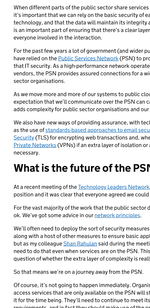
The internet is 'ok'

James Stewart, 20 January 2017 - Technology Leaders



When different parts of the public sector share services and exchange data it's important that we can rely on the basic security of each other's technology, and that the data will maintain its integrity as it moves around. It is an important part of ensuring that there's a clear layer of trust between everyone involved in the interaction.

For the past few years a lot of government (and wider public sector) services have relied on the Public Services Network (PSN) to provide assurance of that IT security. As a high-performance network operated by multiple vendors, the PSN provides assured connections for a wide range of public sector organisations.

As we move more and more of our systems to public cloud services the expectation that we'll communicate over the PSN can cause confusion and adds complexity for public sector organisations and our suppliers.

We also have new ways of providing assurance, with technical controls such as the use of standards-based approaches to email security, Transport Layer Security (TLS) for encrypting web transactions and, where necessary, Virtual Private Networks (VPNs) if an extra layer of isolation or authentication is necessary.

What is the future of the PSN?

At a recent meeting of the Technology Leaders Network, we reviewed our position and it was clear that everyone agreed we could just use the internet.

For the vast majority of the work that the public sector does, the internet is ok. We've got some advice in our network principles.

We'll often need to deploy the sort of security measures described above, along with a host of other measures to ensure basic application-level security, but as my colleague Shan Rahulan said during the meeting we increasingly need to do that even when services are on the PSN. This then opens up the question of whether the extra layer of complexity is really helpful.

So that means we're on a journey away from the PSN.

Of course, it's not going to happen immediately. Organisations that need to access services that are only available on the PSN will still need to connect to it for the time being. They'll need to continue to meet its assurance requirements, and in fact they should make use of the practices that covers when reviewing all their core IT.

But from today, new services should be made available on the internet and secured appropriately using the best available standards-based approaches. When we're updating or changing services, we should take the opportunity to move them to the internet.

What happens next?

There's quite a bit of work to do across the public sector to prepare for these changes and we're not quite ready to provide a full timeline. We'll be staying in touch with users of the network and commercial providers to make sure that those who need to make decisions get clear information.

My colleague Mark Smith, Head of PSN, has been working with data scientists in GDS and the National Cyber Security Centre (NCSC) to prototype other ways of providing assurance data that will help organisations establish trust. He'll introduce that soon in a blog post and is doing some deeper discovery work to ensure we have great options for organisations to verify that their networks meet a set of basic standards.

GDS, NCSC and Crown Commercial Service (CCS) will be working together to ensure that as we update the ways in which we buy network services we have the widest possible range of suppliers and the right options to make sure we get the highest quality connections.

We'll be working with the Tech Leaders Network and the wider PSN community to ensure that common issues are clearly identified and that wherever possible we work together to provide common solutions.

We'll also be working with colleagues in the Cyber and Government Security Directorate and others across the public sector to make sure that we are able to collaborate on upgrading older systems that need new protections and strategies. That's a clear part of the National Cyber Security Strategy and this move just adds some more focus to plans already underway.

To make sure you stay up to date with all the latest developments, you can sign up to alerts from the Government Technology blog.

Tags: PSN, Public Service Network

← Opening up government through open data standards

Breaking down the barriers to change →

14 comments

Michael on 20 January 2017

I hope someone is having this conversation with the police regarding moving OFFICIAL information across the internet, because they don't seem so keen.

Link to this comment

> **Mark Smith** on 27 January 2017
>
> Rest assured we will be talking to a wide range of organisations across the wider PSN community following the decision, Michael. However, the decision was made by the Technology Leaders Network, which represents the senior leaders from all departments including the Home Office.
>
> Link to this comment

Peter on 23 January 2017

Please can we ensure that the NHS is included and that the protocols agreed will require only one CoCo / Toolkit for interoperability with ALL the public sector.

Link to this comment

> **Mark Smith** on 27 January 2017
>
> Thanks for your feedback. Rest assured we'll be talking to a wide range of organisations across the wider PSN community following the decision. However, it's important to understand that the decision wasn't made any one organisation - it was made by the Technology Leaders Network representing all departments across government, including the Department of Health.
>
> Link to this comment

Ben Basson on 23 January 2017

I completely agree that the PSN adds little value over TLS and/or VPN, and indeed, makes mostly everything a lot more complicated (and presumably expensive) than it really needs to be.

One thing I don't clearly understand is how you'll address end-to-end email security for government.

I can see that you can implement TLS for email in transit between government departments, but is that going to be opened up to suppliers // hosting providers as well? Currently cloud services can send email at Official or Official Sensitive via the PSN and know that content will not be compromised. Can there be such a guarantee in the future?

