

# Digital credentials – a commercial necessity

# Management summary

It has never been more important to protect an organisation's information, yet there are increasing demands for information to be more accessible.

This is especially the case with business-critical applications that connect through the internet.

Most confidentiality breaches occur within organisations, and in most cases, it's the employer who is held responsible. In addition, hacking and phishing are major external threats. This means there are security risks both inside and outside the organisation.

## About this white paper

This white paper discusses how to regain control and implement good security practices by using digital credentials – including the electronic identification of users and hardware across intranets (employees) and extranets (trading partners).

Digital credentials control access, privacy, integrity of information and non-repudiation for organisations. This is achieved using secure encryption methods based on international standards.

In addition to providing comprehensive security measures, digital credentials also address the many regulatory and reporting requirements that organisations need to adhere to.

Specifically, this white paper addresses the issues surrounding the Sarbanes-Oxley Act, Basel II Accord and The Turnbull Report.

Bearing all these features in mind The Royal Bank of Scotland provides TrustAssured, a managed identity service.

The TrustAssured service addresses internal and external security issues. As a Trusted Third Party (TTP), RBS assures the integrity of credentials and provides comprehensive policy and procedures that can mitigate the security risks that all organisations have.

# Contents

<b>Security needs and threats</b>	<b>4</b>
<b>Basic security needs</b>	<b>5</b>
Access control	5
Privacy	5
Integrity	5
Traceability	5
<b>Compliance and legislation</b>	<b>6</b>
The Sarbanes-Oxley Act	6
The Basel II Accord	6
The Turnbull Report	6
<b>Why use digital credentials?</b>	<b>7</b>
The gold standard for identity	8
<b>What can digital credentials do?</b>	<b>8</b>
Signed emails	9
Document signing	9
Secure file sharing/transfer	10
Disk encryption	10
Portal access	11
Straight through processing	11
<b>Simplicity of operation and integration</b>	<b>12</b>
Integration with internal systems	12
So why not develop in-house?	13
<b>Compatibility and standards</b>	<b>15</b>

# Security needs and threats

Organisations face many challenges. Traditional boundaries have become blurred through external sales forces, partnerships with external organisations and employees working from home.

These challenges present security concerns such as threats from traditional hacking, phishing and 'man in the middle' attacks. Protecting your organisation's information has never been more important, yet more people need access to it – a need for porous perimeters, letting information flow freely in and out of an organisation.

The media mostly reports on stories that concern external threats you might face, however, the fact remains that the majority of threats come from within.

According to Gartner Inc., more than 80 per cent of high-cost security incidents occur when data from inside an organisation gets out. Mostly, these leaks occur by accident or through poor business processes.

Whether accidental or malicious, internal security breaches are not being properly addressed. In most cases the employer is held responsible and, as a result, inappropriate emails can result in significant financial penalties.

Systems need to be flexible and able to react to new attacks, always evolving.

It is no longer feasible to simply put up shutters and barriers; this just isolates your company from customers and partners around the world.

You can reduce – or entirely remove – the common threats your organisation faces, simply by implementing fundamental practices. By providing digital credentials to those who use and access your systems, it is possible to solve security issues.

# Basic security needs

Common security needs can be summarised as:

## **Access control**

This ensures that only authorised parties can access your organisation's resources.

Access is no longer restricted to people located inside your offices. It now includes people working from external locations – whether employed by your organisation or not. It even caters for the trend in systems towards straight through processing (STP).

## **Privacy**

This ensures your information remains confidential.

## **Integrity**

This detects any changes to your company information and ensures it is protected, every step of the way.

Unlike access control, which aims to prevent unauthorised access, integrity detects where unauthorised access has occurred and tries to correct it.

## **Traceability**

This ensures that activities within your organisation can be traced and the Who? Where? When? What? is recorded securely.

# Compliance and legislation

US and European legislation has specific requirements on security and integrity of information. Each piece of legislation has an important impact on IT security requirements.

