Comodo Authentication Solutions Overview

Client Authentication Certificates
Two-Factor Authentication
Content Verification Certificates
Mutual Authentication

COMODO
ENTERPRISE™

Foreword

Conducting business online offers enormous benefits to an enterprise. Unfortunately, these benefits continue to be challenged by an escalating variety of complex security threats that all too often result in the theft of account information and identities, misappropriated intellectual property, regulatory fines and a resulting loss of business reputation. Consumers have become painfully aware of online fraud through news reports as well as through an increasing occurrence of 1st hand experiences. Online threats have grown beyond simple phishing schemes to significant, organized attacks posed by spyware, credential-stealing Trojans, browser hijacking, keystroke logging and remote administration tools, just to name a few. According to the research firm Gartner, nearly 30 percent of those who use online services say that publicized 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. A disturbing statistic that truly defeats the benefits and cost-savings associated with online business applications and eCommerce.

Why is this? Criminals have organized, and have technologically outpaced the security measures that most institutions put in place. These fraudsters are playing havoc with transactional safety in every aspect of the online experience. They can easily break into password protected applications, and they can build fake sites with authentic looking content to steal sensitive and private details. 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 web content and are no protection against fraudulent sites. As a result, many businesses are paying close attention to two factor and mutual authentication solutions to secure user access to confidential information and services. It is this type of mutual solution that enables an enterprise to authenticate the user and also allow the user to authenticate the enterprise website as genuine.

Client Authentication Certificates

At a Glance: Digital Client Certificates

- Affordable and Easy to Deploy
- PKI Strong Authentication, Binds User and Device Identities
- Enables Transparent Log-on with No User Inconvenience
- No Costly Physical Tokens To Deploy, or Replace
- Mobile - can be stored on smart cards or USB devices when traveling

Digital Client Certificates are an easy to deploy, affordable and effective PKI solution to enabling the enhanced user identification and access controls needed to protect sensitive online information. Client certificates are delivered electronically, and can be automatically installed on just about any computer or mobile device. They can also be stored and transported on smart cards or USB tokens for use when travelling. PKI client certificates are an essential element of Comodo's Two-Factor Authentication solution that provides strong user access authentication, protects the privacy of online data, and offers a transparent log-on method that won't inconvenience users.

Each certificate, in addition to traditional login credentials, establishes a user's unique identity to a remote server Application, in this case the Comodo Two Factor proxy server. Each certificate can only be used to authenticate one particular user because only that user's computer has the corresponding and unique private key needed to complete the authentication process. Self-enrollment for and installation of a client certificate onto an end users machine requires no expertise and will not inconvenience users like other two factor solutions that rely upon expensive physical devices.

A PKI based client certificate assures an enterprise that the person logging into a secure service is indeed one of their users by validating not only their User ID and Password, but their certificate as well. This type of solution can only be delivered by a Certification Authority such as Comodo because only a Certification Authority has the experience, expertise and security infrastructure to manage the full lifecycle of public digital certificates - including issuance, renewal and revocation.

User Authentication generally involves three basic "factors":

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

Businesses benefit from two-factor authentication because it's easy for them. After the certificate is automatically installed on the end-user's computer or PDA, their login process remains unchanged with no new steps to learn, or action to complete. When they need to use a computer that does not have the certificate installed, Comodo's Two-Factor process can issue them single-use passwords (to pre-stored personal destinations including Voice, SMS and eMail).

