

The evolution of strong authentication

Towards a future of ubiquitous, secure digital identities

September 2009

Strong authentication technologies have long been used for providing an extra layer of assurance that an individual accessing computing resources is who they say they are. However, the cost of deploying and managing such systems, including the provisioning of hardware tokens and the strain on helpdesk resources dealing with lost tokens or forgotten passwords, has made their use expensive and complex. New authentication models, however, are changing all that. Key developments include next-generation authentication servers that automate all tasks involved, and services provided in the cloud. New authentication methods such as software, SMS and BlackBerry tokens are further taking the costs out of the use of strong authentication and opening up its use to a whole new range of possibilities.

Fran Howarth
Quocirca Ltd
Tel: +31 35 691 1311
Email: fran.howarth@quocirca.com

Clive Longbottom
Quocirca Ltd
Tel: +44 118 948 3360 ext 200
Email: clive.longbottom@quocirca.com



An independent report by Quocirca Ltd.

www.quocirca.com

Commissioned by CRYPTOCARD

quocirca

The evolution of strong authentication

Towards a future of ubiquitous, secure digital identities

As a technology, strong authentication is coming of age. Authentication systems have evolved so that the new generation of technologies automate all processes involved to remove the costs and complexity involved. New cloud-based services are now emerging that will develop into open authentication platforms whereby users can authenticate themselves once to access a range of services in a highly secure manner. Combined with industry standards, these platforms herald a future where strong digital identities will be provided for everyone for all services.

- **Sensitive corporate and personal information is of value to criminals**
With data losses becoming everyday news, there has never been a stronger imperative to secure sensitive information. To prevent data falling into the wrong hands, governments and industry standards bodies are increasingly mandating that stronger security controls be used to protect data. The use of strong authentication removes uncertainties as to who is accessing what information.
- **Strong authentication systems have evolved to remove the complexities and costs of deployments**
The current generation of server-based authentication systems provide centralised management capabilities that automate all of the tasks involved in strong authentication rollouts, removing the complexities and costs associated with manual processes and reducing the burdens on help desks through provision of self-service capabilities.
- **New services using cloud-based delivery models open up the playing field**
Subscription-based services, provided in the cloud, place strong authentication services within the reach of even the smallest organisation and are especially suited to today's economic climate where capital expenditures are being slashed, since no upfront software or hardware investments are needed.
- **New authentication methods cover a wider range of needs**
Hardware tokens provide high levels of security, but are expensive to purchase, distribute to users and manage on an ongoing basis. New types of authentication form factors are now available as software tokens, SMS tokens or even non-token-based authentication methods. These allow strong authentication to be extended to a wider range of environments, including mobile devices, and online portals and collaboration tools for increased productivity and security.
- **The evolution to open authentication platforms will herald a new era for digital identities**
Open authentication platforms that accept authentication methods from any technology vendor or service provider will see strong authentication come into much more widespread use among organisations, their customers and individuals for identity and access assurance across a wide variety of online services. Incorporation of industry standards such as the security assertion markup language (SAML) will see the promise of federated identity realised, requiring just one authentication event to access a range of services.

Conclusions

Strong authentication is not a new approach for removing the uncertainties of who is accessing what information and has always provided higher levels of security than the use of user name and password combinations alone. However, such technologies have evolved a long way from the manually intensive implementations of yesteryear. Now, efficient, fully automated systems have cut much of the cost and complexity of deploying such technologies and new cloud-based delivery models provide the ability to cut bottom-line costs yet further—something that is essential for many resource-strapped organisations facing today's economic realities. Further evolution will see cloud-based platforms opened to a wider range of constituents and, combined with new authentication methods, will provide the potential for a future where secure digital identities will be available for all users across all communications channels.



Contents

1. INTRODUCTION	4
2. THE EVOLUTION OF SERVER-BASED MANAGEMENT SYSTEMS	5
3. THE ADVENT OF MANAGED AUTHENTICATION SERVICES IN THE CLOUD	6
4. NEW FORMS OF AUTHENTICATION TOKENS EXTEND FLEXIBILITY	8
5. THE FUTURE OF AUTHENTICATION: THE PROMISE OF FEDERATED IDENTITY	10
6. CONCLUSIONS AND RECOMMENDATIONS	12
7. APPENDIX: THE DRIVERS FOR USE OF STRONG AUTHENTICATION	14
ABOUT CRYPTOCARD	16
ABOUT QUOCIRCA	17



1. Introduction

Today we live in a digital age that is characterised by the use of technology that allows for a high degree of mobility and collaboration, with the use of computers almost ubiquitous in some parts of the world. However, this reliance on technology has brought with it new challenges, not least of which is the explosion in the amount of data that is produced electronically and that needs to be managed, stored and secured.

“223 million records containing sensitive material have been compromised since 2005.”

Much of this information is extremely valuable—both to the individuals and organisations that produce it, as well as to criminals looking to steal data such as personal details, intellectual property or business records for financial gain. According to Data Breach DB, a clearing house for data breach information, more than 223 million records containing sensitive material have been compromised worldwide since 2005. As a result, industry standards bodies and government regulators are forcing organisations to comply with regulations that enforce higher data security standards, with some demanding that organisations that suffer a security breach that could compromise the personal identities of individuals notify those individuals concerned.

