COMODO
Certification Authority

SERVICE ORGANIZATION CONTROL 3 REPORT

Comodo CA Digital Certificate Solutions and
Comodo CA Certificate Manager (CCM) Services

For the period April 1, 2017 through March 31, 2018

Table of Contents

1. Independent Service Auditor's Report

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

Tel: +1 (212) 773-3000
ey.com

Building a better working world

Report of Independent Accountants

To the Management of Comodo CA Limited ("Comodo CA"):

We have examined management's assertion that Comodo CA, during the period April 1, 2017 through March 31, 2018, maintained effective controls over its Digital Certificate Solutions and Comodo CA Certificate Manager (CCM) services ("System") to provide reasonable assurance that:

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

during the period April 1, 2017 through March 31, 2018 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 CA'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 CA'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 CA's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

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.

In our opinion, Comodo CA 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

September 12, 2018
New York, New York

2. Assertion of Comodo CA

Management's Assertion Regarding the Effectiveness of Its Controls over Comodo CA's System Based on the Trust Services Principles and Criteria, for Security and Availability

September 12, 2018

We, as management of, Comodo CA Ltd ("Comodo CA") are responsible for designing, implementing and maintaining effective controls over the Digital Certificate Solutions and Comodo CA Certificate Manager (CCM) 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

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.

We have performed an evaluation of the effectiveness of the controls over the system throughout the period April 1, 2017 through March 31, 2018, 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, 2017 through March 31, 2018 to provide reasonable assurance that:

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

based on the Control Criteria.

Our attached description of the boundaries of the Digital Certificate Solutions and Comodo CCM services identifies the aspects of the Digital Certificate Solutions and CCM services covered by our assertion.

Very truly yours,

J. Robin Alden
Chief Technical Officer - SSL
Comodo CA Limited

3. Description of Comodo CA Digital Certificate Solutions and CCM relevant to Security and Availability for the period April 1, 2017 through March 31, 2018

Description of Comodo CA's System

3.1 Overview of Comodo CA and Services

Comodo CA Ltd. is a Certification Authority (CA) based in the United Kingdom that provides global digital certificate services with the support of its corporate subsidiaries, (collectively referred to as "Comodo CA"), based in the United States of America, India & Canada.

Comodo CA provides digital identity solutions for businesses of all sizes – protecting their employees, customers, intellectual property and overall brand – from damages caused by fraudsters impersonating people and devices. As a commercial certificate authority with over 100M TLS/SSL certificates issued worldwide, Comodo CA has the experience and performance to meet the growing need to secure transactions and create online trust.

Francisco Partners acquired a majority stake in Comodo CA Ltd. in October 2017. The acquisition by Francisco Partners led to strategic expansion of leadership resources through the addition of industry veterans and leaders, adding to the growing list of accomplishments from Comodo CA over the last year.

Comodo CA's team addresses the digital security challenges for individuals, e-merchants, small to medium businesses, and large enterprises. Comodo CA'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 lifecycle 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.

Comodo CA offers a variety of products from digital certificates to certificate management platforms that help create the trust needed to successfully secure transactions and create online trust.

Description of Comodo CA's System

Description of Comodo CA's System

Comodo CA Digital Certificates

Comodo CA'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 CA's solution includes standards of confidentiality, system reliability and pertinent business practices and provides customers with:

- SSL (Secure Socket Layer) encryption using SHA-256 and 2048-bit RSA keys as standard.
- Certificates available with Elliptic Curve Cryptography (ECC) Support.
- Securely hosted across multiple co location data centers providing high availability & disaster recover features using Hardware Security Modules (HSM)s.
- Custom configuration of PKI management tools. Comodo CA'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 CA Certificate Manager

Comodo CA 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.
- Securely hosted across multiple co location data centers providing high availability & disaster recover features.
- 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 CA's extensive portfolio of SSL, S/MIME and Client Authentication certificates.
- Customer key escrow that enables a protected recovery of user encrypted data.

Comodo CA IoT Manager

Comodo CA's IoT Manager provides mutual-authentication solutions for IoT devices and networks. Using X.509 PKI certificates and custom hybrid TLS/SSL certificates, Comodo CA's batch-issuance system allows for administrators to easily enroll, download and decrypt certificate batches quickly and efficiently.

