PracSavvy

Clinical Systems Support and Training

www.pracsavvy.com.au

April 2022 — Newsbrief

This last few weeks has seen a continuation of the certificates saga around the country, amplified by some sort of dramatic mishap at the Medicare end in the first week of March. The end result was, for many practices as big a technology disruption as I have seen in my, getting close to twenty years of work in the sector.

In my last issue I tried to convey what practices needed to do, especially around the key date of 13/3, but it's come to my attention that in great majority, practice managers know next to nothing about PKI certificates and what they are specifically used for. So I thought I might do a bit of a "PKI for dummies" article, even though for many practices they will be moving away from reliance on this information in the next 3 months or so. So, yes it's belated and almost certainly boring too, but being short of April inspiration, I'm going with it anyway.

In the beginning.

Back around the turn of the millennium when flirting was legal and you could count gender options on half a hand, computer usage in General Practice was in it's absolute infancy. The advantages of electronic communication were obvious, but at a national health level they were wrestling with issues like security and authentication, i.e. how can we be sure where that electronic message really came from.

It had been established elsewhere that one method would be assigning very long unique numbers to individual sites. This could be installed in their computer software and included in any electronic transmission, and would be a way of identifying them. These numbers or *Public Keys* would be made available in a tiny file called a certificate. The database containing details of these files, including their projected expiry is broadly known as the *Public Key Infrastructure* or PKI.

So these numbers would be unique to a practice and if contained in a transmission would be a verification of where that transmission originated. Effectively the transmission was digitally *signed* by that number. The next challenge was to make sure that the transmission was coded in such a way that it couldn't be intercepted and read by others. That was achieved by creating a second certificate that would *encrypt* your message.

This all resulted in what we now know as your PKI Location Certificates or *Site* certificates, and there are two of them:

- PKI Location Certificate - Signing
- PKI Location Certificate - Encryption

Once applied for these certificates were delivered on a cd to the practice along with a secure pass phrase (sent separately). They usually expired after 5 years with the practice being sent a new cd in the mail around that time. Part of the initial setup included the installation of a program called a *PKI Certificate Manager* on your server. This would be used to create a unique *store* that held your certificates. Your billing software would be configured with the location details of this store.

A few years down the track Medicare began to be able to update your certificates automatically every 5 years via the PKI Certificate Manager. On the plus side, this removed the need for CDs in the mail, on the downside because it happened only every 5 years and in the background, the shared knowledge of how things actually worked became less. For some practices, these certificates were unable to be automatically updated, and so they still received a disc in the mail.

Before we finish the mechanics, I should mention that there are both public and private copies of your PKI Location certificates. The practice alone holds it's private ones but your public ones are freely downloadable from a certificates website. Anyone who wants to communicate with you, needs to install your public certificate in order to *encrypt* information sent to you, and the message can only be decrypted by the owner of the Private certificate which is you. And the reverse applies.

The best example of this is how your billing software talks to Medicare. Your local certificates store contains copies of the Medicare organisation's public certificates.

Continued...

PKI Continued

So your system sends information to Medicare encrypted with their *public* certificate. They decrypt it with their *private* certificate. They send information to you encrypted with your *public* certificate and your system decrypts it with your *private* certificate. All of the services that you communicate with using PKI work along these lines.

medicare

Practice private certificate ← ← ← ← ← Practice Public certificate

Medicare public certificate → → → → → Medicare private certificate

Medicare had so much fun with this they expanded the idea to having PKI Individual certificates, with the idea that each GP would have one. Thousands of GPs were issued with these in the form of little blue plastic tokens that could plug into a USB port. In most General Practice scenarios this was an absolutely impractical and unworkable idea. I think they are still available, but happily in a standard general practice scenario, Medicare settled for all of the GPs to be covered by the location or site certificate.

eHealth

About a decade ago, Medicare introduced the next phase of electronic communication with the *Publicly Controlled Electronic Health Record* or PCEHR. (It was pronounced "Pecker" by the various commonwealth IT types, I kid you not!) Mercifully it transformed to the *My Health Record* or MyHR that we know now. Part of the infrastructure of all this was the creation of a *Healthcare Identifiers Service*, with unique numbers for health facilities, practitioners and patients.

HPI-O Health Provider Identifier *Organisation*

HPI-I Health Provider Identifier *Individual*

IHI *Individual* Health Identifier

In order to operate in this new eHealth world, the provider and Organisation numbers had to configured in the software and the patients IHI had to be looked up and verified by the software. It was decided that the PKI Location certificates would be adequate as security for looking up Health Identifiers.

