



ActivCard®

**How to Catch a Phish**

**White Paper**

[www.activcard.com](http://www.activcard.com)

# Table of Contents

---

**Executive Summary** ..... 3

**Gone Phishing: How Did This All Begin?**..... 4

    Hacker Origins ..... 5

    Very Clever, Very Dangerous ..... 6

**Building a No-Phishing Zone: What Can Banks Do Now?** ..... 7

**Hook the Phish: Anti-Phishing Solutions**..... 8

    Authentication through a Trusted Third Party ..... 8

    Shared-Secret Authentication ..... 8

    Time-Based Passwords ..... 9

**ActivCard Phishing Solutions** ..... 9

    ActivCard Token-Protected Online Consumer Banking ..... 9

    ActivCard PKI Authentication Solution ..... 10

*Phishing, as defined by Gartner Group, is a cyber-attack in which an attacker impersonates a trusted company or provider and sends out a bulk message (“the bait”), typically an email that directs consumers (“the phish”) to a fraudulent website to collect personal and financial information for identity theft.*

*Banks are the prime victims of phishing, representing 15 of the top 20 phishing scams, according to the Anti-Phishing Working Group. Phishing presents a serious challenge to banks, which must move quickly to increase online security or risk continued financial losses, increased insurance rates and customer alienation.*

## Executive Summary

---

Phishing is by far the most dangerous form of fraud to hit online commerce, costing U.S. banks alone \$1.2 billion in direct losses, increasing insurance rates and eroding consumer confidence in online transactions. The FBI calls phishing the “hottest and most troublesome” scam on the Internet, and the Department of Justice has created a special unit aimed at identifying and prosecuting the perpetrators of these scams.

According to the Anti-Phishing Working Group, banks are particularly vulnerable to phishing attacks, with 15 of the top 20 phishing scams aimed at the banking industry. In fact, worldwide banks that utilize static passwords for online access are considered those that are most exposed to potential phishing attacks. Phishing is remarkably sophisticated and successful, having fooled nearly 2 million online users into revealing personal and confidential information in the past two years. The most recent phishing attacks have targeted non-English speaking countries, such as France and Germany, a prime indication that this type of fraud is getting not only more sophisticated, but also gaining wide geographical spread.

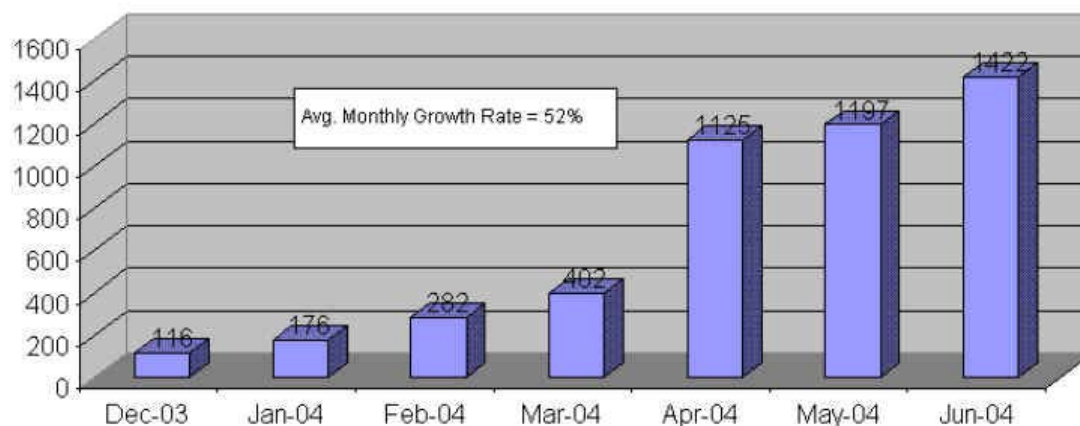
Industry analysts, alarmed by the success of phishing, are warning that the schemes threaten the very foundation of online commerce and fear that left unchecked, phishing could erode online commerce altogether. Phishing scams are growing daily, as these online criminals take advantage of weaknesses in web browsers and Internet authentication, especially the use of static passwords. Strengthening authentication and implementing solutions that will outsmart the phishers are critical to securing and growing your online commerce. One-time, time-limited passwords, multi-factor authentication, smart cards, and digital certificates are among the most prominent solutions available from the security industry.

