



WHITE PAPER

Two Factor Authentication: An Industry Wide Solution

Document Number

GP_WP_IW

Issue Status

1.0

Issue Date

31 July 2005

Prepared by**GPayments**

GPayments Pty Ltd
Pittwater Business Park
Suite 8, 5 Vuko Place
Warriewood NSW 2102
Australia
Tel: +61 2 9913 3088
Fax: +61 2 9913 3077
Email: info@gpayments.com

Copyright © 2005 by GPayments

This work is copyright. Other than as permitted by law, no part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any process without prior written permission.

Contents

1. Introduction	3
1.1 Aim	3
1.2 Target Audience	3
2. The Case for Two Factor Authentication	4
2.1 What is Phishing?	4
2.2 Phishing Attacks and Online Fraud	4
2.3 What is Two Factor Authentication?	5
2.4 Regulatory Mandates	5
3. Current Two Factor Authentication Devices	6
4. Two Factor Authentication Implementation: Issues and Costs	8
4.1 Device Purchase	8
4.2 Device Distribution	8
4.3 Implementation	8
4.4 Infrastructure, Management and Hosting	9
4.5 Non-Income Producing Solution	9
5. The Case for an Industry Wide Solution	10
6. Roles in the Industry Wide Solution	11
6.1 System Owner	11
6.2 Solution Host	11
6.3 System Integration	11
6.4 Device Purchase	11
6.5 Device Distributor	12
6.6 Physical Authentication	12
7. Prospective Subscribers	13
8. Business Models	15
8.1 Solution Provider	15
8.2 Device Purchaser	15
8.3 Device Issuer	15
8.4 User Identity Endorser	16
9. ActiveAccess Solution	17
9.1 Device Independent Platform	17
9.2 Quick Implementation; Lower Cost	17
9.3 Low Cost Devices	17
9.4 Increased Security	18
9.5 Device Agnostic	18
9.6 Easy Integration	18
9.7 Extensive Reporting and Customer Management	18
9.8 Device Sharing	19
9.9 Privacy	19
9.10 Single Sign-On and Federated Identity	19

1. Introduction

A number of organisations have felt the need to provide their customers with enhanced security measures, in addition to username and password, to access online services. The most common enhancement has been to employ a two factor authentication solution. With the increasing number of custom built implementations being developed by these organisations, customers risk having to carry a unique device for each organisation's online service they access.

To eliminate the need for consumers to carry more than one device and to reduce the overall cost of industry adoption, an industry wide authentication platform that enables device sharing needs consideration.

1.1 Aim

The aim of this paper is to discuss the reasons for adoption of a two factor authentication solution, what are the problems associated with implementing such a solution and how many of these problems can be overcome with the provision of an industry wide two factor authentication solution. The paper lists organisational groups who would benefit from such an initiative and proposes business models which could be employed to benefit those organisations supporting the solution.

1.2 Target Audience

This paper is targeted at organisations that would benefit from the establishment, and availability, of an industry wide online two factor authentication solution.

2. The Case for Two Factor Authentication

2.1 What is Phishing?

Phishing is defined as the act of sending an e-mail to a user falsely claiming to be an established, legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The web site, however, is bogus and set up only to steal the user's information.¹ Another form of attack uses a Trojan, a malicious program that is disguised as something else. When a user is directed to a website after clicking a link in a phishing email, the Trojan is downloaded to the user's computer and is once again used to steal personal information such as account details and passwords.

