



dynapass™

U.S. Patent #6,993,658

SECURING YOUR SECURITY®



White Paper

DynaPass® Customer Authentication for Online Banking

**The Affordable Authentication Solution
for Financial Institutions**

September 2011

WHITE PAPER

DynaPass® Customer Authentication for Online Banking

The Affordable Authentication Solution for Financial Institutions

DynaPass Inc.

Background

The WorldWideWeb began in 1991, with the invention of the first Internet browser. By the mid-nineties most significant corporations had websites, and financial institutions were beginning to offer online banking services. Today, online banking is an expected feature for any financial institution, and over 60% of U.S. financial institution customers prefer to bank online¹ – a number that will continue to rise.

Both financial institutions and their customers benefit from the convenience and automation of online banking, and the industry has moved rapidly to provide services via this channel. At the same time, financial institutions have had to face new security risks associated with delivering services over a public network – something they had never done before. And indeed, criminals took advantage of this situation from the onset, attacking security weaknesses, posing as valid customers, and stealing money from online customers' accounts.

Attacks on online banking quickly captured the attention of the U.S. Federal Government, and in 2001, the Federal Financial Institutions Examination Council (FFIEC) issued guidance to banks for establishing secure authentication of online banking customers. As attacks continued to increase in frequency and sophistication, the FFIEC revised their guidance in December 2005, and stated that simple logon credentials such as username and password were insufficient for controlling access to banking functions involving transfer of money and access of personal account information. The FFIEC also just released a Supplemental Guidance to Internet Banking Authentication Guidelines.²

The problem with simple logon credentials is that they can be easily stolen – most frequently by “phishing” – an attempt to fraudulently acquire personal information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. The Anti-Phishing Working Group reports that the country that hosts the most phishing websites and attacks is the USA, and more than 80% of all phishing attacks are aimed at financial institutions and their customers.³

More recently, attackers have begun to implement an even more sophisticated attack called “Man-in-the-Middle” (M-i-M), where they interpose a fake website between the bank and its online customers. Using a M-i-M attack, the attacker can literally hi-jack an online banking session, appearing to be the financial institution to a real customer, and appearing to be the customer to their financial institution – but using the session to alter the transactions and shift money into the attacker's own account. M-i-M attacks are expected to increase in frequency as hackers have published M-i-M code on the Internet, and it is now more available to a large number of electronic criminals.

There is no way to completely defeat phishing or M-i-M attacks, but there are means of limiting their effects, so that online transactions can be sufficiently protected. The best way to deal with the problem of stolen logon credentials is to add



another “factor” for identifying a valid customer, beyond just their username and password (information that can be stolen by phishing attacks). The additional factor is something more than just information – it is either something the customer “has”, or something tied to a customer’s “intrinsic” physical characteristics - for example a fingerprint.

Two-factor for identification are typically used in point-of-sale (POS) and Automated Teller Machine (ATM) transactions. For example, credit card POS transactions use something the customer “has”: the card – and an “intrinsic” identifier: their signature. ATM transactions are protected not only by something the customer “knows”: their PIN – but also by something they “have”: their ATM card. The power of using two-factor authentication for remote transactions is evidenced by the US ATM system, which has been operating virtually flawlessly and securely for over 30 years, and handles over 12 billion transactions annually in the US.⁴

Two-factor authentication systems use any two of the following three factors:

1. Something the customer “knows” (a PIN or password, for example).
2. Something the customer “has” that is unique to them.
3. Something “intrinsic” to the customer (such as a fingerprint or signature).