## Gone Phishing: How Did This All Begin?

Not very long ago, spam seemed to be the most troublesome invasion for Internet users. Similar to telemarketing calls, online users found spam irritating and time-consuming, but not particularly dangerous. Phishing, which some experts have termed spam's "evil cousin," is a far more dangerous and costly phenomena.

Tracing the exact origins of phishing is impossible, however, analysts agree that most phishing attacks began in late 2003 and have risen exponentially during 2004. According to a Gartner Group report, approximately 57 million online users believe they have received a phish, 11 million have been lured to clicking on, and nearly 2 million users have been deceived into divulging personal and financial information. Until recently, most phishing attacks have been aimed at customers of banks in English-speaking countries, such as the US, UK and Australia, but lately a shift to countries like France, Germany and Brazil has become even more prevalent.

**Monthly Unique Phishing Attacks (December 2003 – June 2004)**

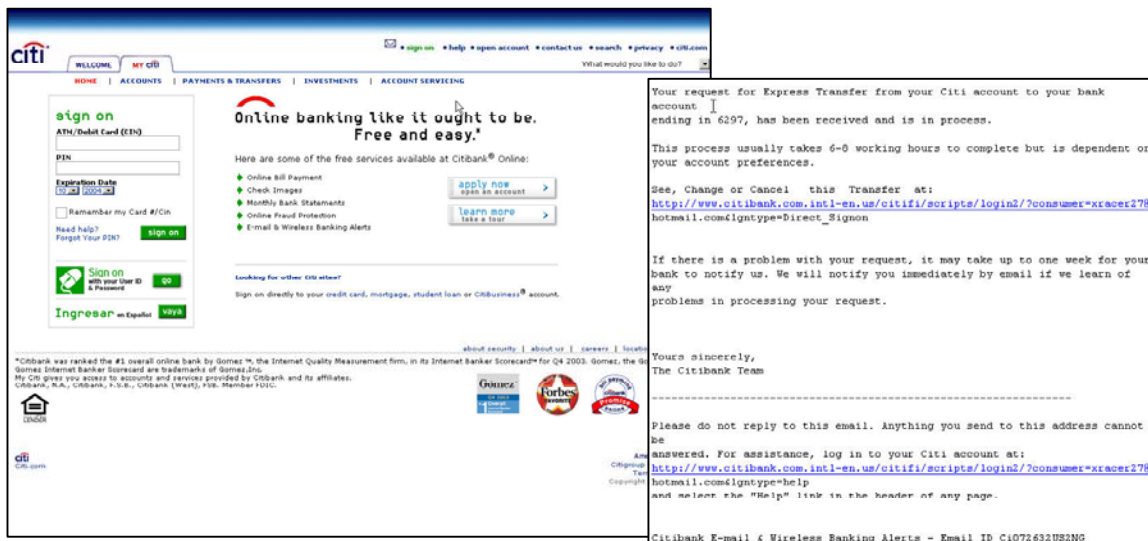


Source: Anti-Phishing Working Group ([www.antiphishing.org](http://www.antiphishing.org)).

Phishers create emails and websites that imitate the look and style of a reputable bank to outwit consumers. The emails are particularly effective, written in business language and asking the user for information. Some emails will present an innocent request, such as telling the consumer that the bank is updating information. It will then direct the consumer to a fraudulent website where the consumer is asked to enter personal information.

Other phishing attacks "bait" the user by sending false statements contained within the email that create the impression of an immediate threat or risk to the user's bank, credit card or financial account. A typical phish will read, "We are in process of updating your account. To ensure security you must re-enter and verify all of your information. If we don't receive a reply within five working days, access to your account may be denied." The consumer is then asked to complete a false "application verification."

## How to Catch a Phish - White Paper



Sample phishing attack imitating Citibank.

The Department of Justice, in the Special Report on Phishing issued on March 2004, warned that once phishers have captured the information, the consumer could be compromised in three significant ways.