Among the most important security controls that organisations can implement for countering unauthorised access to information that can lead to problems with information, and even identity theft, is the use of stronger forms of authentication for users wishing to access applications and networks. Stronger authentication generally refers to the use of additional factors of assurance, such as something a user has in their possession or an identifier that is unique to them. Authentication based on something the user has can be done with tokens, or with USB devices or smart cards, whilst basing decisions on something unique to the user includes the use of biometric identifiers. Most additional form factors for authentication incorporate one-time passwords that are good for one authentication event only—making their capture by a hacker useless. By using security tokens for authentication, problems with weak or easily forgotten passwords as the only form of authentication can be overcome, providing much higher levels of identity and access assurance to sensitive information.

Strong authentication technologies have been available for some time and have proved their worth in terms of added security. However, they have generally been costly and complex to deploy and manage. The costs involved include the procurement and distribution of the hardware tokens themselves, as well as the costs of administering the system and the workloads on help desks caused by users with problems such as lost tokens. This has meant that the use of strong authentication has, in large part, been restricted to large organisations that have the budget and resources available for deploying and managing rollouts to large user populations.

However, much of this has changed. This paper explores the way that strong authentication systems are evolving, from the current generation of efficient server-based systems with centralised management capabilities, to new cloud-based models that provide authentication as a utility subscription model. It discusses how methods of authentication continue to evolve to provide secure identity and access control in a wider range of environments, including mobile devices, and paints a picture of the future promise of secure digital identities for all. It highlights key action points for organisations to consider in terms of their selection of which authentication options are best suited to their needs.

“Standard passwords offered us zero protection against hackers, ID theft, shoulder surfing or other malicious threats.”

Ware Adams, DC Energy

2. The evolution of server-based management systems

Main findings:

- Next-generation server-based authentication systems remove the complexity and hidden administrative costs to provide highly secure identity and access assurance
- Such systems integrate with other technology controls in place to provide secure access to all resources in an organisation
- Reporting and logging capabilities for all events provide help for organisations to ensure that security controls are effective and aid in compliance efforts

In many large organisations, strong authentication has been used from the mid-1990s in the form of security tokens that provide one-time password capabilities in order to boost security controls over who is accessing what resources. Originally, the most common use was for authenticating a user remotely accessing the corporate network via a modem. However, early solutions did not scale well to large user numbers, and many organisations baulked at the cost and complexity of managing early two-factor authentication products, including the provisioning and management of what tokens were issued to which users. In early implementations, the most common tool used for managing two-factor authentication rollouts was spreadsheets, which are notoriously error-prone, and which can be altered by anyone who can access them, meaning that it is hard to define which is the most reliable version. Spreadsheets are also hardly real-time, and entries can grow to unmanageable proportions for organisations with large user populations.

Over time, server-based authentication management systems came onto the market, centred on an authentication server with a management console, that do much to remove the complexity and hidden administration costs of such deployments. Systems available today are designed to provide integrated, streamlined authentication and access control processes across an organisation and many can scale to handle millions of users. The authentication server automates the provisioning and de-provisioning of users and their authentication credentials, which eases administration and management, enables authentication policy enforcement, and helps organisations meet security and compliance goals. This is achieved through reporting and auditing of all authentication events by user or token, as well as activity in terms of what information was accessed, which can be examined for suspicious behaviour and compared against set policies. The burden of management is delegated in systems that provide a user self-service portal for performing authorised tasks such as self-provisioning of tokens, personal identification number resets and new token requests.

