

WHITE PAPER

Reducing Friction and Cost of Customer Interactions: Leveraging Mobile Devices to Deliver New Services and Multifactor Authentication

Sponsored by: ClairMail Inc.

Sally Hudson

Stephen D. Drake

August 2006

IDC OPINION

The ability to identify who is using a computer system or network is of critical importance. The primary means of identification has long been through use of a password. However, passwords can be shared, stolen, or guessed. To have stronger authentication, enterprises historically have relied on hardware tokens.

Today, the idea of utilizing a customer's cell phone as a token for two-factor authentication has moved from theory to practice. For banking and financial institutions, this approach can offer the following immediate benefits:

- Security beyond username and password, offering Federal Financial Institutions Examination Council (FFIEC) compliance
- Easy implementation for IT, no extra hardware requirements
- Easy for customers to understand and utilize
- Stronger user adoption — mobile phones are critical to users; fobs and tokens are not
- No extra device for customers to carry, reducing cost and complexity
- Lower costs of implementation and maintenance

METHODOLOGY

IDC's industry analysts have been measuring and forecasting IT markets for more than 30 years. Our software industry analysts have been delivering analysis and prognostications for packaged software markets for more than 25 years.

The actual strategy for doing so incorporates information from five different, but interrelated, sources:

- Reported and observed trends and financial activity in 2004 as of the end of April 2005, including reported revenue data for public companies trading on North American stock exchanges (CY 1Q04–4Q04 in nearly all cases)

- ☒ IDC's *Software Census* interviews (IDC interviews all significant market participants to determine product revenue, revenue demographics, pricing, and other relevant information.)
- ☒ Product briefings, press releases, and other publicly available information (IDC's analysts meet with hundreds of vendors each year. These briefings provide an opportunity to review current and future product strategies, revenue, shipments, customer bases, target markets, and other key product information.)
- ☒ Vendor financial statements and related filings (Although many software vendors are privately held and choose to limit financial disclosures, information from publicly held companies provides a significant benchmark for assessing informal market estimates from private companies. IDC maintains an extensive library of financial and corporate information focused on the IT industry. We further maintain a detailed revenue-by-product-area model for more than 1,200 worldwide vendors.)
- ☒ IDC demand-side research (This research includes thousands of interviews annually and provides a powerful fifth perspective for assessing competitive performance. IDC's user strategy databases offer a compelling and consistent time-series view of industry trends and developments. Direct conversations with technology buyers provide an invaluable complement to the broader survey-based results.)

Note: All numbers in this document may not be exact due to rounding.

IN THIS WHITE PAPER

In this White Paper, IDC reiterates the need for two-factor and multifactor authentication technologies, especially as they apply to the banking industry and compliance regulations. This document outlines the ClairMail solution for strong authentication utilizing the customer's or end user's cell phone as well as additional functionality and value delivered by the same ClairMail system. This White Paper also details cost and ease-of-use advantages derived from the use of a cell phone as part of a two-factor or multifactor authentication solution.

SITUATION OVERVIEW

Several factors are converging to create growth in the strong authentication marketplace. They are driving the need for positive identification in the IT enterprise and regulatory compliance across all industries. These factors include:

- ☒ Increasingly open networks and mobile workers
- ☒ Fundamental weakness of passwords as a security mechanism
- ☒ Increased number of online users
- ☒ Increasing incidence of ID fraud and theft (A recent article in *CIO* magazine indicates that 2–5% of revenue is lost to online fraud.)

In light of these trends, many organizations are turning to tokens, smart cards, biometrics, and mobile devices for user authentication.

The ability to identify who is using a computer system or network is of critical importance. The primary means of identification has long been through use of a password. However, passwords can be shared, stolen, or guessed. To have stronger authentication, enterprises historically have relied on hardware tokens.

The need for multifactor authentication continues to increase. Many new security challenges, technologies, and opportunities are coalescing to shape this market. Chief among them are regulatory compliance demands and legislation.

IDC has forecast the worldwide hardware authentication token market to grow from \$493 million in 2004 to \$764 million by 2009 (see *Worldwide Hardware Authentication Token 2005–2009 Forecast and 2004 Vendor Shares*, IDC #34452, December 2005). This 9.2% CAGR underscores the growing demand for two-factor authentication in the marketplace. However, new form factors for two-factor authentication are quickly emerging in this market. In addition to smart card and software-only two-factor solutions, companies are beginning to evaluate mobile devices as a form factor for strong authentication.

