COMODO
Creating Trust Online®

SERVICE ORGANIZATION CONTROL 3 REPORT

Digital Certificate Solutions, Comodo Certificate Manager (CCM), and Comodo Two Factor Authentication (Comodo TF) Services

For the period April 1, 2016 through March 31, 2017

Table of Contents

Ernst & Young LLP
5 Times Square
New York, NY 10036

Tel: +1 (212) 713-3000
ey.com

Building a better working world

Report of Independent Accountants

To the Management of Comodo:

Approach:
We have examined management's assertion that Comodo maintained effective controls to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification to achieve Comodo's, commitments and system requirements
- the System was available for operation and use to achieve Comodo's, commitments and system requirements

during the period April 1, 2016 to March 31, 2017 based on the criteria for security and availability in the American Institute of Certified Public Accountants' TSP Section 100A, *Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of Comodo's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Comodo's relevant security and availability policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Comodo's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Building a better working world

Inherent limitations:
There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security and availability are achieved.

Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion:
In our opinion, Comodo's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security and availability.

Ernst & Young LLP

July 28, 2017

New York, New York

COMODO
Creating Trust Online®

Management's Assertion Regarding the Effectiveness of Its Controls Over the Digital Certificate Solutions, CCM and Comodo TF Authentication services ("System") Based on the Trust Services Principles and Criteria, for Security and Availability

July 28, 2017

We, as management of, Comodo are responsible for designing, implementing and maintaining effective controls over the Digital Certificate Solutions, CCM and Comodo TF Authentication services ("System") to provide reasonable assurance that the commitments and system requirements related to the operation of the System are achieved.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in Security controls, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis. Examples of inherent limitations in an entity's Security's controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

We have performed an evaluation of the effectiveness of the controls over the system throughout the period April 1, 2016 through March 31, 2017, to achieve the commitments and system requirements related to the operation of the System using the criteria for the security and availability (Control Criteria) set forth in the AICPA's TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Based on this evaluation, we assert that the controls were effective throughout the period April 1, 2016 through March 31, 2017 to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification to achieve Comodo's commitments and system requirements
- the System was available for operation and use, to achieve Comodo's commitments and system requirements

based on the Control Criteria.

Our attached description of the boundaries of the System identifies the aspects of the System covered by our assertion.

Mr. Melih Abdulhayoglu
Chief Executive Officer &
Chief Security Architect
Comodo

Description of Comodo's System Relevant to Security and Availability

OVERVIEW OF COMODO

Comodo was founded in 1998 and includes Comodo CA Ltd headquartered, in the United Kingdom, and Comodo Security Solutions, Inc. headquartered in the United States of America (collectively referred to as "Comodo"). Comodo CA Ltd is a Certificate Authority (CA), providing digital certificate services out of the United Kingdom with Comodo Security Solutions Inc. providing Public Key Infrastructure (PKI) services in the United States of America.

Comodo issued its first digital certificate in 2001 and has grown to a worldwide presence in the Internet security industry Creating Trust Online® in over one hundred countries. Today Comodo has:

- More than 85 million desktop security installations;
- More than 700,000 business customers and 8,000 global partners and affiliates working with Comodo to make the Internet more secure and trusted;
- Market share leadership, being the #1 SSL Certificate Authority in the world, with more than 36% of the market, according to w3techs.com (as of July 1, 2015).

Comodo's team of over 1,000 employees has a passion for meeting the challenges of Creating Trust Online® for individuals, e-merchants, small to medium businesses, and large enterprises. Comodo's innovative software and services do this by:

- **Authenticating Individuals, Business Websites and Content**: Authentication is at the heart of trust – it's the process of confirming that something or someone is genuine. Hackers are counterfeiters and impersonators - they thrive on deception. Trust is created when individuals, businesses, websites or software publishers are authenticated to ensure that they are who they say they are, and that their information has not been tampered with. This trust is the core of successful online businesses and trusted online interactions.

- **Securing Information**: Encrypting sensitive information at all stages of its life cycle is a proven method of keeping it safe from hackers. Strong Public Key Infrastructure (PKI) encryption through digital certificates ensures that the encrypted information can only be used by authorized parties.

