


The BMS logo consists of the letters 'BMS' in a bold, white, sans-serif font, centered within a solid purple square.The word 'fingerprint' is written in a white, lowercase, sans-serif font, centered within a solid cyan square.The word 'security' is written in a white, lowercase, sans-serif font, centered within a solid orange square.The word 'unique' is written in a white, lowercase, sans-serif font, centered within a solid purple square.

SentriNET—A CASE STUDY

Fingerprint Security Supports Learning In Camden

Camden City Learning Centre (CLC) opened officially in October 2002 at South Camden Community School. It serves more than 1,000 of the school's students, as well as staff and the surrounding community.

A key issue for CLC manager Anne Casey was the provision of secure, reliable network access for users, many of whom were as young as 11.

Camden CLC was designed as a high-quality information communications technology resource, supporting learning in the London borough as part of the Government's Excellence in Cities initiative. It was equipped with a range of leading-edge facilities, such as powerful Dell workstations, an Internet bar, a video and sound editing room, a video conference suite and electronic whiteboards. It is linked to the Internet by a 100mbs broadband connection.

"Our remit was to use the latest technology to support learning in the borough," says CLC manager Anne Casey. "As we are sited at South Camden Community School, we provide an ideal modern education environment for the students, who range in age from 11 to 18. The students can log on to the school's network from the CLC, so they have full access to their work while they are in the centre." With many young people using the facility, it was important that access to networked and online resources was carefully controlled. Anne and her team needed to ensure that students' work was protected from unauthorised users and that Internet sessions were monitored to prevent misuse.

Conventional security controls based on usernames and passwords had several draw backs. Students forgot their passwords and had to be given new ones, or failed to change them from the default PASSWORD setting, which made life easier for anyone wanting to steal their identities for unauthorised access.

CLC technical manager Colin Small was given the task of finding a reliable, alternative system that would be easy to administer.

"We were already aware of logon procedures that used biometrics to identify users," says Colin. "I did a lot of research into the options available in the UK, and we identified BMS Biometrics as a UK-based company that had the kind of system we wanted."

CLC decided that BMS's SentriNET™ system—which uses fingerprints to identify users – offered the reliability and protection needed. "It's easy to use and it enables us to protect our users' information, and reliably trace the source of all activity on the network," says Colin.

"Another key factor was knowing that the people who were actually working on the products were based in the UK and could come and see us if needed. We have had the MD here three times to talk to us about our needs, and also about the direction in which SentriNET is travelling and what new ideas and products are likely to come out of that. We needed a supplier who would really put in the hours to make the product work for us."

We have an on-site maintenance agreement with them and they are very good at phoning up and asking how things are going. Having said that, I haven't needed to contact them for months, which is an indication of how it has been going."

Security

When new users enrol at the CLC, they are given usernames and their fingerprints are scanned electronically, a process that takes just a few seconds.

SentriNET™ uses a unique algorithm to convert the visual data into digital form. This number – up to 250 characters – cannot be used to recreate an impression of the fingerprint. “It’s a number that only SentriNET can read,” says Colin. “The system doesn’t actually store a copy of the fingerprint, which is reassuring for anyone who has concerns about the civil-liberty implications of fingerprinting.”

Once they are fully enrolled, students can access the system through any one of 120 keyboards equipped with fingerprint scanners. At log-on, a student is prompted to enter a username and is then instructed to place his or her finger against a sensor. If username and fingerprint match, access is granted within a few seconds.

BMS has impressed Colin by the way it has worked with the CLC to integrate SentriNET alongside conventional password mechanisms, which are still in use. “At first we had a few issues integrating the new system, but they have been ironed out now,” he says. Initially the sensors could not read a small proportion of young students’ fingerprints because of the narrowness of their fingers. “The devices were calibrated to an extremely high degree of sensitivity, and a few users’ fingers were not providing enough information to trigger access,” says Colin. “However, the system was simply re-calibrated and that problem has been solved. That’s fairly typical of the way they have worked with us to track issues and smooth out the integration process.”

The algorithm used by SentriNET measures the distance between fixed points on the fingerprint. Although a child’s finger might grow, the ratios between the points will remain the same, so the sensor will continue to recognise the fingerprint. In the three months between September and December 2002, 1,200 people successfully registered as SentriNET users – a tribute to the simplicity and reliability of the system. “Most modern servers could host SentriNET,” he predicts. “It’s very low maintenance, because all the information is centrally held and once the fingerprints are captured, there is no need to update them.”

Solid benefits

Feedback from students has been positive – Colin refers to the `wow` factor. “Most are quite excited about the idea of fingerprint recognition,” “To them, it’s a bit like something out of James Bond.”

“Initially we didn’t set up the sixth formers on SentriNET,” says Colin, “because they had enrolled in dribs and drabs. However, as soon as they saw that other students had fingerprint access, they started asking for it too.”

There are other more solid benefits. The **increased security** provided by SentriNET has made students more conscious of logging off properly when they leave a workstation. Now that no one else can steal their identities by using a written password, they recognise more readily that any blame for someone using a machine they have left unattended will be laid at their door. There is also greatly reduced pressure to change passwords frequently as the system is so secure. “It gives a greater level of security for the students and staff, who know that any areas on the network created especially for them can only be accessed by them,” says Colin.

Children who don’t have English as their first language only have to deal with one piece of information (username) rather than two (username and password). “Some of them are being faced with a keyboard for the first time in their lives,” says Anne, “So you are removing some of the obstacles that might prevent them getting into the system successfully.”

The success of SentriNET has led Anne and her team to consider biometric technologies for other areas of students’ academic lives. One is the school canteen, where a swipe card system for payment has encountered problems. “Lots of students forget to bring their cards into school, or lose them altogether, which incurs a £3 replacement charge,” says Colin. “If we could introduce fingerprint identification, it would remove the need for students to carry cards or cash.” This idea and others, such as face recognition, are for the future. In the meantime, Camden has pioneered a new method of securing network access in educational environments, which promises to point the way for the 80 other CLCs across the UK.

About BMS Biometrics

BMS Biometrics design, develop and market software products for authentication to Networks, Remote Access, Application Databases and the Internet. The software platforms Secure-IT, SentriNET and e-SentriNET are designed for use in all organisations including public sector, corporate clients and SME’s. utilising proven hardware technologies such as biometrics, smart card and PIN-controlled tokens which can be used within the Windows and Novell environment. More information can be found at

www.bmsbiometrics.co.uk

BMS