White Paper

Discovering the true cost of buying authentication

CRYPTOCard

Executive summary

The cost of implementing two-factor authentication solutions has recently come under the spotlight, as software-as-a-service oriented models provide some compelling total cost of ownership benefits:

- 50% savings can be achieved by using passwords-as-a-service
- SLAs of 99.999% can be hard to achieve using on-site authentication
- Management and support overheads account for 50% of the TCO of managing a server, but only 25% of the management of a cloud-based service
- IT overheads can be reduced significantly by adopting cloud-based authentication
- Opex models can help organisations utilise cash more effectively
- On-demand features make cloud-based models increasingly attractive.

Many organisations rarely look closely at the total cost of ownership of their authentication solution and instead make a decision heavily driven by the up-front purchase price. This paper – and specifically the tool in Appendix 1 – can be used by organisations as a yardstick in comparing the total cost of ownership of authentication as well as in considering the business and technology benefits of cloud-based authentication.

The affordability of authentication

The pervasiveness of remote access to the internet and web-based applications has enabled our business and personal lives to be transformed to the point where we really can live in a 24x7 online world if we want. The technology that underpins this availability and reliability is increasingly used by organisations to deliver applications to users and to transform their infrastructures. The repeatability and scalability of 'cloud-based' applications and infrastructures is transforming the way that IT departments work and the investments that need to be made.

This technology is now also used to make authentication more affordable. So rather than having to implement on-site servers and spend time integrating applications within the network, passwords-as-a-service is an increasingly popular way to deploy authentication.

Deploying one-time passwords using a service is applicable to organisations of all sizes: large enterprises are using it to replace older, more traditional server-based approaches; mid tier organisations are using it as an alternative to having a service provider manage their authentication server; SMBs are using it because it delivers an affordability that was never previously available.

Drivers for cloud-based services

There are many drivers for organisations to consider using cloud-based services, regardless of their size. The table below shows what are widely acknowledged as the most common reasons for reaching for the clouds.

The most commonly discussed reason for looking at cloud-based services is that of **cost reduction**. Not only is it the most compelling of reasons, particularly in times of economic prudence, but it is also the most subjective of reasons – because it involves many facets of cost discussion and benefits analysis.

Authentication: The evolution of digital passwords

Computers, and the networks that connect them to each other and their users, have changed enormously over the years from mainframes as big as a house to hand held devices that communicate to web-based applications and from squeaky modems through to high speed VPNs that provide reliable and secure connectivity for even the biggest and most disparate of organisations.

The internet and the applications it delivers has made access an everyday part of almost everyone's life and ubiquitous availability of WiFi makes data even more accessible – no matter where you are or what time of day it is. Cost is no longer the issue to sending and receiving vital business data – or simply communicating with friends and relatives via Facebook.

Since its first inception as a commercial entity in the 1950s, computing has changed dramatically – made more portable, more accessible and more affordable.

However, passwords and the way they are delivered have not kept pace with these advances. The password technology that we are all familiar with (username and password) is basically the same now as it was all those years ago. This has opened the door to opportunists: the hackers, ID thieves and fraudsters – with the tools they use being made increasingly easy to obtain and understand by the very medium that has driven us all to be online: the internet.

In the 1980s, things started to change and large organisations started to implement a new digital password. Two-factor authentication, as it became known, was based on the principle of 'something that you have', a token that generates a unique one-time password, and 'something that you know', a unique personal identifier or PIN.

This technology has grown in popularity and is increasingly replacing traditional passwords in our business lives, driven by government and industry legislation and an increasing desire by organisations to secure their digital assets.

Cost reduction and management	The predictability of on going costs and ability to move costs from capital expenditure to operational expenditure
Reducing technology burden	A reduction in the IT support headache by outsourcing processes, technology and reducing the need to dedicate internal people to non-core tasks
Improving service and efficiency	The improvement of access to applications and service that improve people's efficiency and the ability to invest in people as opposed to technology
Achieving standards	Adoption of best practices and the ability to achieve industry or regulatory compliance without major investment
Managing growth	The ability to manage expansion or reduction in service to meet business needs

The true costs of authentication – hard costs v soft costs

This white paper provides detailed cost analysis metrics and discussion points that will help a business of any size decide which is the most appropriate solution to meet their authentication needs. The paper delivers facts based upon technical research and comparison as well as commercial input from organisations (CIOs, CISOs, IT managers) and suppliers (systems integrators, service providers and resellers).

First of all, we need to consider the different costs associated with the implementation of a solution. We can break these down into two different types of cost:

- Soft costs are typically related to the overall solution and can be seen as being related to the desired outcome that this business wants to achieve. They are business driven but technology influenced.
- Hard costs are items that are essential or mandatory to the implementation and use of the solution. The solution would not deliver the level of service required without them. Hard costs are generally calculated on a per user basis and are technology driven but business influenced.

