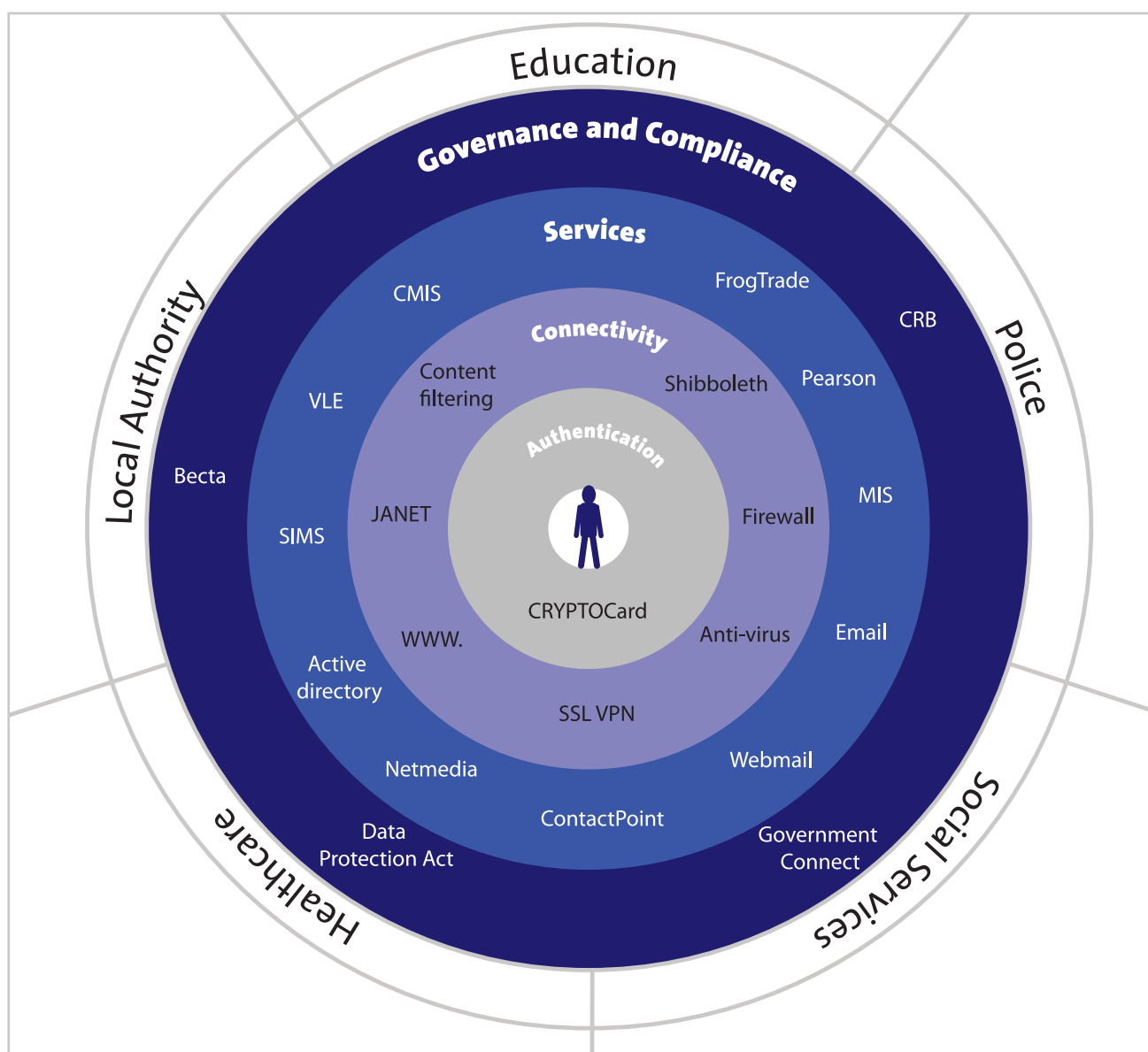


IT Security for Education

A guide to securing data and applications within education, in line with Government guidelines



Introduction

Schools are increasingly using the power of the internet to provide critical services to key education practitioners, such as remote access to school management information systems and online reporting tools.

Additionally, access is required to Government applications such as SIMS and ContactPoint in line with the Government's key 'Every Child Matters' initiative, but given the highly sensitive nature of this data, secure access is tantamount. Passwords are recognised as the weakest link in IT security, as they are easily guessed, copied or hacked, making it far too easy for this information to get into the wrong hands. Therefore Becta have issued some useful guidelines on how to secure these applications against misuse, including the implementation of two-factor authentication, a simple technology that authenticates individual users.

