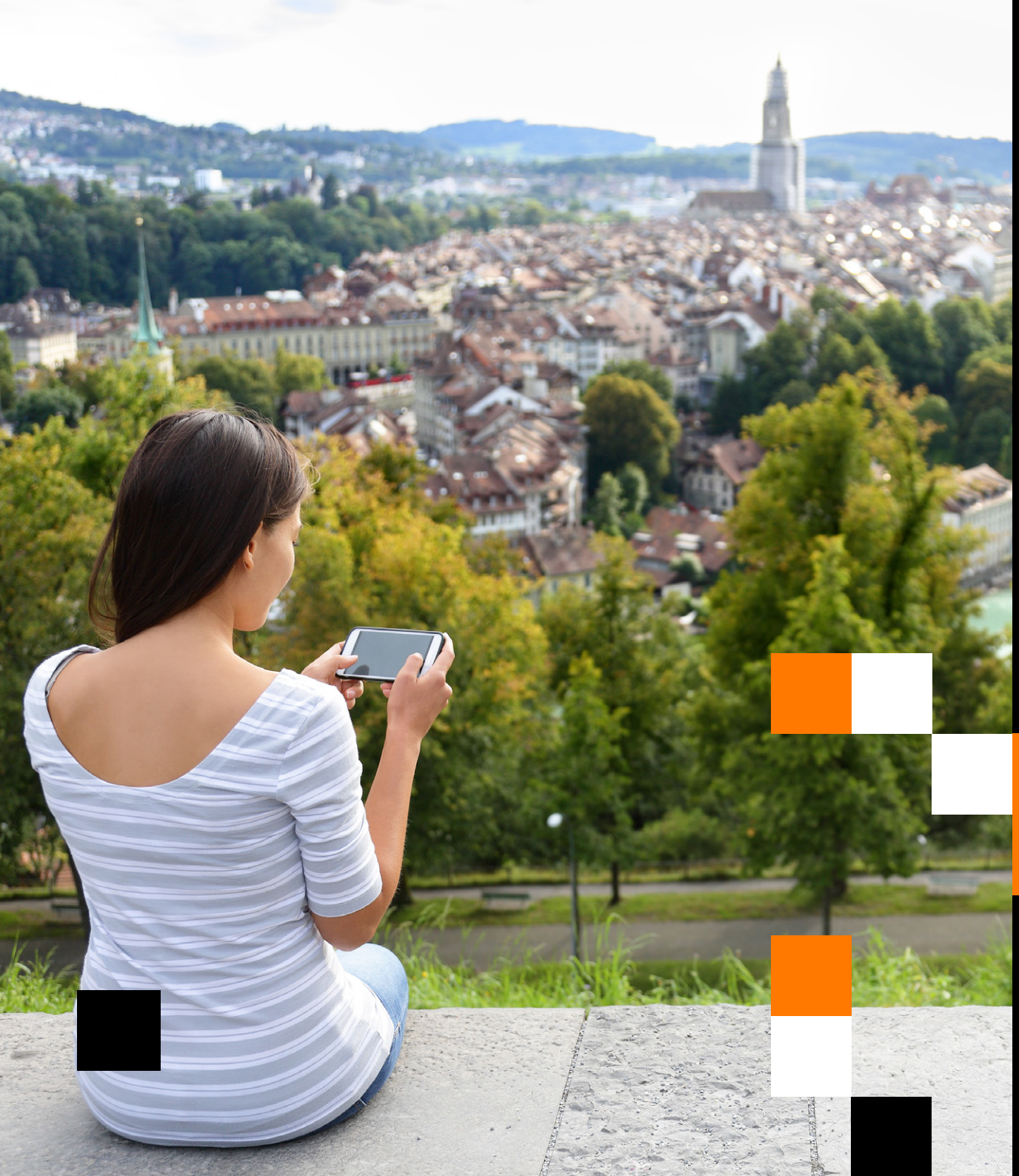
Empowering EU: enabling next generation digital services

orange™ Business



Contents

Infrastructure for next-generation EU service delivery

New ways of delivering government services require new infrastructure. It requires infrastructure that is cloud first, reliable, scalable, and that provides the agility that governments need to serve citizens effectively in the digital era. Because expectations have never been higher: citizens use digital tools and systems for all kinds of work and personal tasks every day, so they naturally expect their governments to deliver services in the same convenient manner.

