C·O·M·O·D·O

Creating Trust Online™

White Paper

Mutual Authentication for Online Banking: One size does not fit all

Abstract

This paper will analyze the relative security and cost effectiveness of current mutual authentication solutions. In addition, this paper will also explore an innovative alternative to achieve not just compliance - but a true best practice PKI-based mutual authentication schema that is low cost, highly secured and highly manageable to deploy. This approach requires leveraging the specialized expertise of Certification Authorities, such as Comodo.

A new approach for achieving Best Practices compliance

May 2006

Executive summary

The best way to protect online users of banking services against an ever-growing variety of threats is with an effective, efficient multi-layered security environment that utilizes a mutual authentication model. This Best Practices approach enables the "User" to authenticate the bank site and the bank to authenticate the user.

Until now, a true, reciprocal, mutual authentication model simply was not possible. Why? Because there was no technology in place that enabled the User to authenticate the bank site with Internet-based trust indicators (e.g. SSL padlock) without falling prey to Internet spoofing or Man-in-the-Middle attacks. Thus, while numerous solutions exists for the bank to authenticate the User (e.g. 2 factor solutions such as tokens or biometrics) none can achieve a best practices mutual authentication model without addressing the lack of User authentication of the bank.

However, that has changed. This paper will explore a PKI based solution that addresses BOTH sides of the mutual authentication equation. PKI is the platform that allows Comodo, a leading Certification Authority, to offer two new digital certificates (X.509 standard) to fully meet the current requirements around mutual authentication. The first digital certificate that allows the User to authenticate the Bank is called a Content Verification Certificate (CVC). CVC's provide non browser based trust indicators to assure the consumer that the bank website they are on is legitimate. The second digital certificate, a PC certificate, is a highly efficient way for banks to authenticate customers.

By deploying this PKI based mutual authentication solution and leaving the management of the solution to a trusted Certification Authority, financial institutions can retain complete control over the entire certificate lifecycle, including issuance, renewal and revocation. At the same time centralized key generation, private-key backup and distributed key recovery ensure maximum security and protection of private keys.

Thus, using the specialized expertise of Comodo, a Certification Authority, financial institutions can deploy a Best Practices mutual authentication process efficiently and at a significant lower cost per customer than virtually every leading solution. This frees financial institutions from draining resources away from core, revenue generating customer focused services.

Table of Contents

Setting the stage

Banking online offers enormous benefits to consumers, but the fact is it also creates enormous vulnerabilities. These include account theft, stolen identities, and loss of all privacy. Consumers are now becoming aware of the growing cases of fraud in online financial services through news reports, word of mouth and, unfortunately, through a large occurrence of user experience. Threats have grown beyond simple phishing schemes to significant new threats posed by spyware, bank-stealing Trojans, browser hijacking, keystroke logging and remote administration tools. According to the research and analyst firm Gartner, nearly 30 percent of those who use online banking services say that online attacks have influenced their activities. Up to 75 percent of this group are logging on less often than they would if security were not a concern, and nearly 14 percent of these people no longer pay bills online, despite the convenience.

Online fraudsters have technologically outpaced the security measures that most financial institutions have put in place.

Why is this? Online fraudsters have technologically outpaced the security measures that most financial institutions have put in place. Fraudsters are playing havoc with transactional safety in every aspect of the online experience. They can break into passwords and other ways consumers identify themselves, and they can build fake bank sites with fake web content to steal bank customers' private details without the customer knowing it. Mistakenly, many financial institutions and consumers believe that if a padlock icon is on the site, the site is authenticated as legitimate. But padlocks do not authenticate the veracity of web content and are no protection against these false “phishing” sites. As a result, regulators have recommended that financial institutions pay close attention to mutual authentication solutions – those which make sure that the bank authenticates the customer and the customer authenticates the bank – to ensure a safe and secure online transaction.