Two-factor authentication systems have also been in use on the Internet for several years – mostly by corporate enterprises that provide a secure method for employees to logon to the corporate internal intranet from an Internet connection. Instead of an ATM card, the employees are issued a small electronic device that generates a one-time password (OTP). The OTP changes each time the user logs on, so if the password is stolen, it cannot be re-used by a thief. Furthermore, the OTP is created by a special cryptographic algorithm that includes a unique identifier linked to the valid device owner. When the device owner logs on to the corporate network over the Internet, they use two-factor – something they “know” (their logon name and/or password), and something they “have” – the OTP device (that is linked specifically to them). This method has proven to be extremely secure and is currently in use by many corporations. Although OTP solutions like this are very effective for this type of application, they are also costly – not only to deploy, but also to maintain. Strict controls must be placed on the process of activating devices for new employees and de-activating them for old employees, or when devices are lost or stolen.

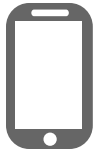
When faced with the FFIEC guidance that simple “single factor” authentication (based only on what a customer “knows” – their username and password) is insufficient for online banking, financial institutions first looked to OTP solutions as a possible way of complying with the guidance. However, solutions engineered for securing corporate networks serving a few thousand employees do not fit consumer banking needs for securing transactions for millions of customers. The expense and complexity of provisioning OTP devices and maintaining a customer base of that size – and accommodating the rapid entrance and exit of customers does not make typical OTP systems financially or logistically feasible for financial institutions.

A more affordable solution appeared on the market, based on “shared secrets” . . . information that only a customer’s bank knows about them, and information that only a customer knows about their bank/account. In theory, this system could protect an online session from attackers, by providing a mutual authentication between the parties, however it has since been shown to provide no protection against M-i-M attacks, as the attacker can easily pass the “secrets” in both directions, while altering the actual transactions in the session – going completely undetected until it is too late.

Mobile Phones as Authentication Devices

While distributing OTP devices are not economically feasible for banks, over 85% of the US population – and virtually 100% of online banking customers (see figure right) – already have personal devices that can be used for identifying them: namely, their mobile phones. Mobile phones can be used for securely delivering OTPs to online banking customers.

Mobile phones are much more powerful communication tools than many people realize. In fact, almost all mobile phones on the market today include the following functionality:



- Audio (voice) communication.
- SMS (Short Message Service) 2-way text messaging.
- MMS (Multi-media Message Service) 2-way delivery of media such as pictures, video clips, etc.
- Downloadable applications via mobile phone app store/market.
- User Applications offering convenience for the user – such as camera, games, calculators, calendar, etc.

(“Smart phones”, such as Blackberry®, Palm®, iPhone®, Android® and various devices powered by the Windows Mobile® operating system are capable of even more functions, including email and the ability to run larger application programs like Word® or Excel®, including downloadable applications from 3rd party vendors.)

When looking at ways of using mobile phones for delivery of OTPs, there are several options:



1. Generate the OTP from a centralized server and send it to the phone via a message (SMS being the simplest, lowest cost and fastest method).
2. Generate the OTP locally on the phone, using an application that has either been:
 - installed on the phone by the manufacturer or carrier.
 - downloaded to the phone after delivery to the customer.
3. Android®, iPhone®, RIM, Symbian, and Windows Mobile-OS enabled application.

The table on the next page compares these options and some of the important considerations for choosing the best method. Given the options summarized in the table, it is clear that only two are capable of reaching a large percentage of bank customers: the centrally-generated OTP sent via SMS, and the OTP generated by a WAP application. Of these two, only the OTP sent via SMS offers a simple user experience and acceptable speed.

	OTP generated centrally and sent to phone via SMS	OTP generated by application downloaded to smart phone by user	OTP generated by a separate security token device
Potential portion of market served*	> 100%	Less than 1% of mobile phones utilize token software on handsets	Less than 10% of corporate market uses token devices
Strength of security/market adoption	Best level of security with high adoption rates using ubiquitous device and delivery method, the mobile phone and text messaging	Moderate level of security with low adoption rates due to software download requirements and only available on certain handsets	Moderate level of security with largest security breach reported in 2011. ⁵ Adoption rates have decreased dramatically as tokens become unreliable and too costly to deploy/manage
Speed of OTP delivery	2-4 seconds	Immediate	> Every 20-30 seconds
Simplicity for user	Simple (SMS used by 100% of cell phone users)	Moderate (after downloading)	Used only by large enterprise / banking institutions
Cost of capable phone and or token device	Low	High	Extremely High
Available, regardless of cell service carrier?	Yes	Yes	Yes
Requires cell network connection?	Yes	No	No

* portion of all mobile phones and/or security token devices with functionality to support the methods shown.