- Implementation of cloud-based PKI:
  - Creation of certificate profile(s)
  - Drafting of certificate policy
  - Drafting of certificate practices statements
  - HSM provisioning and management.
- CA Signing & Hosting Services:
  - Root CA signing
  - Subordinate CA signing
  - Hosted across multiple co location data centers providing high availability & disaster recover features using HSMs
  - Batch issuance & on-demand issuance
  - System issuance capability targeted at 250M certificates per day.
- PKI Management:
  - Cloud-based admin portal
  - Certificate definition policies (X.509, RSA/ECC)
  - Lifecycle management policies (Renewal, Revocation)
  - Representational State Transfer (REST) based API for programmatic interaction.

3.2 Scope of the Description

The scope of this Description has been prepared to provide information on specified processes and controls of Comodo CA, which may be relevant in assessing the internal control of customer institutions or user entities as they relate to an audit of security and/or availability. The Scope of this Description includes the production systems of Comodo CA's Digital Certificate Solutions and CCM products (the "System") that are hosted within the following locations/data centers:

- Digital Certificate Solutions and CCM –
  - Secaucus, New Jersey, USA and
  - Manchester, England, UK

3.3 Description of the Entity Level Controls

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

1. **Control Environment** – sets the tone of Comodo CA, 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 CA are aware of significant events in Comodo CA'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 CA'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 CA's control environment reflects the overall attitude, awareness, commitment and actions of Comodo CA management and other stakeholders concerning the importance of controls, as well as the emphasis given to controls within the organization. Comodo CA'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 CA.

Relevant elements of Comodo CA's control environment that affect Comodo CA'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 CA's organizational structure provides a framework for planning, directing, & controlling business operations. Comodo CA'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 CA'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 CA, supporting the Compliancy and Infrastructure teams that develop, monitor and manage Comodo CA's overall control objectives and control activities, and the communicating and monitoring Comodo CA's internal control policies and procedures.

The Compliancy team (inclusive of the 'Policy Authority') is responsible for the effective development and implementation of Comodo CA's Information Security Policy & supporting documentation. The team communicates the Information Security Policy to Comodo CA's employee's, and monitors the effectiveness of Comodo CA'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 CA 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 candidates must undergo background checks, in line with local employment law and practices. These checks may include, but not limited to:

- Previous Employment Details.
- Education.
- Place of residence.
- References.
- Identity (Government Authorized/Attested Identification – Passport, Driving License, etc.).
- Criminal Record.
- Passport.
- Driving License.

In addition to the above, all persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity.

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 CA's internal policies. It is required that all personnel understand their role within Comodo CA and that they are suitable for the role assigned.

Line managers/senior management are responsible in ensuring personnel under their supervision apply all necessary security requirements in accordance with established policies and procedures.

Comodo CA employees are required to acknowledge Comodo CA's acceptable use policy as part of joining formalities and at regular intervals as deemed necessary, such as incidents or changes in organizational or technical infrastructure.

Terminations of employment follow Comodo CA'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 CA 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 CA. All employees are advised of their responsibility for adhering to the Information Security Policy. 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 CA regards its information (internal and external) as a highly valuable asset. The principles of information protection and risk management apply to all of Comodo CA's information assets. These principles protect assets, networks, and other facilities supporting business systems and operations from threats - whether internal, external, deliberate or accidental.

Description of Comodo CA's System

Comodo CA's information security policies apply to all Comodo CA personnel (whether full time or part time, permanent, and probationary or contract) who use Comodo CA information or business systems, irrespective of geographic location or department. Third parties accessing Comodo CA 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 CA'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 CA 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 CA's employees, as well as for monitoring effective implementation of Comodo CA's information security policy.

Control Activities
Comodo CA maintains policies, procedures and supporting documentation covering a variety of information security and operational matters, including, but not limited to, hiring, physical security, environmental safeguards, logical security, network security, change management, incident management, malicious code protection, system backups, business continuity & disaster recovery.

Refer to the Overview of Comodo CA's Control Activities below for additional information.