To understand specifically how these regulations can be met, please see page 8.

## **The Sarbanes-Oxley Act**

Sarbanes-Oxley requires you to identify and document how information is collected to build your financial reports.

Your company's financial leaders – the CEO and CFO – must review annual and quarterly reports to ensure all information is complete and correct. These reports must have effective disclosure controls and procedures and must also define how your financial information is stored, managed and communicated.

Sarbanes-Oxley also requires that external public auditors review these procedures.

## **The Basel II Accord**

The Basel II Accord, which took effect in most OECD countries in 2006, set new demanding standards. These seek to ensure financial institutions manage credit, commercial and operational risk, so that capital is available to cover their respective risk exposure.

IT security remains at the core of the strategies developed to meet the Basel II requirements. Many of the operational risks defined by the new Basel Accord concerns access to computer data by people.

## **The Turnbull Report**

Following acceptance of the Turnbull Report's recommendations, there is now a legal requirement for directors of listed companies to assess and reduce the risks their company faces – including IT security risks. As a result, IT and information security have become an important corporate governance and compliance issue, and the collective responsibility of the Board.

# Why use digital credentials?

Many vendors have solutions that patch part of the security risk you face, using a variety of tools and processes. Generally, these tools only solve a small part of the problem and can be incompatible with one another – or at least difficult to deploy together.

The gold standard of security for many years has remained digital credentials, based on the x509 v3 standard. These have a proven pedigree, providing security based on mathematically-proven algorithms\* with full legal support.

These certificates can:

- authenticate the identity of a person, or machine, performing an action
- ensure the integrity of the information
- ensure the action cannot be repudiated at a later point
- guarantee the information is protected from prying eyes.

Digital credentials, backed by a TTP, will give you a comprehensive solution to your security problems and can seamlessly grow with your external partners.

When you need to be certain as to the identity of people or systems you interact with – including employees, contractors and third party organisations – digital credentials provide this.

You can access all your systems and reduce the overheads of managing different identities across multiple systems. Also, helpdesks will no longer be burdened with numerous password reset calls, which saves time and means the IT department can concentrate on adding value to your business rather than fire-fighting.

In turn, this provides you with the confidence to grant secure online systems access to your customers, while remaining confident the risk is controlled.

Allowing customers access to your systems also reduces your administrative burden – self-service operation pushes costs outside your business and back onto the customer, increasing your margins.

\*Details of how the algorithm works is outside the scope of this paper. Background to the algorithm can be found in Applied Cryptography by Bruce Schneier (ISBN 0-471-11709-0), which has several in-depth chapters on this subject.

### **The gold standard for identity**

To understand why digital credentials are the gold standard of security, weaknesses with other solutions must first be explored.

All other security solutions – from simple username and password combinations through to secure ID style hardware tokens – rely on shared-secrets. Put simply, this means an authorised user would need to have access to secret information you hold.

This is not to say that all shared-secret systems are the same. It is possible to implement good shared-secret systems – but with care, and at a price.

The flaw with shared-secret systems is that you must have a central repository of shared-secrets. This makes your company a magnet for hackers and phishing attacks.

Through clever mathematics, digital credentials remove these weaknesses.

With digital credentials, you hold publicly available information about users – the user's digital certificate. The users make use of secret information (their private key) to prove their identity. They are able to do this without ever exposing the private key to anyone else. In fact, with modern operating systems, the users themselves may never actually see their private key.

You can validate that the user is genuine by using publicly available information in their certificate. This proves that the only person who could have sent the information had access to the private key. You do not even need access to the user's private key to do this.

## **What can digital credentials do?**

As previously discussed, digital credentials provide you with a ubiquitous security solution.

This section highlights some key examples of how you can use digital credentials within your organisation.

## **Signed emails**

Business today runs on email, yet there remains a basic presumption that anything written in an email cannot be relied upon. This is highlighted by the layer upon layer of disclaimers attached to the bottom of many companies emails.

Digital credentials secure these messages – simply and easily.

