ExpressVPN ISAE (UK) 3000 Type I Independent Assurance Report on Internal Controls

Controls system applicable to TrustedServer services undertaken by ExpressVPN

As of 12 December 2023

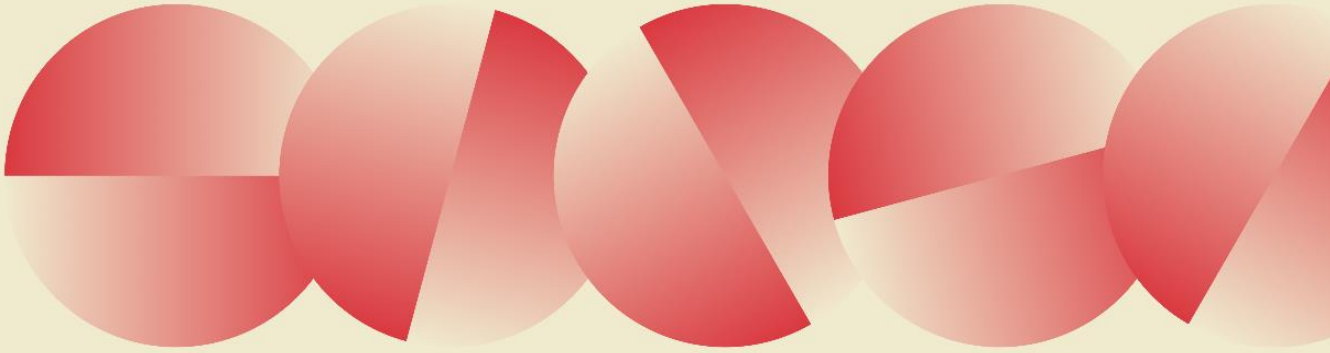


Table of Contents

KPMG LLP
1 Sovereign Square
Sovereign Street
Leeds LS1 4DA
United Kingdom

Tel +44 (0) 113 231 3000

1. Independent service auditor's reasonable assurance report on internal controls

Private & confidential
The Directors
Express Technologies Limited
Mill Mall Suite 6
Wickhams Cay 1
Road Town
Tortola
British Virgin Islands

3 April 2024

Dear Directors

ISAE (UK) 3000 Type I Independent Reasonable Assurance Report on Internal Controls

In accordance with our engagement letter dated 15 November 2023 and our subsequent variation letter dated 10 January 2024 (together, our "Engagement Letter"), we have examined the accompanying description at pages 6 to 33 of the controls in place at the company called Express Technologies Limited ("ExpressVPN") and carried out procedures to enable us to form an independent opinion on whether ExpressVPN's management has fairly described its controls system applicable to the TrustedServer services provided to ExpressVPN's customers as at 12 December 2023 (the "Description"), and on the suitability of the design of controls to achieve the related control objectives stated in the Description. Our opinion is set out below and should be read and considered in conjunction with this report in full.

ExpressVPN's Management's Responsibilities

In this report, references to ExpressVPN's "management" means the directors of ExpressVPN and those employees to whom the directors of ExpressVPN have properly delegated day-to-day conduct over matters for which the directors of ExpressVPN retain ultimate responsibility.

Management of ExpressVPN is responsible for (1) preparing its statement at page 5 and describing in the Description its controls system applicable to the TrustedServer services provided to ExpressVPN's customers, including the completeness, accuracy and method of presentation of the same, (2) having a reasonable basis for its statement, (3) providing the services covered by the Description, (4) selecting the criteria to be used and stating them in the statement, (5) specifying the control objectives and stating them in the Description, and (6) identifying the risks that threaten the achievement of the control objectives and designing, implementing, and documenting controls that are suitably designed and operating effectively to provide reasonable assurance that the control objectives stated in the Description will be achieved.

