our co-author on the composite drafts, Max Pala like to use the example of the cable modem industry (you know, putting a modem in the mail to sit in someone's living room behind the TV for 10 – 30 years). The stuff already in the field wasn't designed to be able to over-the-air-update the crypto. Lessons learned perhaps, but we're here now and we've got to support it. Max is strongly in favour of hybrid approaches as a migration stepping stone for this environment.

2) Organizations that could, but don't want to.

Maybe it's political skepticism of the NIST process. Maybe it's wanting to give all this still-unwritten new crypto code 5 years to shake out the buffer overflows.

Remember that ECDSA was already decades old when the real push for adoption started in the early 2000's. Not so for Dilithium and Falcon.

Whatever the reason, if an organization feels more comfortable with hybrid cryptography, I don't see why we as an industry would refuse to provide it.

All that said, Entrust is very pleased that these patents are now in the public domain. We believe X.509v3 extension based hybrids fill a gap in the current hybrid solution space of composite and multi-cert hybrids; specifically they provide nice backwards compatibility for heterogeneous environments with hard-to-upgrade legacy components.

Thank you ISARA for making this tool publicly available!

Mike Ounsworth

From: Michael Markowitz <markowitz@infoseccorp.com>
Sent: October 27, 2022 1:33 PM
To: Mike Ounsworth <Mike.Ounsworth@entrust.com>; Philip Lafrance <Philip.Lafrance@isara.com>; pqc-forum@list.nist.gov
Subject: [EXTERNAL] 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.

Mike: Sorry, tt's hard to get tongue-in-cheek remarks across via email, but use of "more or less" was supposed to convey some sarcasm with respect to the success of the RSA -> ECC "transition." 😊

In any case, this is beside the point. What's important is to note that parallel, independent PKIs are the way to most efficiently accomplish the classical PKC -> QS PKC migration. The RSA -> ECC transition, whether or not you consider it successful, didn't fail because it was insufficiently "agile." And it should still be the model for how to carry off such a migration with minimal initial and residual impact on relying applications.

-mjm

From: Mike Ounsworth <Mike.Ounsworth@entrust.com>
Sent: Thursday, October 27, 2022 1:01 PM
To: Michael Markowitz <markowitz@infoseccorp.com>; Philip Lafrance <Philip.Lafrance@isara.com>; pqc-forum@list.nist.gov
Subject: RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates

At the risk of fanning the flame war, I'm not sure that this statement is true:

> 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.

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).

Mike Ounsworth

Any email and files/attachments transmitted with it are confidential and are intended solely for the use of the individual or entity to whom they are addressed. If this message has been sent to you in error, you must not copy, distribute or disclose of the information it contains. Please notify Entrust immediately and delete the message from your system.

From: Scott Fluhrer (sfluhrer) <sfluhrer@cisco.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Mike Ounsworth <mike.ounsworth@entrust.com>, Michael Markowitz <markowitz@infoseccorp.com>, Philip Lafrance <philip.lafrance@isara.com>, pqc-forum@list.nist.gov
Subject: [pqc-forum] RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates
Date: Thursday, October 27, 2022 04:11:21 PM ET

From: 'Mike Ounsworth' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Thursday, October 27, 2022 3:42 PM
To: Michael Markowitz <markowitz@infoseccorp.com>; Philip Lafrance <Philip.Lafrance@isara.com>; pqc-forum@list.nist.gov
Subject: [pqc-forum] RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates

Michael,

> Organizations that can do a wholesale one-shot migration from RSA/ECC to PQ should absolutely just do that.

Actually, I'm not so sure about that – Falcon and Dilithium are fairly new; while Lattice as a hard problem have been around for a long time, the study of exactly how hard is still ongoing. I don't believe that it is a ridiculous idea to include an RSA/ECC signature in there as well. That way, we know we're not making the cryptographical security worse (especially given how comparatively cheap RSA/ECC is bandwidth-wise…)

.

From: Michael Markowitz <markowitz@infoseccorp.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Mike Ounsworth <mike.ounsworth@entrust.com>, Philip Lafrance <philip.lafrance@isara.com>, pqc-forum@list.nist.gov
Subject: [pqc-forum] RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates
Date: Thursday, October 27, 2022 04:45:38 PM ET
Attachments: image001.png

Mike: Not at all sure we're on the same track, but here goes…

Please note that I never even mentioned "wholesale one-shot migration" as a possibility. I'm simply advocating for parallel, independent PKIs as opposed to the use of *Catalyst hybrid certificates*.

Let's be very clear… I am NOT saying anything about "hybrid approaches" to key derivation functions or signature operations. (Though contrary to current NSA guidance, I think the former is probably a good idea.) What I am saying is that it only makes sense to keep your classical and QS keys in separate silos. If a relying application wants an RSA key, it pulls a cert from that silo (and performs certificate path discovery/validation, CRL checking, etc., as usual); if it wants a QS key, it pulls from the other silo; if it wants both types of keys, it pulls from both silos. The upgrade to support QS is just a matter of a dropping in the right library and making a few tweaks. Simple, huh?

Pulling a bloated hybrid cert you do not need to completely consume is ALWAYS going to be absurd… both before, during and after the drop-dead phase transition. Consider the development/maintenance costs – not to mention the increased attack surface -- of the *temporary* hacks to certificate parsing semantics, security policy handling, etc. Consider also the required changes to the existing myriad protocol interoperability standards, the waste of communications bandwidth, … (I get tired of listing all the CONs and can't imagine a single PRO.) Why???

As vendor of the first (and currently leading) NIAP/CSfC-certified (algorithm-agnostic) CA (as well as many relying applications), ISC sees the migration to QS algorithms much easier to accomplish and maintain in the "independent PKI" model (though of course our CA can house all types of silos, create cross certificates, and our relying apps can perform cross-validation on "hybrid" certificate chains). Surprising as it may seem, the IETF seems to have come to the same conclusion.

I suggest you reevaluate your two use cases if you still think hybrid certs and these patents provide any benefit. Neither scenario would be better served by using *hybrid certificates of the Catalyst ilk*.