The FFIEC guidelines

In October 2005, the Federal Financial Institutions Examination Council (FFIEC) updated new guidance stating that current authentication methods are not sufficiently secure. The FFEIC recommended that banks have a plan to implement “stronger” forms of authentication (i.e. two – factor as opposed to one) by the end of 2006. They also recommended that banks put in place a “mutual” authentication solution whereby the banks not only authenticates its online customers, but the customer can authenticate the banks legitimate website.

Some highlights of the FFIEC guidelines are:

- Financial institutions offering internet-based products and services should use effective methods to authenticate the identity of customers using those products and services.
- Single factor authentication methodologies may not provide sufficient protection for internet-based financial services.
- The FFIEC agencies consider single-factor authentication, when used as the only control mechanisms, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties

- Risk assessments should provide the basis for determining an effective authentication strategy according to the risks associated with the various products and services available to on-line customers.

The most urgent requirement for organizations in 2006 is for the bank to conduct a complete risk assessment to identify vulnerabilities. They recommend that institutions carefully research authentication methods that will be reliable, scalable and interoperable with existing and future infrastructures.

The FFIEC also recommends that banks put in place a "mutual" authentication solution whereby the bank not only authenticates its online customers, but the customer can authenticate the bank website.

Summary of Risk Analysis Process

A) Business Process Analysis

The FFIEC Risk Assessment recommendation outlines a process that should:

- Identify all transactions and levels of access associated with internet-based customer
- Identify and assess the risk mitigation techniques, including authentication methodologies, employed for each transaction type and level of access; and
- Include the ability to gauge the effectiveness of risk mitigation techniques for current and changing risk factors for each transaction and level of access.

B) Customer Usage Risk Analysis

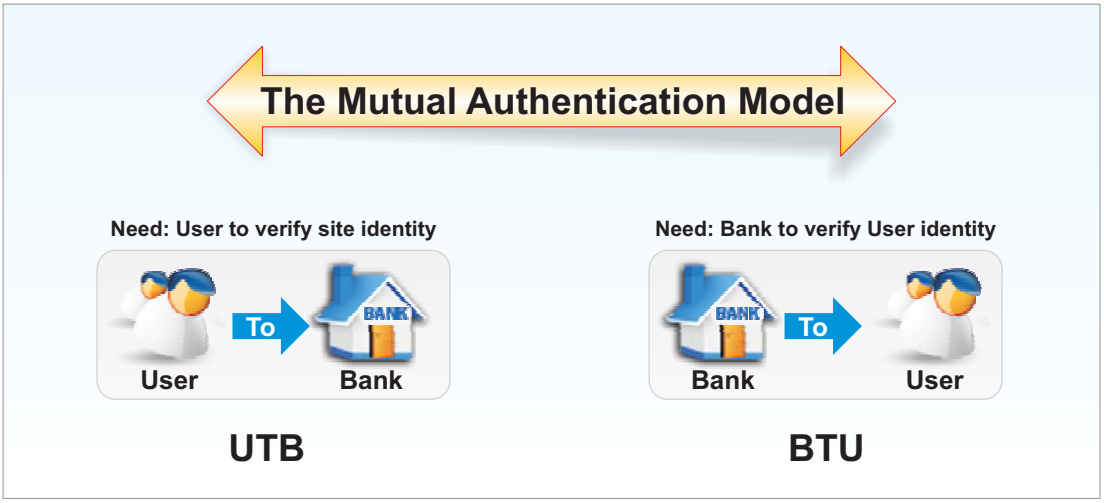
The FFIEC further recommends that risk should be measured by:

- Type of customer (e.g. retail or commercial)
- Customer transactional capabilities (e.g. bill payment, wire transfer, loan origination)
- Sensitivity of accessible customer information (communicated between both institution and customer)
- Ease of use of the communication method, and
- Volume of transactions

The Mutual Authentication Model

This model (see Figure 1) visualizes the reciprocity of the mutual authentication model - Bank can authenticate the user (BTU) and the User can authenticate the Bank (UTB). Much of the FFIEC Guidelines (and, not surprisingly, the industry's solutions) focus on the 2-factor authentication BTU aspect of the equation while ignoring the need for Users to authenticate the bank. Why has this occurred? Largely because it was assumed that SSL padlock were enough to establish site legitimacy. However, that is simply not the case. SSL certificates do not always authenticate the business legitimacy of the site or worse still the padlock can be faked. However, unless the User authenticates the bank as a legitimate site, subsequent 2-factor authentication will provide no security to the customer and their financial details may be stolen.