Becta guidelines

Becta published a report in June 2008 named 'Data Handling Procedures in Government', which sets out in detail the procedures that all departmental and public bodies, including schools, should follow in order to maintain security of the data they hold. This includes encryption, protective labeling of sensitive data, audit and logging, operational controls for use of mobile devices, and a range of measures to ensure secure remote access.

Specifically, the following guidelines must be met by September 2010:

- The majority of school management information system (MIS) data is classified as 'IL3-Restricted'. Becta recommends that any systems giving remote access to such data must be protected by two-factor authentication
- Data held by central Government, such as SIMS and ContactPoint, can only be accessed with two-factor authentication
- MIS and central Government data is not permitted for download onto computers, meaning education practitioners rely on secure, flexible access to this data in a live environment at all times, both at work and remotely.

Remote access

Whilst allowing remote access to school applications and resources is fast becoming a necessity in the school environment, various guidelines, best practice advice and legislative requirements exert a strong influence over what could and should be done to secure this access.

Initiatives around online reporting and other applications requiring access to sensitive data are now impacting how schools, educational stakeholders and third parties (for example, parents) access these resources.

Key systems requiring authentication security to mitigate the risk of identity theft;

- Government Connect
- SIMS
- ContactPoint
- Janet
- MIS remote access
- Online reporting tools
- Access to parent and/or pupil web portals



Accessing Key Public Sector Applications with two-factor authentication

There are several key applications that benefit education professionals which require users to identify and authenticate themselves using 'two-factor authentication'. The key applications are summarised below:

SIMS

SIMS helps raise pupil achievement by giving school leaders, teachers, pupils and parents the information needed to make the right decisions about a pupils' learning. This includes tools such as curriculum planners and pupil performance measurement tools, as well as providing reporting tools for teachers to communicate with parents. SIMS also helps tackle truancy or behaviour issues head on and cuts through school paperwork.

ContactPoint

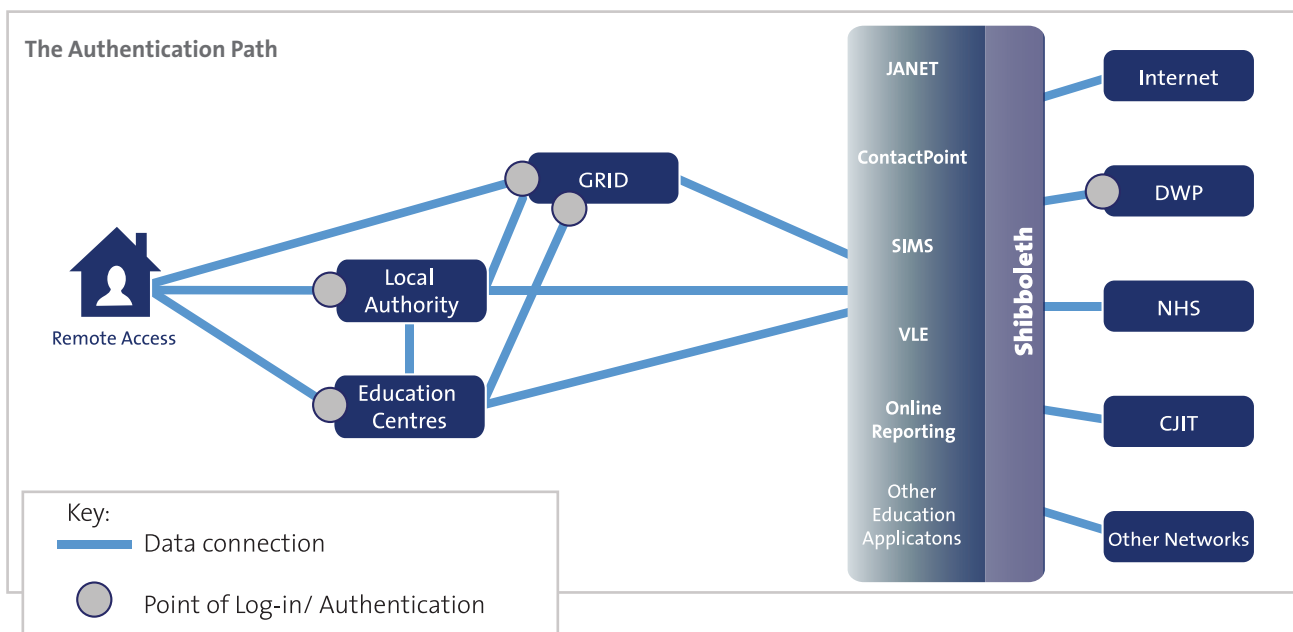
ContactPoint is a key element of the Every Child Matters (ECM) initiative to transform children's services. It is one of a range of tools that helps services work together effectively on the frontline; to meet the needs of children, young people and their families. Access to ContactPoint is strictly limited to trained and vetted practitioners who need access to do their job. This includes those working in education, healthcare, social care, youth justice and some voluntary organisations. ContactPoint holds information such as contact details of the child, their primary carer and any other service providers who have contact with that child.