Aphorism of the day: *hybrid cryptography* does NOT require *hybrid certificates*.

Michael J. Markowitz, Ph.D.

VP R&D

Information Security CORPORATION

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

Phone: 708-445-1704

Web: www.infoseccorp.com

Email: markowitz@infoseccorp.com

From: Mike Ounsworth <Mike.Ounsworth@entrust.com>
Sent: Thursday, October 27, 2022 2:42 PM
To: Michael Markowitz <markowitz@infoseccorp.com>; Philip Lafrance <Philip.Lafrance@isara.com>; pqc-forum@list.nist.gov
Subject: RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates

Michael,

I think we're actually in (almost) full agreement. Organizations that can do a wholesale one-shot migration from RSA/ECC to PQ should absolutely just do that.

That leaves two cases:

1) Organizations that can't.

Our co-author on the composite drafts, Max Pala like to use the example of the cable modem industry (you know, putting a modem in the mail to sit in someone's living room behind the TV for 10 – 30 years). The stuff already in the field wasn't designed to be able to over-the-air-update the crypto. Lessons learned perhaps, but we're here now and we've got to support it. Max is strongly in favour of hybrid approaches as a migration stepping stone for this environment.

2) Organizations that could, but don't want to.

Maybe it's political skepticism of the NIST process. Maybe it's wanting to give all this still-unwritten new crypto code 5 years to shake out the buffer overflows.

Remember that ECDSA was already decades old when the real push for adoption started in the early 2000's. Not so for Dilithium and Falcon.

Whatever the reason, if an organization feels more comfortable with hybrid cryptography, I don't see why we as an industry would refuse to provide it.

All that said, Entrust is very pleased that these patents are now in the public domain. We believe X.509v3 extension based hybrids fill a gap in the current hybrid solution space of composite and multi-cert hybrids; specifically they provide nice backwards compatibility for heterogeneous environments with hard-to-upgrade legacy components.

Thank you ISARA for making this tool publicly available!

Mike Ounsworth

From: Mike Ounsworth <mike.ounsworth@entrust.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Michael Markowitz <markowitz@infoseccorp.com>, Philip Lafrance <philip.lafrance@isara.com>, pqc-forum@list.nist.gov
Subject: [pqc-forum] RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates
Date: Thursday, October 27, 2022 05:39:56 PM ET
Attachments: image001.png

Aphorism of the day: *hybrid cryptography* does NOT require *hybrid certificates*.

Agree. But I counter with: *hybrid cryptography* MAY in some cases be facilitated by *hybrid certificates*

> If a relying application wants an RSA key …. The upgrade to support QS is just a matter of a dropping in the right library and making a few tweaks. Simple, huh?

I'm glad that you can reach all your clients to patch them. I'm glad that you can even find developers for all your clients to make the necessary protocol-level changes to support multiple certificates in a single handshake. I'm glad that the protocols you work with are capable of choosing at runtime which crypto to use. I'm legitimately happy for you that you only have to handle the easiest version of this problem in a fairly well-behaved environment. I'm legitimately happy for you that you can meet your customers' migration needs with a parallel PKIs approach.

What I don't understand is why you are so upset about the existence of hybrid certificates (either of the OR mode variety like Catalyst, or AND mode variety like composite) that you want to block those of us who want to offer it from having a standardized interoperable way of doing it.

You asked for PROS of hybrid certificates.

Composite:

* The only change is to add new algorithm OIDs to the crypto layer. No other application changes needed. I believe that to be much simpler than making protocol or application changes to support multiple certificates.

* Example: we still struggle with getting (especially junior) developers to properly implement hostname and DN filters in applications, and to correctly configure cert chains and trust

stores. This leads to real MitM vulnerabilities in applications. This is not going to get easier if we have to juggle multiple certificates for every connection.

* In some cases that might actually be zero code changes; for example if you can just swap out your openssl dlls.

* Management simplicity: your keys can be treated as one atomic object for name binding, for revocation, for private key storage, for signature validation, for HSM operations, etc.

Catalyst Hybrid:

* Works seamlessly with legacy clients, even if the protocol layer has not been upgraded to know about PQ and hybrids. With a little jiggering of private key formats, you could even imagine the signer being unaware that they hold a hybrid certificate, and everything still working. This gives Catalyst tremendous flexibility for deploy-it-now-use-it-later scenarios without needing to deploy twice as many certificates. As well as I-have-no-way-to-know-if-my-peer-understands-PQ scenarios.

Both hybrid variants:

* Security: dual-signed certificate chains to the root require a forgery to attack both signature chains _*simultaneously*_ vs a parallel PKI where you get to attack each signature chain _*independently*_. This is necessarily a bit handwavy since it's conjecturing about yet-to-be-discovered forgery attacks, but it's clear to me that hybrid cert chains are at least as strong, if not stronger, then parallel PKIs (eg in both cases you need to correctly throw a for loop around your cert / signature validation logic).

* Management simplicity: Your local high-school sysadmin still only has one certificate to buy and load into their web server.

* The cynics would think that a public CA should prefer a parallel PKIs approach because then they get to sell twice as many certs. We don't. We're favouring packing everything into one cert for ease of deployment.

Mike Ounsworth

From: Michael Markowitz <markowitz@infoseccorp.com>
Sent: October 27, 2022 3:45 PM
To: Mike Ounsworth <Mike.Ounsworth@entrust.com>; Philip Lafrance

<Philip.Lafrance@isara.com>; pqc-forum@list.nist.gov
Subject: [EXTERNAL] 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.

Mike: Not at all sure we're on the same track, but here goes…

Please note that I never even mentioned "wholesale one-shot migration" as a possibility. I'm simply advocating for parallel, independent PKIs as opposed to the use of *Catalyst hybrid certificates*.

Let's be very clear… I am NOT saying anything about "hybrid approaches" to key derivation functions or signature operations. (Though contrary to current NSA guidance, I think the former is probably a good idea.) What I am saying is that it only makes sense to keep your classical and QS keys in separate silos. If a relying application wants an RSA key, it pulls a cert from that silo (and performs certificate path discovery/validation, CRL checking, etc., as usual); if it wants a QS key, it pulls from the other silo; if it wants both types of keys, it pulls from both silos. The upgrade to support QS is just a matter of a dropping in the right library and making a few tweaks. Simple, huh?