Yet having multiple clouds brings with it multiple challenges. With every Digital adoption increased markedly during the lockdowns of 2020 and 2021, and European citizens today interact digitally with twice as many industries as they did before the pandemic[1]. Financial services, grocery, and healthcare saw the biggest spikes in digital service adoption, with public sector and utilities lagging behind. It presents an opportunity for the EU to drive ahead and service the demands of citizens for digital service delivery.

But designing and building that new infrastructure comes with challenges: connectivity, cybersecurity, data sovereignty, and data residency are all mission-critical issues that must be addressed. The key priorities for EU digital service delivery are fairness, inclusion, openness, and trust, underpinned by robust cybersecurity. Interoperability and cross-border data sharing among member states must be prioritized, with data security and privacy essential.

Great expectations

Expectation levels continue to evolve. Citizens and companies expect EU service delivery to be of comparable quality and reliability to the private sector – and that delivery starts with an effective IT backbone and related supporting technologies. As things stand, different EU countries have different levels of digital maturity[2], but EU citizens expect services to be delivered online. And the shift extends to all services, not just those that are the most visible like health, education, and welfare.

Digital services refer to any exchange of information or finance, including registering, licensing, applying, paying, borrowing, making enquiries, and more. Services need to be delivered more conveniently and efficiently, always in more cost-effective and more user-friendly ways. Citizens and businesses want public services that are better, faster, and cheaper, easy to access through one-stop shops or multichannel delivery, and, in line with EU plans for e-Government, 'digital by default'.

The EU needs a digital infrastructure that can help it deliver human-centric digital public services that meet targets set for 2030 in the Digital Decade plan. Aligning transformation across all EU Member States can deliver the necessary efficiencies, effectiveness and interoperability while keeping costs minimized. Digital and interoperable public services are imperative in ensuring EU remains a resilient, competitive and innovative entity.

This paper will outline some of the key technologies and approaches required to empower the EU in its ambitious mission of shaping Europe's digital future.

€2.8 trillion

of additional economic value that could be unlocked in the EU by 2030 if digital adoption is accelerated[3]

Activating the "Digital Decade"

The EU has put ambitious plans in place for digitalization in Europe under the "Digital Decade" strategy. Europe aims to empower people and businesses and drive towards a human-centric, sustainable and more prosperous future, enabled and empowered by digital.

The goals are comprehensive: 20 million ICT specialists. A minimum of 80% of the EU population to have basic digital skills. Up to 75% of EU companies to use cloud, AI, or Big Data. Gigabit connectivity for all. And, perhaps most ambitiously, a revolution in digital services: 100% of key public services online, 100% of citizens with access to medical records online via e-Health, and 100% of citizens to have access to digital ID. All this by 2030.

These objectives need specific digital tools and solutions to achieve them. There is a need to strengthen digital sovereignty and communicate the differences between data sovereignty and data residency to citizens. Governments need to focus on the benefits and improvements that data analytics can deliver to service delivery and citizen expectations. Technology and infrastructure are the enablers of next-generation public service delivery and it's essential to get them right at the start.

Ambitious goals

The Digital Decade has ambitious goals. The future can be brighter and more economically successful when citizens are empowered with digital skills, businesses are digitalized, and public services are delivered more effectively.

Some EU countries are ahead of others: Estonia for example offers a case study in what is possible with digital best practices[4]: it already has 99% of public services available online and a nationwide digital twin project that enables visualization of real-life situations to test projects in VR before putting them into action. Furthermore, 98% of Estonian citizens use eIDs, which produce over 10 million digital signatures per year and contribute savings of 2% of the Estonian GDP per year. The Estonian data exchange layer project, X-Road, saved the country's administration 804 working years in 2022 compared to previous years.