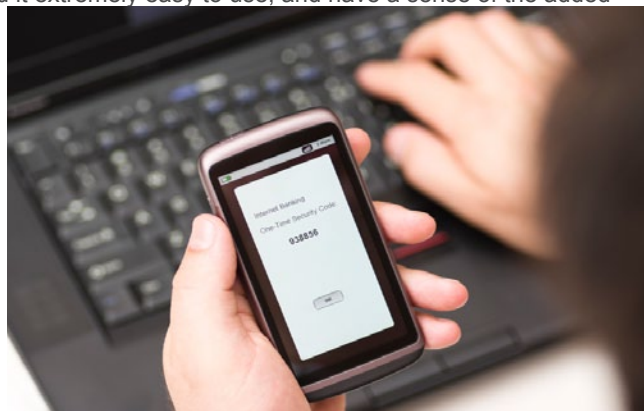
DynaPass® Patented OTP-over-SMS Solution

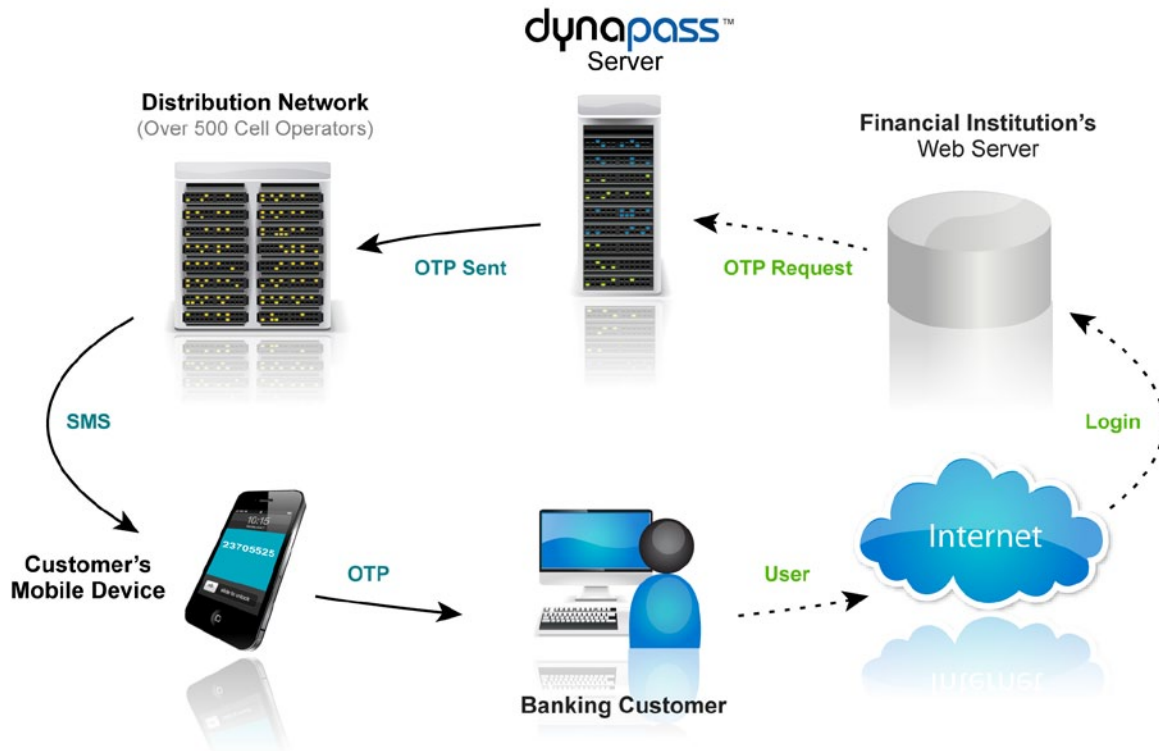
DynaPass Inc.'s patented **DynaPass® OTP System** offers financial institutions all the advantages of OTP-over-SMS, and has been proven in commercial enterprise operation. Users find it extremely easy to use, and have a sense of the added security it provides for protecting their private information.

