It is no secret that the UK Government is still running at a significant loss. It is therefore no surprise that organisations are having to cut costs and, for the public sector, this has fast become its mantra. The NHS, Children’s Services, Housing and Regeneration, local government, the police force—everywhere you turn there is a generic call to introduce changes that will save money. With this in mind Robert Campbell, Managing Director at Ecommnet, talks about implementing and managing secure access in a period of rapid change.

One popular initiative has seen many local councils consolidate their operations by co-locating their staff. NHS, education, council employees and others are all congregating together in one central location in an effort to reduce property costs. While on the surface this seems a practical solution, for the IT team it’s a logistical nightmare.

Physical connectivity
Imagine, if you will, each department existing in its own locale. Part of the infrastructure would typically include a physical IT network. Just like a building has walls protecting the contents inside, the network too would have barriers, or gateways, to prevent external access. As organisations come together under one roof, so too do the networks on which they function and this is where the complexity begins.

Sticking with the physical building analogy, if you give someone a key to the front door without a thought to the security within the building, then that person is free to roam all the floors, corridors, offices and potentially rifle through the unlocked drawers and filing cabinets. Similarly, a physical network is made up of several layers and it’s reliant on someone physically locking all the areas, or compartments, to prevent unauthorised access.

It is imperative that a company controls which individual has access to which services, applications and information and from where. They also need to ensure that each individual is actually who they claim to be. While this sounds pretty straightforward, it can be very complex to manage without the right tools.

Before I continue it’s worth clarifying that inadequate data protection will get you into a whole heap of trouble. If you’re in any doubt, a quick internet search of ‘public sector data breaches’ will bring up a long list of organisations that stand testament to the size of the problem and the penalties they’ve incurred as a result.

NETWORkLESS WORKING – THE FUTURE OF THE PUBLIC SECTOR?

As organisations come together under one roof, so too do the networks on which they function and this is where the complexity begins.

Sticking with the physical building analogy, if you give someone a key to the front door without a thought to the security within the building, then that person is free to roam all the floors, corridors, offices and potentially rifle through the unlocked drawers and filing cabinets. Similarly, a physical network is made up of several layers and it’s reliant on someone physically locking all the areas, or compartments, to prevent unauthorised access.

It is imperative that a company controls which individual has access to which services, applications and information and from where. They also need to ensure that each individual is actually who they claim to be. While this sounds pretty straightforward, it can be very complex to manage without the right tools.

Before I continue it’s worth clarifying that inadequate data protection will get you into a whole heap of trouble. If you’re in any doubt, a quick internet search of ‘public sector data breaches’ will bring up a long list of organisations that stand testament to the size of the problem and the penalties they’ve incurred as a result.
**Networkless connectivity**

Instead of building separate physical or rigidly constructed networks for each organisation, one method that is gaining popularity is to create one network and to control access to the services and data it houses at the point of entry.

Networkless connectivity removes the dependency on how the network is physically constructed and is instead dependent on an individual’s role within the organisation. Using access control technology, the services and information each individual is granted access to will be determined at the point that they attempt to connect to the network. Returning again to the building analogy, it is akin to each person having their own unique key to the building that, when they unlock the front door, automatically opens all the doors inside the building that they can legitimately enter, but also seals all the doors that they should not.

Access can be further controlled by what type of device is being used to connect and where people authenticate themselves. For example, if a user connects to the network from a PC within the organisation’s premises, then they can access all files and information needed to perform their duties. However, if they connect from a laptop from home, they may be restricted to just calendar information or basic applications. Taking it a step further, access can be further controlled by the day of the week and/or time of day that the person is accessing the network to determine what they can do and see.

While this might all sound extremely complex, fundamentally networkless connectivity is far more flexible, with the underlying infrastructure easier to build and manage.

**Secure authentication**

As previously mentioned, a key security consideration is proving that the user is who they claim to be. Historically, many access gateways required an individual to enter their username and password combination to authenticate themselves. While this may have been adequate for one organisation functioning from one location, as soon as you start co-locating or even allowing remote access, single factor authentication is woefully inadequate and easily circumvented.

For this reason the introduction of two factor authentication (2FA) is increasingly being driven by legislation and/or the need to be more secure. 2FA fundamentally is the combination of two of three elements:

1. Something you know – a username or password, for example;
2. Something you have – an authentication device such as a smartcard;
3. Something you are – referred to as biometrics, this involves retina or fingerprint scanners, for instance.

*Just so we’re all straight, a username and password combination is not 2FA as it is two variations of one element, i.e. two things you know.*

Now that we’ve established what 2FA is, it’s time to look at what the options are. There are two main forms of authentication device:

1. A physical token or smartcard.
2. A virtual token – a mobile phone used to receive a passcode via an SMS message or generate the code via an app.

While physical tokens have been used for numerous years, many would argue that they’re an outdated technology. In addition to the administrative nightmare of configuring each token and the logistical headache of distributing them to users, they also have a shelf-life of typically two to three years. In contrast, virtual tokens on smartphones are far cheaper to manage (usually via a self-service portal), practically every pocket houses a device and people are comfortable with their handset so user acceptance is easily overcome.

Networkless connectivity combined with strong 2FA allows straightforward user access without constraints to deliver a completely dynamic set-up at the time of connection. So, whether you’re merging, re-merging, de-merging or just looking to introduce a more flexible working practice, securely, make sure it’s future-proof and cost-effective. Instead of getting physical, it’s time to start thinking outside the box and even the building.