Benefits of Comodo Two-Factor Authentication

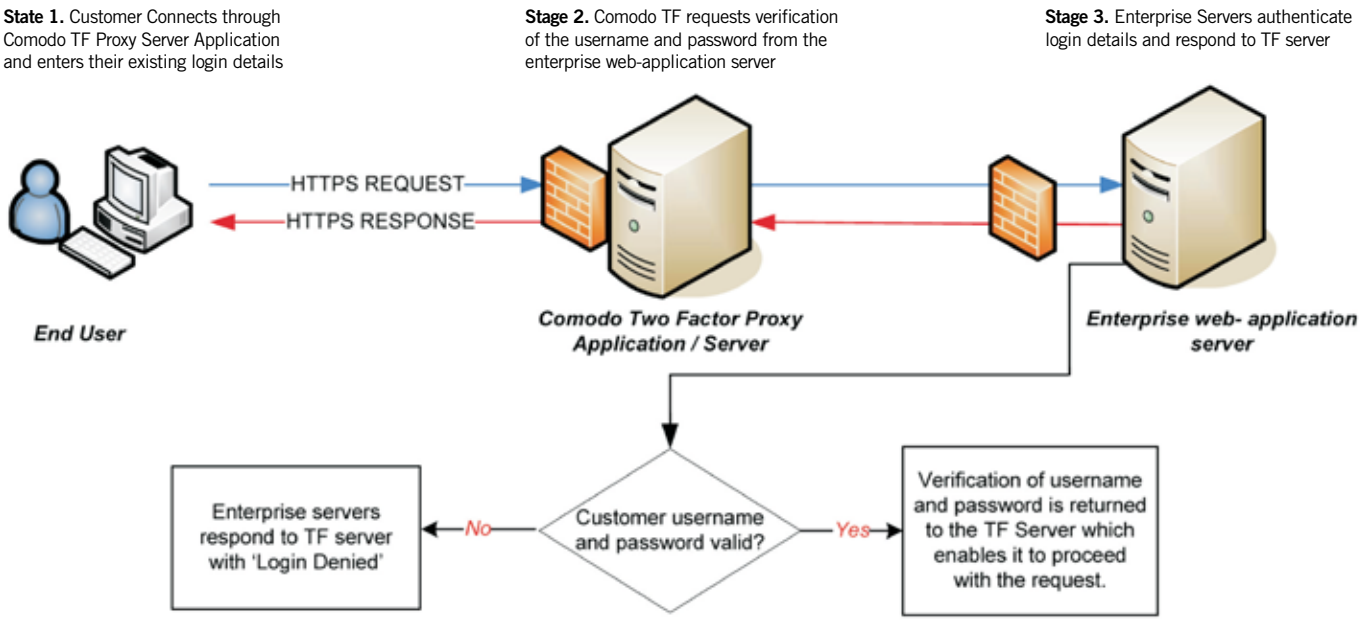
- Highly flexible and configurable proxy-based authentication solution that can be virtually deployed in hours. Seamless front-end for most user-access web pages, as well as for Microsoft Outlook Web Access and Sharepoint.
- Leverages Comodo's Public Key Certificate Authority Infrastructure, widely recognized as supplying the strongest form of authentication and encryption service available.
- Low cost automates the digital certificate issuance and management keeping administrative overhead to a minimum. No modification to existing applications.
- Easy to Use simple client account setup conveniently allows continued use of existing usernames and passwords. Certificates are automatically installed.

Comodo Two Factor Outline of Processes and Deployment

Comodo's Two Factor Proxy Server sits in front of an enterprise's firewall and the web server that hosts their secure services. The Domain Name Server (DNS) will direct all traffic to a login page hosted on the Two Factor server which in turn is configured to "HTTPS" proxy all requests to the enterprise website. The enterprise web application can be just about any type that generally requires an ID and password for user authentication. This also includes Microsoft Outlook Web Access (OWA) and Microsoft Sharepoint.

First Factor Authentication Existing User Credentials

The login page hosted on the Two Factor Server is an exact copy of the enterprise's existing login page, making the Two Factor application transparent to the end user. Once the account holder enters their username and password, the Two Factor application hands the request off via a secure SSLconnection to the enterprise's server. The enterprise server then processes the login request and responds to the Two Factor proxy server. The Two Factor server does not keep a record of any user details such as passwords or account information - nor does it require such information in order to deploy the Two Factor Client Certificates to the end user. The Comodo Two Factor Server will only proceed to the provisioning and/or authentication of the client certificate after the enterprise's web server has validated the account holder's username and password. This initial verification process is the First Factor of a Two Factor authentication solution (see diagram below).