Pulling a bloated hybrid cert you do not need to completely consume is ALWAYS going to be absurd… both before, during and after the drop-dead phase transition. Consider the development/maintenance costs – not to mention the increased attack surface -- of the *temporary* hacks to certificate parsing semantics, security policy handling, etc. Consider also the required changes to the existing myriad protocol interoperability standards, the waste of communications bandwidth, … (I get tired of listing all the CONs and can't imagine a single PRO.) Why???

As vendor of the first (and currently leading) NIAP/CSfC-certified (algorithm-agnostic) CA (as well as many relying applications), ISC sees the migration to QS algorithms much easier to accomplish and maintain in the "independent PKI" model (though of course our CA can house all types of silos, create cross certificates, and our relying apps can perform cross-validation on "hybrid" certificate chains). Surprising as it may seem, the IETF seems to have come to the same conclusion.

I suggest you reevaluate your two use cases if you still think hybrid certs and these patents provide any benefit. Neither scenario would be better served by using *hybrid certificates of the Catalyst ilk*.

Aphorism of the day: *hybrid cryptography* does NOT require *hybrid certificates*.

Michael J. Markowitz, Ph.D.

VP R&D

Information Security CORPORATION

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

Phone: 708-445-1704

Web: www.infoseccorp.com

Email: markowitz@infoseccorp.com

From: Mike Ounsworth <Mike.Ounsworth@entrust.com>
Sent: Thursday, October 27, 2022 2:42 PM
To: Michael Markowitz <markowitz@infoseccorp.com>; Philip Lafrance <Philip.Lafrance@isara.com>; pqc-forum@list.nist.gov
Subject: RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates

Michael,

I think we're actually in (almost) full agreement. Organizations that can do a wholesale one-shot migration from RSA/ECC to PQ should absolutely just do that.

That leaves two cases:

1) Organizations that can't.

Our co-author on the composite drafts, Max Pala like to use the example of the cable modem industry (you know, putting a modem in the mail to sit in someone's living room behind the TV for 10 – 30 years). The stuff already in the field wasn't designed to be able to over-the-air-update the crypto. Lessons learned perhaps, but we're here now and we've got to support it. Max is strongly in favour of hybrid approaches as a migration stepping stone for this environment.

2) Organizations that could, but don't want to.

Maybe it's political skepticism of the NIST process. Maybe it's wanting to give all this still-unwritten new crypto code 5 years to shake out the buffer overflows.

Remember that ECDSA was already decades old when the real push for adoption started in the early 2000's. Not so for Dilithium and Falcon.

Whatever the reason, if an organization feels more comfortable with hybrid cryptography, I don't see why we as an industry would refuse to provide it.

All that said, Entrust is very pleased that these patents are now in the public domain. We believe X.509v3 extension based hybrids fill a gap in the current hybrid solution space of composite and multi-cert hybrids; specifically they provide nice backwards compatibility for heterogeneous environments with hard-to-upgrade legacy components.

Thank you ISARA for making this tool publicly available!

Mike Ounsworth

Any email and files/attachments transmitted with it are confidential and are intended solely for the use of the individual or entity to whom they are addressed. If this message has been sent to you in error, you must not copy, distribute or disclose of the information it contains. Please notify Entrust immediately and delete the message from your system.

From: Michael Markowitz <markowitz@infoseccorp.com> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum@list.nist.gov
Subject: [pqc-forum] RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, hybrid crypto doesn't require hybrid certificates
Date: Thursday, October 27, 2022 05:51:41 PM ET
Attachments: image001.png

Corrections to my first rant, with apologies to those affected:

- In the personal attack "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?" should have been in phrased in the past tense; I've just been informed that Mark Pecen is no longer the chair of that ETSI working group.
- Also, reference [5] cited here, ETSI GR QSC 001 V1.1.1 (2016-07), should probably have been to ETSI TR 103 619 V1.1.1 (2020-07)

  Section 6.1 of the latter document perpetuates the rather poor advice: "This ["phased migration"] may be achieved using individual classical and Quantum Safe end-entity certificates, or by using hybrid certificates depending on the cryptographic agility of the existing application." (I choked on the use of the word "agility" here.)

Regards,

Michael J. Markowitz, Ph.D.

VP R&D

Information Security CORPORATION

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

Phone: 708-445-1704

Web: www.infoseccorp.com

Email: markowitz@infoseccorp.com

From: Mike Ounsworth <mike.ounsworth@entrust.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Michael Markowitz <markowitz@infoseccorp.com>, Philip Lafrance <philip.lafrance@isara.com>, pqc-forum@list.nist.gov
Subject: [pqc-forum] RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates
Date: Thursday, October 27, 2022 06:43:44 PM ET
Attachments: image001.png

Basically, my Pro-composite (and to a lesser extent Catalyst) argument boils down to this:

I've met some of the developers at openssl, BouncyCastle, JRE crypto, Golang crypto, etc. Those folks are more than capable of correctly putting a for-loop around their crypto, especially if there's an RFC and specific OIDs for it.

I've also met some of the developers who find themselves on the pycrypto or webCryptoAPI docs (and then shortly thereafter on stackoverflow) thinking they're gonna build some awesome crypto thing. They are not, in general, capable of correctly putting a for-loop around their crypto – or even knowing that this is a thing people do. And I'm not talking about high school projects here; I'm talking about professional developers writing, I don't know, HIPAA compliant data management applications.

So I personally strongly believe that it's in the best interest of the Internet to bury the hybridization inside expert-written crypto libraries, rather than leaving it to application developers to figure out that they should go get two separate sets of public keys, and then what exactly they're supposed to do with them.

Mike Ounsworth

From: Mike Ounsworth
Sent: October 27, 2022 4:39 PM
To: Michael Markowitz <markowitz@infoseccorp.com>; Philip Lafrance <Philip.Lafrance@isara.com>; pqc-forum@list.nist.gov
Subject: RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates

Aphorism of the day: *hybrid cryptography* does NOT require *hybrid certificates*.