The financial industry is often considered one of the leading industries in terms of mobility adoption and penetration. IDC's latest *Mobilizing the Enterprise in 2006 Survey* (IDC #33677, July 2005) indicated that 36% of organizations within the financial industry had deployed multiple mobile applications — more than any other industry surveyed — and that the financial industry was among the top industries to have deployed a mobile device management solution, underscoring its keen awareness of administration and security of mobile devices.

IDC Definitions

Two-factor authentication requires customers to confirm their identities through something they know, such as a personal identification number (PIN) or password, as well as something they physically have, such as a hardware token, a smart card, or even a fingerprint. Traditional types of two-factor authentication for use with personal computers include hardware authentication tokens and smart cards, which either generate one-time passwords (OTPs) or are inserted into designated readers on a user's computer or other device.

Hardware authentication tokens rely on software servers or existing software authentication systems (see the Appendix for definitions). However, these traditional types of token implementations typically can range in cost from \$110 to \$150 per seat per year for a period of five years. Such implementations generally include two tokens at year zero and replacement tokens two years later when the batteries need to be replaced. Typically, the cost to replace stolen, lost, or compromised tokens ranges anywhere from \$20 to \$50 per token.

This price range does not account for other deployment and maintenance costs, such as:

- Help desk support
- Training costs
- IT management
- Ongoing integration issues with custom back-end software
- Deployment logistics (including mailing and shipping charges for dispersing tokens)
- Professional services

The average token costs approximately \$41; this price does not include back-end software and server expenses. Even with a large company discount from vendors for organizations with 10,000+ employees, the cost of initial implementation and rollout of a traditional token-based solution for a company this size averages between \$800,000 and \$1 million. This cost of course includes the systems infrastructure software and professional services necessary to the success of such an undertaking. It is reasonable to expect that the costs associated with dispensing such a solution to the general retail banking customer base would result in even higher costs (e.g., replacement, training, customer support inquiries).

Compliance and Legislation to Secure Systems, Protect Privacy, and Combat ID Fraud

Government and industry regulations have placed unprecedented pressure on corporations to secure access to information and applications — not just with employees but also with customers, partners, and contractors. Organizations addressing compliance issues surrounding Sarbanes-Oxley (SarbOx), Gramm-Leach-Bliley (GLB), the Health Insurance Portability and Accountability Act (HIPAA), and other federal regulations are increasingly looking toward identity and access management solutions to help them comply. The importance of regulatory compliance has become a C-level issue. Each of these regulations can carry criminal penalties and/or civil penalties. Criminal penalties include criminal prosecution of individuals as well as substantial fines. Successful criminal convictions generally lead to civil lawsuits. Civil lawsuits (especially in class-action situations) can carry substantial financial penalties and damage a company's reputation with its customers.

Further, a recent FFIEC report requires that banks adopt two-factor authentication by the end of 2006 to reduce account fraud and identity theft. According to the report, *Authentication in an Internet Banking Environment*, single-factor authentication is inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Although the FFIEC has not specifically documented the penalties for noncompliance, the expectation is that financial institutions will face stiff fines if they are not in compliance by year-end.

Online services have become a mainstay for financial institutions. Consumers enjoy the convenience of PINs and passwords and, we believe, are hesitant to adopt new security technology unless it is easy to use and/or until they personally become the victims of identity theft. PINs and passwords have become very easy for criminals to exploit. Phishing has become a major problem for consumers and threatens the online banking industry as a whole. Victims of phishing attacks receive an apparently innocuous email that directs them to visit what appears to be a legitimate Web site, where they are asked to update personal information. The Web site, however, is bogus and set up only to steal users' information. The Anti-Phishing Working Group, an industry association, reported 13,776 phishing attacks in August 2005.

While daunting in its scope, current regulatory legislation from the FFIEC moves beyond "best practice" and lays out a very specific set of requirements for implementing more robust security measures.

Cost, Convenience, and Security: The Impossible Dream?

As previously discussed, two-factor authentication requires customers to confirm their identities through something they know, such as a PIN or a password, as well as something they physically have. Traditional types of two-factor authentication include hardware authentication tokens and smart cards, which either generate OTPs or are inserted into designated readers on a user's computer or other device. These solutions, while very effective, are correspondingly costly to deploy and maintain.