1. **Loss of Funds.** Using the data obtained, phishers can access existing accounts to withdraw funds and purchase expensive merchandise or services online.
2. **Identity Theft.** Phishers can also create new bank or credit card accounts in the victims' names, and use the new accounts to cash bogus checks paying themselves, take out loans or purchase merchandise. Phishers are sophisticated and will often open new accounts using the victims' names, but with a different address. Victims may not realize they are a target of identity theft fraud until creditors contact them or they check their credit reports.
3. **Viruses and Spyware.** On occasion, phishing schemes may deploy computer viruses and worms to disseminate the phishing emails to more people and add spyware onto the user's computer.

## Hacker Origins

The word "phishing" has its origins in the underground language used by hackers. It first entered the Internet lexicon in 1996 when hackers were stealing America Online accounts and passwords. Always clever, these early hackers defined their crime as "sport," instituting angling metaphors to describe their work. They would send email "lures" (i.e. hooks or bait) to "fish" for passwords and financial data from the Internet "sea" of millions of users.

The "ph" instead of the "f", used in hacker language, is an acknowledgment to the original form of hacking known as phone phreaking, invented in the 1970s. A blue box emitting audible sounds let the phreakers hijack phones, placing thousands of dollars in long distance calls. The legitimate phone line owner would not know of the fraud until a bill for the unauthorized phone calls arrived in their mailbox.

From the earliest days of hacking to today's phishing schemes and other forms of fraud, success is achieved because consumers or companies are oblivious to the fraud for some period of time –

## How to Catch a Phish - White Paper

minutes, hours, days or weeks. Hackers and phishers work in the anonymous world of the Internet, which makes tracing these criminals extremely difficult. In addition, fraudulent websites are up for an average of only two days, disappearing before anyone is even aware of their existence.



## Very Clever, Very Dangerous

The remarkable success of phishing attacks has alarmed law enforcement, financial institutions and consumers. Phishing works, in part, because it is sophisticated, clever and quite diabolical. Phishing uses a bank's good name and the trust of its customers to lure unsuspecting users into divulging confidential information. Public education is helpful, but that alone will not stop phishing and increased warnings will discourage consumers from using online commerce. Criminal indictments and harsh penalties will help, but making something illegal has never stopped criminal activity in the past, and will not do so now.

The sheer number of phishing attacks is alarming. The Gartner Group reports that 57 million (47 percent) of U.S. adults have, or think they have received a phishing attack email. Nearly 11 million adults (19 percent) report clicking on the link in the email, and approximately 1.8 million (3 percent) remember giving phishers sensitive information, including credit card numbers, checking account information, and social security numbers and billing addresses.

Phishing attacks more than bank accounts; it attacks the fundamental foundation of online commerce, trust. Left unchecked, Internet analysts fear that phishing will slow and possibly erode online commerce altogether. A recent Gartner poll revealed 58 percent of consumers who shop, bank or pay bills online are "very concerned" about online security and only 22 percent believe banks are "extremely competent" in protecting their information. In another study, Javelin Strategy reports consumers by an 8-to-1 margin to be letting fears of identity theft affect their use of more advanced online financial services.

The Gartner Groups warns, "Unless consumers' security concerns are adequately addressed ...the recent annual growth rates of 20 percent or more will shrink more than they based on the nature of the expanding user base. If phishing antidotes are not implemented consumer trust will erode and annual U.S. e-commerce growth will slow to 10 percent or less by 2007."

Phishing has even made its way into the national security debate. A phishing scheme appeared under the name of the Federal Deposit Insurance Corporation (FDIC). An email appeared telling consumers that the FDIC had denied insurance due to suspected violations of the Patriot Act. The email then warned "As a result Department of Homeland Security Director Tom Ridge has advised the Federal Deposit Insurance Corporation to suspend all deposit insurance on your account until

such time as we can verify your identity and your account information. Please verify through our IDVerify below." Consumers were then sent to a fraudulent website. Financial institutions and the government fear these kinds of attack could be deliberate attempts to undermine the financial integrity of the nation's banking system.

## **Building a No-Phishing Zone: What Can Banks Do Now?**

---

The success of phishing cannot be blamed entirely on naïve or uninformed consumers. Beyond its uncanny ability to fool consumer, phishing takes advantage of specific weaknesses in web browsers and Internet authentication, especially the use of static passwords. In testimony before a congressional committee investigating fraud, Internet security was compared quite convincingly to airport security. A simple photo ID check does not strengthen the airport's infrastructure, the committee was told, and neither do simple, static passwords strengthen Internet security.