Agree. But I counter with: *hybrid cryptography* MAY in some cases be facilitated by *hybrid certificates*

> If a relying application wants an RSA key .... The upgrade to support QS is just a matter of a dropping in the right library and making a few tweaks. Simple, huh?

I'm glad that you can reach all your clients to patch them. I'm glad that you can even find developers for all your clients to make the necessary protocol-level changes to support multiple certificates in a single handshake. I'm glad that the protocols you work with are capable of choosing at runtime which crypto to use. I'm legitimately happy for you that you only have to handle the easiest version of this problem in a fairly well-behaved environment. I'm legitimately happy for you that you can meet your customers' migration needs with a parallel PKIs approach.

What I don't understand is why you are so upset about the existence of hybrid certificates (either of the OR mode variety like Catalyst, or AND mode variety like composite) that you want to block those of us who want to offer it from having a standardized interoperable way of doing it.

You asked for PROS of hybrid certificates.

Composite:

* The only change is to add new algorithm OIDs to the crypto layer. No other application changes needed. I believe that to be much simpler than making protocol or application changes to support multiple certificates.

* Example: we still struggle with getting (especially junior) developers to properly implement hostname and DN filters in applications, and to correctly configure cert chains and trust stores. This leads to real MitM vulnerabilities in applications. This is not going to get easier if we have to juggle multiple certificates for every connection.

* In some cases that might actually be zero code changes; for example if you can just swap out your openssl dlls.

* Management simplicity: your keys can be treated as one atomic object for name binding, for revocation, for private key storage, for signature validation, for HSM operations, etc.

Catalyst Hybrid:

* Works seamlessly with legacy clients, even if the protocol layer has not been upgraded to know about PQ and hybrids. With a little jiggering of private key formats, you could even imagine the signer being unaware that they hold a hybrid certificate, and everything still working. This gives Catalyst tremendous flexibility for deploy-it-now-use-it-later scenarios without needing to deploy twice as many certificates. As well as I-have-no-way-to-know-if-my-peer-understands-PQ scenarios.

Both hybrid variants:

* Security: dual-signed certificate chains to the root require a forgery to attack both signature chains _*simultaneously*_ vs a parallel PKI where you get to attack each signature chain _*independently*_. This is necessarily a bit handwavy since it's conjecturing about yet-to-be-discovered forgery attacks, but it's clear to me that hybrid cert chains are at least as strong, if not stronger, then parallel PKIs (eg in both cases you need to correctly throw a for loop around your cert / signature validation logic).

* Management simplicity: Your local high-school sysadmin still only has one certificate to buy and load into their web server.

* The cynics would think that a public CA should prefer a parallel PKIs approach because then they get to sell twice as many certs. We don't. We're favouring packing everything into one cert for ease of deployment.

Mike Ounsworth

From: Michael Markowitz <markowitz@infoseccorp.com>
Sent: October 27, 2022 3:45 PM
To: Mike Ounsworth <Mike.Ounsworth@entrust.com>; Philip Lafrance <Philip.Lafrance@isara.com>; pqc-forum@list.nist.gov
Subject: [EXTERNAL] 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.

Mike: Not at all sure we're on the same track, but here goes…

Please note that I never even mentioned “wholesale one-shot migration” as a possibility. I’m simply advocating for parallel, independent PKIs as opposed to the use of *Catalyst hybrid certificates*.

Let’s be very clear… I am NOT saying anything about “hybrid approaches” to key derivation functions or signature operations. (Though contrary to current NSA guidance, I think the former is probably a good idea.) What I am saying is that it only makes sense to keep your classical and QS keys in separate silos. If a relying application wants an RSA key, it pulls a cert from that silo (and performs certificate path discovery/validation, CRL checking, etc., as usual); if it wants a QS key, it pulls from the other silo; if it wants both types of keys, it pulls from both silos. The upgrade to support QS is just a matter of a dropping in the right library and making a few tweaks. Simple, huh?

Pulling a bloated hybrid cert you do not need to completely consume is ALWAYS going to be absurd… both before, during and after the drop-dead phase transition. Consider the development/maintenance costs – not to mention the increased attack surface -- of the *temporary* hacks to certificate parsing semantics, security policy handling, etc. Consider also the required changes to the existing myriad protocol interoperability standards, the waste of communications bandwidth, … (I get tired of listing all the CONs and can’t imagine a single PRO.) Why???

As vendor of the first (and currently leading) NIAP/CSfC-certified (algorithm-agnostic) CA (as well as many relying applications), ISC sees the migration to QS algorithms much easier to accomplish and maintain in the “independent PKI” model (though of course our CA can house all types of silos, create cross certificates, and our relying apps can perform cross-validation on “hybrid” certificate chains). Surprising as it may seem, the IETF seems to have come to the same conclusion.

I suggest you reevaluate your two use cases if you still think hybrid certs and these patents provide any benefit. Neither scenario would be better served by using *hybrid certificates of the Catalyst ilk*.

Aphorism of the day: *hybrid cryptography* does NOT require *hybrid certificates*.

Michael J. Markowitz, Ph.D.

VP R&D

Information Security CORPORATION

Mike Ounsworth <mike.ounsworth@entrust.com>

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

Phone: 708-445-1704

Web: www.infoseccorp.com

Email: markowitz@infoseccorp.com

From: Mike Ounsworth <Mike.Ounsworth@entrust.com>
Sent: Thursday, October 27, 2022 2:42 PM
To: Michael Markowitz <markowitz@infoseccorp.com>; Philip Lafrance <Philip.Lafrance@isara.com>; pqc-forum@list.nist.gov
Subject: RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates

Michael,

I think we're actually in (almost) full agreement. Organizations that can do a wholesale one-shot migration from RSA/ECC to PQ should absolutely just do that.

That leaves two cases:

1) Organizations that can't.

