Considerations and solutions for the Public Sector digital workplace

Alcatel·Lucent Enterprise

eBook

Table of contents

Overview

Across all public sector organisations are the workers who perform the critical business of government on which we all rely. Their role cannot be understated. They often have a direct impact on the lives of many thousands of people.

Digitalisation has been underway for some time. With ongoing pressure to improve public services and cut costs, the pandemic has further accelerated this trend. However, there was no way the world could have foreseen, two years ago, the large percentage of public sector workers that would shift to working from home, and the distributed workforce that would emerge.

The challenges of workers expecting a more digital world, and the complex requirements of supporting a distributed workforce, have created a need for public sector organisations to move from temporary solutions to more permanent solutions to support the new hybrid workforce.

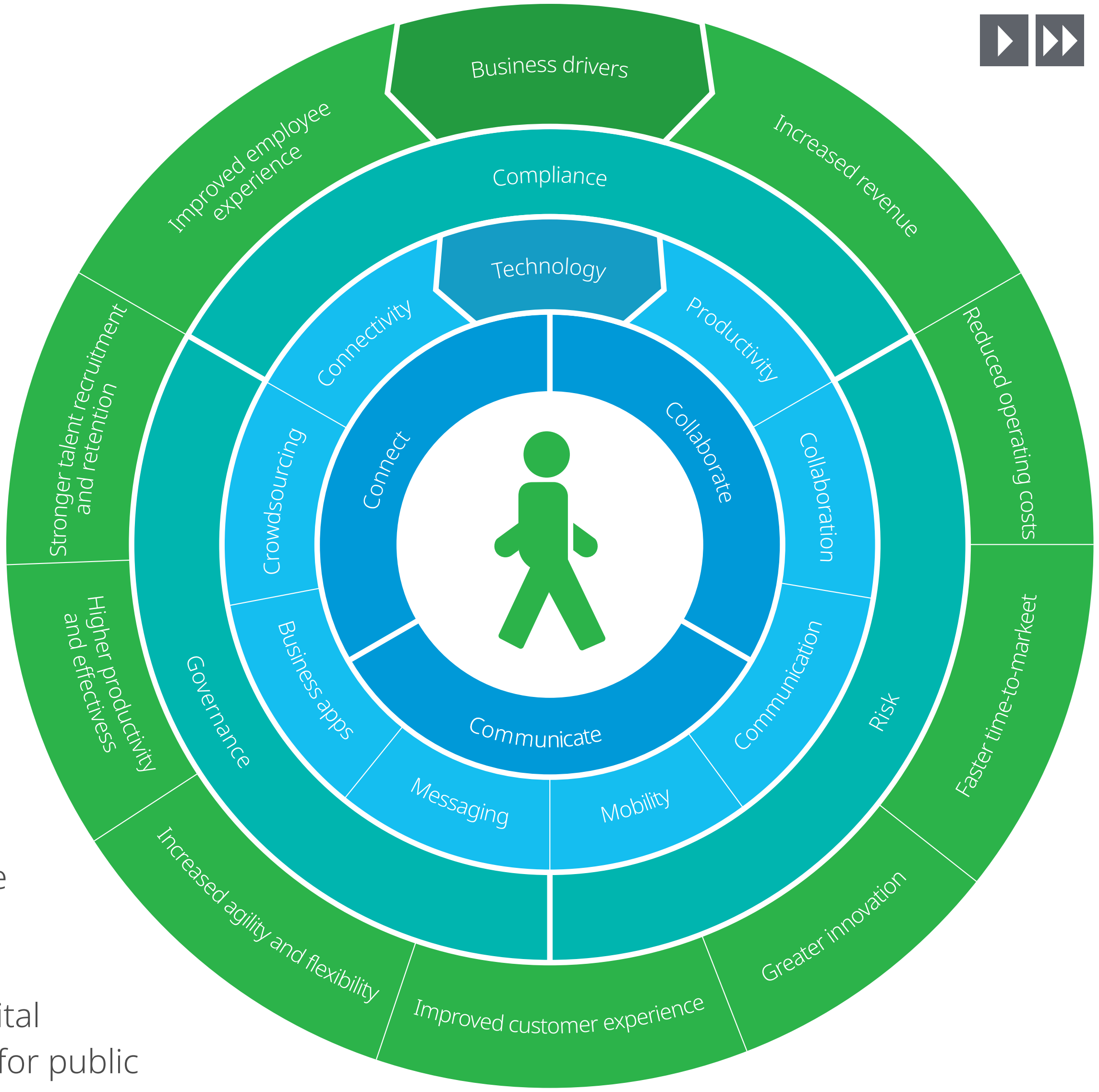
Deloitte[1] provides an excellent graphic that explains how the digital workplace fits together and the advantages that it offers.