Online commerce has been living on borrowed time for quite awhile now, relying on consumer trust, goodwill and simple authentication techniques to protect its assets from fraud. Phishing has ended any hope that online commerce would not be the target of serious attacks. Experts also predict that phishing attacks will grow even more sophisticated, and each attack has the potential to damage a bank's brand, reputation and credibility.

Internet security has risen to meet each challenge advanced by online commerce, developing new tools, including encryption and anti-spam software to shore up weaknesses. Banks and other online commerce sites are also relatively good at spotting a phish attack, but only after it has occurred and, by then, a customer's account may already be compromised.

In the past, credit card companies faced similar challenges and have made great strides in preventing and detecting fraud. Credit card companies are now very astute at spotting fraudulent activity and shutting down a suspect account. Gartner Group reports that 21 percent of consumers learn about credit card fraud through the card's issuer, whereas only 13 percent of consumers learn that their checking accounts have been hijacked from the bank.

Online consumers are also more likely to blame poor Internet security when their accounts are compromised, whether or not it is true. A Gartner Group survey of fraud victims 17 percent felt their information "had been stolen off the Internet" compared with 10 percent who thought the fraud was a result of a lost wallet.

Banks need immediate solutions to defend against phishing attacks while they investigate more long-range, comprehensive solutions. Several more long-term solutions are emerging and research is underway to prevent Internet fraud including caller ID for the Internet and increased infrastructure security. But banks need to make changes today.

To make the right selection, a solution must provide banks with several critical elements of the solution must:

- Authenticate both the sender (the bank) and the user (the customer)
- Be cost effective and standards-based for the bank
- Be easy to implement and understood by the customer
- Add value to the bank, increasing its credibility with the customer

## Hook the Phish: Anti-Phishing Solutions

---

Banks now face enormous pressure to quickly and effectively shore up their online commerce sites. Many long-range solutions are in the works, but immediate solutions are necessary to ensure the well being and growth of online banking commerce.

A review of anti-phishing solutions reveals a general agreement about where the technology is heading to prevent phishing attacks. Most concentrate on managed anti-phishing services, password management, user and provider authentication through a trusted third party, shared-secret authentication and Internet caller ID.

### Managed Anti-Phishing Services

Anti-Phishing Services work to quickly detect a phish attack after it has been launched and to minimize damage by monitoring accounts that have been compromised. The services try to catch phishers by monitoring suspicious domains or trying a version of entrapment, setting up false accounts to try and bait the phisher at his own game. These services are aimed more at catching phishers, than preventing attacks. Once an attack has been made, the services use varied methods to shut the phisher down.

### Internet Caller ID

Many companies are working on creating an Internet Caller ID, similar to caller ID for the telephone. This solution would correct weaknesses in Internet security and web browsers, but will also involve major Internet infrastructure changes and significant changes in commonly used web browsers. Industry experts agree that although the solution is very promising, Internet Caller ID is more of a hype technology rather than a solution ready for mass deployment.

### Authentication through a Trusted Third Party

Employing smart cards and biometric authentication, online commerce sites can employ a trusted third-party approach to secure their transactions. Users would have to verify their identity through a fingerprint or other biometric method. Practical for static participants, the system may be too complex and economically unfeasible for banks, which have a changing consumer base.

### Shared-Secret Authentication

A consumer would select a secret that is shared only with the bank, such as a photo of the family pet. The picture is then displayed to the consumer when he or she logs on, and the consumer would have to verify the secret to continue. The secret is not entered during the login process, so even if a phisher captures a consumer's account information, he would be unable to access the account because he doesn't know the secret. This type of shared-secret authentication, however, raises numerous questions regarding privacy issues and is impractical for banks with a global customer base with differing laws and cultural sensitivities. Shared-secret authentication schemes must be more sophisticated and be based on modern cryptographic technology.