Information and Communication
Comodo CA 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 CA has implemented formal policies and procedures that address critical business processes, human resources, and information systems. Comodo CA's management believes that the internal control contained in these policies and procedures are crucial to the effective operation of business operations.

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

Comodo CA has implemented both web based and telephone based systems for Customers to communicate any issues, questions, concerns, or to receive support for services, products and applications.

Monitoring

Comodo CA 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 CA's service delivery.

Business critical systems and applications used in the operation of Comodo CA's services provide both real time and historical data in the form of logs. The level of monitoring is based on the business value of the system/application (asset) and the level of risk associated with that asset. Monitoring provides an invaluable asset to finding improvement opportunities, investigating into the causes of disasters and capacity management.

The Compliancy Team actively reviews compliance with internal policies and procedures. Any Comodo CA employee who violates the 'Information Security Policy', or who knowingly or negligently allows those under their supervision to do so, may be liable to disciplinary action up to and including termination of employment. Each employee is equally responsible for reporting security incidents or security violations that they may come across within the organization. Security incidents/violations can be reported through email, formal memos or over the phone to the Compliancy Team or Senior Management.

Third party service providers to Comodo CA are approved by Comodo CA's Management prior to engagement. All third party suppliers to Comodo CA's business critical processes are required to adhere to Service Level Agreements (SLAs) established between Comodo CA and the third party supplier. The requirements outlined in the SLA are reviewed and monitored on a regular basis to ensure that contractual obligations are being adhered to.

Risk Assessment

Comodo CA 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 CA's assets. The Compliancy Team oversees and monitors Comodo CA's risk assessment activities, including management's actions to address any identified significant risks. The risk management process consists of the following activities:

- Risk Assessment
- Asset Register, Business Impact Assessment
- Threat & Vulnerability Assessment
- Likelihood Assessment

- Risk Measure
- Risk Treatment
- Risk Measure Review
- Risk Treatment Decision
- Control Selection & Implementation and Residual Risk

3.4 Components of the System Providing the Defined Service

Infrastructure
Comodo CA's production infrastructure supporting Comodo CA Digital Certificate Solutions and CCM 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 CA operates in two (2) core data center sites, which are located in, Secaucus, New Jersey USA and Manchester, England. All Comodo CA's offices and data center locations are networked using VPN technology, providing secure communication channels between all locations.

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

- Linux based systems: Gentoo, Red Hat Enterprise Linux, CentOS, & Debian;
- Junos network operating system;
- Windows Domain servers;
- Databases: Oracle and PostgreSQL;
- Internally developed applications for the management & issuance of digital certificates:
    - The order management of certificates: Order Management System (OMS),
    - The validation of certificates: Advanced Validation System (AVS);
    - 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 such as:
    - Backup: SSH, rsync/rdiff-backup, pg_dump;
    - Patch management: Portage, Windows update, APT, up2date;
    - Anti-virus: Industry recognized Anti Malware programs, for example, Comodo Antivirus, Windows Defender, Kaspersky, ClamAV, rkhunter';
    - Database management tools: PSQL, Toad, SSMS, Oracle Enterprise Manager.

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

People
Back office processing for Comodo CA's Digital Certificate Solutions and CCM systems, business development and management functions**,** operate from Comodo CA's worldwide office locations.

All personnel are recruited as per Comodo CA's global HR procedure as described below. Refer to the organizational structure described above for further information regarding the people supporting Comodo CA's production systems.

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

Data
Customer data supplied to Comodo CA 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 CA 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. Proper encryption is utilized to protect data in transit and when stored on backup media.

Information
Comodo CA regards its information as a highly valuable asset, with information and information processing systems being critical to 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 CA's businesses, including those of 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 CA applies a default deny policy to all information it holds with access limit to a 'need to know' basis.

3.5 Overview of Comodo CA's Control Activities

Policy Management
Comodo CA has developed and implemented a formal security architecture based on industry standard security practices. Comodo CA's security architecture is supported by formal policies & procedures and backed by senior management's commitment to information security. Policies contain the requirements on the confidentiality, integrity and availability of Comodo CA's information and information processing facilities. Policies, procedures and supporting documentation are updated regularly by their document owners based on business and technological challenges posed with approval from members of the Comodo CA management team.