It is clear that IT infrastructure enabling agility is essential to this type of progress. Old, monolithic applications and infrastructure cannot support and deliver the innovations required.

94%

of government CIOs experienced a surge in demand for digital services in 2020, directly related to the COVID-19 pandemic[5]

Digital infrastructure for a demanding world

Meeting people's digital service expectations in today's more demanding world is complex. New technologies are always emerging, and the landscape is always changing in terms of regulation, privacy, data sovereignty, and data residency. Citizens want to know where their data is being stored, who has access to it, and what they intend to do with it. Trust is imperative and needs to run through all service delivery activities as a foundation.

The more people get used to digital delivery of services in their private lives, at work, for shopping, for entertainment and so on, the more expectant they become of it in other areas of life. Technologies that enable this enhanced delivery, increased convenience, and security include connectivity, voice, cloud, artificial intelligence (AI), big data, and cybersecurity.

However, managing the infrastructure can be a challenge. The latest applications expected by EU citizens need cloud-first infrastructure to enable the requisite agility, flexibility, and scalability. There are many new tools to integrate and orchestrate, with multiple vendors updating their technologies frequently, with little standardization.

The infrastructure must meet the needs of distributed organizations, have interoperability built-in, and address data sovereignty and data residency concerns. And ultimately it must be capable of handling massive amounts of data securely – because digital delivery of services means a hugely increased threat surface, turning networks into critical national infrastructure like water, gas, and electricity. So, security must be built in by design.

Cloud: the essential enabler of digital services

Governments across the EU have been implementing digital transformation projects and initiatives addressing public demand for digital services. People and businesses are consuming more digital content than ever, and becoming increasingly expectant of digital sources providing them with information and services.

Cloud is the infrastructure that will make the transformation of public sector services and the wider EU digital agenda possible. Today, EU citizens are already reliant on the cloud for many areas of daily life and work. Cloud connects ecosystems of diverse technologies, making services accessible, and is the key enabler of digital modernization for governments and public services. It delivers the necessary flexibility, efficiency, resilience, cost-effectiveness, agility, and scalability that governments need.

However, more choice of solutions to support your objectives also means more complexity. There are more cloud vendors than ever, developing more different types of solutions and applications, supporting environments and platforms. All these alternatives are pitched as plug-and-play and promoted as simple to use and integrate, but it isn't always that straightforward.

There are challenges in terms of interoperability, the need to ensure systems are upgraded and patched as required. Plus, the cloud is only as reliable as the connectivity that powers it, and connectivity speed and quality still vary from country to country.

Overcoming multicloud challenges

A multicloud world brings big benefits in terms of agility and scalability, and is an approach that can support the EU's Digital Decade goals, but it also comes with its own complexities. Every new deployment makes visibility into multiple connections more complex. Multiple types of cloud mean multiple providers, who are often based outside of EU regulatory boundaries. This means it is essential to have accurate oversight into where the data is gathered, stored, and processed and that governance is of the highest standards –in line with the EU Data Governance Act (DGA).

Take action on the cloud

Some tips to help maximize cloud investments:

- **Interoperability:** make sure systems are designed to work in harmony with one another, ensure systems are always upgraded and patched
- **Remember the skills gap:** ensure IT and cloud teams communicate and share knowledge, focus on upskilling staff on latest cloud technologies
- **Increase cloud governance:** put frameworks in place to defines, implements, manage and monitor policies effective cloud deployments
- **Ensure security:** have appropriate policies, controls, and processes in place to protect pan-EU data

70%

of public service executives see migration to cloud as key to transformation[6]

€900m

annual potential savings for European taxpayers by moving 10% of government IT systems to the cloud[7]

Case Study

ESA – transforming space exploration with private cloud

Challenge

- European Space Agency (ESA) works across 20 EU member states, 2,200 employees and an annual budget of around €4 billion
- It generates huge swathes of data that need high availability, storage and security
- Traditional tech was unable to meet scientific and operational simulation and testing needs of ESA
- Projects were taking too long to set up
- ESA needed rapid access to greater data computing that was easy and secure and lower cost