Our co-author on the composite drafts, Max Pala like to use the example of the cable modem industry (you know, putting a modem in the mail to sit in someone's living room behind the TV for 10 – 30 years). The stuff already in the field wasn't designed to be able to over-the-air-update the crypto. Lessons learned perhaps, but we're here now and we've got to support it. Max is strongly in favour of hybrid approaches as a migration stepping stone for this environment.

2) Organizations that could, but don't want to.

Maybe it's political skepticism of the NIST process. Maybe it's wanting to give all this still-unwritten new crypto code 5 years to shake out the buffer overflows.

Remember that ECDSA was already decades old when the real push for adoption started in the early 2000's. Not so for Dilithium and Falcon.

Whatever the reason, if an organization feels more comfortable with hybrid cryptography, I don't see why we as an industry would refuse to provide it.

All that said, Entrust is very pleased that these patents are now in the public domain. We believe X.509v3 extension based hybrids fill a gap in the current hybrid solution space of composite and multi-cert hybrids; specifically they provide nice backwards compatibility for heterogeneous environments with hard-to-upgrade legacy components.

Thank you ISARA for making this tool publicly available!

Mike Ounsworth

Any email and files/attachments transmitted with it are confidential and are intended solely for the use of the individual or entity to whom they are addressed. If this message has been sent to you in error, you must not copy, distribute or disclose of the information it contains. Please notify Entrust immediately and delete the message from your system.

From: Rafael Misoczki <rafa.misoczki@gmail.com> via pqc-forum@list.nist.gov
To: Mike Ounsworth <mike.ounsworth@entrust.com>
CC: Michael Markowitz <markowitz@infoseccorp.com>, Philip Lafrance <philip.lafrance@isara.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 06:54:16 PM ET
Attachments: image001.png

Adding to Mike's comments:
1) Composable security isn't a simple topic (for example, see [Bindel et al 2017] on the non-separability property of different hybridization approaches).

2) History has shown that any room left for ambiguity ("the higher-layer protocol will take care of this" or "the user will know which certificate chain to use") may lead to real-world security problems down the road.
[Bindel et al 2017]: https://eprint.iacr.org/2017/460

-Rafael

On Thu, Oct 27, 2022 at 6:43 PM 'Mike Ounsworth' via pqc-forum <pqc-forum@list.nist.gov> wrote:

> Basically, my Pro-composite (and to a lesser extent Catalyst) argument boils down to this:
>
> I've met some of the developers at openssl, BouncyCastle, JRE crypto, Golang crypto, etc. Those folks are more than capable of correctly putting a for-loop around their crypto, especially if there's an RFC and specific OIDs for it.
>
> I've also met some of the developers who find themselves on the pycrypto or webCryptoAPI docs (and then shortly thereafter on stackoverflow) thinking they're gonna build some awesome crypto thing. They are not, in general, capable of correctly putting a for-loop around their crypto – or even knowing that this is a thing people do. And I'm not talking about high school projects here; I'm talking about professional developers writing, I don't know, HIPAA compliant data management applications.
>
> So I personally strongly believe that it's in the best interest of the Internet to bury the hybridization inside expert-written crypto libraries, rather than leaving it to application developers to figure out that they should go get two separate sets of public keys, and then what exactly they're supposed to do with them.

Mike Ounsworth

From: Mike Ounsworth
Sent: October 27, 2022 4:39 PM
To: Michael Markowitz <markowitz@infoseccorp.com>; Philip Lafrance <Philip.Lafrance@isara.com>; pqc-forum@list.nist.gov
Subject: RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates

Aphorism of the day: *hybrid cryptography* does NOT require *hybrid certificates*.

Agree. But I counter with: *hybrid cryptography* MAY in some cases be facilitated by *hybrid certificates*

> If a relying application wants an RSA key …. The upgrade to support QS is just a matter of a dropping in the right library and making a few tweaks. Simple, huh?

I'm glad that you can reach all your clients to patch them. I'm glad that you can even find developers for all your clients to make the necessary protocol-level changes to support multiple certificates in a single handshake. I'm glad that the protocols you work with are capable of choosing at runtime which crypto to use. I'm legitimately happy for you that you only have to handle the easiest version of this problem in a fairly well-behaved environment. I'm legitimately happy for you that you can meet your customers' migration needs with a parallel PKIs approach.

What I don't understand is why you are so upset about the existence of hybrid certificates (either of the OR mode variety like Catalyst, or AND mode variety like composite) that you want to block those of us who want to offer it from having a standardized interoperable way of doing it.

You asked for PROS of hybrid certificates.

Composite:

* The only change is to add new algorithm OIDs to the crypto layer. No other application changes needed. I believe that to be much simpler than making protocol or application changes to support multiple certificates.

* Example: we still struggle with getting (especially junior) developers to properly implement hostname and DN filters in applications, and to correctly configure cert chains and trust stores. This leads to real MitM vulnerabilities in applications. This is not going to get easier if we have to juggle multiple certificates for every connection.

* In some cases that might actually be zero code changes; for example if you can just swap out your openssl dlls.

* Management simplicity: your keys can be treated as one atomic object for name binding, for revocation, for private key storage, for signature validation, for HSM operations, etc.

Catalyst Hybrid:

* Works seamlessly with legacy clients, even if the protocol layer has not been upgraded to know about PQ and hybrids. With a little jiggering of private key formats, you could even imagine the signer being unaware that they hold a hybrid certificate, and everything still working. This gives Catalyst tremendous flexibility for deploy-it-now-use-it-later scenarios without needing to deploy twice as many certificates. As well as I-have-no-way-to-know-if-my-peer-understands-PQ scenarios.

Both hybrid variants:

* Security: dual-signed certificate chains to the root require a forgery to attack both signature chains _*simultaneously*_ vs a parallel PKI where you get to attack each signature chain _*independently*_. This is necessarily a bit handwavy since it's conjecturing about yet-to-be-discovered forgery attacks, but it's clear to me that hybrid cert chains are at least as strong, if not stronger, then parallel PKIs (eg in both cases you need to correctly throw a for loop around your cert / signature validation logic).

* Management simplicity: Your local high-school sysadmin still only has one certificate to buy and load into their web server.