Technology provides tools to improve communications and collaboration wherever the location or whatever the device, however, ensuring you have the right technology for the desired outcome can be trickier.

Alcatel-Lucent Enterprise has been working with customers worldwide to understand the new challenges they face and to provide digital technology solutions that enable workforces to work from anywhere, with any device. The digital workplace has created efficiencies for public sector workers, enabling greater productivity, with less travel, which is a bonus for the planet.

This eBook will focus on three key elements of the public sector digital workplace:

- Communications and collaboration
- Connectivity
- Security



And we'll look at ALE solutions that can help public sector organisations successfully move toward the digital workplace with flexibility, agility, and security.

[1] https://www2.deloitte.com/content/dam/Deloitte/be/Documents/technology/The_digital_workplace_Deloitte.pdf

Key considerations for the Public Sector digital workplace

Communications and collaboration

Today employees split their workplace between home, remote locations, and the office. The office is no longer the place where work takes place on a daily basis. It's used more often for group meetings, training, and face-to-face meetings with citizens. Employees no longer go to a single place to work and meet with their teams. This has had a fundamental impact on the work environment, making communications and collaboration more important than ever before.

Communications are a critical component for digital workplace success. Keeping employees engaged, productive, and motivated is the challenge. Employees need communications tools that enable their daily activities, and allow them to communicate and collaborate with colleagues, teams, and citizens wherever their workplace location or whatever their device.

To ensure connected communications we recommend:

- Advanced communications functionality for employees including; high quality voice, group chat, voice messages, and the ability to escalate from a call to a video whatever the device
- Collaboration functionality such as screen sharing, remote desktop control, and large file sharing
- Secure communications and collaboration with external contacts
- Call continuity across the organisation with instant connection and a consistent contacts directory
- A broadcast channel for news, keeping everyone up-to-date on the latest announcements or regulations
- Communications and collaboration must be intuitive

To ensure employees have everything they need, we recommend:

- Evaluating user profiles and communications requirements, based on employee duties, mobility, and need to access business applications
- Offering front-line employees optimised devices that enable quick access to information and communications while on-the-go

- Ensuring citizen service staff have optimised access to call and interaction management, integrated with CRM or business apps
- Enabling collaboration with back-office staff to improve citizen services and first-call resolution
- Evaluating local/country legal requirements to protect data privacy

To ensure high-performance work from home, we recommend:

- Group chat, audio and video meeting capabilities with screen sharing to collaborate on any device
- Call continuity using one underlying infrastructure to connect all profiles
- A DeskPhone option for employees who spend more than one hour on the phone and manage important calls such as: Citizen services, healthcare, and emergency situations
- Communications within the preferred business app to ease user adoption and keep the desktop clutter-free
- Secure remote access to safely access sensitive information

Connectivity

The digital workplace relies on high-quality, resilient, secure connectivity. As new ways of working become normalised and the digital workplace takes shape, the digital infrastructure to connect employees must be in place. Regardless of the location, some key points must be taken into consideration.