Second Factor Authentication – Digital Client Certificates

The second part of the Comodo solution is for the user to set up the primary and auxiliary two-factor authentication systems. The primary two factor system is the provisioning of an X.509v3 client certificate onto the end user's machine. This certificate, once installed into the certificate store of the user's internet browser (e.g. Internet Explorer, FireFox, Opera, etc.) will be requested and verified every time the user logs into the Two Factor server and will authenticate them as the genuine account holder. Each client certificate contains two distinct yet equally important elements - the account holder's username and a 128 bit encrypted public key that was generated by the end user's computer during the enrollment process. This certificate is then digitally signed by the enterprise. (The enterprise will have been set up by Comodo as a sub-Certification Authority. A sub-CA is an entity entitled to sign their own user's authentication certificates from their own sub-CA certificate. In turn, the sub-CA's certificate is signed by Comodo - a trusted root CA). By signing the certificate, the sub-certification authority 'binds' the username to the public key. The presence of this certificate on the and users machine, along with the corresponding private key, is needed to complete the authentication process. This means that even if a hacker obtained an account holder's username and password, they would still be denied access to the account because the Two Factor server would not detect the client certificate on the machine the hacker is connecting from.

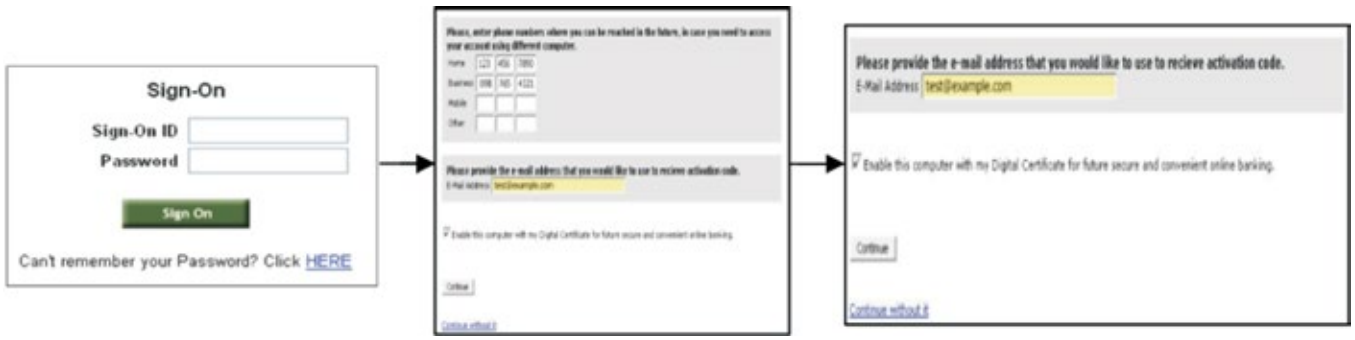
New User Enrollment

If a verified account holder is connecting to the Two Factor Server for the first time, they are provisioned with a client certificate and asked to set up contact details for the auxiliary authentication system. The diagram below is a quick illustration of the user sign up experience.

Step 1: User connects to Comodo TF proxy server and logs into with their existing username and password. This process is transparent to the end user because the TF login page is a duplicate of the enterprise's existing login page.

Step 2: After the enterprise server verifies the username and password, the user is required to provide contact telephone numbers and a contact email address. These will be used to contact the user to supply the one-time activation password. This information forms the basis of the auxiliary two factor authentication process.

Step 3. On the same form, the user is provided with the option to secure their computer with a digital certificate. This box is checked by default.



Step 4: The user must consent to the certificate subscriber agreement prior to installation

Step 5: After accepting the subscriber agreement, the user's certificate is automatically downloaded and installed onto their machine.

The next time the user logs into his account, the TF servers will automatically detect this certificate on their computer - meaning the enterprise web application server identifies the user as the true owner of the account by authenticating not only their User ID and Password, but their certificate as well.

A returning user will be asked to select one of the contact numbers or the email address they set up in Step 2 if they: (i) Choose not to install a digital certificate in Step 3 of 'New User Enrollment' (above) (ii) Are attempting to login to their account from a different machine.