2.2 Phishing Attacks and Online Fraud

With the increase in Internet usage and the demand for providing cost-effective consumer services, there has been a significant shift to provide these services online. One of the most popular examples of this trend is the availability of Internet banking services. In the Asia-Pacific region alone, it was estimated that 22 million cardholders were active Internet banking users in 2003, 43 million in 2004 and an anticipated 107 million by 2007. Associated with the increase in popularity of providing and accessing services online, there has also been an increase in fraud and identity theft. Statistics from three independent sources indicate that phishing attacks continue to rise:

- The Anti-Phishing Working Group statistics show the number of reported phishing attacks more than doubled in the period October 2004 (6,597) to April 2005 (14,411). In the same period, the number of reported phishing sites almost tripled from 1,191 to 2854. In excess of 75% of these attacks were targeted at the financial services sector, a figure which continued to rise.²
- Incidents of phishing attacks increased by more than 200 percent in May 2005, according to figures released by IBM. MessageLabs collected 9,139,704 phishing e-mails in May 2005, a 226 percent jump from April, topping the previous record of 7,724,659 phishing e-mails in April.³

¹ Reference: <http://www.webopedia.com/TERM/P/phishing.html>

² Reference: <http://www.antiphishing.org/>

³ Reference: <http://www.extremetech.com/article2/0,1697,1833793,00.asp>

- MessageLabs Intelligence Annual Email Security Report 2004 shows that in 2004, MessageLabs Anti-Spam managed email security service scanned more than 12.6 billion emails. Of these, more than 9.2 billion, or 73.2% were identified as spam. For the same period, MessageLabs Anti-Virus managed email security service scanned a total of 147 billion emails of which 901 million or 1 in 16 (6.1%) contained a virus.
- Postini email security and management services protected its customers from 16,667,444 phishing attempts in June 2005, a 71 percent average per day increase compared to May.⁴

With such exponential rises in phishing attacks and the increased sophistication of such attacks, it is apparent that the existing username and password mechanism for access to online accounts needs to be complimented with additional security. As a result, two factor authentication has become one of the most popular solutions to address this need for additional security.

2.3 What is Two Factor Authentication?

The access control mechanism on the Internet has been predominantly username and password. This basic, single factor authentication has become inadequate in the face of increased cyber fraud activities in recent years.

The alternative, more secure mechanism is commonly known as two factor authentication. Two factor authentication is based on something that a user has (a physical device) and something that a user knows (a PIN number or password). A common application of two-factor authentication in everyday life is withdrawing money from an ATM. The user is required to enter their card in the ATM (something they have) and then type their PIN (something they know). By using something a user knows with something a user has, the same level of authentication can be brought to the online world.

2.4 Regulatory Mandates

Many governing bodies have indicated the need for additional security. In particular, there has been a significant push from within the banking industry. Regulatory authorities of the UK⁵ and Hong Kong⁶ have recently announced common industry standards for two-factor authentication. The US⁷, Singapore⁸ and Australia⁹ have also seen movement from regulatory authorities to enhance security for online transactions in a bid to combat cyber fraud.

⁴ Reference: <http://www.wwwcoder.com/main/parentid/472/site/5450/266/default.aspx>

⁵ APACS

⁶ Hong Kong Monetary Authority (HKMA)

⁷ Federal Deposit Insurance Corporation (FDIC)

⁸ Monetary Authority of Singapore (MAS)

⁹ Australian Bankers Association (ABA)

3. Current Two Factor Authentication Devices

Due to the increase in phishing scams and the risk organisations face by having services available over the Internet, there has been increased activity and implementations of two factor authentication solutions. Many implementations models have been employed to provide the additional security and there have been many different end user devices to support these models. Following is a sample list of end user devices capable of providing two factor authentication.



One time number generating tokens



Chip cards and online chip card readers



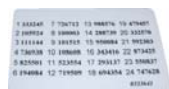
Chip cards and offline chip card readers



Mobile phones with SMS or applet



Chip enabled USB devices



Scratch Cards, TAN Lists or Printed Cards

Two factor authentication has been the solution to enable remote logging in to services over the Internet for quite some time, particularly for corporations and government for staff to access internal VPN's.