- Security must be a top priority. A network solution with several layers of security within the network is required. A zero trust framework assumes that every device or user is a security risk. Network access control must be enabled.
- Secure access to applications anywhere creates the need for user-based access connections. User-based profiles provide secure and flexible connectivity with no loss of service, wherever the location.
- Remote workers with high security and data privacy requirements must be able to connect to the corporate network from home or branch locations. This ensures that corporate policies and security are maintained, and the IT team maintain control.
- Workers now use laptops for real-time applications (voice, video) in the office and at home. This is a big change for many public sector organisations. The wireless network must be able to support a greater use of real-time applications across a larger area. This should be considered when scoping the network.
- Resilience in the wireless network has moved up the priority list as many more workers connect wirelessly. A distributed wireless network with intelligence in the access points means there is no single point of failure, and in the event of an access point going down, other access points in the network will take over the service. A distributed wireless intelligent network also removes the need for duplication in the network, saving both time and money.
- The accelerated pace of digital transformation creates pressure for the IT team who are already dealing with day-to-day tasks. Efficiencies that can be gained should be considered. Reducing the number of management interfaces and operating systems on the network will reduce workloads and training time. Additionally, automation will reduce deployment and operational network management time.
- High-quality access is essential. The digital workplace creates efficiencies to allow greater productivity, if connectivity falls short increased productivity is lost.

Security

Communications Security

Government and public sector organisations are significant targets for cyberattacks. Implementing the most secure equipment available is essential. Integrated management tools must allow security supervision across all elements.

Additionally, mobile devices are transforming the communications landscape and heightening the need for security as cyber attackers exploit the increasing volumes of code contained at every point of access. Defense-grade encryption, data privacy, and secure communications environments require a secure, available infrastructure that is efficient and easy-to-manage.

Our recommendations:

Update and monitor your communications system:

- System updates are critically important in terms of cybersecurity. This keeps your communications systems up-to-date with protection against software vulnerability.
- Enable monitoring of your communications system to track suspicious activities by configuring use thresholds and alarms in the network management system

Authenticate and encrypt:

- Enable mutual authentication between all devices (phones and gateways) and the communications system
- Signalling must be encrypted to prevent protocol poisoning attacks and man in-the-middle attacks
- IP communications must be encrypted to avoid eavesdropping

Make your systems redundant and add a security component:

- Risk can never be equal to zero. If a gateway or the main communications system is down, a back-up system can take over seamlessly when there is spatial redundancy.
- Add the necessary components to protect your communications system, such as a Session Border Controller or a Reverse Proxy, while notifications servers are used to alert the necessary people

Educate:

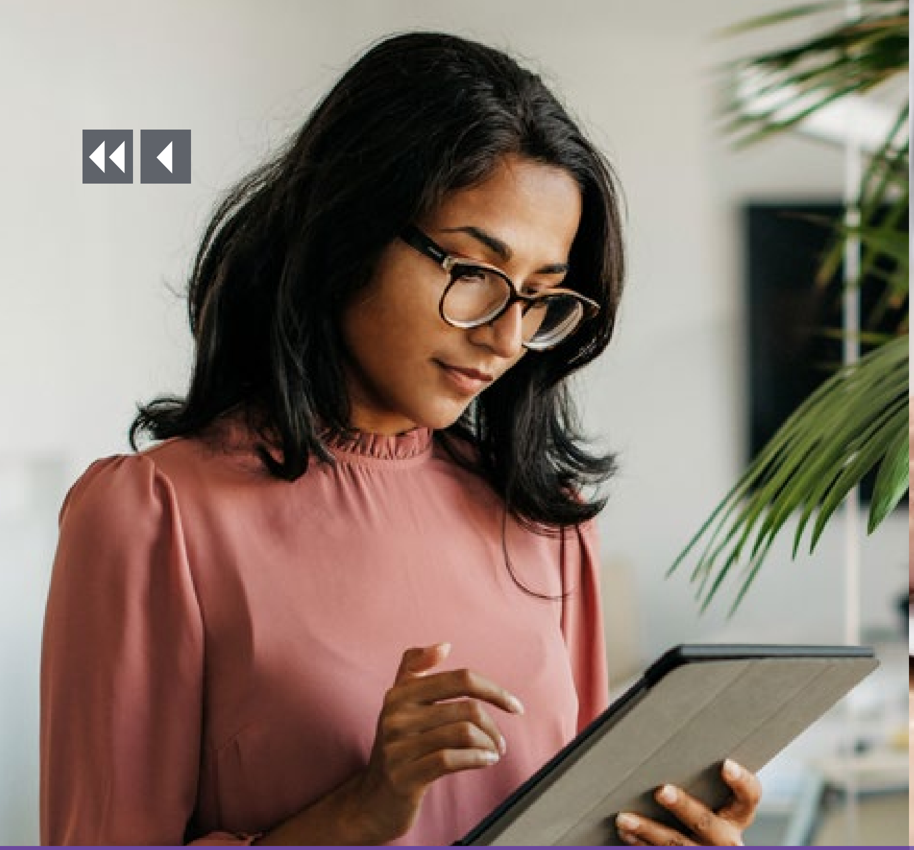
- Educate users and administrators; apply best practices within your teams including, reminders for updating passwords, train users on how to fight cybercrime and how to recognise an encrypted call with the padlock icon on the phone