Link to this comment

> **Mark Smith** on 27 January 2017
>
> You're right Ben, things have moved on a long way since the PSN was originally conceived. Re your question, we've recently published guidance on securing government email(https://www.gov.uk/guidance/securing-government-email). It's based on widely-used open standards and any organisation working with government can use it too, without needing a PSN connection. While no security measure is ever 100% perfect, the guidance is appropriate for information at Official and Official Sensitive.
>
> Link to this comment

Kay on 25 January 2017

So once again departments can look forward to on-going and continued meddling in procurement processes leading to huge hikes in contract costs as we end up procuring costly extensions at the eleventh hour because you can't understand the issue we are trying to fix, and just keep bleating out the phrase 'put it in the cloud'?

Link to this comment

> **James Stewart** on 25 January 2017
>
> Thanks for your feedback Kay.
>
> Whilst I accept that the changing ICT landscape can be frustrating, I'm keen to underline that the decision was made by the Technology Leaders Network, which represents all departments across government.
>
> As I mentioned in the post, there's lots of work still to be done following the decision. That includes making sure there are good commercial options for departments to buy the high-quality, resilient internet connectivity they need, and that techniques for migration are well documented and shared. We'll keep you up-to-date as things progress.
>
> Link to this comment

> **Steven** on 13 April 2017
>
> I like the idea but currently there are literally thousand of services on GCloud which is not PSN specific and can be made use of by internet connectivity. Whilst vendors make assertions of security I'm very skeptical that those assertions could hold up to formal testing. Whilst I like the idea of pushing everything HMG to a free market, we also need to keep in mind that free markets cut costs and cut corners to make what is most important to them and that is profit, having said that the other side of the coin is also true they also heavily invest in innovation. Would be good if we could have the best of both worlds.
>
> Link to this comment

Giles Letherren on 27 January 2017

How does this play into the NHS commissioning a new private network in the form of HSCN? As a supplier to both local government and health bodies it's a constant frustration that we have to support multiple secure networks that don't trust each other. More power to the 'almost everything over the Internet' argument.

Link to this comment

Paul on 01 February 2017

Before long, the only services we will consume from PSN will be from ToO and IER. Which means a huge outlay for very little traffic (albeit important). Do you know if the provider of these services has a plan or timetable for moving from PSN?

Link to this comment

> **Mark Smith** on 06 February 2017
>
> As mentioned in the blog post, Paul, when services are updated or changed we'll take the opportunity to move them to the internet but, for the time being at least, some services will only be accessible via the PSN. However, it's important to understand that the PSN is a fully operational network service that's been built (as with other infrastructure) with public sector investment. It makes absolute sense that we maximise the return on investment for as long as possible. The changes won't happen overnight, so there's no timetable at present, but we'll keep you informed as things develop.
>
> Link to this comment

Steve Halliday on 04 February 2017

This just needs a "use case".

The PSN began with a vision that it should be used for *all* communications. It anticipated shared services at scale. This is clearly policy making "of its time" - i.e. wrong now.

The internet can, of course be used for a big chunk of public sector communications. But it's problems are not only security. It's also not possible to guarantee user experience over the internet.

User experience is why all big businesses buy WAN connectivity to join their buildings together, instead of opening secure internet channels. As well as guaranteeing user experience, they also architect network security to protect their interests.

All public sector bodies will continue to buy WANs. For low volume communications with other public sector bodies, that do not require instant user interface the internet can be perfectly secure enough.

The PSN use case is only really there when you are delivering shared services - which is what the original PSN vision was all about. Ten years later, shared services are few and far between, making the PSN's value forecasts seem somewhat naive.

If we are making the bold statement that the PSN is not necessary after all, we are effectively giving up on shared services at scale.

This effectively says to any group of public sector bodies entering looking for a network to share digital/IT assets over: "Buy Your Own".

Have we given up on shared services at scale?

Link to this comment

Steve on 14 February 2017

I agree with Peter about the assurance framework(s).

The number of multiple overlapping assurance frameworks together with the changes being brought in by EU GDPR has created a burden in a time of austerity. These frameworks have been put in place by differing central Government Departments (and some areas of the private sector) vying for some semblance of control in their respective areas of service whilst the NCSC sits in the background with a £1.9billion budget saying 'we don't set frameworks, we just advise'.

However, the PSN was one of the only recognised, externally accredited, common assurance standards across non-central Government organisations. With its imminent disappearance I have noticed that various bits of both central and non-central Government have started to call into question the assured security of each others systems with NHS now stating that some Police email systems are no longer trusted as being secure and some Government arms insisting that providers sign up to CJSM email immediately because "TLS won't work with their email system".

And now the upheaval from N3 in March 2017 to HSCN no earlier than September 2018 and changes in NHS IG Toolkit by 2018, how can organisations provide simple, efficient, recognised information assurance maturity in the near future? ICO audits? I think they are going to be a bit busy!

Seems like this 'deeper discovery' you mentioned is too little too late?

Link to this comment

Recent posts

This blog is now archived.
Making the Technology Code of Practice better.
GDS's next top model contract.
How we're connecting new services with legacy systems.
Interoperability and security: learning from business.