Firstly, the email itself generates a digital signature, which allows a recipient to validate two key features:

- who the sender of the email actually was
- that the email has not been changed since it was originally sent.

These alone add genuine security to email, but digital credentials go one step further. By making use of the recipient's credential the message can be further protected:

- the email is encrypted so no one sees the contents
- the only person who can decrypt the email is the recipient.

As a result, you have complete confidence over the privacy of your organisation's information.

## **Document signing**

Signing documents is familiar to anyone who has worked in an organisation. The paperless-office myth disintegrates the moment signatures are required.

From simple holiday requests that need line-manager authorisation, to purchase orders requiring sign-off from multiple members of management, the need for paper seems endless.

This is another area where digital credentials deliver immediate benefit to an organisation – through use of legally binding digital signatures.

Using digital credentials, a digital signature is created around a document, capturing information such as what was agreed, by whom and when. This digital signature is then attached to the document, stored as an audit trail in a separate database or both.

Multiple electronic signatures are possible on the same document. This means that command chains currently implemented on paper can be done electronically.

The cost savings are significant. Fewer printers, less paper, more storage space and faster processes result in benefits which can then be passed onto your customers and staff.

### **Secure file sharing/transfer**

As with email, documents and files which contain sensitive company information are open to prying and hacking. Often, these are sent – both internally and externally – without realising that your company’s reputation could be damaged should information fall into the wrong hands.

Digital credentials are used to encrypt files, making them unreadable to outside parties. Financial findings, audits and other sensitive information are sent in the secure knowledge that they are marked ‘for your eyes only’ and can only be opened by the desired recipient(s).

### **Disk encryption**

Most companies store information in files that are scattered across local servers and hard disks. With the proliferation of laptops and USB memory sticks, this information has never been more scattered – or more at risk.

One strategy is to restrict storage of information onto central file servers, which are then controlled by the IT department. Most have supporting stringent access requirements, which can frustrate a user’s ability to do their job. For example working from home becomes impossible.

Again, digital credentials can help. Complete disks or selections of files have strong cryptographic protection applied to them. By making use of key recovery techniques, organisations are also protected against provisions of the Regulation of Investigatory Powers (RIP) Act 2000.

Digital credentials also ensure you can recover information when employees leave your organisation.

### **Portal access**

It can be difficult to remember all the different username and password combinations which are needed in business today.

Again digital credentials help to resolve this, often in a far more seamless manner than other technologies.

Most people are familiar with the SSL (Secure Socket Layer) method of securing websites. If not, most people at least know to look for the trusted padlock symbol appearing at the bottom of web browser windows.

What you might not know though, is that SSL is based on digital credentials, and that the SSL protocol can support authentication of both sides of the transaction.

This means that digital credentials can be used to authenticate access to online portals. After doing so the standard SSL protocol ensures the privacy and integrity of the network link.

### **Straight through processing**

The previous sections identified the low-level processes that are delivered efficiently with digital credentials. Even when used in this limited way, your business processes are optimised without significant changes to your existing infrastructure.

Enhanced benefits from digital credentials come when they are used to optimise processing flows within your organisation.

The above sections concentrate on removing the source of paper from within the organisation. These improvements assume that signatures are generated in documents by users, and those documents are read and processed by other users.

Validating these signatures and certificates through an automated online process allows internal flows to be optimised. The result is being able to remove the steps in a process which add little or no overall value.

With electronic signatures, produced using RBS digital credentials, you can easily automate processes. This leaves you free to handle the exceptional conditions that make best use of your time, rather than wasting your time passing different forms around your organisation.

All optimisation can be done secure in the knowledge that these credentials are compliant with the important EU directive 1999/93/EC on electronic signatures.

# Simplicity of operation and integration

This paper shows how digital credentials have long been held as the gold standard for security. It also demonstrates their flexibility in solving many different business problems, many of which are seen as 'out of the box'.

However, digital credentials are not the prevalent security standard in the market, which might make you wonder whether they have drawbacks.