Soft costs

The following areas have been highlighted by organisations and their suppliers as being the key areas that they need to consider when purchasing an authentication solution. The priority and relevance of each area varies greatly between organisations – dependent on factors such as size, number of locations and type of user.

Appendix 1 provides a more detailed table and also explains how this data can be used to evaluate both options against the needs of the organisation.

Desired benefit	Server-based authentication	Cloud-based authentication
99.99 % SLA	Implementing this level of service availability would typically require significant investment in IT infrastructure, tools and people resources.	Delivery of a service that leverages high availability infrastructures and behind the scenes resources to underpin effectiveness and use satisfaction by minimising disruption or outages.
Resilience provided	Design, implementation and support of a fully resilient network infrastructure could be a significant investment.	Fully redundant architecture that delivers maximum performance, availability and replication of core data.
Support overhead removed	Developing the knowledge and skill in house, as well as investing in resources to deliver a high level of 'on tap' responsiveness is likely to be prohibitive.	Cloud based services are managed by trained and experienced resources who maintain the high level of SLA, as well as offering fast response to technical questions.
Expert 1st and 2nd line support provided	Building sufficient in-house knowledge can be time-consuming and expensive.	A service provider will ensure that all problems are escalated rapidly to specialists to assure fast resolution, maximum up-times and high levels of user confidence.
No up-front purchases	A server model is likely to require the up-front purchasing of a server, associated licences, the 2FA application, tokens and a support contract.	A cloud based service leverages a full software-as-a-service (SaaS) oriented model – where on going payments and an all-in pricing will also means there are no up-front purchases – not even tokens.
Opex vs. capex	It is unlikely that a server based model can be totally supported by an opex model due to the up-front investments in hardware and licences.	With cloud-based services you typically have the choice of 100% opex payments or ability to blend this with a capex model. This flexibility can improve business cashflow and budgeting.
Proactive monitoring	Investment in the tools and resources to deliver fast and consistent diagnosis and resolution of trends and incidents can be prohibitive to even the largest of organisations.	The infrastructure of a cloud-based authentication service will be built to deliver immediate notification, action and resolution of issues to assure effectiveness, up-time and service delivery.
Simple integration	Most server based installations require complex set-up and configuration – with some vendors even expecting you to pay for the agents required to get you going.	Cloud-based services require minimal change to an infrastructure to be up and running – typically the change can be made remotely.
High level of security	Achieving audit and compliance can sometimes require heavy investment in tools and equipment. It also requires specialist knowledge and investment in consulting services.	Cloud-based authentication is typically hosted in an ultra-secure datacentre with regular security auditing conducted to assure high levels of security. Industry standard tools and equipment will assure security of data and access.

> "Not only is it faster and more flexible, it is cheaper... the emergence of cloud models radically alters the cost benefit decision

FT, 6 March 2009

Hard costs

This section provides a detailed view of the key elements of cost and overhead that a company should consider when purchasing an authentication platform. The elements are based upon research and reflect best practice elements that a managed service provider or outsourcing company would calculate in terms of delivering a managed server environment.