In late 2004, AOL launched the first ever consumer implementation of a two factor authentication solution using one time password tokens. By far the largest interest in rolling out two factor authentication solutions to consumers has come from within the banking sector, particularly relating to Internet banking security. Notable consumer implementations include:

- ◆ National Australia Bank offering an SMS solution to its retail Internet banking customers
- ◆ HSBC in Hong Kong offering two factor authentication tokens to its retail Internet banking customers
- ◆ ING in Luxemburg offering two factor authentication tokens to its retail Internet banking customers
- ◆ UBS offering smart cards and smart card readers to its banking customers
- ◆ Rabobank in Belgium offering two factor authentication tokens to its retail Internet banking customers

4. Two Factor Authentication Implementation: Issues and Costs

One of the challenges an organisation looking to strengthen their defences against online fraud faces is to determine what level of security is suitable. An organisation must choose their preferred security method based on a number of factors including solution availability, usability, portability, cost effectiveness, appropriate security, manageability and flexibility.

When an organisation eventually strikes the appropriate balance between cost and security, there is usually a substantial upfront investment required in the implementation of a preferred solution. This cost is usually made up of the following factors.

4.1 Device Purchase

The organisation wishing to implement the enhanced security will be required to purchase devices, where a hardware device is chosen, for all of their end users. This cost is not an insignificant and can range from US\$10-15 per device.

4.2 Device Distribution

There is an associated cost to distribute devices to all end users. The management and logistics of device distribution and handling of returns can potentially be greater than the cost of the initial device purchase.

4.3 Implementation

Each two factor authentication implementation requires appropriate resources to integrate with or develop a solution. In most cases, the effort required to integrate with an existing platform or develop a solution to cater for the complexities required to manage users and devices is significant and could consume considerable time and resources.

4.4 Infrastructure, Management and Hosting

As with the implementation of any new in-house system, a significant initial investment must be made to setup the necessary software and hardware infrastructure. In addition, ongoing system management adds to the project cost.

4.5 Non-Income Producing Solution

As the implementation of an enhanced security system is largely a risk and cost reduction exercise, the project does not produce any income for the organisation.

5. The Case for an Industry Wide Solution

As with the implementation of any industry initiative, organisations move to implement solutions at different stages. Some organisations move quickly to gain the “early mover advantage”, some follow after early implementers have gained experience and some will not move at all unless obliged by legislation. The move by organisations to protect online services with two factor authentication solutions is typical of this trend. However, while each of the organisations is looking at their own implementation, they each face the challenges listed previously.

With organisations implementing solutions at different times, looking at their own system requirements without regard for what others are doing or are planning to do in the future, it is possible that end users will suffer from the results. It is possible that without a solution which caters for device sharing, an end user may be issued a device (or more if a customer of more than one bank) to access a bank account via the Internet, their employer may issue a device for access to its secure Internet services and the government may issue a separate device to facilitate access to government related documents and services. This undesirable effect, producing a “device necklace” for each user, will result from the lack of industry collaboration. This can be avoided using an industry wide solution enabling device sharing.

The key features of an industry wide solution include:

- ◆ Managed by a trusted party
- ◆ Facilitates two factor authentication for any organisation who subscribes to the service by providing the device distribution, infrastructure and management.
- ◆ Allows issuing organisations to participate, even if they have independently implemented a two factor authentication solution
- ◆ Provides two factor authentication (at a cost) to other participating organisations who subscribe to the service, especially those who could not otherwise afford an in-house two factor authentication implementation
- ◆ Requires ease of integration to the solution by participants
- ◆ Allows the sharing of devices, thereby allowing end users to carry only one device for their authentication requirements, eliminating the “device necklace”.
- ◆ Provides an array of devices from which issuing organisations can choose i.e. be device and vendor independent.

As the device vendors have been the key facilitators in the push for two factor authentication implementations, an independent and trusted third party operated industry wide solution would provide benefits otherwise not available . A solution which focuses on the key factors above would reduce the overall cost of two factor authentication to the industry, and assist more organisations to implement solutions, reducing the impact of phishing attacks and online fraud and providing a securer environment for end users to access information online.

6. Roles in the Industry Wide Solution

To implement a two factor authentication solution with end user devices such as one time number generating tokens, certain roles need to be undertaken. At a minimum these roles need to facilitate the implementation, hosting and support of the solution, system integration by the organisation and the acquiring and dissemination of end user devices. For an industry wide solution, in addition to the roles above, the system needs to be owned and operated by a trusted party.

