C·O·M·O·D·O

Creating Trust Online™

Comodo Mutual Authentication Solution Overview:

Comodo Two Factor Authentication
Comodo Content Verification Certificates

January 2007

Setting the stage

Banking and doing business 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 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 organizations have put in place.

Why is this? Online fraudsters have technologically outpaced the security measures that most 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 sites with fake web content to steal customers' private details without the customer knowing it. Mistakenly, many online businesses and consumers believe that if a padlock icon is on the site, the site is authentic. But padlocks do not authenticate the veracity of web content and are no protection against these false “phishing” sites. As a result, many businesses in highly regulated industries such as healthcare, education, insurance and others are paying close attention to mutual authentication solutions – those which make sure that the online businesses authenticates the customer and the customer authenticates the online site – to ensure a safe and secure online transaction.

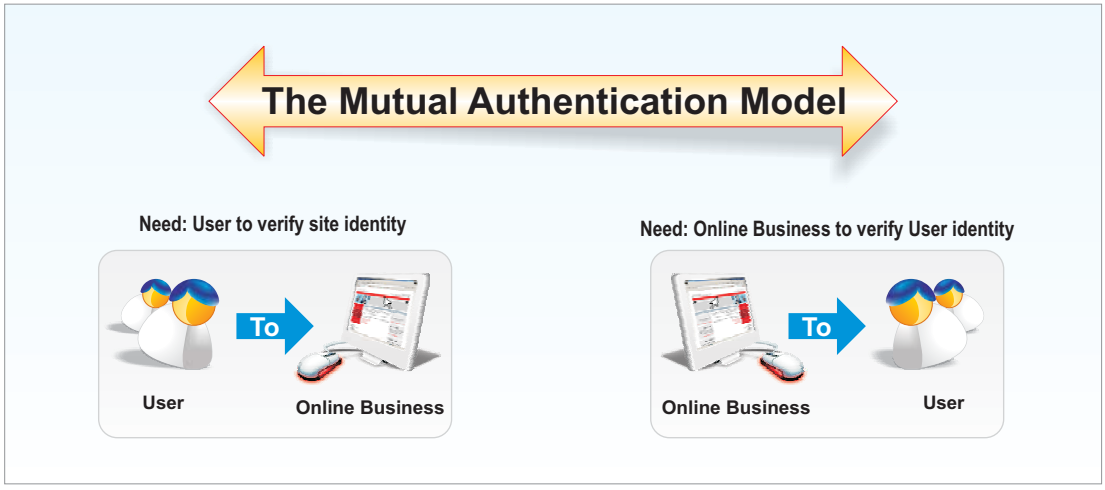
New Regulatory Environment

Many regulated industries, such as insurance or financial institutions have new regulatory requirements. For instance, in October 2005, the Federal Financial Institutions Examination Council (FFIEC) updated new guidance stating that current authentication methods are not sufficiently secure. The FFIEC recommended that banks have a plan to implement “stronger” forms of authentication (i.e. two – factor as opposed to one) by the end of 2007. They also recommend 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's website identity.

The Mutual Authentication Model Today

Federal guidelines recommend that "high risk transactions" require a "mutual" authentication solution whereby reciprocal authentication can take place.

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



(Figure 1)

Evaluating current User authentication models

The gold padlock used by consumers to authenticate site identity, offers scant protection against sophisticated Man-in-the-Middle attacks because :

- Many padlocks today only indicate that the transaction session is encrypted but do not offer attestation to the identity 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 identity 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” and can not be relied on as an icon of authenticity.

Evaluating current Two factor authentication solutions

Strong authentication of the consumer means that the site 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).

It was assumed that the padlock was enough to establish site identity. In 2005, there were over 500 phishing attacks utilizing an SSL certificate with the padlock icon.