- **Securing Websites and E-Commerce**: Uncovering and alerting IT organizations to vulnerabilities in their server/site's technical configuration or security procedures that could be exploited by hackers, and providing advice or solutions to eliminate them.

- **Securing and Maintaining PCs**: Denying hackers access to the information and resources they need to succeed, such as your personal or business financial information, and at a more fundamental level, your computer's Internet connection and processing capacity.

Comodo offers a variety of products from digital certificates to desktop software for the purpose of Creating Trust Online®. These include: Comodo Digital Certificate Solutions; CCM; and Comodo TF, ultimately serving as the authentication mechanism for various Customer facing applications.

Comodo Digital Certificates

Comodo's Digital Certificate Solutions offer a wide range of hosted products with the flexibility and technical capability to meet customized Customer PKI needs. As a WebTrust certified CA, Comodo's solution includes standards of confidentiality, system reliability and pertinent business practices and provides Customers with:

- 2048-bit (Secure Socket Layer) SSL certificates as standard.
- Flexible and innovative solutions to meet Customer needs.
- Trusted by 99.9% of browsers.
- Custom configuration of PKI management tools.

Comodo's digital certificates include:

- Extended Validation (EV)-SSL.
- Multi-Domain EV SSL.
- Wildcard SSL.
- Unified Communications (UC).
- Intel Pro Series.
- General Purpose SSL.
- Secure E-mail – S/MIME.
- Client Authentication.
- Code Signing.
- EV Code Signing.
- Personal Authentication.

Comodo Certificate Manager

CCM is a hosted solution that reduces the time, management, development and operations needed for PKI security and administration. CCM offers Customers:

- Centralized administration of digital certificates with an easy-to-use web-based console,
- Secure, multi-tiered web interface for administering digital certificates,
- Certificate discovery that scans the network to pinpoint and record certificate deployments,
- Configurable email alerts for pending administrative tasks,
- Life-cycle administration for Comodo's extensive portfolio of SSL, S/MIME and Client Authentication certificates, and
- Customer key escrow that enables a protected recovery of user encrypted data.

Comodo Two Factor Authentication

Comodo TF, a secure authentication solution for Customers, is purchased and maintained on Customer premises (or 3rd party providers contracted by Customers). The solution can be deployed easily and administered effortlessly, and is supported 24/7 by Comodo's Customer Service Team who access Comodo TF through secure Virtual Private Network (VPN) tunnels.

Comodo TF supports the Federal Financial Institutions Examination Council (FFIEC) guidelines and employs technologies to address the needs of financial institutions, including:

- Two Factor Authentication.
- Multi-factor Authentication.
- Mutual Authentication.
- A Secured Execution Environment.

DESCRIPTION OF THE ENTITY LEVEL CONTROLS

This section provides information about the five components of Comodo's internal control:

1. Control Environment – sets the tone of Comodo, influencing the control consciousness of its personnel. It is the foundation for all other components of internal control, providing discipline and structure.
2. Control Activities – policies, procedures and supporting documentation that help make sure that management's directives are carried out.
3. Information and Communication – systems, both automated and manual, that ensures those connected with Comodo are aware of significant events in Comodo's operations, such as product launches, strategic direction of the company, and changes to published policies and procedures.
4. Monitoring – is a process that assesses the quality of Comodo's internal and external service delivery, and internal control performance to ensure effective business operations.
5. Risk Assessment – is the entity's identification process to pro-actively identify, monitor and manage business and operational risks.

Control Environment

Comodo's control environment reflects the overall attitude, awareness, commitment and actions of Comodo management and other stakeholders concerning the importance of controls, as well as the emphasis given to controls within the organization. Comodo's organizational structure, separation of job roles by department and business function, documented policies and procedures, are the methods used to define, implement and assure effective operational controls at Comodo.

Relevant elements of Comodo's control environment that affect Comodo's defined system are described below and include; organizational structure and assignment of authority and responsibility, direction and oversight provided by the management, policies and procedures, and confidentiality measures.