6.1 System Owner

As it is likely the solution would facilitate participation from all corporate and governmental levels alike, very few organisations could be considered for the implementation of an industry wide two factor authentication solution. An independent organisation that has already established trust within industry is an ideal owner for the service. As the system is used for online authentication, the organisation needs to be respected for their security, honesty and independence.

6.2 Solution Host

An ideal solution host would already have or know a partner organisation who has the infrastructure in place to host the authentication service.

6.3 System Integration

An ideal solution owner would already have the capability to perform the task of system integration or know a partner organisation that could provide the minimal support necessary support to assist organisations in integrating with the solution.

6.4 Device Purchase

The solution owner could have the capacity to negotiate competitive device pricing for device issuers due to the economies of scale available to an industry solution. The solution owner may also like to purchase and brand the end user devices or co-brand with the issuing organisations.

6.5 Device Distributor

An ideal solution owner could already have the capability to distribute devices (if required) or know a partner organisation who could provide the necessary local coverage and physical access points for the retail sale and distribution of tokens to end users.

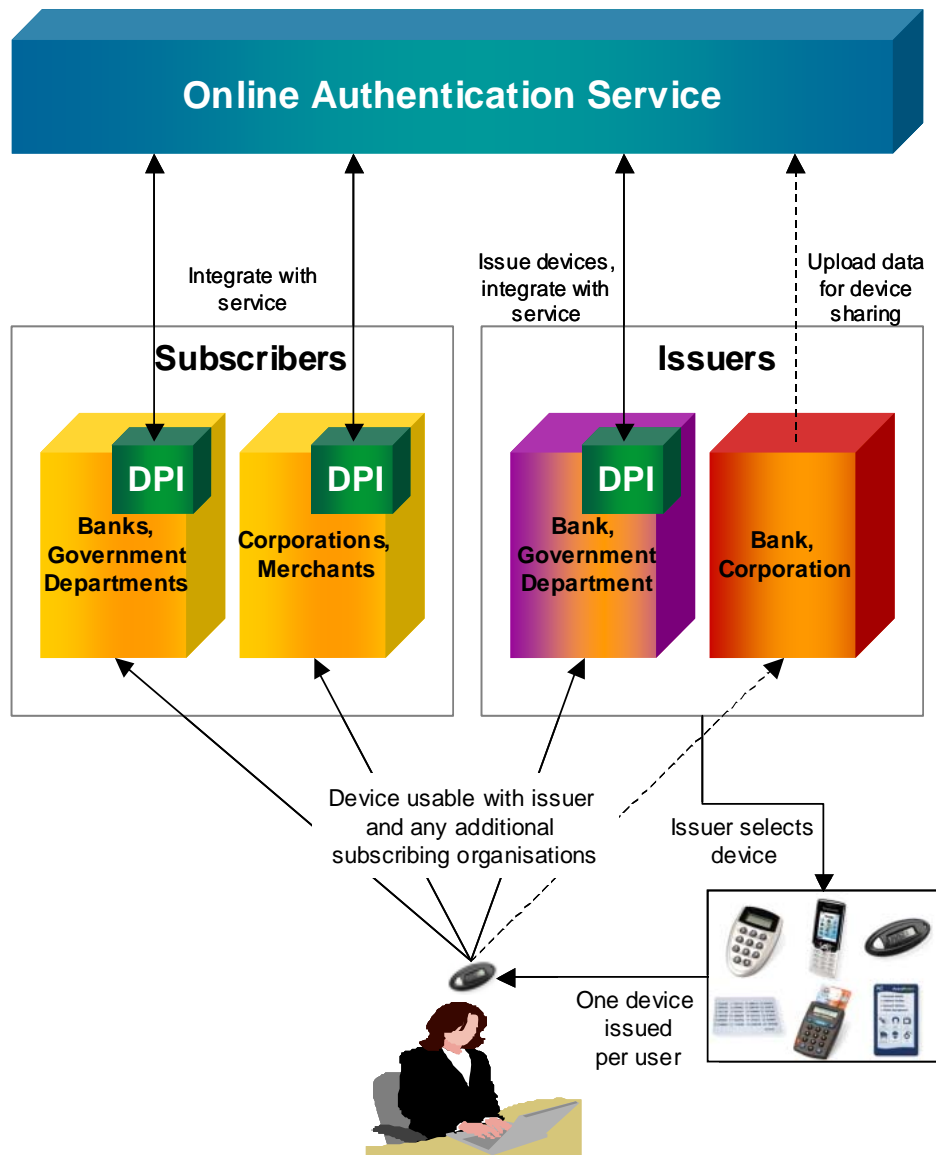
6.6 Physical Authentication

If physical user authentication were to be supported by the model, the system owner would need an extensive network to perform identity checks of users in the physical world. These checks could be used for a range of purposes including setting up bank accounts, passport checks or accessing governmental services online. Device distribution is a natural extension of this role.

7. Prospective Subscribers





In providing an online authentication service, the system is likely to appeal to a number of different organisations. The main factors these organisations would have in common is the requirement to enhance the security users require for access to online systems and to provide users with a device to facilitate this additional security. These subscribers, organisations who would benefit from such a service, include:

- ◆ **Government departments:** providing access to online government services by users and for remote access to online systems by government staff.
- ◆ **Banks:** providing customers with secure online access to services such as Internet banking.
- ◆ **Corporations:** providing employees access to online corporate services.
- ◆ **Online Merchants and Service Providers:** providing customers secure access to online goods and services.



Online Authentication Service Components

Legend

-  **Subscriber:** an organisation who subscribes to the service, using shared devices for two factor authentication.
-  **Issuer:** an organisation who issues devices to end users and subscribes to the service for two factor authentication.