In 2005, there were over 500 phishing attacks utilizing an SSL certificate with the padlock icon.



(Figure 1)

a. Evaluating current User to Bank (UTB) Authentication Models

There are two ways that consumers currently try to authenticate financial institutions' websites. Unfortunately, none of these provide protection against today's aggressive fraudster climate. These include:

1. SSL certificates to authenticate site identity. This method is recommended by FFIEC guidelines to enable User to Bank (UTB) authentication. However, SSL certificates and the "padlock" offer scant protection against sophisticated man-in-the-middle and phishing attacks because:

- Many padlocks today only indicate that the transaction session is encrypted but do not offer attestation to the legitimacy of the business. These low assurance SSL certificates have the same padlock icon as a high assurance padlock in which a Certification Authority has authenticated the legitimacy of the business behind the website. In recent months there were over 500 phishing attacks utilizing SSL certificate padlocks.

- Phishing sites now have sophisticated techniques that let them fake anything that is in the browser including the padlock icon. Therefore, even the padlock can be "spoofed" - easily able to be copied onto a phishing site and therefore meaningless as an icon of authenticity.

2. Private Key Signing. This is where the customer sends a random "nonce" to the bank for signing with its private key. The customer verifies the reply with his securely stored copy of the bank's public key, which it obtained from a certificate signed by a Certificate Authority. The downside to this is that this solution requires a lot of computing power continually from the financial institution's web server as a public key encryption is required for every log in.

In addition, padlocks are browser-based and are "spoofable" – easily able to be copied onto a phishing site and therefore meaningless as an icon of authenticity.

Effectively, mutual authentication can not be deployed when consumers have no means to verify a site or log-in box authenticity with any browser-based trust indicators (e.g padlock).

b. Evaluating current Bank to User (BTU) Authentication Methods (a.k.a. 2-Factor)

The FFIEC guidelines recommend that authentication of the consumer be two-factor, meaning the bank must request two of the three different ways for consumers to prove their identity; 1) what consumers know (e.g. password), 2) what consumers are (e.g. biometrics) and / or 3) what consumers have (e.g. tokens). An example would be when someone goes to an ATM to withdraw money, they use something they have (an ATM card) and something they know (a PIN number).

There are a variety of two-factor technologies to choose from. Let us examine the strengths and weaknesses of these solutions.

1. Multiple passwords. Multiple or rotating passwords may be more secure than a single password, but only marginally so. And the stronger passwords are, the more difficult it is for consumers to remember them, and the more money is spent by financial institutions on password resets. In addition, most users have only a couple passwords for just about everything they do online, and once a cyber-thief has stolen this pool of passwords, any multiple password scheme can be bypassed effortlessly. Unfortunately, even multi-factor personal information can easily be forged and attacked by fraudsters.

2. Image or phrase recognition. Image, such as typing a password onto a screen keyboard with a mouse, or a pre-chosen phrase or image recognition solutions depend on a shared secret which is supposedly not accessible to the on-line attacker. But, forgers and fraudsters have found a way around that. They essentially become a "man in the middle." The fraudster contacts the real bank at the same time and relays authentication requests to the victim and his replies back to the bank. This then gives him access to the victim's accounts.