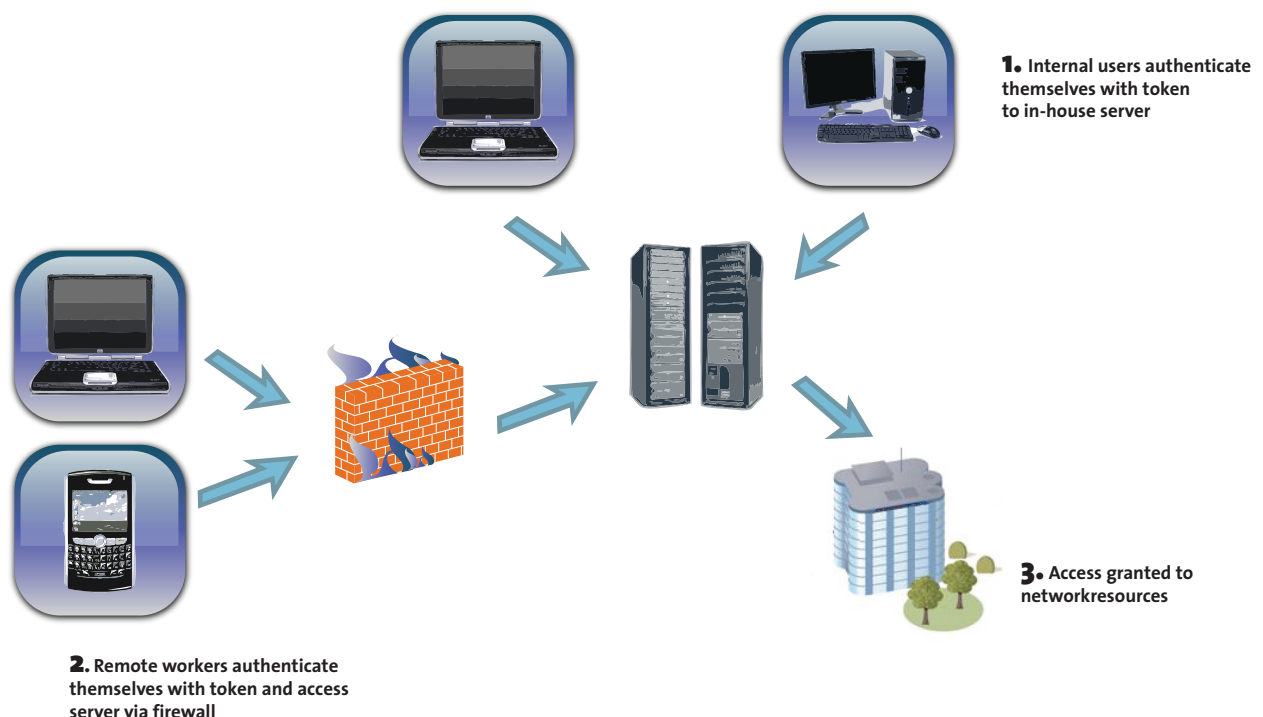


Diagram 1: Server-based authentication systems

A feature of good authentication systems is that they are designed to reduce the number of authentication methods a user must employ across the numerous systems and applications for which access is needed. This is achieved by natively integrating with other technologies already in use in an organisation, including directories, databases and all flavours of operating systems in order to securely control access to all areas and content.

3. The advent of managed authentication services in the cloud

Main findings:

- New cloud-based services, provided as a utility subscription model, mean that authentication can now be achieved simply and for low cost, making it affordable for even the smallest or most distributed of organisations
- Cloud-based services slash the need for capital expenditures as services can be procured as regular monthly operating expenses
- The use of the cloud-based delivery model provides the benefits of having services provisioned and managed by experts, backed up by stringent service-level agreements that incorporate high levels of security and that guarantee service availability

On-premise, server-based authentication systems continue to be popular, especially among organisations with large user populations, or where security or regulatory concerns are given such a high priority that organisational security policies demand that data is kept in-house.

However, they are no longer the only option. Technology continues to develop, enabling greater flexibility in terms of mobile working and distributed computing, which has been enabled by the growth of the internet and other public, as well as private, networks. The latest paradigm shift in technology is the advent of the cloud computing model, in which dynamically scalable resources are provided as a service via secure remote data centres in the cloud.

The cloud-based computing model grants access to managed applications and services, generally provided as subscriptions with pricing models linked to simple metrics such as the number of users served, the range of services consumed, or the performance requirements for the application. As opposed to the traditional licence model used for software applications, a subscription model for accessing such services in the cloud reduces the need for incurring

expenses such as the upfront investment required for purchasing software licences and hardware to house the applications. This is a particular bonus in hard economic times when budgets are being squeezed and capital expenses, in particular, are coming under greater scrutiny. With an on-demand model, subscriptions can be paid for out of operating budgets and the number of subscribers can be scaled up or down as required to meet demand.

The simplicity and low upfront costs of subscribing to a managed authentication service open up the possibility of using such services to a wider range of organisations that lack the budgets and resources required to deploy an in-house, server-based system. The use of cloud-based services provides smaller companies with the benefits of having services provisioned and managed by experts, backed up by stringent service-level agreements that incorporate high levels of security and that guarantee service availability. By putting security in the hands of a third party, users of managed services can benefit from enterprise-class service level agreements, including the provision of automated backups, real-time analysis of

“The recent economic climate has driven many of our customers to consider adding remote access to their networks to increase efficiency, and the delivery of reliable and secure remote access infrastructure is critical to every business we work with. In our view, the integration of two-factor authentication should be mandatory for a remote access network.”

Mike Pencavel, Control Key

events, online reporting, maintenance of databases, and authentication management and enforcement—all of which ease the burden of providing and managing authentication services considerably. This puts smaller companies on the same level playing field as their larger counterparts.

Managed authentication services are also attracting many larger enterprises and government agencies, sometimes for particular branches or divisions of their organisations. For larger organisations, the use of cloud-based services will be beneficial, especially where they have large numbers of users requiring remote access to the network, for which a cloud-based managed authentication service is especially suited.

The outsourcing of key operational and resource-intensive elements of maintaining and supporting an authentication server can dramatically reduce the long-term cost of ownership calculations that many enterprises are now looking closely at in terms of their existing authentication installations. Recent reports show that organisations are expecting to reduce IT costs and improve IT operational effectiveness through outsourcing and adoption of software-as-a-service models.

The ability to readily support large volumes of dispersed users and to rapidly scale up the number of users served is especially topical given, on the one hand, economic and environmental pressures to reduce unnecessary travel and, on the other, increasing awareness of the importance of full-spectrum business continuity plans that include the ability to support widespread and long-term forced home working models. This has been something that has been on business agendas since the SARS outbreak of 2002, which was defined as a “near pandemic”. Today, the spectre of swine flu is one for which organisations should prepare. In July 2009, the director general of the British Chambers of Commerce was quoted as saying: “Home working should be considered as one potential way for businesses to reduce employees spreading swine flu.”