Network Security

Cybersecurity has long been a top priority for government organisations. However, cybersecurity demands are changing due to digital transformation. As transformation accelerates, the old network security methods are becoming obsolete. As a fundamental component of the network architecture, security must be built-in from the ground up and applied universally across all network access — wired and wireless. Following are some areas to consider to secure your network at all levels.

- **User level:** Verify that users are always authenticated and authorised with the correct access rights (using policies and profiles)
- **Device level:** Check that devices are authenticated and compliant with IT-established security rules. This can be achieved with agents installed on devices that perform a quick security scan before devices connect to the network. For example; the scan can ensure that the devices joining the network have up-to-date anti-virus software, and the latest version of the operating system.
- **Application level:** Set rules associated with specific applications (including blocking, limiting bandwidth or identifying who can use them)
- **Smart analytics:** Analytics capabilities in switches and access points help provide visibility and detailed information about the network, users, devices, and applications being used on the network. They can also provide deep packet inspection capabilities, which detect the type of data and applications moving through the network, making it possible to identify unusual network traffic patterns and unauthorised activity and network intrusion.
- **Network segmentation techniques**: Placing IoT devices in secure virtual containers allows multiple devices and networks to use the same physical infrastructure, while remaining isolated from the rest of the network. If a breach occurs in one part of the virtual network, it does not affect other areas of the network or applications.

These security techniques help build a Zero Trust Architecture framework, the next level in network architecture which operates from the premise, “Never Trust — Always Verify”, where all users must be authenticated, authorised, and continuously validated before being granted access to applications and data.



Digital workplace

Flexible cloud models

Connect everything

ALE solutions for the Public Sector digital workplace

Communications and collaboration

Alcatel-Lucent Enterprise Digital Age Communications (DAC) provide comprehensive on premises and cloud-based communications and collaboration solutions to address digital transformation. The digital workplace is evolving to a distributed work environment where remote working has become normal, making real-time communications essential to connect colleagues, citizens and partners. Alcatel-Lucent Enterprise communications solutions enable call continuity from anywhere, in any situation, and from any device.

ALE key communications features:

- **Seamless connection** inside and outside the organisation. The underlying communications infrastructure connects hybrid workers to back-office and front-line employees, whatever their device, through a variety of standard technologies such as, PSTN, TDM, IP, SIP, VoWIFI, DECT and also provides metrics for IT to monitor the Quality of Service (QoS).
- **One number routing** across the business phone and softphone is perfect for hybrid work. Whether employees are working from home or at the office, no calls are lost, and call forwarding is not required.