Additionally, while banks must comply with federal security regulations, they cannot afford to annoy their customers by diminishing the convenience of online banking. While hardware tokens, smart cards, and biometric-based solutions provide a wide variety of authentication options to the market, they are also costly for financial institutions and often resisted by consumers.

With this cost/convenience-versus-security dilemma in mind, banks are seeking cost-effective solutions that provide strong authentication, yet are palatable for mainstream customers who require frequent and unobtrusive access to their account information. For several years, certain security and communication sectors have proposed the use of cell phones as part of the authentication equation. The technology is now coming to market, and IDC anticipates that it will receive a warm reception. The idea of utilizing a customer's cell phone as a token for two-factor authentication and consumer-related transactions in banking can offer the following benefits:

- Security beyond username and password, offering FFIEC compliance
- Easy implementation for IT, no extra hardware requirements
- Easy for customers to understand and utilize
- Stronger user adoption — mobile phones are critical to users; fobs and tokens are not
- No extra device for the customer to carry, reducing cost and complexity (see earlier section on costs associated with hardware authentication tokens)

In the following sections, IDC examines ClairMail's approach to enabling the cell phone as the token in two-factor authentication and offers a customer case study of this technology. Further, IDC looks at ClairMail's capabilities beyond authentication and examines how features such as Text Banking can benefit consumers.

The ClairMail System

The ClairMail system extends all forms of messaging (i.e., SMS or email) for instant, one-click access to all applications and services from any mobile device. All email and SMS communications can be utilized to access virtually any type of data from any system, including corporate, financial, and customer data. This approach allows financial institutions (as well as enterprises in other vertical markets) to leverage mobile devices for customers to access and act upon their financial information for a fraction of the time and cost associated with many other alternatives. The idea of utilizing mobile phones as a trusted authentication device is gaining ground in many sectors of the economy, particularly in banking and financial services, healthcare, retail, and even utilities.

The ClairMail system provides enterprise customers with on-demand, one-click mobile access to applications and services. The ClairMail system appliance is a transactional messaging server that sits behind a financial institution's firewall and can be integrated with the interactive voice response (IVR) system, call center systems, and computer telephony integration (CTI) systems to extend SMS and email (essentially any messaging capability) as a trusted and secure access method to any or all of a financial institution's internal systems, such as the customer information systems and applications that contain customer records.

In a banking scenario, customers can use their cell phones for a variety of everyday banking needs, including to check balances, review recent transactions, check credit availability, transfer funds, and confirm bill payments. These tasks can be accomplished with a single text message to the ClairMail system, which then connects to a financial institution's systems. Inasmuch as it utilizes the messaging functionality that users are already familiar with, the ClairMail implementation requires no client software or end-user training; it works the same way on any mobile device, regardless of device type, platform, or operating system, and is therefore capable of working with the hundreds of millions of mobile devices that are currently in use. This approach saves financial institutions significant costs in both product and human resource initiatives, and it offers customers an easy-to-use and nonintrusive method of authenticating to the bank.

The product includes capabilities such as Actionable Alert functionality, which allows financial institutions to deliver alerts for bill paying, antifraud notifications, important account change information, and so forth, empowering customers to take action immediately using SMS on their mobile phones. For example, banks can significantly reduce losses from fraud and identity theft by enabling customers to quickly respond to antifraud alerts from questionable account activities directly from their mobile phones.

The ClairMail system can also be configured to allow for a CallMe function, which enables customers who are calling the bank's customer service center for information or assistance to insert themselves into the call queue. The system generates a return call when the appropriate customer service representative becomes available. This is another example of reducing stress on both sides of the equation: Banks save considerable resources (i.e., telecom charges, IVR costs) by not having call lines tied up with customers on hold, and customers save time by being able to move on to other activities, knowing that they will receive a timely return call from a customer service representative who is already familiar with their account.

And, importantly, the ClairMail system is capable of cost-effectively delivering two-factor authentication by utilizing a customer's mobile phone. In the first use case, ClairMail is used in the customer's initial log-in process. In order to access his or her account, the customer is required to enter a time-expiring one-time password (OTP) that has been sent by the financial institution to his or her mobile device. This significantly reduces the risk of identity theft.