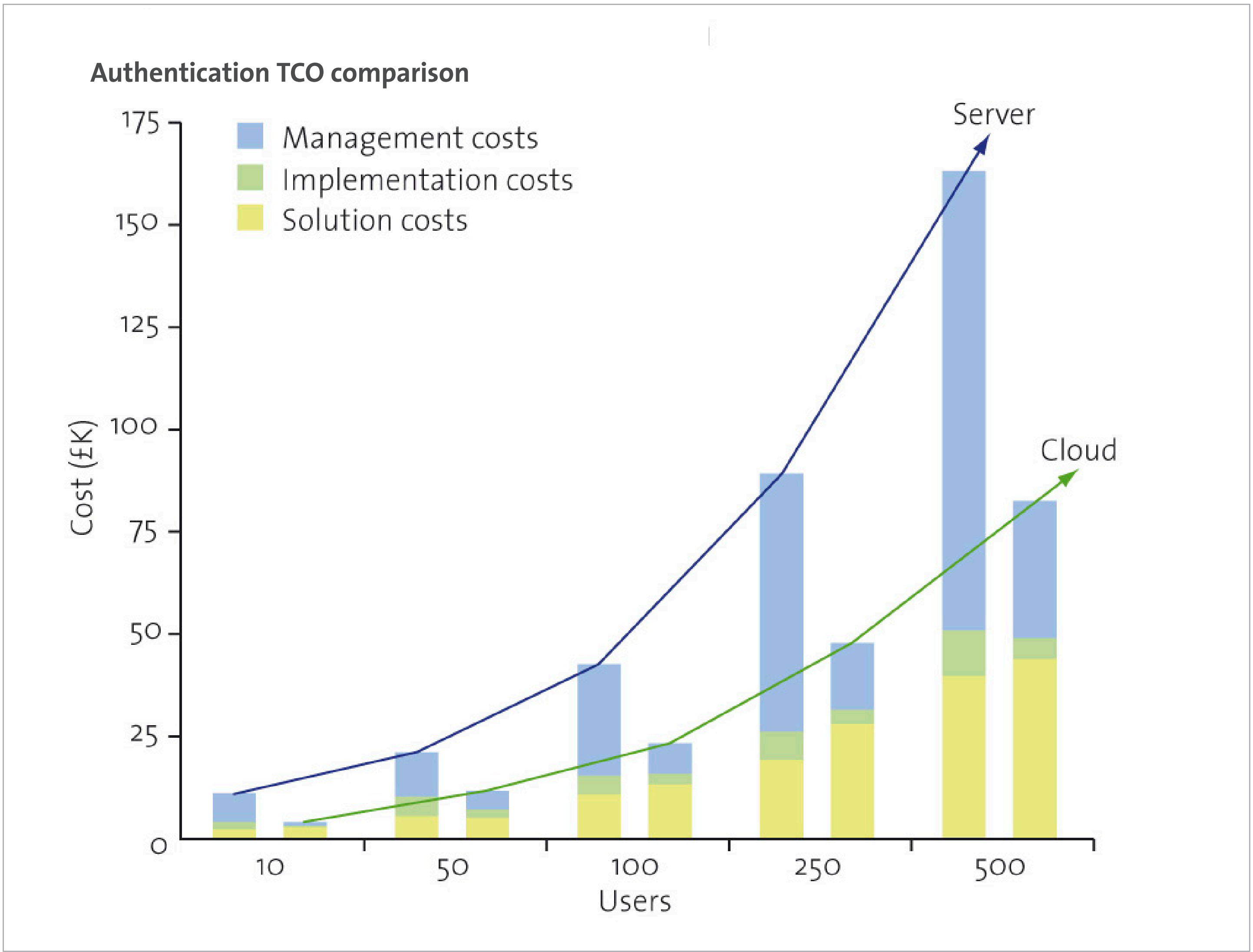
Putting costs into a TCO perspective

Let us now take a look at how soft costs and hard costs contribute to the Total Cost of Ownership (TCO) of an authentication solution. The graph below shows costs for each solution type across defined numbers of users.

The management cost has been calculated by applying industry standard costs to the time taken to undertake each of the tasks outlined previously in the' hard costs' section. Soft costs have been included within the implementation cost figures and are based upon feedback from both customers and systems integrators. Solutions costs are based on the typical purchase prices of traditional server based authentication and CRYPTOCard's CRYPTO-MAS Passwords-as-a-Service solutions across a range of business sizes.

As the graph illustrates, the solution cost for each type of authentication solution is a misleading indicator for the total cost of ownership. If a true like-for-like comparison is to be carried out, with consideration given to the full TCO of each authentication solution to the organisation, it is clear that the cloud-based solution is more cost effective, with savings in the region of 44-60%, depending on the number of users.

Spending a few minutes using the tool in Appendix 1 to assess the total cost of authentication for your own organisation can support a business case and, more importantly, could enable you to select the right solution and save money.



> “Economies of scale, shifting users to a services-oriented relationship, delivering much faster, forcing software prices to align with usage, charging business units based on usage. Sounds like cloud computing to me.

Tom Bittman
Gartner, 11 August 2009

Cost area	Description of consideration
Incident resolution	Resolving faults within the infrastructure – either from the service desk or from automated tools (e.g. performance, disk space, user support)
Change installation	Implementing changes within the infrastructure, adding disk, service packs, memory, etc
System documentation	Documenting the infrastructure, maintaining the documentation and the configuration
Virus/security management	Ensuring solutions and updates are deployed to protect the server and the infrastructure
Reporting	Monitoring server and infrastructure performance and availability etc
Housekeeping	Clearing/archiving log files, general file management, storage reclaim, etc
Performance capacity management	Ensuring ongoing server availability and capacity
System software upgrades	Ensuring latest patches are implemented, preventative analysis and execution
Security audit	Checking security logs, maintaining service integrity etc, implementing and maintaining security policy
Print admin	File and print server management etc
User admin	Managing user accounts, MAC, permissions
Storage management	Storage connectivity, resilience, failovers etc
Token admin	Managing provisioning, deployment etc
System monitoring	Ongoing monitoring using system tools and reports, correlation and investigation.
Back-up operations	Back-up and storage of the application, as well as user data. Includes: monitoring of tapes; storage; off-siting
Team leadership	Management the team who support the server, application, infrastructure, help desk, escalation processes, etc

Appendix 1. Identifying the best solution and impact of desired benefits

The tool below has been created to help you identify the most appropriate solution for your organisation's two-factor authentication requirements and to help identify the importance and cost of the individual desired benefits of your authentication solution.