By subscribing to an on-demand managed authentication service, organisations can ensure that they are prepared for such an eventuality as a major flu outbreak in their area—or any other disaster occurring, whether that be a natural

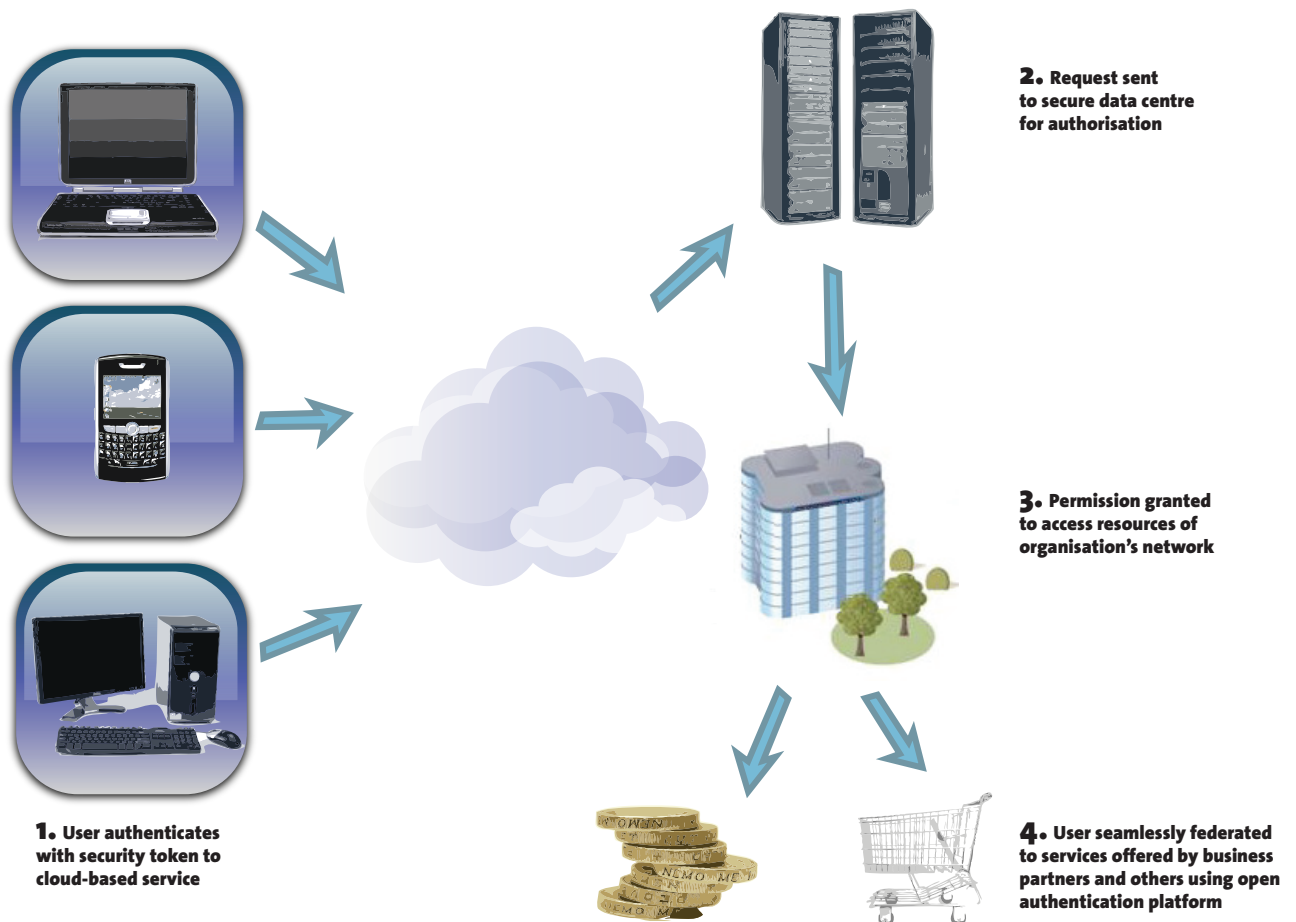


Diagram 2: Cloud-based authentication systems

disaster, such as flooding, or a terrorist attack—that would prevent large numbers of employees being able to get to the office. Organisations can prepare themselves for such an eventuality by ordering security tokens to be provisioned to users that need them in advance. Then, when a disaster strikes or workers are sent home, an organisation can request that the service is turned on and employees can immediately use their tokens for accessing the corporate network remotely. This has major benefits for any organisation in terms of its ability to weather the storm and keep the business running.

Case study: DC Energy

Headquartered in Vienna, Virginia, DC Energy is a quantitative trading firm, offering targeted analysis of markets within the energy field for its customers. To do this, its 55 employees require real-time access to market information to quickly deliver information and check on changing market conditions.

For DC Energy, it is vital that the integrity and confidentiality of data is maintained since the value of the company is directly related to the uniqueness of the data held in its technology systems, making it vital to know who is accessing what. Because of the need for high security, it realised that user name and password combinations alone were nowhere near sufficient for its needs.

The firm initially looked to implement an on-premise server-based solution, but realised that this would be a burden to set up and maintain owing to lack of resources and time required, and because monitoring was required 24x7.

In late 2007, DC Energy decided to implement CRYPTOCard's MAS management authentication service which, according to Managing Director, Ware Adams, was implemented "literally over lunchtime" and for which virtually no ongoing support has been required. Another key point about use of the service is that, since implementing the service, DC Energy had grown by almost 40% and has had no hitches in expanding the scale of the service for new users as they come onboard. All in all, the experience has been a positive one, and one that DC Energy would have no hesitation recommending to others.

