TECH CHOICES

March 31, 2005

What To Look For In Consumer Strong Authentication Solutions

by Jonathan Penn

FORRESTER® Helping Business Thrive On Technology Change

March 31, 2005

What To Look For In Consumer Strong Authentication Solutions

by Jonathan Penn
with Martha Bennett, Bruce D. Temkin, and Adele Sage

EXECUTIVE SUMMARY

Online fraud and identity theft are growing plagues to eCommerce and are eroding consumers' trust in the Internet. In response, some organizations — especially financial institutions — are evaluating strong authentication solutions to protect customers' accounts and curb account hijacking. The key criteria when evaluating such solutions are ease of use, portability, cost, security, manageability, and cross-channel utility. No one solution will dominate adoption, as organizations will pick different options for different reasons. But Entrust IdentityGuard scores strongly across all criteria and emerges as an especially attractive option.

TABLE OF CONTENTS

NOTES & RESOURCES

Forrester interviewed the leading strong authentication vendors, as well as many financial institutions that are exploring the use of strong authentication and other defenses against fraud and identity theft.

Related Research Documents

"Rebuilding Consumers' Trust In The Internet" February 24, 2005, Best Practices

"Keeping Financial Transactions Online" January 12, 2005, Best Practices

STRONG CONSUMER AUTHENTICATION: NECESSARY AND INEVITABLE

Consumers are under relentless assault by fraudsters and identity thieves using spyware, phishing attacks, and hacking to capture account credentials. In response to consumers' rising concerns about fraud and identity theft, many organizations are evaluating strong authentication solutions so they can provide greater assurance that only the authorized customers themselves are gaining access to their own accounts.[1]

European financial firms have been the early adopters of such solutions. Outside this community, adoption of consumer strong authentication has been slow or nonexistent. Yet today we are seeing significant interest in North America and elsewhere, expanding even beyond the financial services sector. ISPs, retailers, government organizations, healthcare companies, and others are realizing that consumer strong authentication can address a variety of security, privacy, and regulatory concerns.

Finding The Right Strong Authentication Solution

While the key examples of strong authentication are in commercial banking services and European financial firms' experiences with retail consumers and remote employee access, these deployments are only moderately useful guides for other firms. Why? Because many of the European solutions are homegrown and are outdated in the current environment. Firms are looking for more packaged solutions, and solutions need to address today's more sophisticated Internet users. Although the European experiences aren't directly applicable, we examined their efforts and have identified a number of key criteria for any solution. Our analysis shows that an ideal solution must:

- **Let customers use it anywhere.** Solutions must not require firms to turn their customer support centers into technology help desks. Solutions should not require any specialized computer software or hardware, such as requiring a particular operating system, browser, or peripheral like USB or PC card. Because people use multiple machines (e.g., accessing sites at work and at home) as well as share machines (such as between spouses), the solution also cannot be tied to any one computer or assume that a computer is tied to any one person.

- **Be easy for customers to use.** Solutions must be simple and intuitive to use and must not scare customers away with confusing or cumbersome technology impediments. Otherwise, customers won't use it, or they will flood the customer support center with questions and complaints. The solution should support use by those with visual impairments, who employ special software for navigating the Web. Ease of use also extends beyond the isolated instance of any one B2C relationship to scale across multiple relationships. Thus, it also needs to be easy for customers to manage if the same solution were adopted by several organizations with which they do business.

- **Be cost-effective.** Organizations simply can't afford to pay for rolling out strong authentication for every online customer if it costs too much. So firms need to look at the total cost for the solution, including: the original license costs, annual maintenance fees, the cost of distribution

and loss replacement if there's a physical element of the solution, and the maintenance implications based on the device's resilience (hardiness) and longevity.

- **Provide appropriate levels of security.** Naturally, the solution must adequately defend against phishing, spyware, hacking, man-in-the-middle attacks, and other threats driving organizations to adopt strong authentication. The solution must provide protection during "normal" usage as well as during loss periods pending replacement of a device or card. An added value is for the authentication method to work bi-directionally: Customers can validate the authenticity of your communications to them. Organizations may also look for a solution to provide both strong authentication and digital signatures for transactions.