Comodo CA's policies are made available to all Comodo CA employees on the Company Intranet site and targeted email campaigns. Each employee is required to understand the policies and procedures relevant to their job function as part of their ongoing training.

Vendor (Third-Party) On-boarding & Risk Management Program
Comodo CA maintains a Third Party vetting program for all new and existing vendors. Vendors are required to sign contractual agreements which outline the vendor's security and availability commitments and responsibilities.

At point of vendor creation (after vendor acceptance), each vendor is categorized by vendor risk profile and classified into Critical, High, Medium or Low risk categories. All third parties are monitored on an ongoing basis as part of the quarterly internal audit process.

Physical Security and Environmental Safeguards
Access to the Comodo CA data centers (located in Secaucus, New Jersey USA, Seattle, Washington USA, and Manchester, England UK), as well as business offices (located in Bradford & Manchester UK, Roseland, New Jersey & Murray, Utah USA, Ottawa Canada, and Chennai, India) is protected through physical security barriers that require a variation of biometric, key/key fob and key card access for entry. In addition to these access control mechanisms, video cameras have been deployed in strategic locations inside and outside each of the data centers and security guards are present at the main building entrances for further protection.

All Comodo CA equipment located at the data centers are housed in secure lockable cabinets or/and cages and kept locked when unattended. Access to these cabinets is only available to authorized Comodo CA personnel under dual custody access, or authorized data center staff that provide support. All IT equipment used to store and process information with a 'Highly Confidential' classification is located in a further secured area. Access to this secure area requires at least two authorized Comodo CA personnel for entry.

Access to the Comodo CA data centers is restricted to authorized employees and other approved individuals (e.g., visitors) who require this level of access to perform their job responsibilities. Requests for access to the data centers require completion of a 'Data Center Access Request form' and approval from the Director of IT or Senior Management. Visitors gaining access to the data centers are also required to be escorted by at least one Comodo CA employee at all times.

When an employee leaves Comodo CA, the Director of IT, or delegate, will advise the data center operators to revoke the employee's access within 24 hours. In the event of an employee being suspended, the employee's data center access will be disabled within 24 hours and remain disabled until the outcome of any investigations is complete.

The location of buildings selected for Comodo CA's data centers are reviewed (prior to occupation by Comodo CA) for suitability and general security of the surrounding area.

The data centers that house the production environment (including supporting infrastructure) are equipped with the following environmental safeguard: Fire detection and suppression devices, air conditioning system for temperature and humidity control, Uninterruptible Power Supply (UPS) devices and backup generators to provide additional time to resolve power outages.

Logical Security
User access requests to the production environment (including network, operating systems, applications and databases) are formally submitted through the use of a 'Systems Access Request Form' and approved by the appropriate line manager/senior management prior to access being granted. Users are granted privileges on systems according to their assigned roles and duties based on a "need to know" basis.

The Systems Administration Team or Application Owner creates or modifies accounts only upon receipt of a fully authorized 'Systems Access Request Form'. When new users are created, the System Administrator ensures that User IDs are unique.

When an employee leaves Comodo CA, the Systems Administration Team; disables all assigned accounts (across all systems), changes the user's passwords, and revokes the user's keys/certificates, as required within 24 hours. In the event of an employee being suspended, all user accounts will be disabled within 24 hours and remain disabled until the outcome of any investigations is complete.

Privileged access to the production environment (including network, operating system, applications and database layers) is limited to authorized administrators based on current roles and responsibilities. The process for granting and removing privileged access follows Comodo CA's user administration process and requires approval from the administrator's manager.

Password configuration rules have been implemented across all layers of technology (where technology permits) based on Comodo CA's logical access policies. These configuration rules include forced password change upon initial log-on, maximum password age, minimum password length, history, account lockout duration and threshold, masked passwords, complexity, and workstation screen saver passwords. Additionally, Comodo CA displays a general notice warning that computers should only be accessed by authorized users and logging of successful and unsuccessful log-on attempts are recorded and maintained for a minimum of 30 days.

