



Paper Presentation

For



**Title : Agility of Authentication Management
in Banking and Finance**

Theme: Agility in Testing

Industry: Banking and Finance

Domain: Security and Identity Management

Team:

M.Hemasree B.Com,PGDPMIR,ADST, PGDCA,

ISTQB Certified Tester,MBA(SEM)

M.Mohan Kumar B.E ,ISTQB Certified Tester

Agility of Authentication Management in Banking and Finance

Index of the Presentation

S.No	Session
Front Page	
Abstract	
1	Introduction: Agility in Testing
1.1	The Need for Stronger Authentication
1.2	Case Studies in Banking Sector Regarding Agility in Testing
2	Challenges in Banking
3	Authentication in an Electronic Banking Environment
3.1	Background
3.2	Existing authentication methodologies involve three basic “factors”
3.3	Risk Assessment
3.4	Phishing
3.5	ATM Authentication
4	Authentication Techniques, Processes, and Methodologies
5	Tokens
5.1	USB Token Device
5.2	Smart Card

5.3	Smart Tokens
5.4	Fingerprint Recognition
5.4	Password-Generating Token
5.5	Out-of-Band Authentication
5.6	Internet Protocol Address (IPA) Location and Geo-Location
5.7	Mutual Authentication
5.8	Biometrics
5.9	SMS Text Password
5.10	Other Approaches
6	Conclusion

List of Tables
Title of the Table
Case Studies in Banking Sector Regarding Agility in Testing

List of Pictures
Title of the Picture
Time Vs Sophistication of Attack
Process Flow of Phishing attack
Deployment Architecture of ATM
Example of Single Use Password Token

<p>Author 1: Profile</p> <p>Hemasree.M</p> <p>Contact: + 91 – 9003916503</p> <p>Softwaretesting.cmmi@gmail.com</p> <p>Qualification: B.Com. P.G. Dip. Personnel Mgt & Industrial Relations, Advance Dip. In Software Technology, PGDCA, MBA(SEM)</p> 	
Company:	Indian Institute of Software Testing
Location:	Coimbatore, Tamilnadu, India.
Certification:	ISTQB, Foundation Level Exam
Career Summary:	A qualified I.T. Professional and keen strategist with over a decade of experience across diverse facets such as Business Centre Operations, Business Development, Client Servicing, Statutory Compliance & CBS Implementation in Banking Industry. Presently working as a part of Core Group for implementation of CBS in Bank of Baroda across the branches. Proficient in heading routine banking operations involving marketing, customer relationship, financial product planning. Proven track record of establishing and

	restructuring systems/ procedures, thereby contributing in a major way towards augmented growth and profitability levels. Possess excellent interpersonal, communication and organizational skills with demonstrated abilities in team management and customer relationship management.
Experience:	13 Years of work experience in Managerial cadre into Banking both Operational and Information Technology. Experienced in Foreign Bank as well as Nationalized Bank.
Technical Training:	<ul style="list-style-type: none"> • LAMP program at IDRBT, Hyderabad. • Structured Programming and Analysis, Noida Core Banking Solutions –Finnacle Training at Infosys, Bangalore.
Technical Skills:	C, C++,Ms-SQL Server, Oracle 8i, PHP, MySql, Manual and Automation Testing Tools, .NET technologies
Achievements:	<ul style="list-style-type: none"> • Best Student Award during college. • Best Performer Award in Savings Account mobilization received from CMD of Bank of Baroda.

Author 2: profile

M.Mohan Kumar

mmktesting@gmail.com

Mobile: 99448 86057

Qualification: B.E in Electronics and Communication

Company: Indian Institute of Software Testing

Location:

Branch @ S.N High Road, Tirunelveni.

Reg off @ Coimbatore, Tamilnadu.

Certification: Certified in ISTQB, Foundation Level Exam,

Computer Society of India, SQTA

Hardware (A+) & Network (N+)

Experience: 1+ Years Experience in Software Testing Field.

Proficiency in Manual testing

Automation tools: QTP & WR

Test Management Tool: Test Director

Projects Handled:

❖ RFID Based Toll Gate.

Reference: Micron Technologies, Coimbatore.

❖ GMO Application, Inventory in Banking.



Agility of Authentication Management in Banking and Finance

Abstract:

Authentication has come a long way. From simple handwritten signatures to official seals pressed into wax on sealed envelopes to advanced cryptography techniques used by the military and government agencies, authentication techniques seek to validate the authenticity of someone or something.