Assessment of Two Factor Solution Alternatives

Alternative Technology	How it works	Limits
Image recognition	Users select images which the User must identity before transaction can take place	- Subject to Man-in-the-Middle attacks - Requires changes user experience
Multiple passwords	Users selects multi layered password which must be correctly submitted before transaction can take place	- Subject to User error - Requires changes to User experience
Tokens	Users are given a token which then generates a random code which must be submitted before transaction can take place	- Expensive to deploy - Difficult to support - Requires changes to User experience
Biometrics	Users initiate a process that authenticates them physically – e.g. fingerprint recognition	- Expensive to deploy - Requires change to User behavior
Cookie Monitoring	Users behaviors are tracked by cookies thus allowing banking transaction to take place	- Subject to User deletion of cookies - Least strong of all authentication processes

Summary

One size mutual authentication does not fit all

“When risk assessments indicate that the use of single factor authentication is inadequate, institutions should implement multifactor authentication, layered security or other controls reasonably calculated to mitigate these risks.” The government recommends that regulated industries need to design solutions that meet the needs of their customer base Consumer and organizations will benefit from a simple, progressive solution that ensures speed to compliance and a truly User friendly mutual authentication solution.

C·O·M·O·D·O
Creating Trust Online™

Comodo Mutual Authentication Solution

Government recommendations are suggesting that highly regulated industries use multifactor authentication solutions. That's because single factor authentication is not strong enough and too easy for fraudsters to attack. But many solutions are complex, costly and difficult for customers to use.

Now there is an easy, inexpensive solution: Comodo Mutual Authentication Solution

"When risk assessments indicate that the use of single factor authentication is inadequate, institutions should implement multifactor authentication..."

FFIEC

Comodo Mutual Authentication Solution at a Glance

What Online Business need	The Solution	How it works
Mutual Authentication schema so that;		
1) Online Business can authenticate User	1) Two Factor Client Certificate solution plus server application to automatically issue/manage Client Certificates for User authentication	**Two Factor Client Certificate for Online Business to authenticate User:** • "Plug 'n authenticate"-requires no online banking application integration • Customers can continue current behavior • Can be deployed within days • PKI based - recognized as highly secure • Very cost efficient • Offers high configurability • Easy to deploy and support
and	***PLUS***	
2) User can authenticate Online Business site identity	2) Comodo Content Verification Certificates (CVC)	**CVCs enable User to authenticate Online Business:** • CVCs are digital certificates that protect content so Users can irrefutably verify site ID • Key content such as log-in box or site logo are protected via CVCs • Protected content will display a green border OUTSIDE the browser environment making it impervious to publishing, pharming and Man-in-the-Middle attacks. • Phishing / Pharming sites are immediately exposed

1) What are Two Factor Client Certificates?

Easy to deploy and low cost solution provides strong PKI authentication

Digital Client certificates comply with Two Factor Authentication by installing a digital certificate onto a User's PC therefore "converting" their computer into a "smart token". Client Certificates are easy to deploy, affordable, secure and convenient solution for online business to authenticate customers. Client certificates can be delivered electronically while providing strong 2 factor authentication of users.

Digital certificates protect the integrity of data and provide a transparent log-on method that won't inconvenience users. These certificates 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 or online organization that the User logging in is indeed the customer. This type of solution can be delivered only by a Certification Authority because only a CA manages the full lifecycle of these digital certificates including issuance and revocation.

Client Certificates at a glance:

- PKI digital certificates based on X.509 standards
- Can be deployed in days
- Very low cost
- Secure and convenient
- Delivered electronically
- A transparent log-on with no inconvenience to customer

2) What are Content Verification Certificates (CVC)?

Anti phishing innovation so Users can bank online with "Verifiable Trust".

Unless a consumer authenticates the website he or she is on, there is no point worrying about how the site 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 online business website before any other authentication begins.