Historically there has been a significant problem in deploying this solution. This has not been based on technical complexity, but lies in the complex policy which underlies the credential.

As you will see, the RBS TrustAssured service takes all of this into account.

## **Integration with internal systems**

Implementation in your business is as simple as providing you with administrator credentials, which gives you the ability to request secure digital credentials whenever you need them. With the exception of your administrators, no special software or hardware is required.

Of course, the usual debate is that an in-house solution would be more flexible and responsive to your needs. The RBS TrustAssured architecture is designed to deliver ultimate flexibility – quickly and easily.

All credentials are based on the common x.509v3 standard, which means integration with modern operating systems and applications such as Adobe, Microsoft and Outlook can be seamless.

### **So why not develop in-house?**

Since credentials are based on the x.509v3 standards, and because integration with different applications is so straightforward, you might think your internal IT department should just implement their own PKI infrastructure. Especially since Microsoft provides a Certification Authority bundled alongside Windows 2003 server.

Unfortunately, implementing successful PKI schemes is not simply a technical problem. In fact, technology is a very small part of the solution.

If you would like to use your credentials in a wider community – now or in the future – you will need a TTP to act as an independent body. A TTP undertakes roles such as the reliable registration of a business and its users, secure generation and delivery of credentials and additional administrative functions, e.g. time stamping.

You also need to bring external auditors into the process to ensure you are compliant with the following policies:

#### ***The Certificate Policy (CP)***

This sets out the overarching policies for your use of digital certificates, now and in the future, and defines the foundation policies that govern the successful deployment of a PKI system.

#### ***The Certification Practice Statement (CPS)***

This defines the processes and procedures governing the operation of the PKI, including the life-cycle of certificates issued from it.

For the certificates to have any value, all subsequent operations must adhere to this. Define this too loosely and the security of the PKI is compromised; too tightly and you won't be able to operate effectively.

#### ***PKI Disclosure Statement (PDS)***

This restricts what users are permitted to do with different certificates issued from your PKI. The statement 'these are the things you can do with this certificate' is provided. Whoever receives a certificate from you needs to understand what they are receiving and what it means to them.

#### ***The Relying Party Agreement (RPA)***

This defines what recipients must do to check the validity of the certificate and the level of trust they can place in it. This is important to the integrity of certificates and associated liabilities.

Additionally, there are terms and conditions that explain what you agree to in your use of certificates.

With a home-grown PKI system, you must address each of these areas in order to create trust in the credentials you are providing, whilst also ensuring liabilities are covered. Each relying party must understand what your certificate means to them and why they can trust it.

These policies need to be written and overseen by your operations and technical departments, your internal lawyers and possibly even external counsel. They then need to be propagated to the organisations that will rely on your certificates. All of this needs to be done in a manner that doesn't tie you into a technology solution, and allows your use of certificates to grow and evolve over time.

**Get any element wrong and any digital certificate you create and send is not worth the paper it isn't written on.**

Finally, you need to set up your Certificate Authority (CA) (which again needs external auditors to oversee) and back up the root keys in a secure manner. Only then can you start issuing certificates.

Your staff will need to support the CA throughout, which is a specialised skill in its own right.

This is where the RBS TrustAssured service can help. As a TTP, we provide you with a complete solution. Not only that, you also receive the practices and policies which assure that the highest levels of trust can be placed on these credentials.

Before RBS credentials are generated, each organisation is reviewed using the official FSA regulated Know Your Customer (KYC) process. This ensures that anyone receiving information with RBS digital credentials attached can see that your organisation has been independently identified. By understanding these processes, you can easily access the levels of confidence based upon the integrity of the party providing the service.

Banking is a trust-based industry and there are few organisations which have as much experience as RBS. We have been providing trust to customers since 1727.

It is worth noting that the payment clearing system in the UK is secured using digital credentials and PKI technology, with a large section of the BACS community running on credentials managed by RBS.