Today more than ever, the rise in online fraud as one result of the anonymity of the Internet necessitates the use of strong authentication techniques. The username/password login that has been the standard user identification since the inception of online banking put the bonus on the user not to divulge personal information to anyone, deliberately or unwittingly. The procedures such as not carrying one's Username and password so they could not be stolen or closing a browser window after an online banking session served the industry well in preventing widespread online banking fraud. However, the industry did not foresee the evolution of Internet fraud techniques and their effects.

Key words:

Authentication, Security and Agility

1. Introduction: Agility in Testing:

Organisations looking to get the most value from testing are often also interested in adopting software development processes which reduce risks. Agile is a term which embraces a number of lifecycle models, characterised by iterative development and cross-disciplinary working. These can reduce risk by providing faster and clearer information on which to base project decisions. One facet of agile development is the reduction in compartmentalisation of testing within the overall software development lifecycle.

More information can be found from the Agile Alliance. Tool vendors are moving to support agile development and testing within a unified environment.

For example, Microsoft's Visual Studio 2005 includes an integrated load testing tool. On the Open Source side, Eclipse includes a web performance testing plug-in



and Eclipse supports performance testing tools such as JMeter (as well as proprietary tools including IBM's Rational Performance Tester).

Banking regulations require financial services organizations to conduct independent testing of their computing and networking environment at regular intervals. Many organizations comply with this requirement by conducting penetration testing and vulnerability analyses.

These tests offer a snapshot of an organization's security posture during a given point in time. Further, these tests are valuable in maintaining the overall security architecture of the organization by identifying vulnerabilities that could cause important information to be compromised.

The management of an organization seeking to conduct an evaluation of the current environment must clearly understand the scope, methodology and the process for conducting penetration tests and vulnerability analyses.

1.1 The Need for Stronger Authentication:

Internet security and the potential for online fraud have been, and will continue to be, an ongoing concern for institutions, consumers, and government agencies. Its openness and anonymity make the Internet an environment that is ripe for fraud and deception.

For institutions, the initial focus of Internet security was on their own corporate systems: ensuring that data was not compromised and that system were not harmed. Internal security measures at financial institutions are generally considered to be sound. However, several senior security officers at financial services institutions (FSIs) have expressed a growing concern over the vulnerability of the consumer desktop, an area that is outside the banks' control.

Time Vs Sophistication of Attack



Increasing Sophistication of Online Attacks and Associated Defenses (1995–2005 and Beyond)

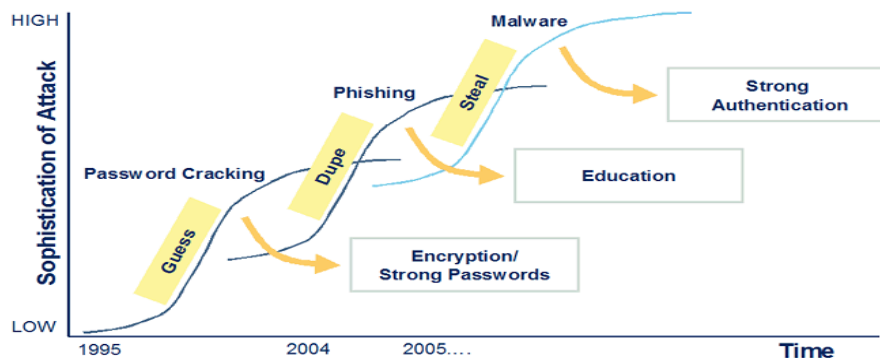


Exhibit #: 42:27N-E3
Source: TowerGroup

1.2 Case Studies in Banking Sector Regarding Agility in Testing

System	Overview	Challenges	Approach
Ensure acceptable quality of upgrades of Core Banking application	Need to ensure reliable quality of a continuously evolving implementation.	Ensuring product quality for future releases and required to collaborate with the bank & ensuring constructive criticism and maintaining neutrality.	Focusing on Test Coverage (Design and Execution),

UAT for a Collections Tracking System	Tracking of delinquent accounts and collections	Mainframe based application the non GUI front end and navigation mechanisms required special focus Both Loan and Credit Card account delinquencies.	Constitutes a multi-skilled team, mainframe testing experience
Automating testing of an Equity Trading Tool	With the application a rewrite of Terminator GUI, this acts as an equity warrant quoting and deal execution tool.	Application complexity relating to functions such as Execute/amend trades, manage prices and refill buckets, contribute prices, manually respond to price requests, enter and manage orders etc	Ensure that the test design provided adequate test coverage for the application
E-Finance Application	The e-Finance Framework pack provides the necessary business logic that lets an institution create a presence in cyberspace.	Internet Banking - Retail and Commercial. Mobile Banking - WAP and SMS Brokerage - Equities and Mutual Funds Electronic Billing and Payments Financial Portal.	Automation framework using QTP, Test Director as well as Excel functionalities was used in coming up with a scaleable solution.