-  **Issuer:** an organisation who issues devices to end users, shares their devices with the online authentication service but implements their own two factor authentication solution.
-  **DPI – ActiveDevice plug-in:** used for integration with the online authentication service for two factor authentication

8. Business Models

The two most significant costs in implementing a two factor authentication solution are the establishment of the service and the purchase and dissemination of end user devices. To offset these costs, a number of business models are available. Organisations can perform one or any number of the roles below which provide examples of how revenue can be generated from the solution.

8.1 Solution Provider

To offset the service implementation cost, the solution provider can charge all subscribers a fee for using the service. This fee could be in the form of an upfront or regular ongoing fee or through the system's reporting, a fee can be based on a per user, per device or per authentication calculation.

8.2 Device Purchaser

An organisation wishing to purchase a large number of devices would be in a position to negotiate a reduced device price due to the economies of scale. As the solution is device agnostic, discounts could be negotiated among the device suppliers. An agency fee can also be charged to each vendor.

8.3 Device Issuer

Organisations who issue devices to end users may share these devices with subscribers of the service. To recoup the cost of purchasing devices, device issuer's can charge other service subscribers a fixed fee per device or a per authentication charge. This not only means the end user only requires one token, it means the device issuer could receive revenue from issuing devices which may exceed the cost of purchasing the device over time.

8.4 User Identity Endorser

The system allows a device issuer to issue a user with a device, once they have verified the user's physical identity, and associate the user's identity with the device by enrolling them in the service. Organisations that currently require physical identity verification could utilise this device-identity association to offer substantially more automated online services without the need for additional physical verification.

As an example, when a bank customer opens a bank account, they may be required to perform a physical identity check with the bank or a bank's agent. If the customer is issued a device at the time of the physical identity check, the bank could allow the customer to automatically complete the enrolment of their bank account online, using the device as the verification of their identity. This device-identity association could then be used for any purpose, by organisations that subscribe to the service, without the need for physical verification.

9. ActiveAccess Solution

GPayments' ActiveAccess is an authentication platform providing two factor authentication for Internet transactions. By providing a high level and abstract authentication layer, it hides the intricacies of each specific device authentication process and simplifies the integration with a subscriber's online environment.