3. Smart cards and tokens. Many financial institutions have considered one time pads, smart cards, and distributed time-based tokens that generate a random number the user must supply along with a PIN at login time. But at up to $25 each, traditional time synchronous tokens are not that cost effective. In addition, there is significant cost to manage lost or stolen smart cards, tokens, or "bingo" cards.

4. Biometric solutions. Fingerprint scanners and voice-recognition software – are a strong security solution, but the cost is even steeper and accuracy rates are varied.

In summary, therefore, for Banks to authenticate User can be accomplished a variety of ways. However, irrespective of approach, all solutions require consumers to change their behavior for every interactions.

Existing Authentication Methods:
For authenticating the user (BTU)

	Benefit	Liability
Multiple Passwords	Inexpensive	Easy for fraudsters Easy for userto access
Time-based tokens One-time pads, smart cards	Easy for user	Cost-prohibitive Accessible to fraudsters
Fingerprint scanners	Secure	Costly and room for error
Private Key Signing	Accurate	Very expensive To implement

(Figure 2)

Summary

One size mutual authentication does not fit all banks

The FFIEC states, "When 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 these risks." In other words, banks need to design solutions that meet the exact needs of their customer base. Some banks do require complex global solutions, but the majority of banks need solutions that are customer friendly, secure and only as involved as the level of their risk requires. Most banks will benefit from a simple, progressive solution that ensures speed to compliance and mutual authentication before the end of this year.

Today's progressive solution for Best Practices compliance

Solution Overview for Mutual Authentication

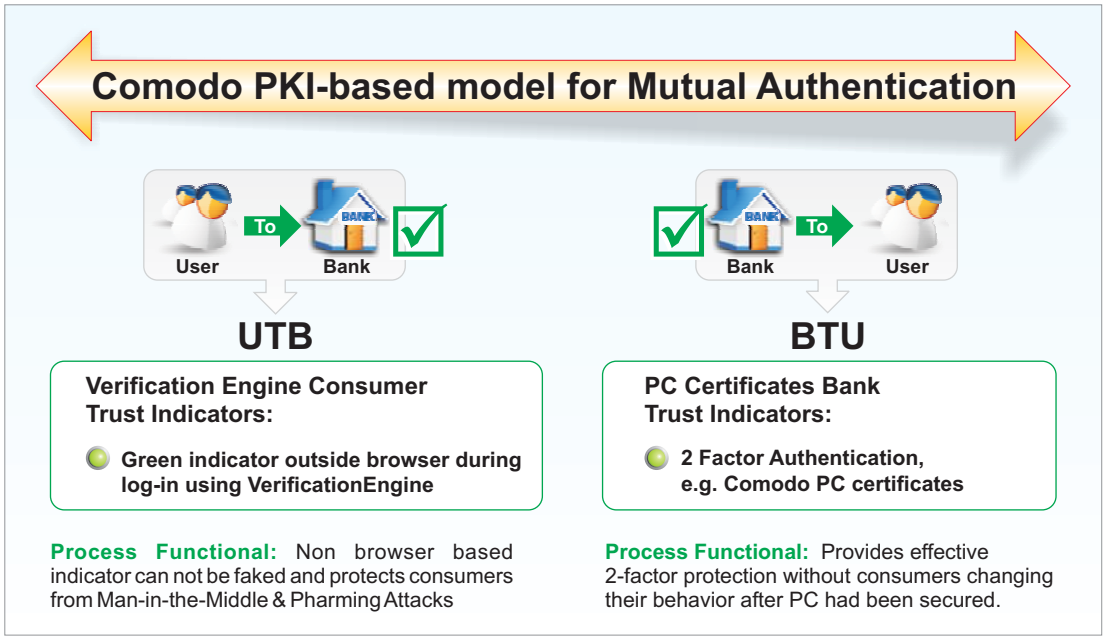
Technology has now caught up with the challenge of authentication and, finally, there is a progressive solution for both parts of the mutual authentication equation. The key to that solution is in the word "authentication." Clearly, site identity, web content and consumers have to be authenticated within an accessible process that provides protection and does not interrupt the customer experience. Only a Certification Authority, such as Comodo, has the expertise to develop and manage the infrastructure and processes to authenticate online e-commerce and communications.