- ALE DeskPhones provide **3D Symphonic HD-quality**, rugged handsets and smartphone apps for front-line mobile staff, including notifications and alarms while roaming on-site
- **Easy access** to customer greetings and agent features such as call groups and queues, enable customer service staff to answer all customer calls
- Emergency call crisis conference enables pre-defined contacts to automatically be pulled into a conference for disaster or crisis management with just the press of a button
- **End-to-end encryption** provides security and privacy reassurance required for public sector organisations
- Communications and collaboration for the digital workspace is easy with a **simple click-to-call** a contact or start a conference, or more advanced features like group chat, screen and file sharing, audio and video meetings all in a single app, available as a web client. No installation required. Apps are available for Android and iOS devices as well as PCs. Customers with ALE solutions can use existing handsets with WebRTC technology.
- Connectors for Microsoft® Teams and Google, lets employees **communicate easily** with the entire organisation, from their digital workspace. With connectors for SaaS CRM, and ITSM, employees can communicate and collaborate from their business apps.

Connectivity

Alcatel-Lucent Enterprise Digital Age Networking deliver an Autonomous Network that provides a resilient and seamless connected experience with the Alcatel-Lucent OmniSwitch® (LAN), and the Alcatel-Lucent OmniAccess® Stellar (WLAN) with ultra-fast convergence time, secure network access control, and assured QoS. New generation enterprise Wi-Fi with embedded WLAN control in access points removes the need for physical centralised controllers. ALE solutions can be managed on premises and from the cloud.

ALE key connectivity features:

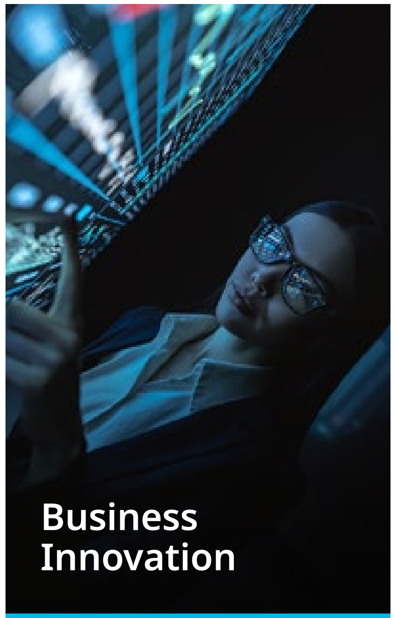
- **A single Network Management System (NMS)** provides an additional level of integration between wired and wireless networks reducing the IT manager workload as the is no need to handle two management systems with two sets of policies and configuration rules. The Alcatel-Lucent OmniVista® Network Management System provides unified management and network-wide visibility, which can improve IT efficiency and agility.
- **Automated provisioning** of a secure network infrastructure simplifies adds, moves and changes while reducing time needed to maintain and operate the network creating operational efficiency while decreasing cost and risk.
- **Shortest Path Bridging (SPB)** designed to support the creation and operation of a less complex network, dynamically builds and maintains the network typology between nodes. SPB load shares and uses all available physical connections making more bandwidth available.
- **Hybrid workers (option 1). Secure remote access** is enabled with the Remote Access Point (RAP). The enterprise network can be easily extended outside the main site, providing connectivity to remote workers as if they were in the company LAN. Depending on the model, the RAP may also provide wired connectivity for IP phones or for other IoT devices. Access is supported by centralised and unified security policies across wired and wireless networks, ensuring easy management and highly robust and consistent security.
- **Hybrid workers (option 2) SD-WAN and SASE.** The Secure Access Service Edge (SASE) securely connects remote sites, branch offices, and remote workers. The SASE solution for remote workers consists of software in the user's laptop which provides secure access to applications in the company data centre, in private data centres or Internet or public clouds, with centralised management and without requiring additional hardware at the worker site. SASE provides advanced security with Next-Generation Firewall (NGFW), including URL filtering and application firewall, and Unified Threat Management (UTM), including Next Generation Intrusion Prevention System (NGIPS), antivirus, and anti-malware functionality.

Autonomous Network

Automate mission-critical network operations and improve user experience

IoT

Scale up digitalisation with secure IoT onboarding and management



Business Innovation

Accelerate transformation with automated workflows

Security

Communications security

Whether you are responsible for a small local or large country government body, your communications network is at risk to be targeted by hackers.