4. New forms of authentication tokens extend flexibility

Main findings:

- Hardware tokens with perpetual licences reduce costs associated with procurement and deployment and provide high levels of security where risks are considered to be highest
- Software tokens boost security when combined with encryption by keeping data safe from prying eyes and can also extend authentication to physical access for greater control of users
- Software and evolving types of authentication methods, such as SMS tokens, or even non-token-based authentication methods, extend the benefits of authentication to a wider range of environments
- New on-demand tokens will boost productivity by enabling more secure remote working

Tokens for strong authentication come in two basic forms—hardware and software. These provide a second factor for authentication, but some tokens can also be supplemented with a further form factor for added security in the form of biometric identifiers and data encryption. There are also new technologies coming onto the market that incorporate tokens into devices that are in general everyday use, such as mobile phones. These provide users with the convenience of using items already in their possession as authentication devices, avoiding the need to carry an extra piece of equipment. They can also be provisioned on-demand via SMS services, so that the phone user always has an authentication token ready for use.

Organisations looking to deploy tokens should consider the entire range of tokens available and decide which is best for what purpose. For the highest levels of security, hardware tokens are the best option, especially those that contain additional security features that allow their use to be extended to leverage other existing investments, such as physical access controls. However, their cost is generally higher than other forms of tokens, which can provide greater flexibility for the user and enable higher levels of mobility.

- **Hardware tokens**

Hardware tokens have been around the longest and are in the most widespread use. These are physical devices that generate a one-time password at the touch of a button, which is only valid for one authentication event and which provides added security as the password generated can be used only once, making its capture by key-loggers useless.

Common forms of hardware tokens include key fob-style tokens or calculator-style tokens that contain a keypad. The main disadvantages of hardware authentication tokens are the cost of procurement and distribution, as well as the fact that they can easily be lost. However, for controlling the costs of the tokens themselves, some vendors are starting to offer perpetual licensing, rather than having to renew tokens every two to three years.

In terms of their advantages, many consider hardware tokens to be the most robust form of strong authentication and they are especially suited to environments where security risks are considered to be high. For example, new forms of credit card-based tokens are coming on to the market for use in applications where containing fraud is a greater concern than the cost of the token, such as in financial services and retail transactions. This is being done by equipping credit cards with one-time password generators that provide greater levels of assurance for card-not-present transactions. In the future, this may be extended to cards used for cash withdrawals at automated teller machines (ATMs).

Case study: TTT Moneycorp

Headquartered in London in the UK, TTT Moneycorp provides global retail and wholesale currency services in the form of commercial foreign exchange, wholesale banknotes, retail bureau de change, and currency and commodity trading. It offers services to individuals and corporate clients, including processing transactions for large-scale currency trading and cross-border transfers, and claims to service more than 2.8 million clients per year.

Many of the services that it offers its clients are provided via an online portal or the phone. Given the nature of these services, managing risk is a high priority for TTT, requiring that it has in place a highly secure mechanism for identifying and authenticating customers. Having already used two-factor authentication tokens within its business for authentication of users, TTT took the decision to offer such services to its customers to provide a higher level of security for the transactions that they undertake.

Having looked at a variety of options, TTT decided to subscribe to CRYPTOCARD's cloud-based MAS managed authentication services. It ships hardware authentication tokens to its customers that generate a one-time password when a PIN is input into the device—meaning that the PIN is never captured by the service, just the password that is randomly generated for each particular session.

Overall, TTT is impressed with the flexibility that a cloud-based subscription service offers in terms of the ease and speed of adding new users to the service. Plus, because it is offered as a subscription service, there are no upfront investments required—even for the tokens, which are included in the monthly user-based fee for using the service.

TTT is now looking at expanding the service to include on-demand SMS tokens in order to extend the service to mobile phones without the need for a human operator to intervene in the authentication process.

- **Software tokens**

Another way to control the costs of hardware tokens is to use software-based tokens incorporated onto the computing device itself, such as a desktop or laptop. Intelligent software tokens are also available on smart cards and USB devices and provide additional security benefits, as they can contain extra functionality such as combining one-time password capabilities with digital identities, or can be fitted with radio frequency identification (RFID) chips so that they can also function as physical access authentication mechanisms when integrated with door access control systems. Smart cards are often integrated with USB or PCMCIA (personal computer memory card) readers for interfacing with computers. Through use of encryption, such tokens can lock down all data at a device level so that the computer is immediately locked for use when the USB device is removed, adding an extra layer of certainty that data is secure. USB tokens can also enable a user to access the network from any computer, making them useful for authenticating users in environments where use of computers is shared, such as in a hospital or a warehouse.

Software tokens can also be deployed on mobile devices such as BlackBerry smart phones. This provides organisations with the benefits of strong two-factor authentication without the need to purchase additional hardware tokens, plus takes advantage of the widespread use of such devices. By combining the token with a device that a user routinely carries, user acceptance of the use of strong authentication is improved since they don't need to carry a specialised hardware token that can easily be forgotten or lost.