New User Enrollment After the enterprise's web-application server has confirmed the account holder's Username and Password, a new user will automatically begin the client certificate enrollment process

Auxiliary Out of Band (OOB) Second Factor Authentication

In order to validate themselves to the Two Factor servers, a user must connect from a machine that they have installed a certificate on. If this is not the case, and no certificate is detected, then the primary Two-Factor process cannot be completed. Example scenarios include:

- The user chose not to install an authentication certificate during the New User Enrollment Process. In this instance, the user will have to go through the activation procedure every time they log on or until such time as they decide to install a certificate.
- The user is attempting to access his account from a different machine to the one they installed the certificate on. For example, they are using their work computer or laptop for the first time to access their account but installed the certificate on their home PC; they are trying to access from a 'public' computer such as those in internet cafes or libraries; they are trying to access from a mobile device for the first time; they are trying to access from a recently purchased computer.

To ensure the highest levels of validation are used at all times, Comodo Two Factor also incorporates an out-ofband second factor authentication process via telephone or SMS.

During enrollment the user is required to supply a minimum of one and a maximum of four contact telephone numbers. They are also required to enter a contact email address. In the event that a certificate is not detected on the user's machine during a subsequent connection attempt, then user will be presented with a pre-populated list of these contact details and asked to choose one. The Two Factor server will then send a randomly generated, one-time activation password to the chosen location. (If they selected a telephone number, they will receive an automated voice message. They also

have the option to receive the password as an SMS text message or email).

The user must then enter this activation password at the website. If it is verified as correct by the Two Factor server, then the user is allowed to connect to their account. They are also provided with the opportunity to install a client certificate on the machine they are currently attempting to connect from. For computers and devices that the user wishes to be trusted (computers they own or use at work) then a certificate should be installed. For computers that the user does not wish to be trusted (computers in public places such as internet cafes or computers they do not plan to use regularly), then the user should use the activation password mechanism.

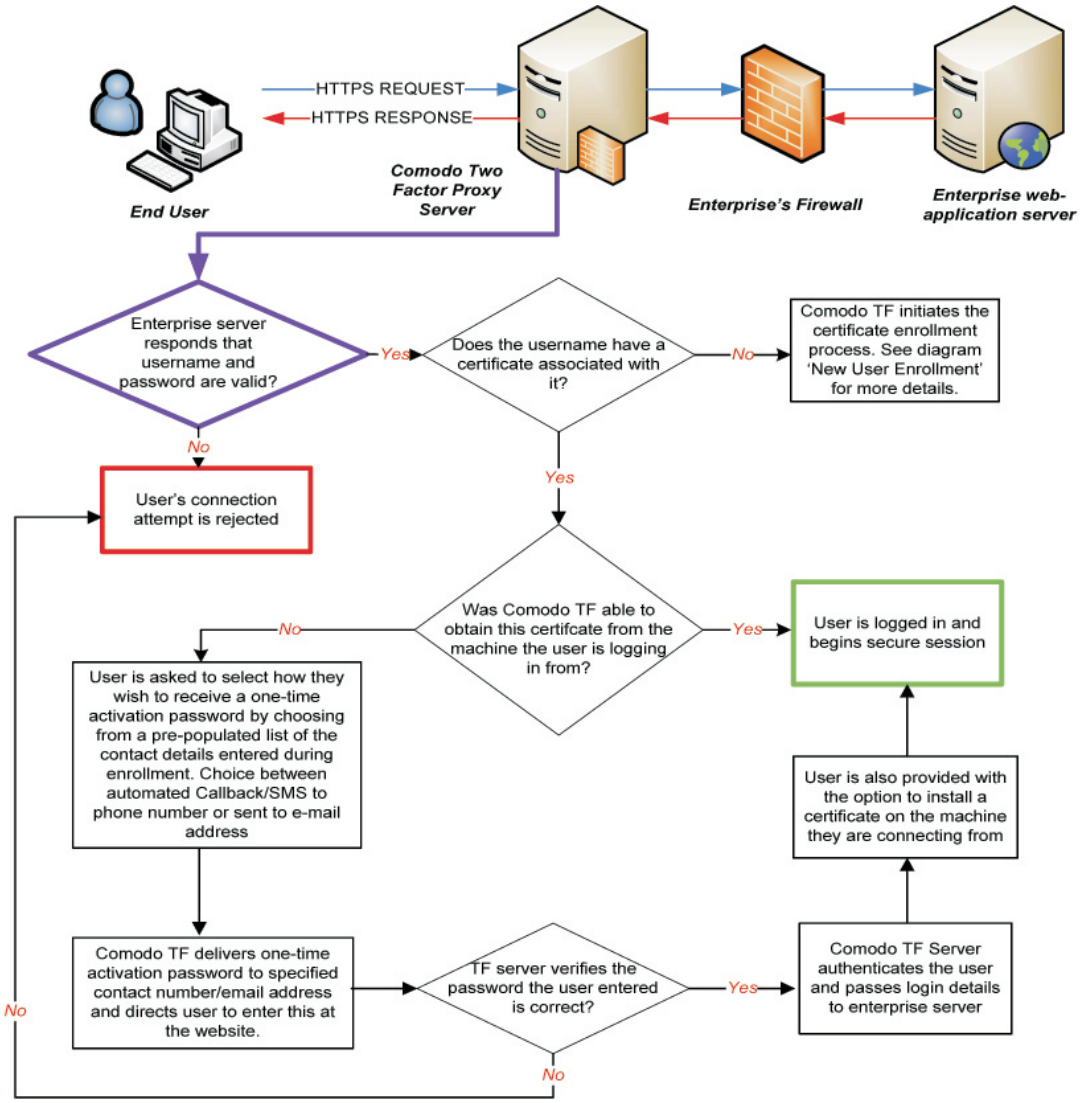
Authentication of certificate holder's: From the user's perspective, enrolling into the Comodo Two Factor service is a simple, one-time experience. Once they have a Two Factor Client Certificate installed on their computer, they will just continue to log-in to their account with just their existing username and password. All certificate authentication procedures are carried out seamlessly in the background and the user faces no interruption to their regular routine. If a user 'passes' the first factor authentication of username and password but is attempting to log on from a different machine (one that does not have a certificate installed) then they will have to obtain a one-time activation password that will be sent to the email address/phone number they specified during the initial enrollment process. After the user has entered this activation password and it has been validated by the Two Factor servers, the user is given the opportunity to install a client certificate on that machine too. The diagram below is an overview of the Two Factor authenti-cation process for an existing client certificate holder.