In order to confirm Comodo CA's systems are being used by authorized employees and access restrictions are appropriately assigned, reviews of user access are carried out by the Compliancy Team on a quarterly basis across all layers of technology and is documented within the Audit Check List. As part of this review, the Compliancy Team compares active user listings against terminated employee reports provided by HR to confirm accounts have been properly suspended or deleted along with checking that third party user accounts are still required with the respective Comodo CA Manager or Senior Management. Additionally, for a sample of active accounts, further review is performed by validating the proper Access Request form is present for the account and access agrees to what was requested and required for the individual's job responsibilities.

Network Security

Access to Comodo CA's network and the related network devices (e.g., routers, switches, etc.) is restricted to employees whose job responsibilities require them to have such access. User access requests to the network and related assets are formally submitted and approved by a Comodo CA manager prior to access being granted. This follows Comodo CA's formalized user account administration process described above and is protected by adequate username and password restrictions.

Remote access to the Comodo CA network is protected and secured through encrypted VPN tunnels from Comodo CA's locations. HTTPS authentication to the network requires a variation of valid User IDs, passwords, certificates, and/or USB token/smart cards. Encrypted VPN access is available to users on a "needs" basis and is protected by USB token certificates generated for that purpose.

Firewall devices are installed within Comodo CA's network to filter and segregate internal and external network traffic. Comodo CA's network is segregated based on the information services they support. For example:

- Networks used to process sensitive information are segregated from those that host web based services.
- Senior developers may be given specific access to production systems for support related activities.
- Non-Administrator Office Desktop systems are segregated from production systems.
- Production services are not provided from Office locations.
- Production systems are located at dedicated Data Centers and segregated from office networks via authentication and fire-walling.
- Firewalls are used to isolate/segregate production systems from the Internet as well as the office systems. They also segregate/isolate office systems from the Internet.
- All network traffic is denied/dropped unless it is required and authorized for business use.

Windows desktops have Anti-Virus products installed that are monitored by the Infrastructure Team for virus attacks. Desktops with Linux-based operating systems have various methods of mitigating virus/malware threats, such as root kit detection software, hardened tool chains and hardened kernels. In addition, email servers have Anti-Virus software installed to prevent infection from email. These signature files are updated on a regular basis (every 2 hours). Emails are scanned as mail passes through the mail servers, i.e., scanning is applied during ingress and egress processes. All desktops are located behind firewalls that block ports that are known vectors of attack. Servers having Linux based operating systems also have methods for mitigating virus/malware threats that include, but are not limited to, installation of root kit detection software, hardened tool chains, and hardened kernels.

Change Management
Changes to the production environment within Comodo CA originate from a variety of sources, including information owners, system owners, project/Infrastructure teams, and Customers and are categorized into one of the following:

- Implementation of a New System or Business Process – A new release of an information system or the implementation of a new business process that provides new or/and enhanced functionality (project driven).
- Problem with an IT System/Business Process or a Security Incident – Fixing a user identified system defect that is impacting service delivery, or patching a system to address a newly identified security vulnerability (incident driven).
- Preventative Maintenance – Applying routine system patches and standard upgrades.

Change requests are documented using a 'Change Request Form' that contains all required details of the change and is utilized from initial request to final production deployment. Changes are classified as Normal, Pre-Approved or Emergency. The majority of changes fall into the Normal classification. The Emergency classification is only used for an incident driven problem to fix a critical issue in a critical business system. Pre-approved changes consist of standardized, low risk, or routine related changes such as server patches and routine server restarts.

Change requests are submitted to the Asset Owner/Delegate, who assess the request by capturing the necessary requirements and the possible impact on Comodo CA's business/systems. Asset Owner/Project Managers are then responsible for reviewing and authorizing change requests and assigning a developer.

Once the development of the change is complete, testing is performed dependent on the nature of the change to confirm the changes align with the request and the change does not have a negative impact on the overall security within the systems. Testing may be performed against data within the development environment, System Administrators and, in some cases business users, may be asked to perform user acceptance testing within the test environment. If testing is successful, the responsible tester provides a sign-off that testing is complete and changes are ready to be migrated to production. If testing is un-successful, the change is re-developed until corrected.

Change requests ready for production migration undergo pre-deployment verification and a risk assessment to determine the impact of the change on the production environment which is completed by the Asset Owner/Project Manager. The risk assessment decision will be made based on the category to which the change is classified. All changes must have fully documented development, pre-deployment testing, and defined regression plans before being deployed to the production environment. Once completed, changes are then approved by the Asset Owner/Management for migration to production.