CoCo (Code of Connection)

The GSCx (secure Extranet) Code of Connection specifies security controls with which local authorities must be compliant before their GSCx circuit can be activated. This applies to local authorities who are connecting directly, or via an aggregated gateway. One of these security controls is the requirement for passwords to meet several conditions, such as containing both alpha and numeric keys, being changed every 90 days, not containing any part of the users account name and not being shared or written down. Two-factor authentication is an easy way to meet these controls.

Online reporting

Schools need to start preparing for online reporting alongside secure remote access requirements, to ensure key practitioners and parents can access online reports in a user-friendly, secure manner. This is also an opportunity for schools to look at how they can use their existing data and systems more efficiently and effectively to share protected information



What is 'Two-Factor Authentication'?

Two-factor authentication is a well established technology that is widely used throughout Government and enterprises to replace insecure static/traditional passwords. It requires two components to validate the identity of a user who wants to be granted access to a database:

- Something you know – a PIN
- Something you have – a token or card which provides a unique 'one time-password'

These two factors combined eliminate the ease with which passwords can be guessed, copied or hacked, thereby ensuring those accessing a network or application are only those who are authorised to do so.

Public sector bodies are increasingly turning to two-factor authentication as the standard for user authentication, to ensure the integrity of the sensitive data they hold.

Key benefits of two-factor authentication

A solution for any organisation, of any size

Within education, there are various organisations and facilities which must implement two-factor authentication in line with Becta guidelines. In some cases Grids for Learning or Local Authorities will implement the solution and cascade this down to school or college level, in some cases schools or colleges will implement this solution themselves, either by choice or necessity. CRYPTOCARD's two-factor authentication solutions can meet the needs of all these organisations and facilities by providing:

- Access to ALL relevant central Government applications requiring two-factor authentication
- The ability to authenticate regional, local or organisation-specific services
- A solution that can be up and running in a matter of hours, or at a later date as required
- No need to enroll through a pre-defined system, CRYPTOCARD can configure the authentication according to specific needs, on a system either based in-house or managed by us

Trusted supplier to the education sector

To date, CRYPTOCARD have over 100 existing customers in both Government and education including Yorkshire and Humber Grid for Learning, Redcar Local Authority and Ashcombe School. Each of these customers had specific needs and preferences for their two-factor authentication, including trials and implementation, server type and token design.

Consultation service

CRYPTOCARD and their Partners recognise the need for a personal service to ensure each implementation meets customer needs and preferences. Partners have been chosen for their expertise in areas such as security, portals, web design and infrastructure. Coupled with CRYPTOCARD's extensive experience in two-factor authentication and in-house sales, technical and management expertise, together we provide exceptional levels of consultation, ensuring each implementation meets customer needs and is implemented with the minimum effort and disruption.



Yorkshire & Humber Grid for Learning Case Study



The Customer

Yorkshire & Humber Grid for Learning (YHGfL) is a regional body consisting of 12 Local Authority members which in turn consist of over 2000 schools and their partners in learning. Along with the other nine Regional Broadband Consortia, YHGfL, based in Scunthorpe, was created to meet the Government target of providing all schools in the region with secure and reliable broadband connections, providing access to licensed content and free resources to schools.

The Business Need

YHGfL offer Local Authorities and Schools within their region a full suite of value-added services including internet access, VPN, webmail, email domains, anti-virus, content filtering and access to school backend systems. Crucially, the Grid also provides access to key central government systems and applications which provide the standard tools for education professionals and students and are increasingly becoming a key requirement for parental access.

YHGfL realised that standard passwords and usernames, the traditional form of user authentication, were not enough to ensure the safety of the data and transactions the Grid provides access to.