2. Challenges in Banking:

As banks offer more high-value services online it should come as no surprise that the number and intensity of online attacks continues to grow. The challenge for banks is to economically deploy solutions that balance increased security with customer convenience and that promise to defend against future generations of attacks.

3. Authentication in an Electronic Banking Environment:

We are focusing on risk management controls necessary to authenticate the identity of retail and commercial customers accessing Internet-based financial services. There has been a significant legal and technological change with respect to the protection of customer information; increasing **incidents of fraud, including identity theft; and the introduction of** improved authentication technologies.

This guidance applies to both retail and commercial customers and does not endorse any particular technology. Financial institutions should use this guidance when evaluating and implementing authentication systems and practices whether they are provided internally or by a service provider. Although this guidance is focused on the risks and risk management techniques associated with the Internet delivery channel, the principles are applicable to all forms of electronic banking activities.

3.1 Background

Financial institutions engaging in any form of Internet banking should have effective and reliable methods to authenticate customers. An effective authentication system is necessary for compliance with requirements to safeguard customer information, to prevent money laundering and terrorist financing, to

reduce fraud, to inhibit identity theft, and to promote the legal enforceability of their electronic agreements and transactions.

The risks of doing business with unauthorized or incorrectly identified persons in an Internet banking environment can result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data, or unenforceable agreements.

These methods include the use of customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of “tokens”, transaction profile scripts, biometric identification, and others

3.2 Existing authentication methodologies involve three basic “factors”:

- Something the user *knows* (e.g., password, PIN);
- Something the user *has* (e.g., ATM card, smart card); and
- Something the user *is* (e.g., biometric characteristic, such as a fingerprint).

3.3 Risk Assessment:

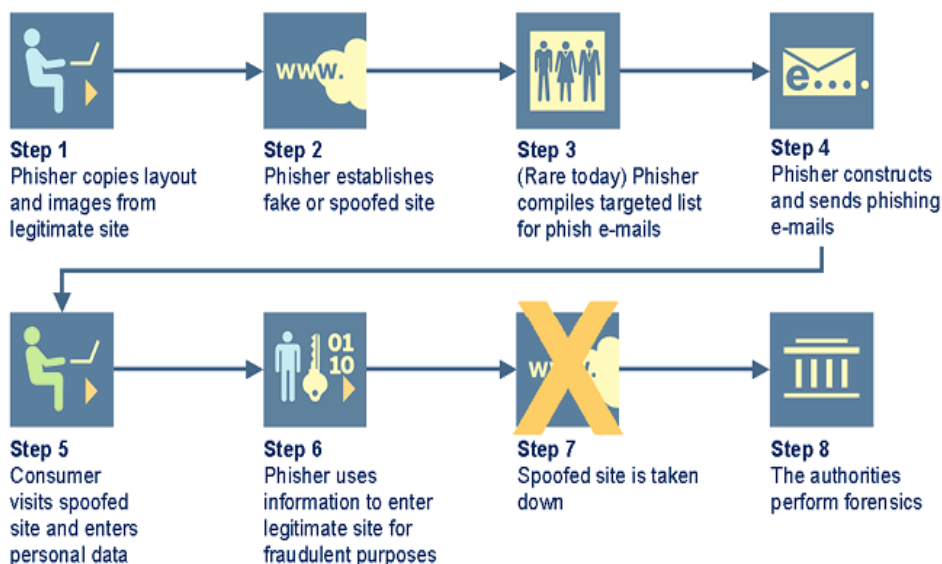
The implementation of appropriate authentication methodologies should start with an assessment of the risk posed by the institution’s Internet banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or commercial); the customer transactional capabilities (e.g., bill payment, wire transfer, loan origination); the sensitivity of customer information being communicated to both the institution and the customer; the ease of using the communication method; and the volume of transactions. Prior agency guidance has elaborated on this risk-based and “layered” approach to information security. Single-factor authentication tools, including passwords and PINs, have been widely used for a variety of Internet banking and electronic commerce activities, including account inquiry, bill payment, and account aggregation. However,

financial institutions should assess the adequacy of such authentication techniques in light of new or changing risks such as phishing, pharming, malware, and the evolving sophistication of compromise techniques.

3.4 Phishing:

A "phisher" sends e-mail to thousands of recipients, or "phish," directing them to a Web site where, under the pretext of completing security verification or other process, they are instructed to enter their essential account data, such as account number, personal identification number (PIN), and user ID.