The ClairMail system is also used for two-factor authentication in online banking as a second factor of authentication for specific transactions benefiting from additional security. After the customer has logged on from his or her personal computer and proceeds to execute a specific transaction that requires a higher level of security, the bank sends an OTP to the customer's mobile phone. The customer then enters the OTP as the two-factor authentication and the transaction is securely completed.

Furthermore, in a strictly mobile banking scenario, the ClairMail system integrates with the financial institution's IVR system to perform a two-factor authentication of the transaction. In this use case, the customer uses SMS to initiate a transaction. The ClairMail system invokes the IVR to call the customer's mobile phone and the customer is asked to enter a PIN. The mobile phone (what you have) and the PIN (what you know) constitute the two factors of authentication.

Security and Integration Are Key

The ClairMail system employs a mobile single sign-on (SSO) capability that integrates with any financial institution's back-end systems. This technology ensures that the user has the appropriate privileges for accessing account information. From a Web services perspective, the product relies on a variety of connectors, including an HTML connector for Web applications, a proprietary connector that allows IT professionals to write to internal custom applications, and an API connector that processes requests to all J2EE-based application servers. This inherent flexibility is essential for working with an industry that has a mix of proprietary and standards-based applications and systems.

FUTURE OUTLOOK

Consumers represent the greatest potential growth factor for the strong authentication market. If consumers are presented with authentication solutions that conveniently deliver secure and easy access to all of their financial account information, IDC believes that they will become satisfied and routine users of these services. The mobile phone has greater promise for delivering the necessary functionality combined with ease of use and is a better and more cost-effective solution than tokens or other authentication devices.

While traditional tokens are too cumbersome for the average consumer and too expensive for the typical organization to deploy on a widespread basis, other form factors such as cell phones can now be configured to meet this need. Like ClairMail, these solutions can extend beyond the security and identity management requirements and offer consumers an easy and simple way to manage and benefit from the ever-increasing number of systems and accounts they must access on a regular basis.

IDC believes that continued demand for regulatory compliance across industries, coupled with increased incidence of ID fraud, will drive revenue for the strong authentication market during the forecast period.

CHALLENGES/OPPORTUNITIES

Financial institutions today employ several techniques to weigh risk and verify identities. A major factor when choosing an authentication solution is whether it will be capable of adapting to the ever-changing online security threats.

The challenge for ClairMail will be to convince more conservative financial institutions, government agencies, and healthcare facilities that its solution does not sacrifice security for online end-user or customer convenience.

The appeal of allowing customers to utilize their own cell phones should be extremely compelling from a cost equation for banks, and we anticipate that consumers will welcome the use of cell phones as authentication devices in the majority of instances.

Although the extension of applications to mobile devices can be challenging in terms of supporting device types, operating systems, and applications, the commonality of a mobile phone provides few obstacles to the deployment of the mobile phone as an authentication device. In addition, the mobile phone is a much more ubiquitous device by a huge magnitude than a smartphone, and the penetration rates of mobile phones for workers in the United States are high.

Outside the United States, the ability to roam is increasingly easy, especially for GSM-based carriers, such as Cingular and T-Mobile. Essentially, roaming in Europe and parts of Asia, while sometimes costly, is quite seamless. For CDMA carriers, such as Verizon Wireless, roaming is available in many parts of the Americas and some parts of Asia such as China, Korea, Thailand, India, and New Zealand. If users are traveling more frequently to Europe and other parts of the world where GSM is prevalent, a global phone including both CDMA and GSM radios is required to provide much broader coverage.

CONCLUSION

Continued demand for regulatory compliance across industries, coupled with increased incidence of ID fraud, will drive revenue for the strong authentication token market during the forecast period. Financial institutions must develop an ongoing process to review authentication technology and ensure appropriate changes are implemented. A sound authentication system should include audit features that can assist in the detection of fraud, money laundering, compromised passwords, or other unauthorized activities.

Solutions such as those from ClairMail, which are targeted at providing consumers with convenience and ease of use while offering financial institutions security and cost savings, are in a strong position to deliver the right combination of functionality, ease of use, and security for mobile banking and other forms of mobile commerce.

CASE STUDY

Financial Services Firm Leverages SMS Infrastructure to Add Value for Customers and Reduce Costs

A large financial services firm based in the U.S. provides banking, insurance, investments, and mortgage and consumer finance for more than 23 million customers through over 6000 stores, the Internet, and other distribution channels across North America and elsewhere internationally.