- **On-demand tokens**

For even greater flexibility, new types of token services are now available that do not require software to be physically installed on the device being used for authentication. An alternative to software tokens for smart phones, such as BlackBerry devices, is to push one-time passwords on demand to any mobile phone via SMS services. This provides the advantages that a user can authenticate to the network any time required and from anywhere with no requirements for set up or management of tokens. These are also the easiest types of tokens for users and organisations since no set up is involved, no purchase of software licences is required and the system does not need ongoing management.

5. The future of authentication: the promise of federated identity

Main findings:

- Open, flexible cloud-based authentication platforms and industry standards such as SAML will lead to the promise of federated identity finally being realised
- Organisations embracing such platforms to serve not just employees, but customers or business partners as well, will see their brand differentiated by the convenience and security that they are able to offer
- The commercial attractiveness of using an open authentication platform is that an organisation can securely offer its customers a wide portfolio of services under one brand
- The use of strong authentication for newer Web 2.0 applications and services will allow organisations to reap the benefits of greater interaction with their employees and customers whilst providing the robust levels of security that are currently lacking in such environments

In some cases, hybrid models are emerging whereby organisations are looking to extend authentication services to a wide range of constituents. Increasingly, authentication services are being deployed that are made up of a combination of in-house, server-based authentication services for internal personnel, combined with on-demand managed authentication services for customers and business partners. Early demand is expected to be seen from government agencies looking to most strongly authenticate users of their online services, and areas such as education with large, technically competent, but dispersed, user populations.

In vertical industries such as retailing, online gaming and financial services, organisations are looking to extend strong authentication services to their customers to provide them with a greater degree of privacy and data protection. In an increasingly IT-savvy world, offering strong authentication capabilities is rapidly shifting from being a differentiator of services to being an entry cost of doing business. The most common services offered presently are the provision of two-factor authentication tokens to customers, which are often branded with the name of the organisation providing

them, and most are specific to the services being offered. For the end user however, there is often a proliferation of such authentication tokens as little effort has traditionally been made by organisations to collaborate with the broader market, including competitors, in order to build a unified authentication service.

In response, as on-demand managed authentication services continue to expand in popularity, they are likely to become open authentication platforms, managed by service providers in the cloud. This could allow an organisation to sign up to the services provided and then provide two-factor authentication tokens to customers that are not limited just to the specific service that they offer, but that could also be used for accessing services offered by other organisations that are business partners. For example, a retailer could supply tokens to its most loyal customers, allowing them to not only access services that it offers itself, such as internet shopping or to view their account details for the retailer's store card online, but also to access those of business partners of the retailer offering, for example, financial or insurance services. Thus, they are able to achieve the promise of single sign-on (SSO).


Over time, access could be opened up to services from other, unrelated, organisations using the same common authentication platform. To achieve this, the platform and the tokens chosen should adhere to industry standards such as the security assertion markup language (SAML) specification developed by the OASIS Security Services Technical Committee, which has become the definitive standard underlying many web-based SSO products. SAML relies on the first organisation from which a service is requested, which is known as the identity provider, vouching for the identity of the requestor based on the authentication information provided. When a user browses to a site operated by another service provider, the original identity provider passes a SAML assertion to that service provider that indicates that it has already identified and authenticated that individual. In this way, the user's identity can be "federated" among organisations using the same authentication platform.

The commercial attractiveness of this approach is that a company can offer a wide portfolio of services under a single brand, where the services are actually delivered in a white label arrangement by third parties. A customer of the central company, who has been issued an authentication credential by that company, can then seamlessly access all the services offered via the browser, dipping in and out of the third party sites, unaware that they are doing so as the look and feel of the sites can be made the same, while an underpinning of SAML ensures that the user does not need to re-authenticate to the third party sites.

- **Extending authentication to a Web 2.0 world**

The term Web 2.0 has been coined to refer to a new generation of web development and design capabilities that enable greater levels of information sharing and collaboration. These capabilities have led to the development of a range of new interactive applications such as online networking sites and socially oriented applications such as wikis and blogs. The impact of the introduction of such services can be seen in the fact that one social networking site alone—Twitter—claims that the number of active users of its service grew 900% in 2008 alone. At first, organisations looked to block use of these social networking sites, believing that they were a drain on productivity, but it is a fact of life that many computer users employ the same computing device for work and leisure purposes, and this is especially true for mobile computing devices such as smart phones.

It is now widely recognised among organisations that, rather than necessarily being damaging to their businesses, the new ways of communicating and sharing information that they encourage can actually be beneficial to them. A recent survey by the Security Executive Council found that 86% of organisations that responded no longer block social networking sites such as Facebook, LinkedIn and Twitter. Rather, the majority of human resource managers would first look up a potential hire on LinkedIn, at the very least, before extending a job offer to them. LinkedIn currently has more than 40 million users in over 200 countries.



“There is lots of interest in federated identities online, but it also needs two-factor authentication to log in across the net, but to lock down access to a physical item for greater security.”
John Jeffries, Iron Key

Organisations are also using Web 2.0 applications to reach out to existing employees and customers, as well as for finding new employees. Social networking sites can aid in collaboration among employees in the form of instant messaging, web conferencing and finding colleagues with the specific skill sets required for a particular project—all

“Many socially oriented services offered over the internet require little in the form of authentication, leaving them weakly defended against attempts to inappropriately access the information they host.”

of which can aid greatly in terms of productivity. They can also help organisations build brand loyalty with customers by enabling their customers to more easily interact with the company, such as by allowing them to provide feedback on products offered, or by extending special offers to customers visiting certain online sites. Advertising is also becoming increasingly popular and many organisations and recruitment agencies are routinely placing job adverts on social networking sites as well as trawling through user profiles proactively seeking strong candidates.