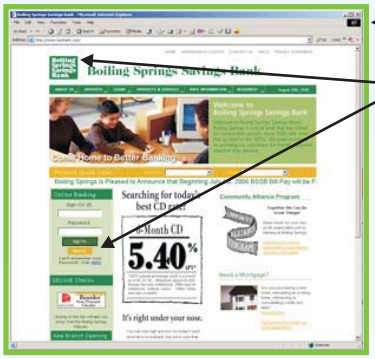
CVCs ensure that digital content and therefore site identity can be certified and verified in real time and without disrupting the normal transaction process. CVC's work by providing trust indicators that verify:

- Log-in box belongs to the site it claims to be
- Contact or rate information has not been tampered with
- Third party credentials, (like FDIC) can be verified

How they work?

Comodo's See Verify Trust technology takes the site's web content (e.g. log-in boxes), IP addresses and domain names, and embeds them into a digital Content Verification Certificate (CVC). This CVC is stored either on the webserver or centrally on Comodo's servers and serves as proof of authenticity. The online customer uses a free reader called VerificationEngine (a downloaded reader) to enable real time verification. Online customers simply roll their mouse over the website's content that contains a CVC, and VE displays a green border outside the browser.

CVC's at a glance



Authenticated site will display green to go border.

"Green is Good to Go" trust indicator happens automatically when Customer puts mouse over log-in box or logo protected with a CVC. This anti phishing tool authenticates site identity in real time. This is the only non browser based, non spoofable ID assurance technology on the market today.

- Digital certificates based on X.509 standards
- Ties log-in boxes to a specific site with a verifiable URL/IP address
- Phishing or Pharming sites are exposed instantaneously
- Does not disrupt the normal transactional process
- Non-browser based indicator is spoof proof and protects against Man-in-the-middle attacks
- Content is authenticated by Comodo and CVCs are stored on either the webserver or Comodo's servers
- Green border indicator outside the browser provides instant, direct consumer feedback about authenticated content

Benefits to Online Business

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

This solution delivers specific and measurable benefits including:

- ease of customer adoption
- no business-side integration
- ease of configurability
- low cost

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

Centralized key generation, private-key backup and distributed key recovery ensure maximum efficient certificate management.

Why Comodo Delivers more value to you

While consumers like banking and shopping online, they have become more sensitive to protecting personal information. At least 85% of Americans worry about becoming victims of identity theft ("Steely-Eyed about Identity Theft," eMarketer, May 4, 2004) and 64% of online shoppers have abandoned an online transaction because they didn't feel secure submitting sensitive payment information (TNS market research June-July 2004).

With Comodo's Mutual Authentication solution, you empower your customers with a “Verifiable Trust” authentication model that is cost effective, simple for customers to adopt, virtually transparent for the bank to support and requires no bank side integration.

With Comodo's Mutual Authentication solution, you empower your customers with “Verifiable Trust” authentication model ...

Comodo Credentials

- Serving and securing over 200,000 customers worldwide including:
  - 7 of the top 10 Fortune 1000
  - 5 of the top 7 leading U.S. universities
  - Top 2 U.S. automotive manufacturers
  - Top 2 global software providers
  - Top 3 wireless providers
  - Top 2 U.S. military manufacturers
  - Leading multi-national companies such as NASA, Xerox, SONY Europe, GE, Kaiser Permanente, BASF,
  - Deutsche Bank AG and U-Haul
- Portfolio of 10 Public root certificates under direct ownership
- Fully automated process for certificate issuance with unlimited re-issuance policy
- Virtually universal browser ubiquity (99+%) with 128/256 bit industry standard encryption and up to $1million USD warranty
- SGC (Server Gated Cryptography) certificates to enable older system to achieve 128-bit equivalent encryption
- First to market with Multi-Domain SSL certificates specifically addressing the multidomain needs of the enterprise
- A fully WebTrust compliant CA the highest globally recognized standard and a member of the Microsoft Root Certificate program
- Diverse set of customer management systems aligned to customer requirements and SLA's

About Comodo

Comodo is a leading global provider of Identity and Trust Assurance services on the Internet, with over 200,000 customers worldwide. Our global presence includes offices in the US, 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
525 Washington Blvd.,
Jersey City, NJ 07310
Tel : +1.888.COMODO.1
email : sales@comodo.com

Comodo
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

www.comodo.com