Stage 1. User connects through Comodo TF Proxy Server application and logs in with their existing login details

Stage 2. Comodo TF requests verification of the username and password from the enterprise application servers

Stage 3. Enterprise application servers positively authenticate login details and respond to TF server

Stage 4. After receiving First Factor confirmation of UN/PW, Comodo TF Server begins the certificate authentication / provisioning process



Comodo: the natural choice for secure authentication and regulatory compliance

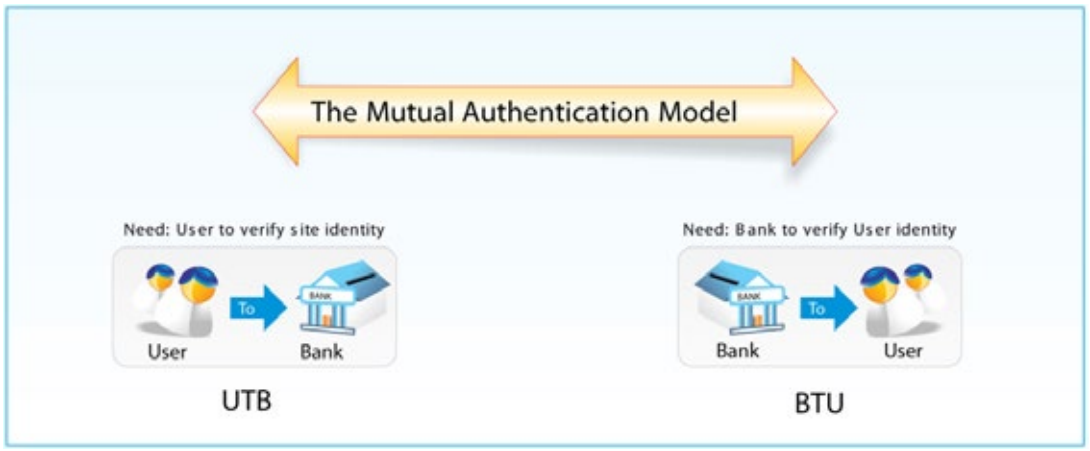
By deploying this PKI based Two Factor authentication solution and leaving the backend provisioning of the client certificates to a trusted Certification Authority, enterprise's can retain complete control over the entire certificate lifecycle - issuance, renewal and revocation. At the same time, centralized key generation, privatekey backup and distributed key recovery maximizes efficient certificate management. This solution delivers specific and measurable benefits including:

- True, Two-Factor authentication services, compliant with many regulations
- Ease of customer adoption
- No business-side integration
- Ease of configurability
- Low cost and fast deployment

Using the specialized expertise of Comodo, enterprises can deploy a Best Practices authentication process efficiently, and at a significantly lower cost per customer than virtually every other solution on the market.

Appendix 1: Comodo Mutual Authentication with Content Verification Certificates

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 enterprise web-site with Internet-based trust indicators without them falling prey to fake, Phishing websites or Man-in-the-Middle attacks. Thus, while solutions exist that have locked down the way an enterprise authenticates its users (i.e. Comodo Two Factor Solution), this still leaves the problem of how that user authenticates the enterprise's website. Comodo's patent pending Content Verification Certificate (CVC) is the first digital certificate that allows the user to authenticate the website they are at. An end user simply needs to place his mouse cursor over protected content and a green, browser-independent, border appears only if they are on the genuine website.



By also protecting website elements such as a login boxes and corporate logos with a Content Verification Certificate, Comodo helps online enterprises achieve a best practices mutual authentication model.

Comodo's patent pending Content Verification Certificate (CVC) is the first digital certificate that allows the user to authenticate the website they are at. An end user simply needs to place their mouse cursor over protected content and a green, browser-independent, border appears only if they are on the genuine website.

Content Verification Certificates (CVC's) at a glance

Content Verification Certificates enable end users to conclusively establish that they are on an authentic website. CVC's authenticate and verify web page content to the visitor. The content requiring protection is digitally bound within an X.509v3 certificate that then binds that content to a specific domain or IP address - an essential requirement for trusted services whose customers are now being attacked with increasing frequency by ever more convincing web page spoofs and Phishing attempts.

As an X.509v3 compliant certificate type, CVC's are created, distributed, and revoked using proven PKI (Public Key Infrastructure) methods to provide the highest level of security for web page content.

Facilitating the deployment of verifiable login boxes, navigation panes, rate cards and website logos, CVCs deliver trust and assurance to billions of online users. Deploying CVC's on both the online service provider's website and the two factor login pages means customers can proactively verify they are visiting the genuine site and can eliminate the chance of them disclosing confidential login details to a Phishing website.

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

Appendix 2: Additional Documentation

Comodo can provide the following Two Factor documentation upon request:

ComodoTwo FactorAdmin guide

ComodoTwo Factor Installation guide

End User Enrollment and Client Certificate Installation guides for:

- Internet Explorer on Windows Vista systems
- Internet Explorer on Windows XP systems
- FireFox internet browsers
- Opera internet browsers
- Konqueror internet browsers
- Safari internet browsers

About Comodo

The Comodo companies provide the infrastructure that is essential in enabling e-merchants, other Internet-connected companies, software companies, and individual consumers to interact and conduct business via the Internet safely and securely. The Comodo companies offer PKI SSL, Code Signing, Content Verification and Email Certificates; award winning PC security software; vulnerability scanning services for PCI Compliance; secure email and fax services.

Continual innovation, a core competence in PKI, and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo secures and authenticates online transactions and communications for over 200,000 business customers and 10,000,000 users of our desktop security products.

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

Comodo CA Limited
3rd Floor, 26 Office Village,
Exchange Quay,
Trafford Road, Salford,
Manchester M5 3EQ,
United Kingdom
Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161 877 1767

Comodo Group, Inc.
1255 Broad Street
Clifton, NJ 07013
United States

Tel: +1.888.266.6361
Tel: +1.703.581.6361
www.instantssl.com
Email: Sales@Comodo.com