* The cynics would think that a public CA should prefer a parallel PKIs approach because then they get to sell twice as many certs. We don't. We're favouring packing everything into one cert for ease of deployment.

Mike Ounsworth

From: Michael Markowitz <markowitz@infoseccorp.com>
Sent: October 27, 2022 3:45 PM
To: Mike Ounsworth <Mike.Ounsworth@entrust.com>; Philip Lafrance <Philip.Lafrance@isara.com>; pqc-forum@list.nist.gov
Subject: [EXTERNAL] 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.

Mike: Not at all sure we're on the same track, but here goes…

Please note that I never even mentioned "wholesale one-shot migration" as a possibility. I'm simply advocating for parallel, independent PKIs as opposed to the use of *Catalyst hybrid certificates*.

Let's be very clear… I am NOT saying anything about "hybrid approaches" to key derivation functions or signature operations. (Though contrary to current NSA guidance, I think the former is probably a good idea.) What I am saying is that it only makes sense to keep your classical and QS keys in separate silos. If a relying application wants an RSA key, it pulls a cert from that silo (and performs certificate path discovery/validation, CRL checking, etc., as usual); if it wants a QS key, it pulls from the other silo; if it wants both types of keys, it pulls from both silos. The upgrade to support QS is just a matter of a dropping in the right library and making a few tweaks. Simple, huh?

Pulling a bloated hybrid cert you do not need to completely consume is ALWAYS going to be absurd… both before, during and after the drop-dead phase transition. Consider the development/maintenance costs – not to mention the increased attack surface -- of the *temporary* hacks to certificate parsing semantics, security policy handling, etc. Consider also the required changes to the existing myriad protocol interoperability standards, the waste of communications bandwidth, … (I get tired of listing all the CONs and can't imagine a single PRO.) Why???

As vendor of the first (and currently leading) NIAP/CSfC-certified (algorithm-agnostic) CA (as well as many relying applications), ISC sees the migration to QS algorithms much easier to accomplish and maintain in the "independent PKI" model (though of course our CA can house all types of silos, create cross certificates, and our relying apps can perform cross-

validation on “hybrid” certificate chains). Surprising as it may seem, the IETF seems to have come to the same conclusion.

I suggest you reevaluate your two use cases if you still think hybrid certs and these patents provide any benefit. Neither scenario would be better served by using *hybrid certificates of the Catalyst ilk*.

Aphorism of the day: *hybrid cryptography* does NOT require *hybrid certificates*.

Michael J. Markowitz, Ph.D.

VP R&D

Information Security CORPORATION

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

Phone: 708-445-1704

Web: www.infoseccorp.com

Email: markowitz@infoseccorp.com

From: Mike Ounsworth <Mike.Ounsworth@entrust.com>
Sent: Thursday, October 27, 2022 2:42 PM
To: Michael Markowitz <markowitz@infoseccorp.com>; Philip Lafrance <Philip.Lafrance@isara.com>; pqc-forum@list.nist.gov
Subject: RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates

Michael,

I think we’re actually in (almost) full agreement. Organizations that can do a wholesale one-shot migration from RSA/ECC to PQ should absolutely just do that.

That leaves two cases:

1) Organizations that can’t.

Our co-author on the composite drafts, Max Pala like to use the example of the cable modem industry (you know, putting a modem in the mail to sit in someone’s living room behind the TV for 10 – 30 years). The stuff already in the field wasn’t designed to be able to

over-the-air-update the crypto. Lessons learned perhaps, but we're here now and we've got to support it. Max is strongly in favour of hybrid approaches as a migration stepping stone for this environment.

2) Organizations that could, but don't want to.

Maybe it's political skepticism of the NIST process. Maybe it's wanting to give all this still-unwritten new crypto code 5 years to shake out the buffer overflows.

Remember that ECDSA was already decades old when the real push for adoption started in the early 2000's. Not so for Dilithium and Falcon.

Whatever the reason, if an organization feels more comfortable with hybrid cryptography, I don't see why we as an industry would refuse to provide it.

All that said, Entrust is very pleased that these patents are now in the public domain. We believe X.509v3 extension based hybrids fill a gap in the current hybrid solution space of composite and multi-cert hybrids; specifically they provide nice backwards compatibility for heterogeneous environments with hard-to-upgrade legacy components.

Thank you ISARA for making this tool publicly available!

Mike Ounsworth

Any email and files/attachments transmitted with it are confidential and are intended solely for the use of the individual or entity to whom they are addressed. If this message has been sent to you in error, you must not copy, distribute or disclose of the information it contains. Please notify Entrust immediately and delete the message from your system.
--
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/CH0PR11MB5739B8CC61562FD39D51E98B9F339%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/CAA68G3eLvWBBHsjQjGOAXJcxwT0SEtO2BUHxLbSj2Ufhwt31gA%40mail.gmail.com.

From: Michael Markowitz <markowitz@infoseccorp.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Mike Ounsworth <mike.ounsworth@entrust.com>, Philip Lafrance <philip.lafrance@isara.com>, pqc-forum@list.nist.gov
Subject: [pqc-forum] RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates
Date: Thursday, October 27, 2022 07:11:54 PM ET
Attachments: image001.png

Mike:

> I counter with: *hybrid cryptography* MAY in some cases be facilitated by *hybrid certificates*

Sorry, don't see it… and I've spent some time looking.

>I'm glad that you can reach all your clients to patch them. I'm glad that you can even find developers for all your clients to make the necessary protocol-level changes to support multiple certificates in a single handshake. I'm glad that the protocols you work with are capable of choosing at runtime which crypto to use. I'm legitimately happy for you that you only have to handle the easiest version of this problem in a fairly well-behaved environment. I'm legitimately happy for you that you can meet your customers' migration needs with a parallel PKIs approach.

If these are your constraints, some of your PROs below will have to be reevaluated.

>What I don't understand is why you are so upset about the existence of hybrid certificates (either of the OR mode variety like Catalyst, or AND mode variety like composite) that you want to block those of us who want to offer it from having a standardized interoperable way of doing it.