## Time-Based Passwords

The quickest way to prevent most phishing is the use of token-protected, time-limited passwords. Almost all industry experts believe that static passwords have no place in online banking and e-commerce and that they will soon be obsolete. Requiring little consumer education and cost effective to employ, time-limited passwords may prove to be the first defense against phishing attacks. Proven to be scalable, low total cost of ownership and robust enough, time-based passwords can be rapidly deployed and seamlessly integrated with other bank applications.

## ActivCard Phishing Solutions

---

ActivCard delivers two solutions aimed at thwarting phishing: ActivCard Token-Protected Online Consumer Banking and Public Key Infrastructure (PKI) Authentication.

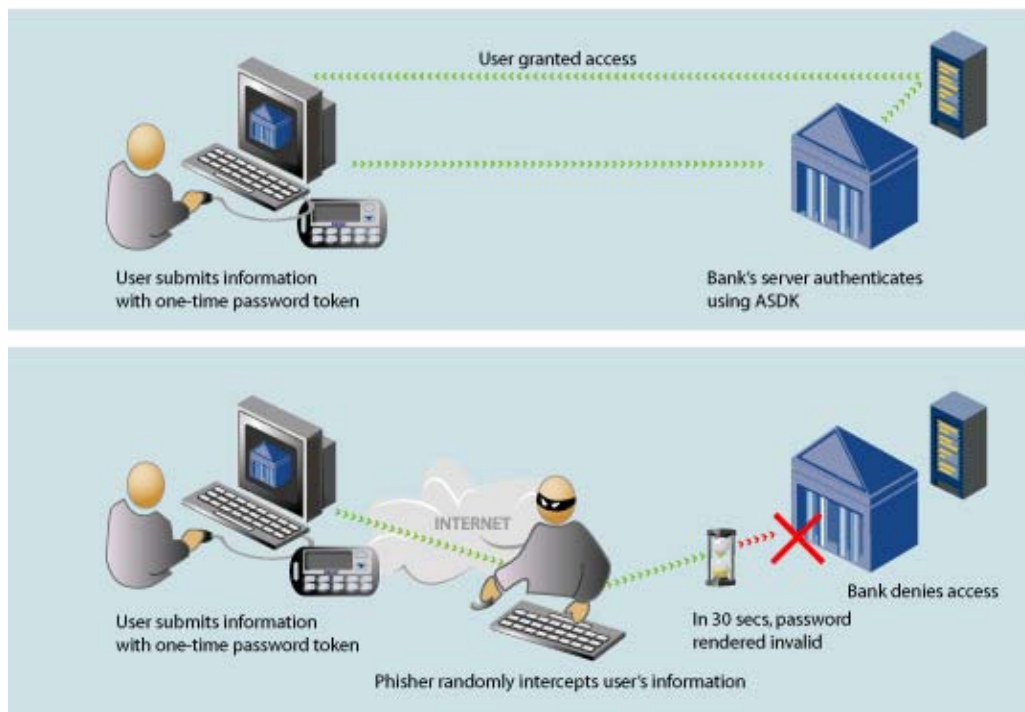
### ActivCard Token-Protected Online Consumer Banking

Static passwords, at this point, have become a dangerous gamble for both online users and the online banking systems they employ. Once stolen by a phisher, a password can be used to steal funds, set up new accounts and even steal a customer's identity.

ActivCard Token-Protected Online Consumer Banking is an advanced, multiple network and access point security solution providing banks with the full benefits of online banking and e-commerce. Designed for immediate implementation, the Token-Protected Online Consumer Banking solution can be easily added to a bank's network infrastructure, without any additional software required on a user's computer, delivering critical safeguards against phishing. To protect customers from phishing attacks, the Token-Protected Online Consumer Banking solution allows administrators to set a time limit on passwords. For example, a password could be effective for only 30 seconds, allowing customers to access account information, but making the token, should a phisher steal it, virtually useless.

Housed within the bank's infrastructure, the solution is fully synchronized with ActivCard devices, facilitating and managing all remote login requests by B2C, B2B and mobile users. A multi-factor authentication solution, Token-Protected Online Consumer Banking is built with proven technology that empowers financial institutions to provide secure remote banking services from anywhere around the globe, allowing banks to significantly reduce major losses due to phishing and other fraud.