Approved change requests are then scheduled for deployment to the production environment by a segregated group of individuals from the development team and based on their business requirements and impact by the Asset Owner and/or Project Manager. Where possible, changes affecting Customer facing applications and systems are scheduled at times of low demand.

Post deployment testing is performed to determine if the change was successful and meets expectations. Should any of the tests fail, the change may either remain in place with further rework or undergo the regression plan to be rolled back.

Responsibilities of personnel within Comodo CA are organized so that it is not possible for one person to develop, test, authorize and migrate a change to the production environment, infrastructure or data. Personnel in systems development may not authorize code changes to the production environment or sign-off testing.

Incident Management

Comodo CA defines an incident as any breach of information security; that is, any event that compromises the integrity, confidentiality and availability of the information stored in Comodo CA's systems. Non-compliance to Comodo CA's policies, procedures and legal requirements is also treated as an incident.

Incidents can be identified through a manual notification or through automated alerts. Monitoring over Comodo CA's production systems (e.g., operating systems, applications, database and networks) is the responsibility of the Infrastructure Team who utilizes various tools such as Cacti Xymon, and/or Big Brother for internal monitoring. External monitoring is also performed through independent third parties such as PeriscopeIT and Securityspace.com. Notifications and alerts are automatically presented to the Infrastructure Team through the use of web pages, graphical interfaces, emails, and SMS alerts and then escalated to core System Administrators and applicable members of Senior Management, as necessary.

All incidents, or suspected incidents, are also reported to the appropriate asset owner, or Comodo CA's Management team for investigation. As an incident could come from any area of the company, third party, or even from an automated system, an initial assessment of the incident is performed to determine the validity of the request.

Incidents are then escalated to an Incident Handler/Investigator who is responsible for conducting a detailed investigation of the incident through resolution. The investigation encompasses a detailed study of all events relating to the incident, from initial warnings received, personnel on call to systems/applications/processes affected. Details of incidents are then documented within an 'Incident Management and Handling Report' which contains the following relevant information:

- Incident Details - incident date & time, incident handler/investigators name, asset owner/delegate.
- Executive Summary of the Incident - how the incident was detected and raised along with step by step details of what was performed in the initial investigation.
- Summary of Key Events - summary of the key events that occurred during the investigation and resolution of the incident.
- Impact of Incident on Business Operations - details of the impact of the incident on business operations.
- Root Cause Analysis - details of the root cause of the incident and how this effected business operations.

Once all relevant information has been gathered, it is the duty of the Incident Handler/Investigator and the relevant asset owner to produce a detailed post-incident review. This includes details of any solutions and/or preventative measures required to avoid any further incidents of this nature along with any changes to Comodo CA's business processes as required.

Where an incident involves a breach of any Comodo CA policy, whether it has directly or indirectly led to any actual compromised data or not, the review contains details of such breaches and any recommendations for educational or disciplinary measures.

In cases where data loss, or probable data loss, may directly impact Customers and/or partners, a suitable report is generated and distributed. This explains the source, & scale, of any data loss, any risks to data security, and, where suitable, a suggestion of steps to perform to limit potential damage. This may include advice to reset passwords, or cancel credit/debit cards etc.

In order to ensure that incidents are being recorded as per the procedure and that investigation and resolution are completed in a reasonable time, reviews of incident reports are carried out by the Compliancy Team on a quarterly basis. The review takes a sample of reports and analyzes them for completeness. Any findings are raised to the incident handler, asset owner and/or senior management.

System Backups
Servers within the production system are backed-up according to a predefined schedule. The schedule performs a daily local backup of all running servers (physical and virtual) that is stored, via an encrypted network connection, on a server located in the local data center. On a weekly basis the local backup servers execute rsync that pushes the backups from the local backup server to an encrypted file system on a backup server located at the Bradford data center using Secure Shell (SSH) over an encrypted network connection (VPN/GRE). The encrypted file system at the Bradford location employs Linux Unified Key Setup-on-disk-format (LUKS) specification.