As I said in my first post, I see Catalyst certs as presenting a severe impediment to the efficient and orderly migration to a QS world.

>You asked for PROS of hybrid certificates.

No, I don't think I did. I said ***I*** couldn't find any. And even if I had asked for some, I'd be regretting it now. This is turning into a holy war and I just wanted to speak up and recommend a careful analysis of the proffered patents… and a weighing of the obvious risks of their adoption.

>Composite:

* The only change is to add new algorithm OIDs to the crypto layer. No other application changes needed. I believe that to be much simpler than making protocol or application changes to support multiple certificates.

* Example: we still struggle with getting (especially junior) developers to properly implement hostname and DN filters in applications, and to correctly configure cert chains and trust stores. This leads to real MitM vulnerabilities in applications. This is not going to get easier if we have to juggle multiple certificates for every connection.

* Management simplicity: your keys can be treated as one atomic object for name binding, for revocation, for private key storage, for signature validation, for HSM operations, etc.

Do these “benefits” apply to clients you can’t reach to patch? I personally haven’t seen an LDAP repository that can’t hold two certificates per user. But can we restrict the war to the patents in question?

* In some cases that might actually be zero code changes; for example if you can just swap out your openssl dlls.

Ah, if life were only that simple. 😊

>Catalyst Hybrid:

* Works seamlessly with legacy clients, even if the protocol layer has not been upgraded to know about PQ and hybrids.

Amazing… but so do legacy certs.

With a little jiggering of private key formats, you could even imagine the signer being unaware that they hold a hybrid certificate, and everything still working.

You mean your client and their network provider are not going to notice the bloat of an *unnecessary* QS public key in every cert?

This gives Catalyst tremendous flexibility for deploy-it-now-use-it-later scenarios without needing to deploy twice as many certificates. As well as I-have-no-way-to-know-if-my-peer-understands-PQ scenarios.

One might argue – if they had the strength – that the legacy certs are already deployed, so deploying an additional pure QS cert costs the same as deploying a Catalyst cert (well, actually less, if you consider bits on the wire). Still looking for a valid CON, are we?

>Both hybrid variants:

* Security: dual-signed certificate chains to the root require a forgery to attack both signature chains _*simultaneously*_ vs a parallel PKI where you get to attack each signature chain _*independently*_. This is necessarily a bit handwavy since it's conjecturing about yet-to-be-discovered forgery attacks, but it's clear to me that hybrid cert chains are at least as strong, if not stronger, then parallel PKIs (eg in both cases you need to correctly throw a for loop around your cert / signature validation logic).

Won't pretend to grok this, but will answer with some questions: how do you revoke the RSA component of a Catalyst cert while keeping the QS component active? You have an IETF spec for that? Your CA security policies/relying apps provide/understand the semantics for that? Or does the QS key go down the drain with the RSA key. Keep in mind what will happen when the apocalypse is upon us. Consider also how you migrate AWAY from the RSA baggage once those keys are completely deprecated. Oh, we just go back to X.509 business as usual? Come on!

>* Management simplicity: Your local high-school sysadmin still only has one certificate to buy and load into their web server.

If he can manage to load one, he can surely load two... though if I were a HS sysadm, or even a university sysadm (which I once was!), I'd simply bet the farm on pure QS certs once browsers support them ubiquitously and be done with it.

* The cynics would think that a public CA should prefer a parallel PKIs approach because then they get to sell twice as many certs. We don't. We're favouring packing everything into one cert for ease of deployment.

Pricing is always negotiable, but ours is typically "per SDN" which should quiet your cynics.

If I was keeping score, I'd note that you haven't addressed the main (overwhelming) CONs: development/maintenance or ISARA code licensing costs, increased attack surfaces, ephemerality of required hacks to certificate parsing semantics, modifications to security policy handling, changes to protocol interoperability standards, waste of communications bandwidth, lack of IETF support.

Let's sleep on it. G'night.

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

From: Mike Ounsworth <mike.ounsworth@entrust.com> via pqc-forum <pqc-forum@list.nist.gov>
To: Michael Markowitz <markowitz@infoseccorp.com>, Philip Lafrance <philip.lafrance@isara.com>, pqc-forum@list.nist.gov
Subject: [pqc-forum] RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates
Date: Friday, October 28, 2022 11:34:54 AM ET
Attachments: image001.png

Hi Michael,

I think this will be my last email on this thread because yeah, we're well into a holy war. I will say that you're being very high on criticism, and very low on any concrete details or examples. 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.

I'll respond to your more fact-based questions.

>>Catalyst Hybrid:

>>* Works seamlessly with legacy clients, even if the protocol layer has not been upgraded to know about PQ and hybrids.

> Amazing… but so do legacy certs.

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.

>>This gives Catalyst tremendous flexibility for deploy-it-now-use-it-later scenarios without needing to deploy twice as many certificates. As well as I-have-no-way-to-know-if-my-peer-understands-PQ scenarios.

>One might argue – if they had the strength – that the legacy certs are already deployed, so deploying an additional pure QS cert costs the same as deploying a Catalyst cert (well, actually less, if you consider bits on the wire

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.

> If I was keeping score, I'd note that you haven't addressed the main (overwhelming) CONs:

Alright, let's go through them.

> 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.

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: https://stackoverflow.com/questions/tagged/x509 and tell me that this is fine; that we can make this more complicated on end users and nothing is going to go wrong.

> or ISARA code licensing costs

Huh?

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

> increased attack surfaces

Moot point: any hybrid mechanism will have very similar increased attack surfaces compared to non-hybrid systems.

Moreover, I would rather bury the increased attack surface inside openssl, BouncyCastle, etc, rather than hand it to the citizens of stackoverflow to figure out.

> 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?

> 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.

> waste of communications bandwidth

This is probably the only legitimate CON in your list. Yes, this is a well-documented CON of Catalyst and a legitimate reason why an organization might opt for a different hybridization scheme. But bandwidth is certainly not a deal-breaker for all use cases, and some would happily trade bandwidth for the PROS mentioned above.

> 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.

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?