ALE key security features:

- **Secure connectivity** between on premises communications system (PBX and phones) and the cloud infrastructure, fully developed and operated by Alcatel-Lucent Enterprise, with mutual authentication, encryption and security border elements (SBC)
- **High-availability** with spatially redundant architectures, on premises, in private or public clouds, protection against denial of service (DoS) attacks, built-in security with hardened hardware and operating systems
- **Communications confidentiality** with strong encryption based on industry standards natively implemented into the solution, without any impact on voice quality and performance, delivering the experience customers and employees expect
- **Data privacy and protection** with role-based access control and encryption of stored data. This ensures all the crucial data gathered in the evolving business environment is fully protected from end-to-end and under your control.
- **Compliance to regulations and standards** such as (but not limited to) General Data Protection Regulation (GDPR), ISO27001, Common Criteria EAL2+, HDS ("Hébergeur Données Santé" certification of ALE cloud services for data patient protection compliance in France)
- **Security as a process** with Product Security Incident Response Team (PSIRT) for active vulnerability management, regular up-to-date software and policy platform

ANSSI (CSPN)

ENS (Esquema Nacional de Seguridad)

Certification established by the Spanish National Security System in order to have a system that guarantees the proper protection of information systems against external threats and incidents.

ISO27001 - 017/018

The Agency for a Digital Italy is under the Presidency of the Council of Ministers. It regulates the use, storage and access to key data, guaranteeing security.

CERTIFICATIONS IN PROGRESS

BSI Certification

The Federal Office for Information Technology Security (Bundesamt für Sicherheit in der Informationstechnik). Equivelant to the CSPN of the ANSSI (Q3 2021)

Network security

Digital transformation has profoundly changed cybersecurity requirements as the number of connected devices increases, the network perimeter disappears, and change continues to accelerate. Alcatel-Lucent Enterprise Digital Age Networking keeps your IT assets and data secure in today's digital transformation age. With this solution, you can closely manage user access, reduce vulnerabilities created by IoT, mobile, and network devices, keep any inevitable breaches from providing a point of attack, and provide a trusted enterprise ecosystem.

ALE solutions are secure by design with:

- **Secure Diversified Code** which promotes security and assurance at the network device level using independent third-party verification and validation including:
  - Source code analysis, white box, and black box testing by a company specialising in cybersecurity to eliminate vulnerabilities including:
    - ¬ Back-door threats
    - ¬ Embedded malware
    - ¬ Exploitable vulnerabilities
    - ¬ Exposure of proprietary and/or classified information
- **Software diversification:** ALE software implements Address Space Layout Randomisation (ASLR). Each switch boot dynamically generates a unique memory layout to impede or prevent software exploitation.
- **Zero trust security (micro- and macro-segmentation):** The zero trust framework assumes there are hackers present. The enterprise is no longer considered an implicit trust zone. This involves actions such as authenticating all connections. No asset and no user are inherently trusted.
- **Security by default:** Remote access on the OmniSwitch must be enabled, which is the opposite of most other switches where all accesses to the switches/routers is turned on by default and the administrators are left to figure out how to secure the device
- **Built-in Denial of Service (DoS) protection:** OS and management module protection from a host of DDOS attacks that are typically used to cause the CPU to go 100% utilisation
- **No software packages** to purchase and track: Every feature and capability, even ALE secure code, is included with the price of the switch — no modules to add, no upgrades to purchase. All the software is included.
- **Automated and secure IoT onboarding:** Through device fingerprinting, classification and containerisation

EU GDPR

US Federal

US Joint Interoperability

US MIL-STD

US Trade Agreements Act (TAA)

Learn more

Learn more about Alcatel-Lucent Enterprise Public Sector solutions for the digital workplace or contact us to discuss your needs.

www.al-enterprise.com/en/industries/government

Alcatel·Lucent
Enterprise