DynaPass® is also simple for financial institutions and their online banking hosts to install and operate. The figure below shows the main components of the patented **DynaPass®** solution, and how they operate together to provide true two-factor secure customer authentication.

First, customers enroll their mobile phone number with their financial institution using a secure enrollment process, similar to the way credit cards are activated. Once enrolled, the customer's mobile phone number is associated with their account in a database managed by the **DynaPass®** server. The **DynaPass®** server interfaces directly with a financial institution's existing web server.

When a customer logs on to the online banking website, the **DynaPass®** server generates an OTP, sending it simultaneously to the Web server and to the customer's mobile phone. The message is sent to the mobile phone via an SMS message through an aggregation network that can reach virtually any mobile phone through links with all major carriers. The process typically takes about 2-4 seconds. Once the customer has the OTP on the phone, they read it and enter it into the logon screen on the financial institution's website. The Web server then uses its standard logon authentication code to compare the OTP received from the customer to the OTP generated by the **DynaPass®** server. If there is a match, the customer has been authenticated with two factors – their logon ID and an independently-generated OTP associated uniquely with them via their mobile phone number.





Since the OTP is generated based on the customer's "second form of identification" – their unique mobile phone number – and transmitted to them across a private mobile phone network independent of the Internet, there is an extremely high degree of assurance of the customer's identity – true two-factor authentication!

Furthermore, users typically embrace the experience enthusiastically, appreciating the true sense of personal security and ease of use. Users familiar with token-based two-factor authentication had the following responses to using **DynaPass®**:

- Users preferred DynaPass® to other multi-factor authentication methods.
- 75% of participants rated DynaPass® as "extremely easy to use." The remaining 25% rated it as "fairly easy."
- Users were asked to rate DynaPass® against a token device on a scale of 1 to 10 (with 10 being the best score), and gave it an average ranking of 9.
- Users like the "hip" factor of TEXT messaging.

Sample comments from current users include:

"... the response time for the return text message was much quicker than I expected."

"This is REALLY neat – it is so quick, and really gives me a sense of the added security."

"I LOVE this method. I always have my phone with me. The response is quick and always works."

DynaPass®/DynaPay® + Mutual Authentication

As stated earlier, the “Man-in-the-Middle” attack presents a looming threat to online services – and this attack cannot be detected by most OTP solutions alone. For example, the attacker can intercept the customer’s OTP and pass it along to the financial institution, so it appears that the valid customer is logged on, while the attacker gains control of the session and can divert transactions to their account. DynaPass Inc.’s patent pending **DynaPay™** + solution not only validates the customer to the financial institution, but also validates the financial institution to the customer, to combat M-i-M attackers.

Complimentary Products and Services – and the Move to Mobile Banking

It is important for financial institutions to consider the current wave of “mobile banking” initiatives . . . and this time, it appears that the infrastructure, relationships and customer “pull-through” is sufficient to sustain the trend. A recent analyst’s report estimates that by the end of 2012, mobile banking will be used by 60% of banking customers¹. So, in order to remain competitive – particularly with the tech-savvy generations – financial institutions are considering how best to proceed with delivering more mobile services – including account inquiries, alerts, money transfers and bill-pay. As stated earlier, there are four main options for delivering mobile services:

1. **Messaging (typically SMS, but may expand to include MMS).**
2. **Applications that are installed by the carrier or manufacturer and delivered with the phone.**
3. **Applications that are downloaded to smart phone devices by the user.**
4. **Android®, iPhone®, RIM, Symbian, and Windows Mobile-OS enabled applications.**