Using the TCO comparison tool

The first step is to weight each of the desired benefits according to their importance in your organisation, by giving them a score of 1 to 10, where 1 is 'not at all important' and 10 is 'extremely important'.

Next, rank both server and cloud-based authentication according to the cost that each approach would incur in your organisation, where 1 is 'zero or negligible cost' and 10 is 'extremely costly'.

Finally, complete the score column by multiplying the weight and rank, then totaling the items in each score column.

Interpreting your results

Firstly, review the overall score in each column. This will help you assess which solution is most appropriate for your needs (the one with the lowest overall score), and the scale of difference between one solution and the other (the difference between scores).

Secondly, arrange the desired benefit areas in order of score, from highest to lowest, to identify desired benefits in terms of importance and cost to your organisation. Those with the highest scores demand the most attention

			Server-based authentication		Cloud-based authentication	
Desired benefit	Considerations	Weight	Rank	Score (Weight x Rank)	Rank	Score (Weight x Rank)
99.99% SLA	• Infrastructure availability • Server resilience • Network connectivity • Out of hours support • Incident resolution	7	6	42	5	35

> "... survey results we published earlier this year found that nearly 40% of midsize organisations indicated they would like to have 100% of their servers virtualised within three years; and 70% believe they can have 100% of their servers virtualised within five years.

Neil MacDonald
Gartner, 28 August 2009

TCO comparison tool

Desired benefit	Considerations	Weight	Server-based authentication		Cloud-based authentication	
			Rank	Score (Weight x Rank)	Rank	Score (Weight x Rank)
99.99% SLA	• Infrastructure availability • Server resilience • Network connectivity • Out of hours support • Incident resolution					
User data backed-up	• Replication of token, user and system attributes • Off-site storage • Resources to deliver • Processes to assure it happens					
Resilience provided	• Fully redundant architecture • Performance maximisation • Availability and replication of core data • Network redundancy • Monitoring resources and tools					
Support overhead removed	• Availability of resources on 24x7 basis • Holiday cover for expert resources • Cost of training resources • Keeping resources up to date • Availability of support/test model office					
Expert 1st and 2nd line support provided	• Escalation process management • Managing multiple suppliers (server, network, 2FA etc) • Speed of response to key users					
No up-front purchases	• Investment in server and associated O/S and licences • Purchase of 2FA application • Purchase of tokens • Purchase and manage support contract					
Opex vs. capex	• Ability to allocate costs to opex • Ability to pay quarterly • Availability of cash/budget					
No 'x' year renewal cycle	• Cost of replacement tokens in year 4 • Cost of re-provisioning tokens in year 4 • Disruption to users of replacing tokens					
Reduced environmental concerns/carbon footprint	• Cost of additional server power supply and associated back-up • Provision of management tools • Cost of air cooling • Cost of additional rack space • Provision of additional network infrastructure and tools					
Proactive network monitoring	• Provision of management tools • Availability of resources • Speed of response • Speed of resolution • Diagnosis and resolution of trends and incidents					

Continued...

Desired benefit	Considerations	Weight	Server-based authentication		Cloud-based authentication	
			Rank	Score (Weight x Rank)	Rank	Score (Weight x Rank)
Proactive server monitoring	• Provision of management tools • Availability of resources • Speed of response through to resolution • Diagnosis and resolution of trends and incidents					
On demand growth capability	• Fast access to and availability of server capacity • Rapid access to and installation of licences • Quick availability and distribution of tokens • Immediate ability to cope with a pandemic or emergency scenario					
No-fork lift implementation	• Hardware and device installation resources • Network configuration requirements • Project and change management overhead					
Simple integration	• Authentication specific software install • Server configuration and set-up requirements • Network re-configuration • AD schema change requirements					
High level of security	• Level of token and software OTP complexity available • Datacentre security – access to server • Regular server and infrastructure penetration testing • Datacentre and associated security policy auditing					
High level of data integrity	• Access management • Data and disk encryption implementation and monitoring • Data back-up and security management					
Ability to focus on core business	• Availability of security knowledge • Support process and management • Token and software provisioning and deployment capacity					
Multi-company/ department capability	• Integration into diverse company IP infrastructures • Multiple access point integration and management					
Multi-tier distributed management	• Multi-tier administration and management • Ability to devolve decisions to where it is best managed					
			Total:		**Total:**	

CRYPTOCard Europe
Tel: +44 870 7077 700

CRYPTOCard North America
Tel: +1-613-599-2441

info@cryptocard.com www.cryptocard.com