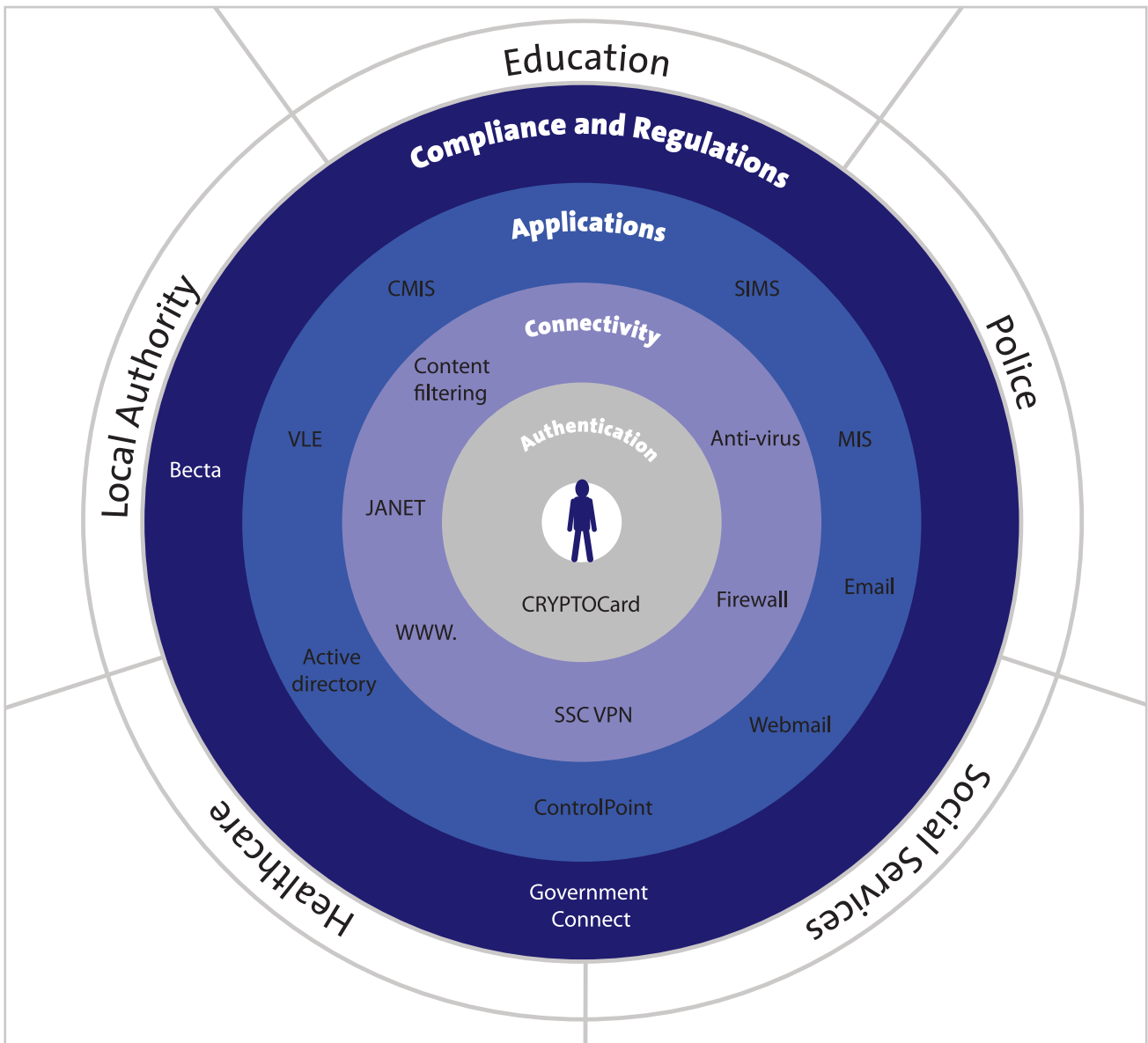


IT Security for Education

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 ControlPoint 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 2009:

- 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 ControlPoint, 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.

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.

CRYPTOCARD offers its clients the ability to initialise their own tokens, so that the unique token seed used to generate the one time password is not shared with an external party.

ContactPoint

ContactPoint is a key element of the Every Child Matters (ECM) programme 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 it to do their job. This includes those working in education, health, social care, youth justice and some voluntary organisations.

