The Secure by Default Partnership Programme

Devices can be both highly usable and secure. We'll work with partners to develop strong case studies that prove this, and show the public sector the business benefits of applying new technologies.

The opportunity and what it could mean for you

The Secure by Default Partnership Programme is a great opportunity for you to get new technologies into the hands of your users and help prove those technologies for the rest of the public sector to follow.

We're looking to:

- help a number of proactive public sector organisations to successfully adopt some particular new technologies
- learn from these experiences
- share the results with the wider public sector

The technologies we've chosen for the case studies already exist in commercial products and are fully supported by their manufacturers. Use of the new technologies is currently limited in the public sector; we're trying to increase their uptake by showing how they can improve the way staff use IT.

We'd like you to adopt some or all of these new technologies, share your experiences and write a case study report. In return, you'll get access to:

- a nominated NCSC technical expert to answer questions about the technologies, give implementation advice, and provide on-site technical support if required;
- a further £25,000 to spend on equipment, infrastructure, software licences, support costs and so on (two-thirds at the start of the programme, one-third at the end on delivery of a case study);
- advice and guidance on accreditation and PSN compliance from nominated individuals

We're seeking government departments, local authorities, healthcare trusts, law enforcement agencies, or other public sector organisations that handle OFFICIAL information, regardless of size or function of the organisation. If you're in a sub-team of one of these organisations, then that's fine too. The main thing is that, given the above support, you should be a good fit for a great case study.

Why are we doing this?

We want to encourage adoption of new technologies that solve current IT problems and target specific pain points users have with IT. However, we're invariably asked the same three risk-related questions:

"Who else is doing this?"
"Will this affect my accreditation?"
"Can I connect this technology to PSN?"

We think that strong case studies are a good way to overcome worries like these. Together we can show that the technologies can be adopted successfully in the public sector with clear business benefits.

We understand that adopting a new technology can seem risky. To mitigate risks and boost confidence we will help where we can; providing technical expertise, access to our policy experts, and upfront funding.

What we're looking for in potential partners

Your organisation must be part of the public sector, and the core part of your application is your proposed case study. Beyond this, we would like to see evidence of:

- you're trialling new things, even if those trials didn't quite work
- your experience of deploying or working with existing NCSC architectures — such as EUD Security Guidance or Walled Garden for Remote Access Architectural Pattern

- teams with existing network architectures that would work well with these new technologies
- willingness to discuss the challenges and benefits associated with deploying the technologies

These points don't need to apply to the entire organisation you work for — if you're in a sub-team that you think would make a good candidate for these partnerships then we'd still like to hear from you.

How we will choose partners

Funding is limited and we want compelling case studies, so we will assess aspects of your organisation to help us decide who to partner with. We will include a number of high-level factors in our decision-making, such as:

- how the technology will fundamentally change the operation of your organisation, or certain business processes within your organisation
- how quickly you'll be able to get started on integrating the technology — we're not looking for overnight deployments, but we expect to see some movement within a few months
- how much control you have over your own IT estate and how your team uses IT — if there are many external parties involved in running your network, the roll-out process will be slower and probably more expensive

Technologies to be showcased

Last year, we focussed on a number of Microsoft Windows 10 technologies which were introduced in 2015. This year, we're not limiting participants to a specific brand of technologies. Instead, we're looking at the broader problem of reducing reliance on passwords, and inviting participants to come up with more usable but equally (or more) secure alternatives to remove or replace passwords. Such as:

- Hardware-backed alternative
- Single sign-on to apps and websites
- Biometrics
- Nothing!

Native security controls and open standards are very much preferred, so avoid adding third-party security products to achieve these outcomes. For example:

- Windows Hello
- Touch ID (iOS)
- Fingerprint authentication (Android 6+)
- FIDO U2F or UAF
- Web app single sign on
- Certificate, Kerberos or Hello
- Bitlocker Network Unlock
- Risk management policies which balance Usability vs Security

Existing network topology requirements

Ideally, your network architecture for End User Devices resembles that detailed in the EUD Security Guidance; but this isn't a strict requirement. Also:

- a remote access VPN (Ideally IKEv2 or DirectAccess, or the option to switch to either of these)
- an internal web service supporting single sign-on (e.g. PKI, Kerberos, or SAML)

What we want from the partners we choose

We know how many technologies work, and how to implement them. But you are the experts in your existing networks and business processes — and navigating this is crucial for successful implementation. So, whilst we're making an investment in terms of time and money, you'll definitely need to provide plenty of help. In short, you'll be expected to:

- produce a plan of key milestones you'll pass in implementing the technologies, together with expected dates for meeting them
- produce a plan of how you'll use the time and money investments
- work with our technical experts on planning and implementing the technologies
- invest your own time and money into the activities
- produce a formal written case study of your experiences which we can share online
- present the case study in a short presentation at a future event (possibly CyberUK in Practice 2018)

How to apply

- Download the attached application form and guidance (or see Downloads tab).
- Use the guidance to help you complete the form.
- Send in your application as described in the form, to reach us by 30 June 2017

The timeline for the Secure by Default Partnership Programme is:

- 30 June 2017: Deadline for applications.
- 17 July 2017: NCSC announce partner organisations chosen for the programme.
- 1 August 2017: NCSC transfer initial funds to partners. Work begins.
- 1 March 2018: Case study completed.
- March 2018: Partner organisations present their case studies.

PUBLISHED

2 May 2017

REVIEWED

2 May 2017