- **Be easily manageable.** Closely tied to cost are the management issues associated with a solution. Solutions should easily integrate with the organization's Web site, security architecture and applications, and should easily scale to support the size of the customer base. Credentials should be easy to distribute, renew, replace in the event of loss, and revoke. Ideally, it would leverage any existing credentials (such as ATM cards, credit cards, or government ID cards) already distributed.

- **Work across different channels of interaction.** Given the efforts to implement and roll out consumer strong authentication for Internet activity, smart organizations will leverage the solution beyond the standard Web browser environment. They'll prefer a solution that works with Web-enabled PDAs and BlackBerrys, in phone interactions, at ATMs, and at tellers and other points of service.

EVALUATING THE LEADING CANDIDATES

Several strong authentication technologies and solutions regularly make the shortlist for consideration. So how do these various options fare against the criteria? We've graded each one to see how they stack up (see Figure 1). Versus other methods like USB drive tokens or fingerprint scanners, all strong authentication solutions score well in portability. Similarly, they rate well cross-channel utility, which is closely tied to portability: If the solution doesn't require a computer, then it can be used in noncomputer interactions.

One-Time Password Tokens

One-time password (OTP) tokens from companies like ActivCard, RSA Security, and Vasco are widely used in the enterprise (chiefly for remote access) as well as in commercial banking. In a consumer environment, the OTP tokens offer high simplicity and cross-channel utility. They suffer in manageability and cost because of both the costs of the unit and the efforts in dealing with loss replacement. Tokens are a bit cumbersome to carry: Ease of use is fairly high in isolation, but it especially suffers when customers are required to manage tokens for multiple companies with whom they do business (a situation referred to as the "token necklace" syndrome). Unit cost ranges from $10 to $40 at the volume level of 100,000 units.

Figure 1 Scoring The Various Consumer Authentication Options

	Portability	Usability	Security	Cost	Manageability	Cross-channel utility
OTP tokens	5	3	4	2	2	5
RSA OTP token service	5	4	4	3	3	5
Smart card calcs (non-EMV)	5	3	5	1	2	5
Smart card calcs (EMV)	5	3	5	3	3	5
PIN/TAN sheet (simple)	5	5	3	3	3	5
PIN/TAN sheet (complex)	5	5	4	3	3	5
Entrust IdentityGuard	5	5	5	4	4	5
Out-of-band authentication	4	3	5	3	5	5
Soft keyboards	5	3	2	5	5	2
Scramble pads	5	2	2	4	5	2

Rating: 1=poor, 5=excellent

Source: Forrester Research, Inc.

RSA's SecurID Token Service

RSA recently announced that it is developing a service offering for its SecurID tokens. To address the three principal shortcomings of tokens — manageability for the issuer, cost, and usability for consumers if they have too many tokens to manage — RSA will distribute the tokens and provide the Internet infrastructure to perform user authentication. A token acquired this way could be commonly used by multiple organizations, each using the service as a second layer of authentication on top of a customer's user ID/password.

This kind of shared usage service model will lower pricing and management costs and minimize token necklace syndrome. Due to become available in the fall of this year, the technical and pricing details of this service are not public at this time. We expect that it will be priced more attractively than standalone tokens, as the goal is to have consumers use the token with multiple organizations.

Smart Card Calculators

ActivCard, Vasco, and Xiring are the leading vendors with solutions using smart cards along with handheld devices. Their use is straightforward, though a bit cumbersome. For authentication, the cardholder inserts the smart card into the device and is prompted for his PIN, which results in the display of a unique OTP used to log in. The devices can also be used for digitally signing transactions, a nice added feature but one which exacts a toll on usability: It requires more numbers to be typed in, with the resulting display typed back into browser. Assuming the smart card is already present, calculator solutions will cost around $8 to $15 per unit at the volume level of 100,000 units.

These solutions are most appropriate for organizations already distributing smart cards to its consumer community — specifically, that applies to European and other financial institutions today undergoing conversion to smart cards under the EMV (Europay-Mastercard-Visa) initiative. This isn't happening in the US, so smart card and calculator distribution is perceived as overly costly and burdensome.