Mike Ounsworth

From: Michael Markowitz <markowitz@infoseccorp.com>
Sent: October 27, 2022 6:11 PM
To: Mike Ounsworth <Mike.Ounsworth@entrust.com>; Philip Lafrance <Philip.Lafrance@isara.com>; pqc-forum@list.nist.gov
Subject: [EXTERNAL] 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.

Mike:

> I counter with: *hybrid cryptography* MAY in some cases be facilitated by *hybrid certificates*

Sorry, don't see it… and I've spent some time looking.

>I'm glad that you can reach all your clients to patch them. I'm glad that you can even find developers for all your clients to make the necessary protocol-level changes to support multiple certificates in a single handshake. I'm glad that the protocols you work with are capable of choosing at runtime which crypto to use. I'm legitimately happy for you that you only have to handle the easiest version of this problem in a fairly well-behaved environment. I'm legitimately happy for you that you can meet your customers' migration needs with a parallel PKIs approach.

If these are your constraints, some of your PROs below will have to be reevaluated.

>What I don't understand is why you are so upset about the existence of hybrid certificates (either of the OR mode variety like Catalyst, or AND mode variety like composite) that you want to block those of us who want to offer it from having a standardized interoperable way of doing it.

As I said in my first post, I see Catalyst certs as presenting a severe impediment to the efficient and orderly migration to a QS world.

>You asked for PROS of hybrid certificates.

No, I don't think I did. I said ***I*** couldn't find any. And even if I had asked for some, I'd be regretting it now. This is turning into a holy war and I just wanted to speak up and recommend a careful analysis of the proffered patents… and a weighing of the obvious risks of their adoption.

>Composite:

* The only change is to add new algorithm OIDs to the crypto layer. No other application changes needed. I believe that to be much simpler than making protocol or application changes to support multiple certificates.

* Example: we still struggle with getting (especially junior) developers to properly implement hostname and DN filters in applications, and to correctly configure cert chains and trust stores. This leads to real MitM vulnerabilities in applications. This is not going to get easier if we have to juggle multiple certificates for every connection.

* Management simplicity: your keys can be treated as one atomic object for name binding, for revocation, for private key storage, for signature validation, for HSM operations, etc.

Do these “benefits” apply to clients you can’t reach to patch? I personally haven’t seen an LDAP repository that can’t hold two certificates per user. But can we restrict the war to the patents in question?

* In some cases that might actually be zero code changes; for example if you can just swap out your openssl dlls.

Ah, if life were only that simple. 😊

>Catalyst Hybrid:

* Works seamlessly with legacy clients, even if the protocol layer has not been upgraded to know about PQ and hybrids.

Amazing… but so do legacy certs.

With a little jiggering of private key formats, you could even imagine the signer being unaware that they hold a hybrid certificate, and everything still working.

You mean your client and their network provider are not going to notice the bloat of an *unnecessary* QS public key in every cert?

This gives Catalyst tremendous flexibility for deploy-it-now-use-it-later scenarios without needing to deploy twice as many certificates. As well as I-have-no-way-to-know-if-my-peer-understands-PQ scenarios.

One might argue – if they had the strength – that the legacy certs are already deployed, so deploying an additional pure QS cert costs the same as deploying a Catalyst cert (well, actually less, if you consider bits on the wire). Still looking for a valid CON, are we?

>Both hybrid variants:

* Security: dual-signed certificate chains to the root require a forgery to attack both signature chains _*simultaneously*_ vs a parallel PKI where you get to attack each signature chain _*independently*_. This is necessarily a bit handwavy since it's conjecturing about yet-to-be-discovered forgery attacks, but it's clear to me that hybrid cert chains are at least as strong, if not stronger, then parallel PKIs (eg in both cases you need to correctly throw a for loop around your cert / signature validation logic).

Won't pretend to grok this, but will answer with some questions: how do you revoke the RSA component of a Catalyst cert while keeping the QS component active? You have an IETF spec for that? Your CA security policies/relying apps provide/understand the semantics for that? Or does the QS key go down the drain with the RSA key. Keep in mind what will happen when the apocalypse is upon us. Consider also how you migrate AWAY from the RSA baggage once those keys are completely deprecated. Oh, we just go back to X.509 business as usual? Come on!

>* Management simplicity: Your local high-school sysadmin still only has one certificate to buy and load into their web server.

If he can manage to load one, he can surely load two... though if I were a HS sysadm, or even a university sysadm (which I once was!), I'd simply bet the farm on pure QS certs once browsers support them ubiquitously and be done with it.

* The cynics would think that a public CA should prefer a parallel PKIs approach because then they get to sell twice as many certs. We don't. We're favouring packing everything into one cert for ease of deployment.

Pricing is always negotiable, but ours is typically "per SDN" which should quiet your cynics.

If I was keeping score, I'd note that you haven't addressed the main (overwhelming) CONs: development/maintenance or ISARA code licensing costs, increased attack surfaces, ephemerality of required hacks to certificate parsing semantics, modifications to security policy handling, changes to protocol interoperability standards, waste of communications bandwidth, lack of IETF support.

Let's sleep on it. G'night.

Michael J. Markowitz, Ph.D.

VP R&D

Information Security CORPORATION

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

Phone: 708-445-1704

Web: www.infoseccorp.com

Email: markowitz@infoseccorp.com

Any email and files/attachments transmitted with it are confidential and are intended solely for the use of the individual or entity to whom they are addressed. If this message has been sent to you in error, you must not copy, distribute or disclose of the information it contains. Please notify Entrust immediately and delete the message from your system.

From:	Michael Markowitz <markowitz@infoseccorp.com> via pqc-forum <pqc-forum@list.nist.gov>
To:	Mike Ounsworth <mike.ounsworth@entrust.com>, pqc-forum@list.nist.gov
Subject:	[pqc-forum] RE: ISARA Dedicates Four Hybrid Certificate Patents to the Public, crypto-agility != hybrid certificates
Date:	Friday, October 28, 2022 02:14:02 PM ET
Attachments:	image001.png

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

Information Security CORPORATION

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

Phone: 708-445-1704

Web: www.infoseccorp.com

Email: markowitz@infoseccorp.com