Token-Protected Online Consumer Banking handles credential and password management for the user, making the solution easy for customers to use. By leveraging a user's identity and credentials only once during login, it establishes the security context for seamless access to applications and resources, safeguarding against the tools used by phishers. Multi-factor authentication is housed in a single, centralized environment, making administration easy and eliminating the need to deploy disparate authentication solutions. Administrators will also find the solution easy to implement, eliminating the need to deploy disparate authentication solutions.



## ActivCard PKI Authentication Solution

Phishing attacks succeed because once the phisher has obtained a user's account information, they in effect, have stolen the user's identity. If the phisher gets to the user's account, third-party authentication will stop them cold.

Often termed "spoof-proof" for its ability to outsmart phishers, ActivCard's PKI Authentication solution is a more comprehensive solution that requires a third-party certificate authority to authenticate communications between the bank and its commercial customers. The system uses ActivCard's proven Universal Serial Bus (USB) Key and ActivClient™ smart-card middleware to support high value, high risk transactions with commercial banking customers. The PKI solution for B2B users also adds additional functionality such as signing documents enabling rapid and low cost business transactions.

Housed within the bank's infrastructure, the third-party authenticates communications between the banks and its customers, reducing the ability of phishers to create a fraud scenario. The PKI-based mutual authentication never reveals the private key to the other party, ensuring the phisher cannot intercept the authentication. Private keys and user credentials are encrypted and kept securely on a portable USB token

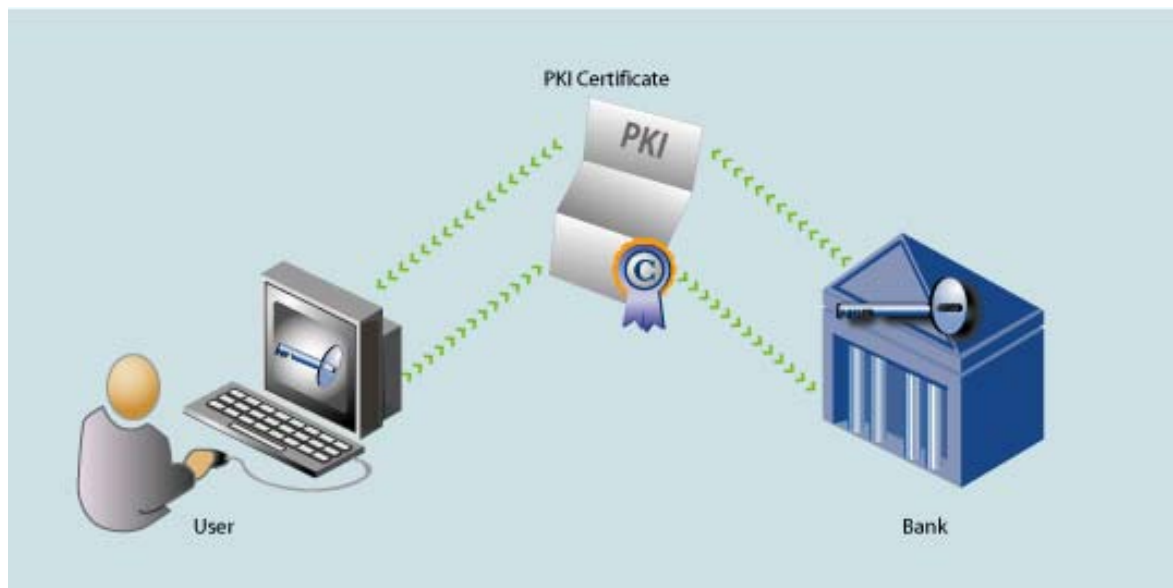
ActivClient provides multi-factor, strong authentication to a variety of services on PCs. Through the use of smart cards and USB keys for PKI services, ActivClient dramatically improves PC and network security. ActivClient enables secure desktop applications, network login, web login, email and transactions. One-time-use passwords are dynamically generated and processed in the smart card or USB key with an ActivCard patented three-variable algorithm. Secure digital certificate management and key storage occurs in the protected environment of the device itself for increased security and confidence.