Certification Authorities achieve mutual authentication by using a public key infrastructure (PKI) which is recognized by regulators as a highly secure platform to authenticate digital content. Additionally, a managed PKI service cuts expensive internal PKI costs significantly by softening the burden on internal resources, placing the operational burden on the Certificate Authority, and eliminating technology obsolescence because the system is built and maintained centrally. And most importantly, browsers and email clients have trusted Certification Authority root keys embedded in them when they are shipped so that individual client certificates signed by one of these Certification Authority roots will be automatically accepted without unfriendly warning dialogs.

A managed PKI service cuts expensive internal PKI costs significantly by softening the burden on internal resources, placing the operational burden on the Certificate Authority.

Functional Mutual Authentication Architecture

Figure 3 provides an overview of the Comodo's Mutual Authentication Solution with a discussion of the key technology that enables this cost effective and highly efficient approach.



(Figure 3)

a. The Comodo Solution for User to authenticate the bank: Content Verification Certification

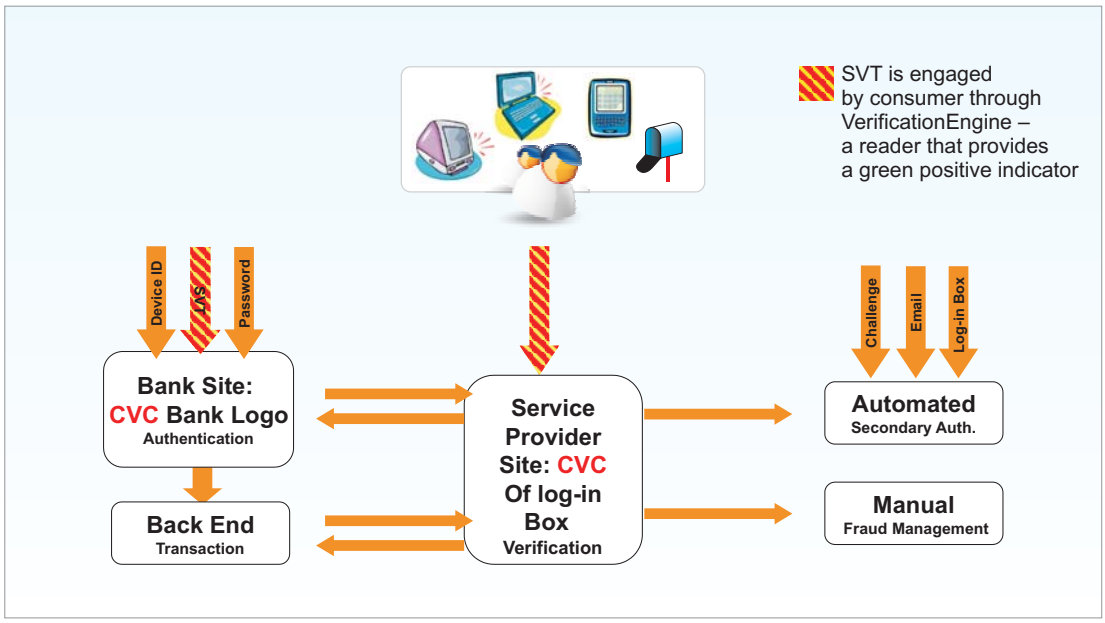
Unless a consumer authenticates the website he or she is on, there is no point worrying about how the bank authenticates them back. If the site is false, then obviously they will authenticate the user to capture their financial details. So it is mandatory that the user authenticates the bank website before any other authentication begins.