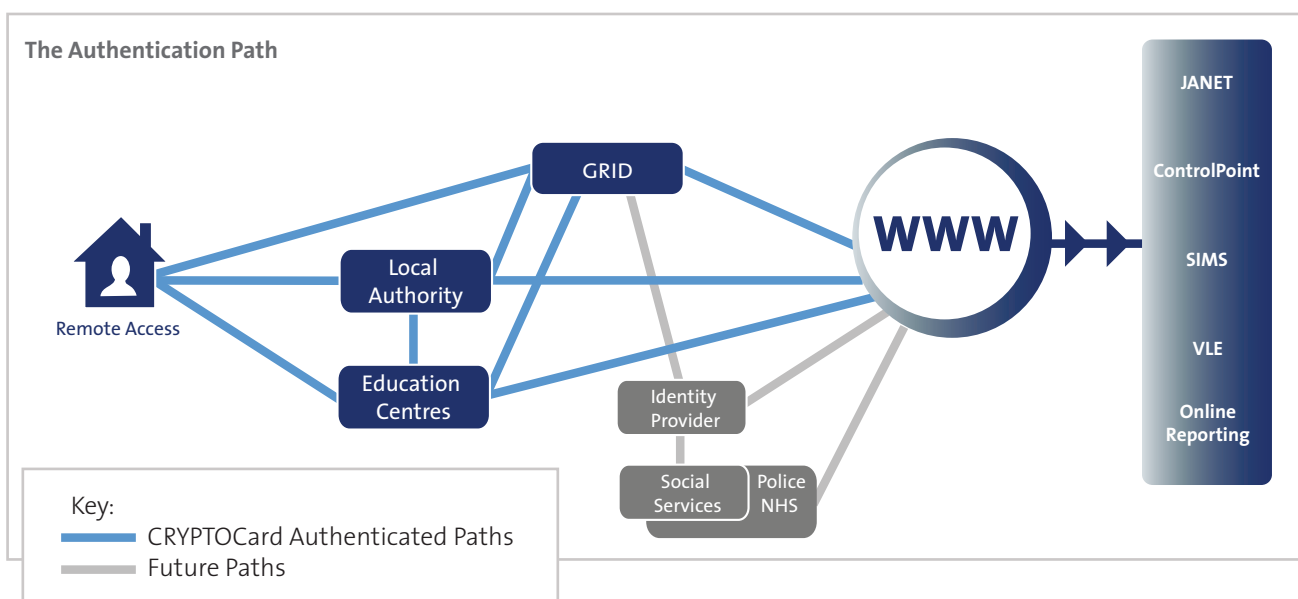
ContactPoint holds information such as contact details of the child, their primary carer and any other service providers who have contact with that child.

CoCo (Code of Connection)

Self-enrolment offers a highly secure deployment option that ensures secure activation of the token by only the intended recipient – irrespective of third party involvement in the deployment process – removing security concerns about insecure token and PIN delivery. There's no need to manually send a PIN and instructions via e-mail, or even to write them on the box in which the token is being delivered! Tokens aren't left 'hanging' and unused until the self-enrolment process is completed or the token is disabled.

Online reporting

Schools need to start preparing for online reporting and consider it alongside the secure remote access requirements. 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 of your choice
- No need to enroll through a pre-defined system, CRYPTOCARD can configure your authentication service to your 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.



Glossary

Becta

Becta is the government agency leading the national drive to ensure the effective and innovative use of technology throughout learning.

Government Connect

A pan-government programme providing an accredited and secure network between central government and every local authority in England and Wales.

Code of Connection (CoCo)

The GCSX Code of Connection (CoCo) is a list of security controls with which ALL LAs must be compliant before their GCSX circuit can be activated. This applies to LAs who are taking a direct connection, or who are connecting via an aggregated gateway.

IL3

Impact level 3 data is restricted to encrypted use only.

SIMS

School Information Management System helps raise pupil achievement by giving school leaders, teachers, pupils and parents the information needed to make the right decisions about pupils' learning.

JANET

Janet is the UK's education and research network.

ControlPoint

Application enabling the sharing of data relating to children across multiple public sector divisions, e.g. schools, social services, healthcare.

MIS

Management information system is based locally (e.g. within a school) holding generic local data, e.g. timetables, teacher proprietary data.

VLE

Virtual learning environment.

2FA

Two-factor authentication is a secure form of password replacement, preventing the risk of hacking and unauthorised entry to IT systems.

Active Directory

Central repository for user details based on a Microsoft platform. Authentication users can be defined according to this directory.

VPN

Virtual private network is a dedicated link between two points, i.e. school and local authority.

SSL VPN

Secure socket layer virtual private network is a secure link, typically between a user and their place of work, e.g. from a teacher's home to the school.



Product Overview

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.



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.

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 Europe

Eden Park
Ham Green, Bristol
BS20 OEB
UK

Tel: +44 870 7077 700
Fax: +44 870 7077 711

CRYPTOCard North America

340 March Road
Suite 600, Ottawa
Ontario, K2K 2E4
Canada

Toll Free: 800-307-7042
Tel: +1-613-599-2441
Fax: +1-613-599-2442

www.cryptocard.com