The Solution

YHGfL decided to implement two-factor authentication and challenged CRYPTOCard with the task of providing a solution. YHGfL chose a complete solution that consists of a suite of applications designed for implementing and operating strong passwords using two-factor authentication and provides everything required for securing remote access, domain and desktop logon or web portal access with two-factor authentication. The solution also integrated seamlessly with the YHGfL infrastructure.

The solution secures VPN access to the YHGfL infrastructure for over 500 users across 60 schools within the region. This number is expected to grow rapidly due to the Government's mandating of compliance to the Becta standards. To help manage this, the lead administrator at YHGfL manages all users and their tokens, allowing them to apply different levels of authority to which access permissions can be granted.

"We found the solution CRYPTOCard offers to be 50 per cent less expensive than the competitors, it does exactly what we need it to for half the cost."

Andrew Yoward Head of Support Services YHGfL

The benefits

YHGfL found CRYPTOCard's solution offered unrivalled levels of security and usability at highly competitive costs. "We found the solution CRYPTOCard offers to be 50 per cent less expensive than the competitors," says Mr Yoward. "It does exactly what we need it to for half the cost. It protects everything – the network infrastructure and the services infrastructure. We're using it for VPN and system access throughout the network for secure authentication – it eliminates having to rely on static passwords."

YHGfL found the ability to authenticate against multiple active directories a key benefit, allowing them to meet the needs of their many schools, regardless of what directory they were running.

By 2009, 500 tokens KT-1 were assigned to staff including 70% of YHGfL staff, Local Authority staff including IT helpdesk and education staff, and teachers and third party support staff within schools, all of whom need access to central systems and applications holding confidential data. It is against policy to download this data to desktop or laptop computers, now that a solution is in place to ensure staff can access this information anytime, from anywhere.

The future

There are nearly 250,000 potential users within the YHGfL region, 75,000 of whom are teachers. Gaining a significant share of this audience will achieve the levels of security and risk reduction, as well as economies of scale and cost savings, that YHGfL are targeting. Having initially deployed 500 KT-1 keychain tokens, YHGfL is now planning to deploy future tokens in keychain, soft and SMS formats, allowing users to select the token format that best fits their mobility needs. One of the key strategies that YHGfL are adopting is to ensure that the many systems and applications that are delivered and mandated by various Government organizations are authenticated by the same system. Essential to achieving this, YHGfL are looking to become an 'Identity Provider' (IdP), enabling them to authenticate individual users across multiple applications from multiple public sector divisions. One of the conditions of gaining IdP status is to have a credible authentication solution in place, a criteria YHGfL have met by implementing CRYPTOCard's authentication solution.



Product Overview

CRYPTO-MAS

CRYPTO-MAS is a cloud based managed authentication service, offering unrivalled flexibility and service levels. No up-front investment is required as it uses utility model pricing to make it affordable to businesses of all sizes. No infrastructure changes are dictated, it easily fits into a remote access network. There are no ongoing overheads, because all of the management and support is done for you by a service provider.



Token Options

A good authentication system gives you the flexibility to provide the users with the most appropriate form of token. Tokens options are:

- Small hardware devices with a button and screen
- Software based, with an access screen on the computer desktop
- USB smart card based
- SMS based for mobile phones.

CRYPTOCard can extend this choice of token formats to your end users, so they can each choose which token type best suits their needs. CRYPTOCard also offers the most flexible and highly secure password and PIN options when configuring your solution.

BlackShield ID

BlackShield ID authentication server from CRYPTOCard combines a broad feature set that delivers low total cost of ownership. Use of leading edge technology simplifies integration and administration while delivering unrivalled performance. Real-time reporting, a comprehensive security policy, compliance and audit capabilities set it alone in the two-factor authentication market.



CRYPTOCard Overview

Twenty-years of technical achievements have won CRYPTOCard the trust of thousands of organisations in over 70 countries including Apple, Fujitsu, Hampshire Council and Raiffeisen Bank. CRYPTOCard's solutions reduce the risks associated with remote access and web-based processes through strong password security and increase compliance, at a price all businesses can afford. With the best token technology in the industry coupled with the lowest total cost of ownership, CRYPTOCard offers unsurpassed value in solutions for positively identifying individuals through strong password security before giving them access to applications, data and networks. The only company to offer authentication in server-based, managed service and build-it-yourself options, CRYPTOCard provides the most flexible solutions on the market for matching customer's password.



CRYPTOCard



Tel North: 0151 2031400 Tel South: 0118 9071600
Email: Info@castleforce.com Web: www.castleforce.com