For consumers and banks who want to be sure that a financial institution site is authentic, Comodo is the only company to date who offers a proprietary technology which securely takes the organization's web content, ip addresses and domain names, and embeds them into a digital Content Verification Certificate (CVC). This CVC is posted to the institution site as proof of authenticity which the customers can verify in real time. Financial institution customers simply roll their cursor over the website's embedded elements, and a VerificationEngine frames the authenticated content pages with a green border that is non-spoofable because it is outside the browser.

The "Green is Good to Go" border is the sign that the web identity is indeed the bank's and not a phishing or pharming site. There are innumerable benefits for both the customer and the bank:

- simple and easy-to-understand technology
- cost efficiency
- not disruptive to the customer and easy for them to use
- easy to support

CVC technology integrated into Bank / Service Provider Verification Process



(Figure 4)

b. The Comodo Solution for Bank to authenticate the customer: PC Certificates

Digital client certificates (for the PC) are an easy to deploy, affordable, secure and convenient solution for banks to authenticate customers. Again, only a Certification Authority, like Comodo, has the infrastructure to put this solution in place. Based on public key infrastructure (PKI) encryption technology, client PC certificates achieve two-factor authentication. Digital PC certificates can be delivered electronically, while providing strong (2-factor) authentication of users. The two factors are made up of the authentication of the user and their PC. In addition, digital certificates protect the integrity of data and provide a transparent log-on method that won't inconvenience users. They can be stored directly on a user's pc, or, for portability, they can be stored on smart cards or tokens. A PKI client certificate assures the bank that the user logging in is indeed the bank customer.

Two forms of PKI certificates meet the current need for mutual authentication.

Comodo's Content Verification X.509 Certificates assure the consumer that the bank website they are on is legitimate.

Similarly, PC certificates are the best way for financial institutions to authenticate customers.

Benefits to Financial Institutions:

By deploying this PKI based mutual authentication solution and leaving the management of the solution to a trusted Certification Authority, financial institutions can retain complete control over the entire certificate lifecycle, including issuance, renewal and revocation. At the same time centralized key generation, private-key backup and distributed key recovery ensure maximum security and protection of private keys.

Thus, using the specialized expertise of Comodo, a Certification Authority, and financial institutions can deploy a Best Practices mutual authentication process efficiently and at a significant lower cost per customer than virtually every leading solution. This frees financial institutions from draining resources away from core, revenue generating customer focused services.

	Benefit to Bank	Benefit to Consumer
For consumers to authenticate bank site:		
Comodo Content Verification Certificates	Accurate Inexpensive to implement Managed by Certification Authority	Accurate Free Cannot be spoofed Interactive
For bank to authenticate customers		
Comodo Client PC Certificates	Accurate Mobile Inexpensive to Implement Managed by certification authority	Simple Foolproof Nothing to remember

(Figure 5)

About Comodo

Comodo is a leading global provider of Identity and Trust Assurance services on the Internet, with over 200,000 customers worldwide. Headquartered in Jersey City, NJ with global offices in the UK, Ukraine, and India, the company offers businesses and consumers the intelligent security, authentication and assurance services necessary to ensure trust in online transactions.

As a leading Certification Authority, and in combination with the Digital Trust Lab (DTL), Comodo helps enterprises address digital ecommerce and infrastructure needs with reliable, third generation solutions that improve customer relationships, enhance customer trust and create efficiencies across digital ecommerce operations. Comodo's solutions include SSL certificates, integrated Web hosting management solutions, web content authentication, infrastructure services, digital e-commerce services, digital certification, identity assurance, customer privacy and vulnerability management solutions.

For additional information on Comodo – Creating Trust Online ™
please visit www.comodo.com

Comodo
US Headquarters,
525 Washington Blvd.,
Jersey City, NJ 07310
Tel : +1.888.COMODO.1
email : sales@comodo.com

Comodo Group Inc.,
3rd Floor, Office Village,
Exchange Quay, Trafford Road,
Salford, Manchester M5 3EQ,
United Kingdom.
Tel Sales: +44 (0) 161 874 7070
Fax Sales: +44 (0) 161 877 7025