Process Flow for a Phishing Attack

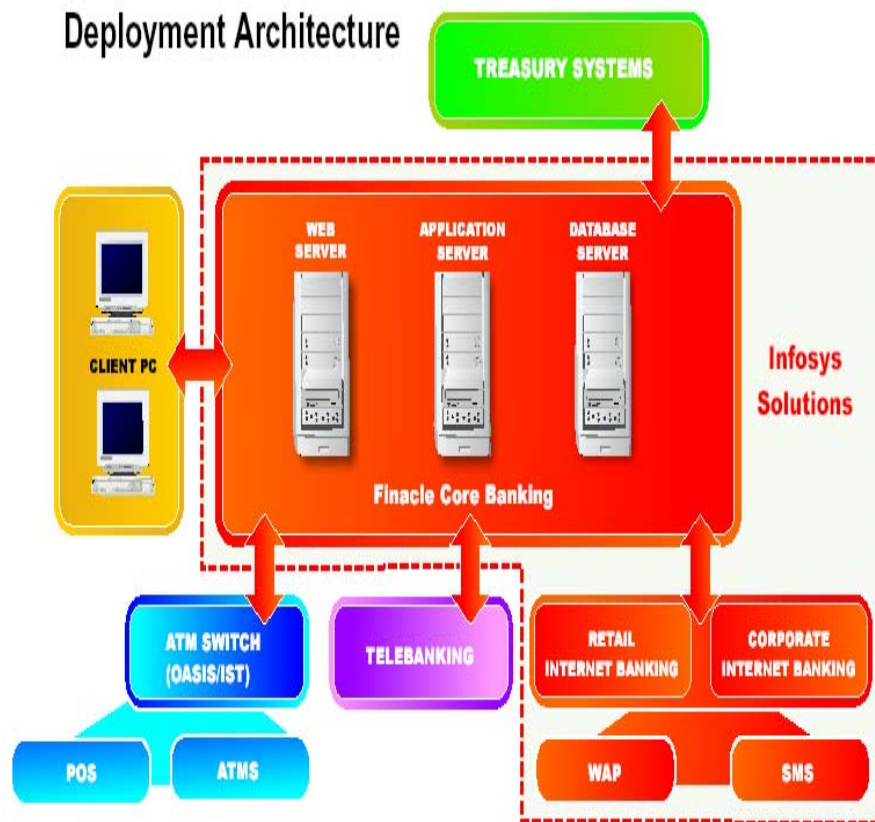


Source: Tower Group

3.5 ATM Authentication:

The term authentication, describes the process of verifying the identity of a person or entity. Within the realm of electronic banking systems, the authentication

process is one method used to control access to customer accounts and personal information.



Source: Tower Group

Authentication is typically dependent upon customers providing valid identification data followed by one or more authentication credentials (factors) to prove their identity.

The complexity of the ATM deposit transaction today lends to the high costs and Vulnerabilities to fraud that bank currently experience; laminating the envelope alone Will save banks 10% of the fraud that originates at the ATM.

- The US banking industry stands to save over \$2 billion annually from decreased transaction costs by automating the ATM deposit.
- Fraud reduction creates even more savings, none of which rely on moving deposit transactions from the teller to the ATM.
- The top 10 banks in the US are currently working on an ATM deposit automation strategy.

4. Authentication Techniques, Processes, and Methodologies:

Material provided in the following sections is for informational purposes only. The selection and use of any technique should be based upon the assessed risk associated with a particular electronic banking product or service.

5 Tokens:

Tokens are physical devices (*something the person has*) and may be part of a multifactor authentication scheme. Three types of tokens are discussed here: the USB token device, the smart card, and the password-generating token.

5.1 USB Token Device:

The USB token device is typically the size of a house key. It plugs directly into a computer's USB port and therefore does not require the installation of any special hardware on the user's computer.

Once the USB token is recognized, the customer is prompted to enter his or her password (thesecond authenticating factor) in order to gain access to the computer system.

5.2 Smart Card:

A smart card is the size of a credit card and contains a microprocessor that enables it to store and process data. Inclusion of the microprocessor enables software developers to use more robust authentication schemes. To be used, a smart card must be inserted into a compatible reader attached to the customer's computer.

5.3 Smart Tokens:

These devices contain computer chips that store information and perform basic computer functions. Smart cards are devices the size of credit cards, and smart tokens are akin to the small Universal Serial Bus (USB) storage devices that attach to key chains.