PIN/TAN Sheets

PIN/TAN sheets are common among German banks as well as others in Europe.[2] Customers receive a list containing between 50 and 100 transaction numbers (TANs). Each number is used one time only to complement a password at login or to authenticate a transaction. In simple implementations, customers select any unused TAN on a sheet for any transaction. In more complex implementations, the banks identify — by grid coordinate or ordinal — which TAN to use.[3]

The simple PIN/TAN method is vulnerable to phishing, and there have been successful attacks against it, but the more complex implementation is invulnerable to phishing. PIN/TAN systems are easy to use. As a paper-based solution, manageability of distribution and renewal is good, but renewals are relatively frequent events. Most deployments today — primarily at German banks — are homegrown. We have heard of administrative costs ranging from $5 to $10 per person at the volume level of 100,000 units.

Entrust IdentityGuard Numeric Grid

Entrust IdentityGuard is an improvement on the PIN/TAN sheet or number card.[4] Rather than each cell holding a TAN, IdentityGuard cells hold only one number, and the OTP is built using a random combination of several cell values. Ease of use is high, as most people instantly recognize the bingo-like paradigm. The solution also possesses a high degree of cross-channel utility and an excellent price point. It also scores well on manageability: Unlike PIN/TAN sheets, IdentityGuard doesn't require frequent renewals.

Properly implemented, IdentityGuard security is on par with one-time PIN tokens and is in some ways superior, as its use is harder for phishers to exploit, and it also supports bi-directional

authentication. In environments like banking and healthcare, grids can easily and inexpensively be imprinted on the back of cards already distributed to consumers. Brokerage, ISP, retail, and other environments would require separate distribution, though this would be at less effort than most competing authentication methods. IdentityGuard costs approximately $2 per user at the volume level of 100,000 users.

Out-Of-Band Authentication

Out-of-band authentication involves establishing a second communication channel outside the Web session used to log on, either to communicate an OTP or to perform a second level of authentication directly. There are several approaches. Typically, a correct user ID and password entry generates an automated phone response to the customer. In one method, the customer receives an OTP via SMS to a cell phone and then uses it to gain entry to the Web site. In another method, a phone call prompts the customer to speak a phrase for voiceprint authentication.

While uncomplicated for the customer, convenience and availability impair ease of use. Customers must register their cell phone numbers with the business; cell phones may not support SMS or customers may be in an area with unreliable SMS service; cell phone coverage may be poor; or customers may not have cell phones at all. Land lines restrict use to particular locations, and wouldn't always be available if that phone happens to be in use — and it would never be available if the customer is on a dial-up connection.

The solution offers excellent manageability: Customers already own the device, and it only requires they register the phone number(s) to call. It is fully portable if using a cell phone; otherwise, it is limited to the phone number registered (the ability to register multiple phone numbers improves portability). It is an effective defense against the Internet threats of primary concern, and it can be used across multiple channels of interaction. Authentify and Strikeforce offer this, while Vasco also offers SMS as an alternative vehicle for providing users with an OTP. Some solutions price on a per transaction basis, others on a per user basis. Cost can range from $5 to $15 for 100,000 customers.

HOW ALTERNATE AUTHENTICATION METHODS COMPARE

Recognizing the need to thwart password thieves but reluctant to roll out strong authentication, some financial sites have implemented special login interfaces. These either require clicks rather than keystrokes or convert static passwords to one-time codes.

- **Soft keyboards.** Soft keyboards are visual representations of a QWERTY keypad. Instead of typing in a password, customers use their mouse to click on the virtual keys. Citibank UK recently implemented this.[5] A simple method, to be sure, but one that is widely perceived by customers as inconvenient. It is effective against key logging spyware but ineffective against phishing. Moreover, it reduces password strength because it doesn't distinguish upper and lower case letters, and it discourages use of long passwords. It has no cross-channel utility and is not

usable by the visually impaired. On the plus side, it's extremely inexpensive (it can be developed internally virtually for free) and carries no added management burden.