In the financial services industry, where the use of paper checks is declining and paper currency is disappearing, this firm recognizes the need to be a player in the ecommerce market and specifically deliver mobile products and solutions to its customer base. The company has embraced the evolution of the mobile phone, from a voice-based handset to what it is today — a communication device. Understanding the opportunity to leverage the mobile device as an identifier, an authenticator, a deliverer of vital information, and a payment maker becomes critical to a financial institution.

The company sought a turnkey solution to deliver critical information to customers in a format that is viable on mobile devices. With the ClairMail system, the firm was able to bring such a solution to market much faster than if it had built the solution itself. The company believes that an SMS messaging architecture is a valuable and important infrastructure to deliver key information and alerts and provide a way to make such messages actionable. The mobile phone is a powerful tool that customers keep secure and provides identification and authorization through the SMS infrastructure. In addition to delivering a product that drives tremendous customer stickiness, such a solution also provides significant cost savings over the use of a typical voice-oriented call center.

For example, the ClairMail system allows a customer to send an SMS message and receive account balance information, inasmuch as where the system already identifies the user through its phone number and knows that the customer is requesting a balance. After the customer speed-dials an SMS, an SMS is received in turn with the account holder's balance and a one-key press is required to talk to a customer service agent. This session is initiated by the customer and is a very popular service for customers who are technologically savvy and prefer a remote relationship. This solution keeps traffic off the 800 number and requires no customer interaction — lowering costs and freeing up call center customer representatives. Future deployments are expected to include alerts where customers can set up an SMS to be sent in certain scenarios; for example, if a balance hits a certain point, the SMS would warn of insufficient funds. This action gives the customer a message and provides actionable options such as speaking to a customer representative or making a transfer.

As this company rolls out the solution, the mobile phone — as the identifier and authenticator — is a channel that customers can trust is delivering personal information in a private and secure manner and one that could be a strong case for job replacements. The company is hoping that this solution is adopted more quickly than some other technology in banking (for example, the adoption period of ATMs lasted 20 years); however, the solution offers many benefits to both customers (convenient, quick, secure, and easy to use) and to the financial services firm (cost savings and closer relationships with customers), and the market is in a much better position to accept such technology adoption, unlike many of the early mobile commerce failures of the past five to seven years. This company expects to leverage such technology as a key differentiator in a consolidating and demanding market seeking ways to enhance the banking experience for its customers.

APPENDIX

Definitions

- ☒ **Traditional authentication tokens** are small hardware devices that allow users to authenticate themselves to the token authentication server using either one-time passwords (OTPs) or challenge/reply methods. These tokens can come in multiple form factors and do not require additional hardware. OTP or challenge/reply tokens are simple to use and provide a robust authentication method.

- ☒ **USB authentication tokens** are small, key-size devices that connect to any standards-based USB port and can have smart card chips and embedded software used to perform user authentication and cryptographic functions, such as digital signing. USB authentication tokens don't inherently require external server software, as do traditional authentication tokens; instead, they can be utilized by nearly any application that can recognize the token. These tokens may have the same capabilities as smart cards and can be used as smart card replacements. They may be increasingly used within OTP security architectures. In this document, hybrid USB/traditional tokens are counted in the USB category because they have the added USB functionality.

- ☒ **SLATs** are parallel/serial port tokens or USB keys that authorize the use of software on a particular device. SLATs generally do not require user intervention because the software application is designed to check for the SLAT prior to running the application. SLATs are used to protect against software piracy and to enforce software licensing.
- ☒ **TASs** are highly configurable authentication servers, which maintain user information, store seed key data, and provide verification of token authentication requests. Each TAS passes authentication verification to the specific application. These systems are designed to integrate tightly into the existing network and security identity management architectures. Users can be grouped into configurable profiles with different rule sets governing the access control for each, and RADIUS server technology is either built in or provided as an option.
- ☒ **Authentication client software**, usually configured as an agent, is designed to operate within almost every conceivable client or other delivery device within an enterprise, allowing access control for the local desktop as well as network and Web resources. These agents are becoming increasingly versatile and can be used in traditional token technology (e.g., key fob, credit cards, and other software, such as Java applets and software for PDAs and wireless devices).

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2006 IDC. Reproduction without written permission is completely forbidden.