But a new certificate was needed in order to actually access the MyHR system, once your system had looked up or verified the IHI number. This certificate was the PKI *National Authentication Service for Health* or NASH certificate. These certificates, once applied for, lasted for 2 years with new ones generally mailed to the practice on CD. There was no capacity for these to be updated automatically in your system.

Whilst being primarily for MyHR access, NASH certificates are also used for communicating with ERX (escripts) as well as being the security method for some secure messaging stuff. NASH certificates generated in the last year or so, have an added superpower, as is shown below.

Certificate Type	**Billing System Usage**	**Clinical System Usage**
PKI Location Certificates	Medicare Claiming and Billing, OPV checks, Tyro & like systems	HI Lookup
PKI Nash Certificates	None	MYHR access, escripts, some secure messaging
PKI NASH Certificates (New)	None	MYHR access, escripts, secure messaging, **HI Lookup**

PKI Continued

Note that the NASH has no application for the billing component of your software and therefore isn't installed in the certificate store that the billing component accesses. The NASH get's installed straight into the software, and for MD users is only installed in MD *Clinical*. The Location certificates are only needed for HI lookups in MD clinical and now, not even for that as the NASH certificates can now do that too. Note that in MD Clinical versions prior to 4.1, despite this you still need to install all the certificates.

2020 Onwards

As Medicare added more and more online health services to it's offerings, a decision was taken to move the security mechanism for most of it's products from PKI certificates to a Web Services system, with login access to different services configured using the *Provider Digital Access* System (PRODA). So, rather than using long encrypted number chains to control security, you would setup security online via your practice PRODA account. Your software would access PRODA using a configuration called a B2B device and this would govern your access to other systems.

The plan was that this would replace any need for PKI Location certificates in your software, and the hope was that compatible software versions would be available and installed by 13/3/22. To foreshadow this many PKI Location certificates were set to expire on 13/3. This may not have been a good idea! Because Web Services versions of MD and BP were not available by this date, let alone installed, it became obvious that after 13/3 most practices wouldn't be able to interact with Medicare billing and claiming systems.

Going forward, whilst the need for PKI Location certificates would be gone, practices would still need their NASH certificate for accessing MyHR and also generating escripts. I actually suspect that originally the plan was to dispense with NASH certificates at the same time, but I may be wrong. What they did do was to expire many NASH certificates on 13/3 as well, claiming that practices needed to download a SHA2 Nash certificate for things to work after 13/3.

What is SHA2 you ask? Well it's one better than SHA1 which is what your certificates used to be. Don't give it a second thought, it just represents a more advanced and secure encryption algorithm. As it turned out, this became a non-event. Either SHA1 or SHA2 will work fine at the present, but practices still running a SHA1 certificate will have to get a new one by 31/12/22.

When it became obvious that the 13/3 deadline was going to be missed, the deadline was extended to late June. **Bottom line is that practices will have to be running Web Services compatible software by then. For BP, that's Saffron SP3 or later and for MD it's 4.2 (not yet released). When you are running these versions, the PKI NASH certificate is the only one you will need to retain.**

March 2022

An Industry that didn't really have an understanding of PKI certificates at all had to contend with the following circumstances.

NASH certificates expiring on 13/3 meant no MyHR or escripts. Previously delivered on CD, it was mandated that NASH certificates had to be requested and downloaded from PRODA, once a PRODA organisation account had been created. This organisation account creation was a nightmare in itself for many, with the practice details in terms of ownership and address etc, needing to exactly match what was held on the Australian Business Registry for the practice. People had the joy of wrestling with PRODA so they could download a certificate that many of them were unsure what to do with.

With the deadline missed Medicare had to issue thousands of new location certificates, many of which updated automatically in the software, some of which were sent on CDs. Practices had to figure out which category they were in.

Catastrophically, in the first week of March, Medicare either deactivated or incompletely activated thousands of already issued Location certificates. The exact circumstance is not clear, (and certainly wasn't publicised) but some practices whose claiming had been working just stopped, days after a new certificate had been installed. For others, claiming continued to work, but HI lookups and therefore MyHR stopped working. This was particularly an issue for MD users. …..*Continued*

PracSavvy

Clinical Systems Support and Training

www.pracsavvy.com.au

PKI continued..

All this was occurring with a deadline looming for an industry and it's support teams not always familiar with the topic in question. Countless stories of practices being handballed between their IT support, clinical software support desks and ebusiness support with me occasionally chipping in to make things worse. Each area understanding their bit, but not necessarily the other bits. I'm sure there were even more factors or nuances than I have accounted for. Corporate practice staff may at least have been shielded from much of the troubleshooting frustration, as compared to stand alone practices, but overall a very stressful time, kicked off by some terrible planning at federal health level.