Solution

- Cloud solution utilizing Orange Flexible Computing infrastructure-as-a-service platform
- Best-in-class virtualization, networking, computing and storage
- On-premise, cloud-based in two ESA data centers in Italy and Germany – full redundancy and active-active data replication
- High security with rigorous role-based access control and security designed to specific requirements
- Private cloud integrated into the ESA IT environment
- Program and partner management – Cisco, EMC, VMware

Benefits

- Reduced costs with pay-as-you-go model
- Easy end-user access to computing resources
- Management of greater data volumes
- Compliance with high security governance
- Fail-safe data BC/DR systems
- Seamless integration into the ESA IT infrastructure

Secure by design

Digital infrastructure faces an ever-evolving threat from cyber criminals and state actors. And as digital delivery of public services evolves, it presents a massively increased attack surface. The network is now critical national infrastructure, in much the same way water, gas, electricity, sanitation and healthcare are. There is a bigger risk and a bigger potential impact.

There are different types of threat actors to defend against, with different motivations and different tactics and techniques. Threats come from many sources, including state-sponsored actors and organized crime to combat, and are increasing rapidly, driven by advances such as AI[8].

New types of attacks are on the rise in the EU, including zero-day exploits, while DDoS attacks are getting larger and more complex moving towards mobile networks and IoT. Supply chains, another element of critical infrastructure as evidenced during the pandemic, are increasingly targeted, with incidents growing massively year on year.

According to Orange Cyberdefense, government and public sector is the fifth highest sector for cyberattacks, and also records the highest proportion of social engineering incidents[9]. Further, EU organizations with operations in areas that have ongoing geopolitical tensions are more likely to be targeted by state actors for political reasons[10].

Be proactive

There is a range of actions that can be taken to mitigate threats and pre-empt attacks. In a cloud-first environment, identity and access management are essential. With users all over the EU accessing digital services through multiple applications in multiple environments from multiple locations, it's a bigger challenge to secure, control, track and manage security. A distributed organization means a changed perimeter, so a transition to a zero-trust network access model is advisable.

Secure access service edge (SASE) is also a security approach tailored to the cloud-first world, as it combines cybersecurity and networking in one single entity to help manage more complex access patterns.

The EU has put in place a proactive initiative called the Cyber Resilience Act, designed to establish universal cybersecurity standards that require all devices, from personal smartphones through to essential infrastructure, to meet specific criteria. It requires manufacturers of EU-market products to deliver timely security updates and is the sort of pre-emptive move that modern cybersecurity demands.

Cybersecurity action steps

Four tips to keep keeping infrastructure robust, reliable and resilient:

1. Adopt secure access service edge (SASE), a cybersecurity approach tailored to the cloud-first world
2. Zero trust network access (ZTNA) meets the security needs of distributed organizations
3. Implement multi-factor authentication (MFA) that requires two or more pieces of information to access data
4. Be proactive: anticipate attacks and deploy robust countermeasures before they happen

20%

increase in cyberattacks targeting EU critical infrastructure by 20% in 2022[11]

Case Study

Belgium Federal Public Service of Foreign Affairs upgrades and secures global network

Challenge

- Belgium's Federal Public Service of Foreign Affairs is a network of around approximately 140 embassies, consulates and other entities with over 3,000 personnel
- It supports Belgian citizens and interests on the international stage
- Belgium FPS' legacy WAN was no longer fit for purpose
- The FPS needed permanent high availability global network with secure routing to end users and secure data storage/archiving and lower TCO

Solution

- Fully managed global IP VPN utilizing mix of terrestrial and satellite links – 100 countries
- Optimized, converged WAN (voice, video, data) network with primary line and secondary line (for offloading of non-critical traffic and back-up)
- Advanced services: firewalls, routers, encryption, WAN optimization and managed voice
- ITIL-based 24x7 trilingual service desk
- Secure, NATO and EU compliant network

Benefits

- Reduced costs and TCO
- 140 sites implemented in 100 countries in only six months
- Fully tested complex deployment with no disruption to end-users
- Meets NATO/EU network compliance regulations
- Increased capacity and security with extended geographical reach
- +99.9% average site availability SLA
- High end-user satisfaction levels

Looking ahead: the inevitable impact of AI

While transforming the delivery of digital services across the EU and empowering citizens and businesses, it's important to look to future opportunities. Artificial intelligence (AI) looks set to have a massive impact on everything.