The experience we have gained from providing these services allows us to offer you a painless solution in deploying digital credentials. We provide every element concerning policies and practices – quickly and efficiently – and these are embedded features within our managed service.

# Compatibility

The table below lists which products are compatible with the RBS TrustAssured service. This list is not exhaustive so please check specific versions, operation and integration against manufacturer documentation.

Company	Product	Company	Product
<b>Popular desktop applications</b>		<b>Gateways &amp; firewalls (continued)</b>	
<b>Adobe Systems Inc.</b>	Adobe Acrobat	<b>BlueSocket</b>	BlueSocket Wireless Gateway Family
<b>IBM Lotus Development Corporation</b>	IBM Lotus Notes	<b>Check Point Software Technologies Inc.</b>	Firewall – 1 VPN – 1 VPN – 1 NG
<b>Microsoft Corporation</b>	Microsoft Office XP Microsoft Outlook/Outlook Express	<b>Cisco Systems</b>	Cisco Aironet Cisco IOS Firewall Cisco IP Telephony solutions Cisco Routers Cisco Secure VPN Client PIX firewall VPN 3000 Series Concentrator VPN 5000 Series Concentrator
<b>Novell, Inc.</b>	GroupWise	<b>Citrix Systems, Inc.</b>	Citrix Extranet VPN
<b>Servers &amp; OS</b>		<b>Computer Associates International Inc.</b>	eTrust Directory
<b>Adobe Systems Inc.</b>	Adobe Form Server	<b>Critical Path</b>	CP Directory Server CP Meta-directory Server
<b>BEA Systems Inc.</b>	BEA WebLogic Server	<b>Data Connection Limited</b>	DC-Directory
<b>IBM Corporation</b>	HTTP Server IBM Client Security Software	<b>DataCert</b>	ShareDoc
<b>IBM Lotus Development Corporation</b>	IBM Lotus Domino Directory Server IBM Lotus Domino Certificate Authority IBM Lotus Domino Enterprise Server	<b>DataPower Technology, Inc.</b>	XS40 XML Security Gateway
<b>Microsoft Corporation</b>	Microsoft Active Directory Microsoft Certificate Services Microsoft Exchange Server Microsoft Internet Information Server (IIS) Microsoft Office SharePoint Portal Server 2003	<b>DigiStamp</b>	SecureTime API Toolkit
<b>NEC Corporation</b>	Enterprise Directory Server	<b>F-Secure Inc.</b>	F-Secure VPN+
<b>Novell, Inc.</b>	eDirectory iChain Novell Modular Authentication Service (NMAS)	<b>Fortress Technologies</b>	NetFortress M-series
<b>Oracle Corporation</b>	Oracle Advanced Security Oracle Internet Directory (OID)	<b>Forum Systems</b>	Forum Sentry 1500 Series
<b>Sun Microsystems</b>	Sun Java System Portal Server Sun One Directory Server	<b>Intel Corporation</b>	Intel NetStructure VPN Gateway
<b>Tivoli, an IBM company</b>	SecureWay Directory	<b>Lucent Technologies</b>	AccessPoint Family
<b>Gateways &amp; firewalls</b>		<b>NCipher</b>	netHSM nShield
<b>Alcatel</b>	PermitGate Enterprise VPN	<b>Nokia</b>	CryptoCluster Family Nokia VPN
<b>Avaya</b>	Avaya VSU Gateways	<b>Nortel Networks Corporation</b>	Contivity VPN Switch Family
<b>Aventail Corporation</b>	Aventail EX – 1500	<b>Red Hat</b>	Stronghold
		<b>SendMail, Inc.</b>	Secure Switch
		<b>Siemens AG</b>	DirX

The Royal Bank of Scotland plc is authorised  
and regulated by the Financial Services Authority.

**The Royal Bank of Scotland plc**  
Registered office: 36 St Andrew Square, Edinburgh EH2 2YB  
Registered in Scotland No. 90312

RBS87431 11/07  
644353