In conclusion, I apologise that this morphed from an intended guide to PKI to a commentary on what occurred in the last month or so. I've assisted a few stressed interstate Practice Managers on a face book group, beefing up/refreshing my own knowledge as I went, and I just felt that it was worth writing all this down….possibly even as closure. As the guide and potted history of PKI goes, it may not be a 100% correct as far as dates and certain technical nuances go, but I'd be confident that it would be at least 90% correct, so please forgive any minor discrepancies.

Not that the preceding article is a good example, but sometimes you feel that you have explained something clearly, only for it to be revealed, that you haven't at all.

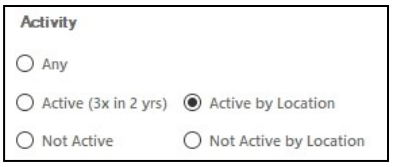
It's good to see that it doesn't just only happen with IT.

I said my name was Marc with a "c"….

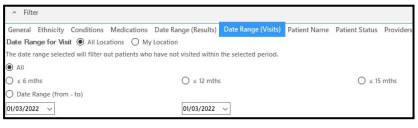
PenCat

If you are part of a multi-location practice sharing a common database, your scheduled data extracts may be showing as one for each physical location as opposed to just one for the whole database. If this isn't the case, but you would prefer that, you can generate separate extracts per location as was highlighted in the October 2018 newsletter.

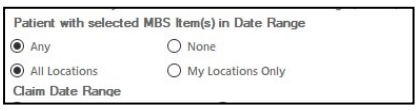
In the last few months, Pen have added buttons for certain filters, letting you choose between whether you want to see the results for all your branches, or just the currently loaded one. Note that these buttons only appear if you have a location specific extract loaded as opposed to one for the entire database.



Activity: Choose between *Active* across all of your locations or just the location loaded.



Visits: Choose the date parameters across all your locations or just the loaded location.



MBS Billing: Billing for all locations or just the loaded one.

Ian McKnight t: (03) 6247 1178 m: 0418 336 804 e: pracsavvy@bigpond.com

PracSavvy

Clinical Systems Support and Training

www.pracsavvy.com.au

Bits

I'm always on the lookout for evidence that improvements in technology have improved health outcomes and edged us a little further away from the fax machine. So it was great to read this month that faxed requests to the National Cancer Screening Registry (NCSR) have dropped by a whopping 94%, largely due to the creation of a provider portal accessed via PRODA and integration with mainstream GP programs like BP, MD and even Communicare!

So, IN YOUR FACE GRETA! ☺ Actually I don't really know the difference in energy required between a faxed request and an electronically transmitted one, but I doubt that you do either. Anyway, there is definitely a paper saving if nothing else. Apparently the Bowel Screening people had also been advocating for an online method for the submission of samples, but it was decided that there was enough sh!t on the internet as it was, without adding to it.

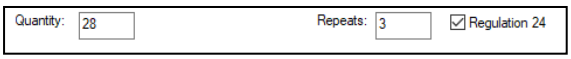
On a more mature note, this news release does seem to indicate that the NCSR have made some real technology related quality improvements in the record over quite a short period of time, so hats off to them, and If I was a GP and nobody had enabled the interface in my software, I might be asking why at this point.

Given that Covid numbers are currently quite high, although thankfully representing fairly minor illness in most cases, GPs may be interested in the Managing Covid at Home resources that the RACGP have put together over the last few months. With regards to vaccines, the ATAGI Clinical Guidelines for Vaccine Providers remains a pretty good one-stop resource.

BP

A couple of bugs that affect prescribing in BP are worth mentioning. If you have updated to Saffron Sp3 and use ERX for escripts, tell your Drs not to use the "<" character in the dose field as apparently it causes the escript to fail.

Another slight prescribing bug that has crept in SP3 is that the label "Regulation 49" has reverted to "Regulation 24" which is it's previous incarnation. For the non-doctors, this regulation allows the pharmacist to supply all of the medications and repeats in one hit. Apparently it's a very popular parameter with certain demographics.



Another related glitch in recent releases of BP is that in order to enable the check-box for selection you have to change the number of repeats, even if the number is the one you want. In the above example a GP would have to delete the "3" and then re-input it to enable the checkbox.

Finally if your templates contain the *Current RX List (Long Term)* field or <RegularRx> as it appears in template design view, know that the medications displayed will not contain any p.r.n. medications. I don't know whether this is by intent or not. Certainly using the *Current RX List (Selected)* field will give you all the patient meds to select from.

Templates

The following new or updated templates are available at my website here:

- LGH EEG Request

Ian McKnight t: (03) 6247 1178 m: 0418 336 804 e: pracsavvy@bigpond.com