9.1 Device Independent Platform

ActiveAccess provides an abstract platform for two-factor authentication. By providing a high level and abstract authentication process, it simplifies integration of the service with existing organisation's online environment. It also hides the device specific intricacies of the authentication process.

As far as the organisation is concerned the process is exactly the same for any given authentication device. This provides the flexibility to roll out different types of devices to different groups of users and to have a seamless upgrade path to other authentication devices (such as CHIP card readers) when and if the need arises.

9.2 Quick Implementation; Lower Cost

Offering a two factor authentication service using ActiveAccess provides a cost-effective implementation in a secure outsourced environment, minimizing subscriber investment and reducing the implementation time. A service also reduces each subscriber's ongoing operational, support and maintenance costs.

9.3 Low Cost Devices

By providing a generic authentication service for potentially any vendor devices, negotiation on the cost of devices can lead to significant discounts.

9.4 Increased Security

A third party outsourced solution increases online security by segregating the task of authentication between a subscriber and the service provider. The subscriber handles the first factor of authentication with their existing username/password whilst the service provider verifies the second factor of authentication with the user's device.

This segregation of roles, provides a higher level of security as two independent parties are required for authentication of users and the user cannot be exposed to any one organization and their staff alone.

9.5 Device Agnostic

The solution is device and vendor agnostic. ActiveAccess supports a wide range of authentication devices, which allows issuers to select their preferred authentication vendor devices by weighing up the balance between user preferences and convenience, security and cost. It also allows issuers to change their preferred authentication device in the future without impacting their existing implementation or losing the value of their initial investment.

9.6 Easy Integration

With ActiveAccess implemented in an outsourced service, subscribers are required to integrate with the service hosted authentication server. To simplify this integration, a client software called the "Device Plug-In" (DPI) is provided. This simple DPI software is installed within the subscribers existing online environment and manages the messaging between the subscriber and service provider, digitally verifying the signed authentication messages.

9.7 Extensive Reporting and Customer Management

Through the Issuer Administration Application, ActiveAccess provides an extensive set of reports and functions, providing statistics about customer online authentication activity and enabling the Issuer to manage customer accounts.

9.8 Device Sharing

It is conceived that end users will receive their devices from either one of two organisations. Typically they would be issued a device from a large organisation with which they hold an account such as a bank. Alternatively they may be issued a device by an independent third party who verifies the customers identity at the same time as issuing the user a device. ActiveAccess has the facility to share the devices with other subscribers in each of these scenarios.

9.9 Privacy

By providing the second factor of authentication only, ActiveAccess does not compromise any of a users personal details. Therefore, there are no privacy issues surrounding the implementation of a two factor authentication service using ActiveAccess.

9.10 Single Sign-On and Federated Identity

ActiveAccess can also facilitate single sign-on or federated identity management integration by exposing web services interfaces to external parties and solutions.



Confidentiality Statement

This work is Copyright 2005 by GPayments Pty Ltd. GPayments reserves all rights to the confidential information and intellectual property contained in this document. This document may contain information relating to the business, commercial, financial or technical activities of GPayments. This information is intended for the sole use of the recipient, as the disclosure of this information to a third party would expose GPayments to considerable disadvantage. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any process without prior written permission.

Disclaimer

GPayments Pty Ltd makes no, and does not intend to make any, representations regarding any of the products, protocols or standards contained in this document. GPayments Pty Ltd does not guarantee the content, completeness, accuracy or suitability of this information for any purpose. The information is provided "as is" without express or implied warranty and is subject to change without notice. GPayments Pty Ltd disclaims all warranties with regard to this information, including all implied warranties of merchantability and fitness for a particular purpose and any warranty against infringement. Any determinations and/or statements made by GPayments Pty Ltd with respect to any products, protocols or standards contained in this document are not to be relied upon.

Limitation of Liability

In no event shall GPayments Pty Ltd be liable for any special, incidental, indirect or consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) whether in an action of contract, negligence or other tortious action, rising out of or in connection with the use or inability to use this information or the products, protocols or standards described herein, even if GPayments has been advised of the possibilities of such damages.