Working with the ActivClient, ActivCard Card Management System (CMS), and a Certificate Authority (CA) Server either through a trusted third-party (TTP) or the bank, the PKI Authentication solution

*How to Catch a Phish - White Paper*

delivers a complete, trusted third-party solution that protects a customers' identity. This solution is available with all appropriate forms of devices from ActivCard, in particular ActivCard USB Key and ActivCard USB Key Java that support comprehensive managed digital identity and consolidated credentials, offering all the power of an advanced PKI solution packed in a simple portable form.

PKI Authentication enables flexible transition from static passwords, which are dangerously weak, to strong authentication and multiple credentials on one proven USB device. PKI keys and certificates for authentication provide additional functions including digital signatures, secure email and encryption will deliver comprehensive security.



## Legal Information and Notice

**ActivCard Intellectual Property:** This document or deliverable(s) contain proprietary information of ActivCard Corp. and/or its subsidiaries and affiliates (collectively, "ActivCard") embodying confidential information, ideas, and expressions, no part of which may be reproduced or transmitted in any form or by any means, electronic, mechanical, or otherwise, without prior written permission from ActivCard. This document may not be modified, copied, distributed, transmitted, displayed, performed, reproduced, published, licensed, derivative works created there from, transferred, or sold unless expressly agreed by ActivCard. The furnishing of this document does not imply or expressly provide a license to any of ActivCard's intellectual property.

**Copyright Notice:** Copyright © 2004 ActivCard, Inc., 6623 Dumbarton Circle, Fremont, California 94555 USA. All rights reserved. This document and ActivCard software products are protected by United States copyright laws and international treaty provisions.

**Trademarks:** ActivCard, ActivCard (logo) and/or other ActivCard products or marks referenced herein are either registered trademarks or trademarks of ActivCard in the United States and/or other countries. The absence of a mark, product, service name or logo from this list does not constitute a waiver of ActivCard's trademark or other intellectual property rights concerning that name or logo. The names of actual companies, trademarks, trade names, service marks, images and/or products mentioned herein may be the trademarks of their respective owners. Any rights not expressly granted herein are reserved.

**Patents:** ActivCard may have patents, pending patent applications, and/or other intellectual property rights covering subject matter contained in this document or deliverable(s).

**Export Control:** ActivCard products, programs, or services referenced in this publication may not be available in all countries in which ActivCard operates due to export restrictions or changes in market conditions. Recipient agrees to comply fully with all relevant export laws and regulations, including but not limited to the U.S. Export Administration Regulations (collectively, "Export Controls"). Without limiting the generality of the foregoing, Recipient expressly agrees that it shall not, and shall cause its representatives to agree not to, export, directly or indirectly, re-export, divert, or transfer the software, programs, documentation, materials, specifications or any direct product thereof to any destination, company or person restricted or prohibited by Export Controls. In the event that Recipient provides the software, programs, documentation, materials, specifications or any direct product thereof to a third party located in any destination outside the country of delivery by ActivCard, Recipient shall ensure that it enters into a written agreement with such third party that protects ActivCard's rights and interests to the same extent protected hereunder and specifies ActivCard as a third party beneficiary. Recipient agrees to provide a copy of such agreement to ActivCard at ActivCard's request and to assist ActivCard, at Recipient's expense, in enforcing ActivCard's rights if ActivCard is not recognized as a third party beneficiary in the applicable jurisdiction.

**Disclaimer:** This publication is intended for informational purposes only. ActivCard makes no warranties, express or implied in this document. Furthermore, the information contained in this document has not been submitted to any formal testing and is distributed 'AS IS'. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the recipient's ability to evaluate and integrate them into an operational environment. While each item may have been reviewed by ActivCard for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Attempts to adapt these techniques to any environment are done so at their own risk. Information in this publication was developed in conjunction with the use of the hardware, software, and networking arrangements specified and is thus limited in application to those specific hardware and software products and levels. The information contained herein is not intended as a specification of any programming interfaces that are provided by ActivCard. This document is subject to change without notice and does not represent a commitment on the part of ActivCard. This document may contain information about product functionality not available in your product release.

[www.activcard.com](http://www.activcard.com)

**ActivCard**  
TEL: +1 (510) 574 0100  
FAX: +1 (510) 574 0101  
[info@activcard.com](mailto:info@activcard.com)

PHI.WP.L.10/04.PDF