5.4 Fingerprint Recognition:

Fingerprint recognition technologies analyze global pattern schemata on the fingerprint, along with small unique marks known as minutiae, which are the ridge endings and bifurcations or branches in the fingerprint ridges.

Fingerprint recognition systems store only data describing the exact fingerprint minutiae;Images of actual fingerprints are not retained. Fingerprint scanners may be built into computer keyboards or pointing devices (mice), or may be stand-alone scanning devices attached to a computer.

5.4 Password-Generating Token:

A password-generating token produces a unique pass-code, also known as a one-time password each time it is used. The token ensures that the same OTP is not used consecutively. The OTP is displayed on a small screen on the token.

Example of a Single-Use-Password Token: E*Trade's Secure ID Device



Source: Tower Group

The customer first enters his or her user name and regular password (first factor), followed by the OTP generated by the token (second factor). The customer is authenticated if

- (1) The regular password matches and
- (2) The OTP generated by the token matches the password on the authentication server. A new OTP is typically generated every 60 seconds—in some systems, every 30 seconds.



This very brief period is the life span of that password. OTP tokens generally last 4 to 5 years before they need to be replaced.

5.5 Out-of-Band Authentication:

Out-of-band authentication includes any technique that allows the identity of the individual originating a transaction to be verified through a channel different from the one the customer is using to initiate the transaction. This type of layered authentication has been used in the commercial banking/brokerage business for many years. For example, funds transfer requests, purchase authorizations, or other monetary transactions are sent to the financial institution by the customer either by telephone or by fax. After the institution receives the request, a telephone call is usually made to another party within the company (if a business-generated transaction) or back to the originating individual.

The telephoned party is asked for a predetermined word, phrase, or number that verifies that the transaction was legitimate and confirms the dollar amount. This layering approach precludes unauthorized transactions and identifies dollar amount errors, such as when a \$1,000.00 order was intended but the decimal point was misplaced and the amount came back as \$100,000.00.

In today's environment, the methods of origination and authentication are more varied. For example, when a customer initiates an online transaction, a computer or network-based server can generate a telephone call, an e-mail, or a text message. When the proper response (a verbal confirmation or an accepted-transaction affirmation) is received, the transaction is consummated).

5.6 Internet Protocol Address (IPA) Location and Geo-Location:

One technique to filter an online transaction is to know who is assigned to the requesting Internet Protocol Address. Each computer on the Internet has an IPA, which is assigned either by an Internet Service Provider or as part of the user's network.



Geo-location software inspects and analyzes the small bits of time required for Internet communications to move through the network. These electronic travel times are converted into cyberspace distances.

5.7 Mutual Authentication:

Mutual authentication is a process whereby customer identity is authenticated and the target Web site is authenticated to the customer. Currently, most financial institutions do not authenticate their Web sites to the customer before collecting sensitive information. One reason phishing attacks are successful is that unsuspecting customers cannot determine they are being directed to spoofed Web sites during the collection stage of an attack.

5.8 Biometrics:

Biometric technologies identify or authenticate the identity of a living person on the basis of a physiological or physical characteristic (*something a person is*). Physiological characteristics include fingerprints, iris configuration, and facial structure. Physical characteristics include, for example, the rate and flow of movements, such as the pattern of data entry on a computer keyboard.

Two biometric techniques that are increasingly gaining acceptance are fingerprint recognition and face recognition. Too many problems continue to plague the biometric approach to authentication to make it a viable alternative as yet. Biometrics authenticates identity by means of physical characteristics, such as fingerprint, voice, retina scan, signature analysis, or keyboard cadence.

5.9 SMS Text Password:

The use of Short Message Service (SMS) messaging for authentication requires a second, registered physical device: a cellular phone. At the time of authentication, a computer-generated code is sent to the user's mobile phone. Assuming the bank's customer base has a high percentage of cellular phone usage and is not opposed to the marginal SMS messaging expense.

5.10 Other Approaches:

Other approaches to two-factor authentication have been proposed or tested, but none yet seem to provide adequate protection at an affordable price. Approaches such as secure cookies, onscreen keyboards for PIN entry, authentication by selecting known images, Scratch cards with single-use validation codes, and others are available to enhance online security, but they have not yet gained traction in the market.

6. Conclusion:

Financial institutions offering Internet-based products and services should have reliable and secure methods to authenticate their customers. The level of authentication used by the financial institution should be appropriate to the risks associated with those products and services. Financial institutions should conduct a risk assessment to identify the types and levels of risk associated with their Internet banking applications. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks. The agencies consider single-factor authentication, as the only control mechanism, to be inadequate in the case of high-risk transactions involving access to customer information or the movement of funds to other parties.