

O₂ – The UK's only CAS(T)-certified mobile and WAN provider

O₂ is the only provider to achieve CAS(T) certification over both our mobile and Wide Area Network (WAN) infrastructures.

CAS(T) is a security standard defined by Her Majesty's Government. It means our network is measured against strict criteria.

At O₂, the provision of network security is at the top of our priorities. We believe that for public sector organisations to undergo a digital transformation, it is vital they can feel secure in their network provider.

Does your mobile network...

- ✓ conduct stringent penetration testing and systems configuration reviews to reduce vulnerability of all their key systems (known as an IT health-check) as part of an accredited process run by CESG?
- ✓ closely monitor activities on systems that carry your data, or could affect the service you receive?
- ✓ not only closely monitor activities on their network, but also log every event so they can ensure your services remain available?
- ✓ implement physical security measures on all of their network sites to the required government standard?
- ✓ implement secure processes and systems to CESG standards to safeguard their customer data and commercial information?
- ✓ conduct stringent cyber-testing to reduce vulnerabilities and the risk of attack to all their systems used to provide your vital services?
- ✓ check all their staff to the Baseline Personnel Security Standard (BPSS), and also vet their staff to Security Clearance (SC) where necessary?

O₂ is the only network that can guarantee to our customers that we meet the security measures as required by CAS(T), independently verified on an annual basis by an external CESG-approved audit company.

O₂ Gateway is the UK's most appropriately qualified, externally scrutinised convergence platform for official government use.

What's more, O₂ possesses a host of other security-related credentials – including ISO 27001 certification. We're also committed to meeting and demonstrating the three tiers of network principles set out by the department of Government Digital Service (GDS). These cover understanding user needs, ensuring that our services protect data and that they are designed for interworking and flexibility.