In terms of government service delivery, AI tools could have a profound effect. Solutions like speech recognition, natural language processing (NLP), machine translation, rules-based systems, computer vision, robotics, and machine learning (ML) could all have potentially transformational roles.

They enhance governments' capacity to process massive amounts of data rapidly and accurately, and enable the automation of repetitive tasks like data entry, document management, and file organization, freeing up human resources for more complex work. AI can empower governments to make better-informed decisions and improve service delivery through identifying patterns and trends in data not seen by humans.

New advances like GenAI can help improve the speed and efficiency of service delivery by automating content generation processes, quickly reflecting policy changes, or performing service updates. And at a base customer experience level, EU citizens are now used to using AI-powered virtual assistants (VA) in other areas of life, so why not in public service delivery?

Estonia, for example, has a plan in place to launch Bürokratt in 2025[12], its speech-based and text-based AI virtual assistant. The VA will help citizens access online public services and the goal is to improve user-friendliness and accessibility.There have been recent discussions around AI workloads, and their regulatory implications for sovereignty, data ownership, and transparency, and also the forthcoming EU AI Act. One of the considerations is around Europe's ability to scale and develop a sovereign AI ecosystem. It is another proactive initiative that makes sense if Europe is to effectively manage and benefit from AI.

.

AI governance

To manage the change effectively, governments need to put AI governance agendas in place, potentially overseen by bodies like the private sector's ethical AI boards. A multilateral approach is advisable, with cross-border policies that drives public sector principles like openness, accountability, and objectivity in AI development. Self-regulation by large, monolithic technology companies seems an approach that is fraught with peril, as evidenced by examples of social media companies.

Further, governments lack specialized AI talent able to ensure that AI is developed in ethical, secure and transparent manners, and with a human-centric approach first. There's also a raft of unclear regulation that can hamper development, and prevent governments from being able to adopting AI use cases that deliver the potential value of AI.

There have been recent discussions around AI workloads, and their regulatory implications for sovereignty, data ownership, and transparency, and also the forthcoming EU AI Act. One of the considerations is around Europe's ability to scale and develop a sovereign AI ecosystem. It is another proactive initiative that makes sense if Europe is to effectively manage and benefit from AI.

25.5%

CAGR of AI market in Europe to 2026[13]

$70bn

European spend on AI tools by 2026, up from $33 billion in 2022[14]

Contact Orange

Giovanni Colin

Public Sector Client Partner

Mobile: +32 485 199 365

Email: giovanni.colin@orange.com

Sources:

1. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/opportunity-knocks-for-europes-digital-consumer-digital-trends-show-big-gains-and-new-opportunities
2. https://digital-strategy.ec.europa.eu/en/policies/desi
3. https://awsdigitaldecade.publicfirst.co.uk/
4. https://e-estonia.com/programme/e-government/
5. https://www.nascio.org/wp-content/uploads/2021/10/2021-State-CIO-Survey.pdf
6. https://www.accenture.com/gb-en/insights/public-service/cloud-imperative-public-service
7. https://awsdigitaldecade.publicfirst.co.uk/
8. https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends
9. https://www.orangecyberdefense.com/global/news/research/orange-cyberdefense-releases-security-navigator-2023
10. https://www.forrester.com/report/european-cybersecurity-threats-2022/RES178002
11. https://www.digitaleurope.org/resources/digitaleuropes-position-paper-on-the-proposal-for-a-cyber-solidarity-act/
12. https://commission.europa.eu/projects/burokratt-programme-and-national-virtual-assistant-platform-and-ecosystem_en
13. https://www.idc.com/getdoc.jsp?containerId=US50350723
14. https://www.idc.com/getdoc.jsp?containerId=US50350723

orange™ Business