Organizational Structure

Comodo's organizational structure provides a framework for planning, directing, & controlling business operations. Comodo's personnel and business functions are segregated into specific departments according to product & operational responsibilities, with defined job responsibilities and lines of authority for reporting & communication.

Comodo's business operations are directed by the executive management team (Chief Executive Officer (CEO), Chief Financial Officer (CFO), & Chief Technology Officer (CTO)). This cross functional management team provides overall executive guidance and support for the planning and execution of the day to day operations of Comodo, supporting the Compliancy and Infrastructure teams that develop, monitor and manage Comodo's overall control objectives and control activities, and the communicating and monitoring of Comodo's internal control policies and procedures.

The Compliancy team is responsible for the effective development and implementation of Comodo's Information Security Policy & supporting documentation. The team communicates the Information Security Policy to Comodo's employee's, and monitors the effectiveness of Comodo's controls as well as employee and system compliance to documented policies.

The Infrastructure team is responsible for providing core IT support services throughout the Comodo group of companies. The protection of IT systems and the information they store, technical evaluation of systems, access administration, access control, desktop support and hosting support is provided by the Infrastructure team.

Human Resources Policies and Procedures

Formal hiring procedures are employed to ensure all new employees are qualified for their assigned duties. The recruiting process is the joint responsibility of the Human Resource (HR) department and the relevant business department managers. Hiring decisions are based on various factors including educational background, prior experience, and past accomplishments.

All employment offers are conditional on the candidate agreeing to, and signing the terms and conditions detailed in their employment contract, including confidentiality and non-disclosure agreements, as well as the employee handbook and Comodo's internal policies. It is required that all personnel understand their role within Comodo and that they are suitable for the role assigned.

Terminations of employment follow Comodo’s 'Disciplinary Procedure’. Any changes to, or termination of employment, must be advised to the required 'Systems Administrators' to ensure the correct access rights are granted, modified or revoked as necessary.

Information Security

All Comodo personnel, regardless of their position or role, are responsible for conducting their work in a manner that safeguards the protection of information (internal and external) within Comodo. The Information Security Policy sets out the means of protecting, preserving and managing the confidentiality, integrity and availability of not only information but also all supported business systems, processes and applications.

Comodo's information security policies apply to all Comodo personnel (whether full time or part time, permanent, probationary or contract) who use Comodo information or business systems, irrespective of geographic location or department. Third parties accessing Comodo information or systems are required to adhere to the general principles of this policy, and other security responsibilities and obligations with which they must comply. Comodo's information security policy covers the following control objectives:

- Information Security.
- Physical & Environmental Security.
- Logical Access.
- Change Management.
- Incident Management.
- Application/System Development & Maintenance.
- Human Resource Security.
- Malicious Code Protection & Vulnerability Management.
- Logging & System Monitoring.
- Supplier Relationships.
- Communication Security.
- Asset Management.
- Business Continuity Planning & Disaster Recovery.
- Security Awareness & Training.
- Compliance with Legislative, Regularity & Contractual Requirements.

Supporting documentation is made available to all Comodo employees on the Company Intranet site. Each employee is required to understand the policies and procedures relevant to their job function as part of their ongoing information security training.

Management and the Compliancy Team are responsible for ensuring that the requirements of the policies, procedures, and any supporting documentation, are communicated to Comodo's employees, as well as for monitoring effective implementation of Comodo's information security policy.

Control Activities

Comodo maintains policies, procedures and supporting documentation covering a variety of information security and operational matters, including, but not limited to:

- Policy Management.
- Hiring.
- Physical Security.
- Environmental Safeguards.
- Logical Security.
- Network Security.
- Change Management.
- Incident Management.
- Malicious Code Protection.
- System Backup.
- Business Continuity & Disaster Recovery.

Information and Communication

Comodo is focused on the satisfaction of its partners, customers, employees, and the quality of its service delivery. To ensure these priorities are continually achieved, Comodo has implemented formal policies and procedures that address critical business processes, human resources, and information systems. Comodo's management believes that the internal control contained in these policies and procedures are crucial to the effective operation of business operations.

Comodo's management encourages the use of internal communication methods to ensure employees are aware of significant events in Comodo's operations, such as new Customer deals, product launches, strategic direction of the company, and changes to published policies and procedures.