- **Scramble pads.** Scramble pads present customers with a way of mapping PIN numbers to other numbers or characters: *4* becomes *2*, *3* becomes *9*, *7* becomes *P*, etc. When logging in, customers type the numbers or letters corresponding to their PIN numbers (to simplify this procedure, passwords are usually numeric), and the mappings are different every visit. Adelaide Bank of Australia has a straightforward implementation.[6] These approaches don't deter against phishing. Those that do are far more complicated, such as the slide-wheel interface provided by the vendor Bharosa. Swivel Technologies also offers a basic Web scramble pad solution, and can offer it in combination with its out of band authentication for greater security. Costs are less than $5 per user at the volume level of 100,000 users.

RECOMMENDATIONS

GET STARTED: STRONG AUTHENTICATION IS COMING

Moving to two-factor authentication is strongly recommended for financial institutions. At the least, investigate solutions before the competitive and customer pressure rises to the boiling point.

Other organizations with a rich set of customers' personal information to protect should be watching the authentication landscape. They are — or might soon become — targets, as identity thieves continue to expand their nets beyond financial services firms.

A word of advice to vendors: Develop a pricing approach that both reassures active users and also coaxes fence-sitters into adoption. Therefore, a low cost solution will be important for providing firms with more flexibility to adopt a charge model (if any) that makes the most business sense.

Strong authentication is not a panacea, however. Even the best technology is only a partial solution, so firms looking into security options should also:

- Continue customer education efforts.
- Examine customer-facing processes, and — where required — redesign them for better protection against fraudsters and identity thieves.
- Extend authentication beyond "factors" by implementing extra safeguards, such as notifications, for key or suspicious transactions: changing an address or password, opening new accounts or enrolling in new services, and unusual money transfers.

ALTERNATIVE VIEW

MONITORING AND PROFILING COULD PREVENT FRAUD

Price sensitivities and fear that strong security measures will alienate customers through inconvenience will hinder adoption of consumer strong authentication. Rather than widespread rollouts, we'll instead see strong authentication support meted out only to top-tier customers, perhaps offered to additional customers as an upsell incentive. Organizations will complement selective use of strong authentication with more profiling of users' activity and their online transactions.

If monitoring can prevent rather than just detect abuse, then profiling based on IP address, Web site behavior, transaction anomalies, and other factors will emerge as a viable alternative to strong authentication.

ENDNOTES

[1] In a recent announcement, E*TRADE became the first North American financial institution to support strong authentication for its retail customers. See March 15, 2005, Quick Take "E*TRADE Battles Online Fraud With Strong Authentication."

[2] A demo of PostFinance's implementation shows how customers are prompted for a one-time security number from their so-called "access card/cancellation list." PostFinance's "access card" (or "cancellation list") is the size of a credit card, printed on both sides. See https://www.yellownet.ch/demo/index_e.htm.

[3] PIN/TAN systems reduce the risk that the customer's bank account will be inappropriately accessed. But both prospective and existing users of such systems must be aware that the level of risk varies across different implementations. See the December 20, 2004, Best Practices "Online Banking Customer Authentication Systems: PIN/TAN Is Not Immune From Phishing."

[4] Entrust's IdentityGuard is a promising approach to consumer strong authentication, and should be considered by organizations finding hardware tokens and smart cards too costly and complex. See the November 19, 2004, Quick Take "Strong Authentication Made Simple."

[5] See Citibank UK's implementation: http://www.citibank.co.uk/uk/productsservices/internetbanking/demo_new/signon.htm. ING Direct in Australia goes one step further by scrambling the location of the keys on the virtual number pad. See http://www.ingdirect.com.au.

[6] Adelaide Bank in Australia uses scramble pads in a production implementation. See www.adelaidebank.com.au.

FORRESTER®

Helping Business Thrive On Technology Change

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617/613-6000
Fax: +1 617/613-5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Australia
Brazil
Canada
France
Germany
Hong Kong
India
Israel
Japan
Korea
The Netherlands
Sweden
Switzerland
United Kingdom
United States

For a complete list of worldwide locations, visit www.forrester.com/about.

For information on hard-copy or electronic reprints, please contact the Client Resource Center at +1 866/367-7378, +1 617/617-5730, or resourcecenter@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

FORRESTER®