

Case study

Cambridge City Council

Security boost for remote workers at heart of local government



Why Cambridge City Council turned to two-factor for remote working security

In Cambridge City Council works with central government and local organisations to provide services to the people who live, work and travel in Cambridge, and to maintain the city's historical and contemporary significance as a university town, with strong commuter ties to London.

The residents of Cambridge elect 42 councillors across 14 wards, who are responsible for setting the budget and policy framework in the city. Backing up every decision and policy change is a workforce of hundreds of employees who ensure that any decisions made by the council are successfully implemented at a practical level.

Getting the right balance

In order to ensure that the council's civic responsibility can be met, many of Cambridge City Council's employees need to be in constant contact with the organisations, businesses and individuals of Cambridge, and with colleagues at the Council itself.

This involves taking calls from the public, visiting homes and businesses, coordinating with council members and relaying information back to the council's central system to ensure that data is kept current and comprehensive.

When dealing with a wealth of information regarding such a wide variety of businesses and organisations, however, there is an inherent security risk – any information mishandled, lost or stolen is a potentially damaging security breach, both for the council and those that it works with.

“The Council encourages employees to maintain a good work/life balance, and being able to log on remotely is an important part of this,” said James Nightingale, Head of ICT Client Services at Cambridge City Council. “However, the more remote workers you have, the more the IT security risk goes up – how can the IT team tell users are who they claim to be when logging on remotely?”

Key facts:

- Cambridge City Council was searching for a security solution that would allow staff to work more flexibly and achieve Government Connect compliance
- The token-based options available were expensive to implement and maintain, extremely time consuming, and held inherent security risks
- SecurAccess from SecurEnvoy was chosen as the most secure, most user friendly and most cost effective option, rolled out to Cambridge City Council employees within time and budget



Going CoCo

Additionally, the Council had to prove it was compliant with the Government's GSCX Code of Connection (known as CoCo). CoCo is part of Government Connect – the pan-government programme providing an accredited and secure network between central government and every local authority (LA) in England and Wales. All LAs must be compliant with CoCo's code of practice to prove they have the necessary network security measures in place.

"To comply with CoCo, it was absolutely necessary to have a system in place to make remote access for our employees more secure," Nightingale continued. "Dealing with information from so many different businesses, people and organisations while on the move is the nature of the job, so there needed to be a way to do that as securely as possible."

Weighing up the options

Cambridge City Council began to consider ways in which it could authenticate remote users to facilitate mobile and home working.

A number of other councils around the UK utilise a token-based authentication system, whereby employees pick up a token containing an authentication code that allows them to connect to the system remotely. The main problem facing this option, however, is the time and effort needed to distribute each token to employees.

"The authentication token as a security measure is incredibly time consuming," said Nightingale. "Staff would have to fill out access request forms, then make a physical appointment to come into the council

offices and pick up the token, wasting a lot of time for admin workers and users."

A token-based system also generates a myriad of other issues – the hardware is often lost, they are easily broken, and creating the large quantities of tokens incurs huge expenses. Frequently, tokens were stored with laptops so if the computer was stolen, the authenticator would go with it.

It therefore seemed logical for Cambridge City Council to turn to SecurAccess, which negates the need for tokens by using employees' mobile phones to deliver authentication codes.

The success of SecurEnvoy

"The main goal was to achieve CoCo compliance, while keeping any new systems as user-friendly as possible," said Nightingale. "But in this tight economic period we wanted to do this without wasting council money on unnecessary expenditure."

"The roll-out of the software at the Council was painless – it took just a few days, and employees got used to the system very quickly," said Steve Watts, co-founder at SecurEnvoy. "Everyone has a mobile phone on them most of the time, so receiving text messages with access codes is easy to grasp and the interface is very straightforward to use – even for the least tech-savvy employees."

Cambridge City Council is now compliant with CoCo, and has a secure workforce safely logging in from remote locations. "Ultimately, we've saved money and our systems are more secure than ever, so we've achieved everything we set out to do," concluded Nightingale.



About SecurEnvoy

SecurEnvoy are the inventors of tokenless authentication and provide two-factor authentication via mobilephones. Passcodes are sent to the user's mobile phone in order to access corporate internal networks, cloud based services or private emails.

SecurEnvoy's products - SecurAccess, SecurPassword, SecurCE and SecurMail - are adopted worldwide.

Customers benefit from reduced support time, no database management as existing LDAP servers are used and zero footprint as no token deployment is required, so ROI for organisations is relatively high.

SecurEnvoy distributes through the channel, providing customers the value added benefits of working with

local partners. It has built up a technical and sales

infrastructure that supports most languages and

cultures around the world. Partners include: Juniper, Citrix, Fortinet, Sonic Aventail, Cisco, Checkpoint, Celestix, Microsoft and F5. SecurEnvoy's customers include T-Mobile, Symantec, John Lewis, NHS and Save The Children.

Founded by Andrew Kemshall and Stephen Watts in 2003, SecurEnvoy is based in Theale, Berkshire.

For more information about SecurEnvoy and its products, visit www.securenvoy.com.



SecurEnvoy Ltd

1210 Parkview

Arlington Business Park

Theale

Reading, RG7 4TY

T: +44 (0) 845 260010

E: info@securenvoy.com

W: www.securenvoy.com