Monitoring

Comodo pro-actively monitors the quality of both its internal and external service delivery across its business operations. Reports are generated on a daily, weekly, and monthly basis to help guide management in its decisions and operational priorities. The first line of support for any system related alerts and/or alarms is the Infrastructure Team. The Infrastructure Team operates 24/7/365 days a year, with on-call senior members providing second level support. Policies and procedures are in place to ensure that corrective measures and/or improvement opportunities are identified and implemented to improve Comodo's service delivery.

Business critical systems and applications used in the operation of Comodo's services provide both real time and historical data in the form of logs.

The Compliancy Team actively reviews compliance with internal policies and procedures.

Third party service providers to Comodo are approved by Comodo's Management prior to engagement. All third party suppliers to Comodo's business critical processes are required to adhere to Service Level Agreements (SLAs) established between Comodo and the third party supplier.

Risk Assessment

Comodo has adopted a risk assessment process to pro-actively identify, monitor and manage business and operational risks. The risk assessment process focuses on identifying, assessing and mitigating identified risks to Comodo's assets. The Compliancy Team oversees and monitors Comodo's risk assessment activities, including management's actions to address any identified significant risks.

COMPONENTS OF THE SYSTEM PROVIDING THE DEFINED SERVICE

Infrastructure

Comodo's production infrastructure supporting Comodo Digital Certificate Solutions, CCM and Comodo TF is comprised of Linux & Windows operating systems, Oracle and PostgreSQL databases, internally developed applications and Juniper networking equipment.

This infrastructure consists of multiple redundant components, such as power supplies, Redundant Array of Independent Disks systems, server systems, networking equipment, communication circuits, points of presence, and load balancing, that maximizes availability. Comodo operates in two (2) core data center sites, which are located in Secaucus, New Jersey USA and Manchester, England and three (3) edge data center sites, which are located in Seattle, Washington, USA, New York, New York, USA (through October 2016) and London, England (through May 2016). Comodo TF operates from a data center managed in Milford, Connecticut, USA. All Comodo's offices and data center locations are networked using VPN technology, providing secure communication channels between all locations.

Software

Comodo uses a combination of industry standard and proprietary software (i.e., applications) to support the Comodo Digital Certificate Solutions, CCM and Comodo TF systems. Software includes the following:

- Linux based systems: Gentoo, Red Hat Enterprise Linux, CentOS, & Debian;
- Windows Domain Servers.
- Oracle and PostgreSQL databases.
- Internally developed applications for the management & issuance of digital certificates.
- Juniper networking equipment.
- PKI management offerings from leading industry providers (nCipher and Utimaco), which are compliant with FIPS 140-1/2 levels 3/4 security standards.
- Environment management utilities.

Access to and use of this software and utilities are restricted to appropriate Comodo Personnel.

People

Back office processing for Comodo's Digital Certificate Solutions, CCM and Comodo TF systems, business development and management functions, operate from Comodo's worldwide office locations. All personnel are recruited as per Comodo's global HR procedure.

Procedures

Comodo has documented policies, procedures, and supporting documents that support the operations and controls over its systems in support of the Digital Certificate Solutions, CCM and Comodo TF systems. Comodo further publishes these policies and procedures through the use of an internal repository, making them available to Comodo employees.

Data

Customer data supplied to Comodo in support of their account or certificate order(s) is treated as confidential with access to data throughout its lifecycle appropriately restricted. Data received is stored electronically by the applicable system/application in the corresponding database. Comodo applies a default deny policy to all information it holds with access limited to a 'need to know' basis following controlled processes for granting, removing, and renewing access.

Information

Comodo regards its information as a highly valuable asset, with our information and information processing systems being critical to our business operation. Information may exist in a variety of forms, for example, electronic data & paper documents, that carries with it important and, at times, critical details regarding the day-to-day and strategic activities of Comodo's businesses, including those of our customers and trading partners. The loss, corruption, or theft of information and supporting business systems could have a serious impact on the integrity of the company's business activities and brand reputation. Hence, Comodo applies a default deny policy to all information it holds with access limit to a 'need to know' basis.