In addition to local & off-site backups, the servers themselves form high availability pairs. That is, complete duplicates of servers that become active if its partner suffers failure. Though not conventional backup in the classical sense, it represents another copy of a given host that can be used to restore any failed hosts. High availability is configured through DRBD (Distributed Replicated Block Device) and Heartbeat.

Database backups are continuously replayed to the standby server at the live site and also to servers at the standby sites after allowing a time delay for corruption prevention. Off-site backups are also pushed to the backup server located at the Bradford data center.

System/Database Administrators at each Comodo CA data center location are responsible for carrying out and maintaining scheduled backup activities. Scheduled backups are automated using approved backup tools and transferred using secure methods. Comodo CA utilizes a number of different types of backup media, including compact discs, digital versatile disks and hard disk drives, to best suit the backup application.

Unscheduled backups of pertinent data occur before carrying out major changes to business critical systems. Unscheduled backup activities are coordinated between information owners and the System Administrators.

The scheduled backup process of business critical systems and applications is monitored using automated tools. In the event of a backup failing, an alert is emailed to the Infrastructure Team or the Database Administrator. These alerts are then investigated and resolved as a matter of high priority. Only System Administrators have the ability to make changes to the back-up scheduling tool.

Business Continuity & Disaster Recovery
Comodo CA has robust, regularly tested Business Continuity and Disaster Recovery Plans, to help ensure the timely resumption of business activities and critical business processes from the effects of major failures of information systems or disasters.

Comodo CA accepts that business continuity is very much dependent on the design of the processes and systems running business critical applications and services. As a result, Comodo CA operates a 'Preventative Policy' for business continuity in that all primary business critical processes, systems, applications and operations are designed in such a way as to prevent predictable, and minimize the impact of unpredictable events. Access to said systems and applications is also governed by the principle that all access is denied unless explicitly authorized by management.

Description of Comodo CA's System

Comodo CA attempts to reduce the risk of a major event compromising business operations by defining four levels of redundancy as detailed below:

Device Level
Critical hardware resources required for machines are configured in 'fault tolerant mode'. Single point of failure is averted. For example, Dual PSU, Multiple hard disk drives in a RAID configuration, multiple network interfaces in bridged mode.

Machine Level
Machines providing Critical services at the data center sites are replicated and configured as master and slave, thereby providing fail-over in case a machine providing a service becomes inoperable.

City Level
Critical services are replicated across multiple core data center sites or across multiple edge data center sites, both core and edge sites are available in geographically separate locations but in the same country. If one of the core/edge sites becomes unreachable due to a natural or man-made disaster, business can be continued from the alternate core/edge sites.

Country Level
At least one of the core /edge sites is geographically located in another country. If there were to be a country-wide disaster affecting all of the core/edge sites in one country, business can be continued from the other core/edge sites located in another country.

All primary public facing systems and applications have built in redundancy in all areas of system design. The minimum hardware redundancy standard is as follows:

- Redundant Power supplies to a minimum level of N+1.
- Redundant Network Connections.
- Hard Drive Redundancy (RAID).
- Infrastructure Redundancy to a level of N+1.

The offices in which Comodo CA operates its business are critical to business operations for back office processing, product & business development and business management. To guard against the loss of office operations, whether this is caused by power failure, natural disaster, fire, theft etc., Comodo CA operates offices based across multiple sites and geographical locations. All office locations operated by Comodo CA are 'fit for purpose' and comply with Comodo CA's requirements for physical security.

The back office processing activity may be carried out from anywhere with Internet connectivity, since the interface is a publicly available web interface. The security of this interface is ensured by having it only available over SSL, and requiring identification by means of an SSL Client certificate and authentication by means of username and password.

Description of Comodo CA's System

In the normal course of events, "back office processing" is carried out from Comodo CA's Manchester, Chennai and Clifton offices. It is conceivable that any of those offices could lose Internet connectivity or mains power, rendering the normal back office processing facility from that location inoperative. In the event of a loss of an office location, local management personnel will inform Comodo CA's Operations Managers (or delegates) of the event along with all relevant details, e.g. cause, estimated time for resumption, systems and operations effected etc. From these details the Operations manager, in discussion with relevant management personnel, shall decide upon, and implement a recovery operation.