Whilst the productivity impact of social networks may no longer be seen as a major problem, the use of such tools is not without risk to the individual and the organisation. At present, many socially oriented services offered over the internet require little in the form of authentication, leaving them weakly defended against attempts to inappropriately access the information they host. For example, creating an account with Facebook requires a user to provide a first and last name, email address, gender and date of birth—however

the registration process is entirely self service and there are no checks made on the veracity of those claims. Even professional networking site LinkedIn requires no more than a first and last name to set up an account. This has led to users of some such services having their accounts hijacked by a person impersonating them.

Further security concerns with sites such as these include the amount of personal information that people disclose about themselves—or even about their employers. This can leave them open to social engineering attacks, where an imposter uses information gleaned from their profile and posts to make unauthorised password changes that could lead to their accounts being hijacked. This leads to the danger that users can be deceived into clicking on a link contained in an email from a purported friend that could install malware on the computer. If the computer is also used for work purposes, that could lead to malware threats being introduced into the organisation.

To counter these security concerns, some social networking and other online Web 2.0 services, such as eBay and PayPal, are starting to embrace strong authentication by supporting authentication tokens with one-time password capabilities. At present, these are still proprietary tokens that can only be used for the specific service offered. In the future, however, as open authentication platforms become a reality, such platforms will accept tokens from any vendor or service provider. This will provide the level of security required for authenticating any user for any service, allowing their digital identity to be federated among all sites embracing the use of the authentication platform. This will greatly reduce the dangers from attacks against social media and through social engineering, thus shielding organisations and individuals from information and identity theft through lack of accountability, and will lead to the promise of secure digital identities for all being realised.

6. Conclusions and recommendations

To protect themselves from the security threats that they face today, Quocirca recommends that organisations should look to boost their identity and access assurance procedures by deploying stronger methods of authentication than user names and passwords alone in the form of security tokens. These provide an extra layer of assurance by basing authentication events on an extra form factor, namely something in their possession or something unique to them. The majority of tokens incorporate a one-time password, which is good for just one authentication event and which is useless to a hacker trying to guess or crack weak passwords.

Today’s authentication systems have evolved to the point where many of the costs and complexities of provisioning users with accounts and security credentials are removed through efficient central administration and management capabilities. This includes the reduction of hidden costs, such as the burden on help desks of users calling who have

forgotten their passwords or lost their tokens through the provision of an online self-service portal for users to fix problems themselves. Quocirca recommends that organisations consider the lifetime cost of ownership aspects of a two-factor authentication solution and look closely at the reductions in cost that workflow automation and value-added support features can bring.

The evolution does not stop there. New delivery models and methods of authentication are further streamlining the processes and driving down costs. This makes strong authentication an even more attractive option for boosting security without the upfront costs of procuring software licences and the server hardware required to manage the system, and of distributing hardware tokens to all users. Quocirca recommends that organisations look to make use of cloud-based managed authentication services that are provided on a utility-based pricing model, paid for as a monthly operating expense. This provides greater flexibility in terms of how services are consumed, allowing organisations to scale up or down the number of users as required as circumstances change. In a poor economic climate, it is not just small companies that are resource-strapped and cloud-based delivery models will allow organisations to do more with less—a mantra chanted by many business leaders today.

As the evolution continues, cloud-based authentication systems will become open platforms for authenticating users for a wide range of services, no matter what authentication method they wish to use. This will see the use of strong authentication becoming more widespread for applications beyond the control of the enterprise, providing greater assurance for dynamic online applications designed for interactivity and collaboration—without the threat that security exploits caused through social engineering, such as password cracking or phishing, will expose an organisation to harmful security incidents. The use of open authentication platforms, when combined with industry standards for federated identity, will also lead to users being able to access a wide range of services without the need to re-authenticate themselves because of the greater assurance that strong authentication provides. This will allow the benefits of secure identity assurance and access control to be extended to all.

7. Appendix: the drivers for use of strong authentication

- **Why the need for strong authentication has become such a pressing concern**

Data breaches are everyday news—especially in the US, where the majority of states have legislation in place making data breach notifications mandatory in most cases. However, an increasing number of data breaches are being seen worldwide. In the UK, the UK's Information Commissioner reported towards the end of 2008 that it had been notified of almost 100 data breaches since the loss of the personal details of 25 million people by HM Customs and Revenue service in November 2007. Even though no specific laws related to security breach notification have been passed, the Information Commissioner's Office is using existing laws such as the UK's Data Protection Act to take action against organisations that suffer data breaches through having inadequate security controls in place. Germany has gone even further and is the first country in the EU to pass laws that specifically refer to data breaches. In July 2009, it amended the Federal Data Protection Act to require mandatory breach notification "if the data loss is likely to have a serious impact on the rights or protected interests of individuals concerned."

