

Case Study

Foreign and Commonwealth Office deploys Becrypt Trusted Client to provide secure remote access

The Foreign and Commonwealth Office's key roles vary from supporting British nationals overseas and promoting British business to legalising documents. FCO policy goals cover key issues that the UK faces today – from counter terrorism to climate security – and funding programmes to deliver these policy goals. The FCO's role is to keep Britain safe.

The FCO employs 16,000 staff worldwide, based at 261 embassies. Like many worldwide organisations, the FCO relies upon its IT infrastructure to enable its staff to carry out their key tasks and to ensure effective communications and transfer of information. In addition, as for many organisations, the increasing challenge for the FCO IT department is ensuring that technology continues to be an enabler – helping employees to work effectively both in and away from the workplace.

Supporting secure mobile working

The organisation has recently piloted Trusted Client from Becrypt to provide a solution where employees based at two overseas locations in New York are able to access documents and email while working away from the office. Previously department documents, email and the secure network could only be accessed from computers in the embassy. This meant that staff involved in lengthy debates then had to work late into the evening at the office, in order to file a report back to the UK.

Following a review of user requirements organised by the IT department, the team identified that enabling mobile working was a key priority for employees. The benefits of mobile working were clear as was the need to keep data secure and the network safe at all times.

According to Jayd Davies, Senior Enterprise Architect at FCO; "A review of our current IT infrastructure has highlighted that our legacy systems do not support mobility tools. We also identified that for our overseas colleagues a key requirement was being able to create documents and access email securely and remotely away from the office."

The IT department looked at opportunities to support the need for mobile working whilst ensuring data and network security remained high. The team evaluated Becrypt Trusted Client as a possible solution that would be fast to implement, deliver benefit and, importantly, would give staff mobility whilst ensuring that data and the network were secure.

Cost effective solution

Trusted Client allows remote workers to access their network from an unmanaged PC over the internet, by inserting the Trusted Client USB device and booting up the machine. It allows people to work remotely and securely and addresses the inherent risks of allowing unmanaged connections to an organisation's secure networks and data.

Simply by inserting the Trusted Client device into a USB port and re-booting, a secure environment is launched, providing a user interface, web browser, email access, and standalone applications, all completely isolated from the host PC's hard drive. Trusted Client is fully configurable to each organisation's individual requirements.

Trusted Client enables staff to access documents and information. "We identified that both sites in New York – the Consulate General and the UK Mission to the UN in

FCO use Becrypt Trusted Client as a secure remote working solution and to help to redress work/life balance for busy staff

New York – were possible test sites for Trusted Client,” explained Davies.

Identifying the need

The IT team conducted user workshops to identify the key priorities and tasks in the New York locations that the employees wished to do on a daily basis. These were mainly to create office documents and log onto the secure network to email reports. At the time these tasks, for security reasons, all had to be done from the office.

The FCO in-house technical expert worked closely with Becrypt to develop the design of a solution, based on Becrypt Trusted Client. Following an eight week period, during which the solution was designed, built and tested, the FCO version of Trusted Client – named Firestick – was ready for use. The term Firestick was the result of an in house competition whereby it was voted the most appropriate name, as the FCO IT infrastructure is called ‘Firecrest’.

Positive feedback

Following an initial trial, the second generation of the product was released to enable WI-FI connections. The feedback from users has been very positive.

“We have had a lot of good feedback,” said Davies. “Many staff have said that it has transformed how they work. In

the past they have had to return to the office following long sessions at the UN that lasted 12-15 hours, in order to type up reports and send them back to the UK. Now they have the freedom to work remotely and from home, yet still in a secure way.”

Currently there are ninety users of the FCO Trusted Client solution in the New York offices. The IT team has recently completed a request from the UK’s Representative to the European Union in Brussels to deploy Firestick to them

“Following the business benefits analysis process in which we fine-tuned the design and deployment processes associated with Firestick, we have been able to go live for nearly sixty users based in Brussels in just six weeks,” said Davies.

Future plans

“Trusted Client has provided us with a relatively low cost solution that is straightforward to support. We hope to be able to work more with Becrypt in the future as we identify our future security needs,” said Davies.

For more information please call 0845 838 2050 or +44 (0) 20 3145 1050, or visit www.becrypt.com

Becrypt Limited, 130 Shaftesbury Avenue, London W1D 5EU. www.becrypt.com info@becrypt.com

Becrypt is a leading supplier of innovative Information Assurance solutions and services with operations in the UK and US. Becrypt provides secure, feature rich, out of the box products suitable for all industry sectors, and is the largest supplier of encryption technology to the UK Government, Ministry of Defence and UK Police.

© Copyright 2009 by Becrypt Limited. All Rights Reserved. The Becrypt logo and trademarks are owned by Becrypt Limited. No material may be reproduced for any purpose, private or commercial, without prior written permission from Becrypt Limited.