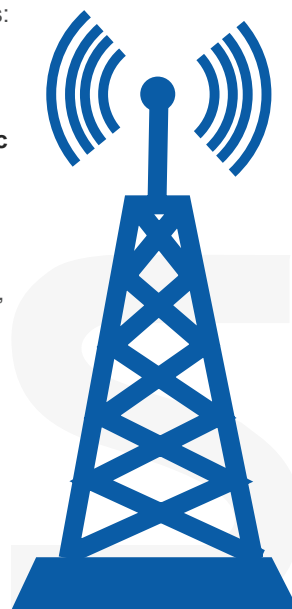
Mobile banking solutions are starting to appear using each of these technologies – some of them tied to specific carriers and devices, while some attempt to address wider audiences by focusing primarily on message-based services, such as account balance or credit card charge alerts. One encouraging trend is that banks, mobile phone carriers, and device manufacturers are beginning to find ways to cooperate and support business models that are sufficiently equitable to all, in order to serve the customer demand for mobile banking.

DynaPass Inc. is committed to delivering secure solutions for all types of remote delivery of banking services . . . including the Internet, as well as, mobile networks. We have developed technology for securely authenticating customers using two-factors for both mobile and online access. **DynaPass® enables banks to take the first step into a mobile-enabled application that not only solves a major security problem for online banking, but also gets customers accustomed to using their mobile device for a banking application.**

DynaPass Inc. also provides one other product that complements the basic **DynaPass®** offerings:

- **DynaAd™ mobile messaging and advertising platform that helps banks communicate with their customers, and provides demographic and psychographic targeted messaging and advertising.**

All of DynaPass Inc.’s solutions for the financial industry are based on SMS and MMS technology, assuring that virtually all mobile phone users can benefit from these services, and the additional security of true two-factor authentication. DynaPass Inc. is a full-service solution provider, since 2004, providing security consulting, system design, integration, and support services.



Summary

DynaPass[®] is one of the best products available to banks today to help them solve security issues, while delivering better service to their customers:

- **Meets FFIEC guidance** for online banking customer authentication.
- **Provides first steps toward mobile banking** services.
- **Delivers security solutions** for both online and mobile banking transactions.
- **Reaches virtually 100% of online customer base** via simple and secure SMS messaging.
- **Stays ahead of Internet hackers**, and protecting private customer information with **DynaPay**[™] protection against Man-in-the-Middle attacks.
- **Provides a “Zero Footprint Solution”** – the one-time password is sent to a device you already have with nothing additional to deploy or install on the device (phone, pager, tablet, etc...).
- **Based on proven and patented technology** – two-way, two-channel authentication.
- **Delivers potential revenue generating services** – product and service advertising and messaging when combined with **DynaAd**[™].

For more information contact:

DynaPass Inc.
John Trinh
COO
Phone: 855-DYNAPASS
Email: john.trinh@dynapass.com

References

1. Survey: Online Banking Surges, Mobile Lags, Jackie Stewart, American Banker, Sept 8, 2011.
http://www.americanbanker.com/issues/176_175/online-banking-surges-1042001-1.html
2. FFIEC Releases Supplement Guidance to Internet Banking Authentication, Federal Financial Institutions Examination Council, June 28, 2011.
<http://www.ffiec.gov/press/pr062811.htm>
3. Phishing Activity Trends; Report for the 1st Quarter 2010, Anti-Phishing Working Group.
http://www.antiphishing.org/reports/apwg_report_Q1_2010.pdf
4. ATM Use in the United States, Tyler Metzger, CreditCards.com, March 2, 2010.
<http://www.creditcards.com/credit-card-news/atm-use-statistics-3372.php>
5. EMC's RSA Security Breach May Cost Bank Customers \$100 Million, Bloomberg News, June 8, 2011
<http://www.bloomberg.com/news/2011-06-08/emc-s-rsa-security-breach-may-cost-bank-customers-100-million.html>