Just how damaging these breaches can be can be seen in the case of Heartland Payment Systems, the sixth largest credit and debit card processor in the US, which suffered the largest data breach to come to light so far, in January 2009. In this breach, it is believed that up to 100 million customer credit card records were compromised, which is equivalent to more than one in ten cards in circulation in the US. This led to its stock value plummeting by 35% in the first five days after the attack, equivalent to \$180 million of shareholder value being wiped out. Although it is not yet known what the full extent of the damage will end up being, at least one class action lawsuit has already been filed against Heartland, and it will have suffered untold damage to its brand and reputation, perhaps leading to customers jumping ship.

"Incorporate two-factor authentication for remote access (network-level access originating from outside the network) for all employees, administrators and third parties."

PCI DSS requirement 8.3

Regulations and standards being imposed on organisations aimed at boosting the use of security controls are becoming increasingly prescriptive, in some cases specifying what specific controls must be in place to protect sensitive data. One example is the Payment Card Industry Data Security Standards (PCI DSS), which is one of the first to require specific technology controls to be used. Another is that of the Federal Financial Institutional Examinations Council (FFIEC), which issued a memorandum in October 2007 that demanded that all government agencies must develop and implement a breach notification policy within 120 days. Specific guidance included in this memorandum with regard to controlling remote access states that agencies should "allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access." According to an article published by the American Banker in December 2007, agencies following the FFIEC guidance show up to a 40% reduction in user account hijacking.

Many organisations today are responding to the demands of such regulations and standards by boosting their identity and access management capabilities, linking access rights to the identity of the user, in many cases by role in the organisation. However, many still rely on the use of user name and password combinations alone for authenticating users. Unfortunately, passwords can be cracked, misappropriated or forgotten and do not, in themselves, provide high enough levels of security—especially when users have to remember multiple passwords for accessing communication and collaboration tools, and business applications. Portable tools such as mobile and smart phones are also proliferating, requiring that the user remember further passwords for each separate device. The need to securely control who is accessing what is leading to the emergence of strong authentication as a critical component of any organisation's security practices.

One recent example of such poor practices leading to an organisation being attacked is that of Twitter in July 2009, which caused sensitive company documents to be leaked. In this case, the hacker targeted an administrative worker by researching the information they had posted on a variety of social networking sites. Enough personal information was available to make it easy for the hacker to guess the answer to the challenge-response question posed when they tried to reset the password for the worker's personal email account. Once the password had been cracked, the attacker was able to browse through emails and their attachments, which led to the discovery of password confirmation messages for a number of websites and services—many of which were identical—including the original password for the email account. This not only allowed the hacker to reset to the original password in order to cover their tracks, but the same password allowed access to the worker's corporate email as well, from which a multitude of details could be obtained, including sensitive company documents and user account details for executives of Twitter. After this attack had occurred, it was discovered that most Twitter employees were using the same passwords for personal and corporate email accounts. To solve this problem, Twitter has now issued its employees with two-factor authentication.

Because of problems with weak passwords, many organisations put in place policies that demand the use of complex, hard-to-guess passwords that are changed regularly and forbid users from storing them on or near to their computers. However, that tends to increase the burden on helpdesks as users forget or lose them and have to call to have their passwords reset, which increases costs and reduces productivity.

By using an authentication method stronger than a user name and password combination alone, an organisation has a higher level of assurance that the user is who they claim to be when they attempt to access particular resources and applications. With that higher level of trust in the integrity and accuracy of the authentication process, the individual authentication challenges that were previously implemented in each individual application may be replaced by a single, strong authentication challenge. This single sign-on (SSO) capability is a key enabler of productivity within organisations. Productivity will also be aided by the provision of comprehensive self-service capabilities, which allows users to request new hardware tokens, provision their own software tokens, or receive help quickly and easily as and when they need it, leaving them free to get on with their everyday tasks.

Another way in which strong authentication systems can enable greater productivity is by facilitating more mobile working, which is driving demand for software-based and on-demand authentication tokens, especially those provisioned through mobile phones and smart phones such as BlackBerry devices. The value for the business is that their workers can now access network resources securely from wherever they are.

About CRYPTOCARD

With the best token technology in the industry and the lowest total cost of ownership, CRYPTOCARD offers unsurpassed value in solutions for positively identifying individuals before giving them access to applications, data and networks. Twenty years of technical achievements have won CRYPTOCARD the trust of thousands of organisations in over seventy countries. CRYPTOCARD's solutions reduce the risks associated with remote access and web-based processes, and increase compliance, at a price all businesses can afford. 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.

www.cryptocard.com

Contact:

Natalie Melton

Head of EMEA Marketing

CRYPTOCARD Europe

Eden Park, Ham Green, Bristol, BS20 0EB, UK

Mobile: +44 7812 121451

email: natalie.melton@cryptocard.com



REPORT NOTE:

This report has been written independently by Quocirca Ltd to provide an overview of the issues facing organisations seeking to maximise the effectiveness of today's dynamic workforce.

The report draws on Quocirca's extensive knowledge of the technology and business arenas, and provides advice on the approach that organisations should take to create a more effective and efficient environment for future growth.

Quocirca would like to thank CRYPTOCARD for its sponsorship of this report and the CRYPTOCARD customers and partners who have provided their time and help in the preparation of this report.

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with firsthand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at <http://www.quocirca.com>

The logo for Quocirca, featuring the word "quocirca" in a lowercase, sans-serif font. The letters "quoc" are in blue, "irca" is in black, and the dot over the "i" is red.