Our Responsibilities

Our responsibility is to express an independent opinion to ExpressVPN, based on the procedures performed and evidence obtained, as to whether (1) ExpressVPN's management's Description fairly presents the controls system that was designed and implemented as at 12 December 2023 and the aspects of the controls that may be relevant to a customer using ExpressVPN's TrustedServer services, and (2) the controls included in the Description were suitably designed as at 12 December 2023 to provide reasonable assurance that the control objectives specified would be achieved if the described

controls were operating effectively. The criteria we used to form our judgements are the criteria used by management in making the statement, and are set out on page 5.

Framework Applied

We conducted our engagement in accordance with International Standard on Assurance Engagements (UK) 3000 *Assurance Engagements Other than Audits or Reviews of Historical Financial Information,* issued by the Financial Reporting Council. That standard requires that we obtain sufficient, appropriate evidence on which to base our opinion.

Our Independence and Quality Management

We comply with the Institute of Chartered Accountants in England and Wales ("ICAEW") Code of Ethics, which includes independence, and other requirements founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour, that are at least as demanding as the applicable provisions of the IESBA Code of Ethics.

The firm applies International Standard on Quality Management 1 *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Scope of Work

An assurance engagement to report on the description and design of controls at a company involves planning and performing procedures to obtain sufficient appropriate evidence about the presentation of the Description of the controls system applicable to the TrustedServer services provided to ExpressVPN's customers, and suitability of the design of those controls. The procedures selected depend on our judgment, including the assessment of the risks that the Description is not fairly presented, and that controls are not suitably designed to achieve the related control objectives stated in the Description if the controls were operating effectively. An assurance engagement of this type also includes evaluating the overall presentation of the Description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the company.

We did not perform any procedures regarding the operating effectiveness of controls included in the Description and, accordingly, do not express an opinion thereon.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of Controls at a Company

ExpressVPN's management's Description is prepared to meet the common needs of a broad range of customers using ExpressVPN's TrustedServer services and may not, therefore, include every aspect of the system that each individual customer may consider important in their own particular circumstances. Also, because of their nature, controls at the company may not prevent or detect and correct all errors or omissions in the provision of the TrustedServer services provided to ExpressVPN's customers. Such control procedures cannot guarantee protection against (among other things) fraudulent collusion especially on the part of those holding positions of authority or trust. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at the company may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. In our opinion, in all material respects, based on the criteria described in ExpressVPN's statement on page 6:

(a) The Description fairly presents the TrustedServer services system provided to ExpressVPN's customers as designed and implemented as at 12 December 2023; and

(b) The controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively as at 12 December 2023.

Additional Information

The information provided on pages 34 to 35 of this report is presented by ExpressVPN to provide additional information and is not a part of ExpressVPN's management's Description of its controls system in operation. This information has not been subjected to the procedures applied in the examination of the Description of controls applicable to the TrustedServer services provided to ExpressVPN's customers, and accordingly, we express no opinion on it.

About This Report Including Disclosure

This report is made to and has been prepared solely for ExpressVPN on the terms agreed and recorded in our Engagement Letter. This report was designed to meet the agreed requirements of ExpressVPN and particular features of our engagement determined by ExpressVPN's needs at the time. This report is confidential and is released on the basis that it shall not be copied, referred to or disclosed, in whole or in part, save as permitted by our Engagement Letter, without our prior written consent.

We have consented to its disclosure to ExpressVPN's customers via their customer accounts on ExpressVPN's website and prospective customers of ExpressVPN.

By customers we mean clients of ExpressVPN who have signed contracts in place as users of the TrustedServer services, which are the subject of this report. By prospective customers, we mean potential clients of ExpressVPN who are considering becoming users of the TrustedServer services which are the subject of this report and for whom a signed contract is not yet in place.

Our consent has been given without in any way or on any basis affecting our responsibility or giving rise to any duty or liability being accepted or assumed by or imposed on us to any party except ExpressVPN. We have consented to enable ExpressVPN to demonstrate, and such customers to verify, that an independent assurance report has been commissioned by ExpressVPN and issued in connection with the controls of ExpressVPN.

Intended Users and Purpose

This report and description of tests of controls and results on pages 15 to 33 are only to be disclosed to customers who have a sufficient understanding to enable them to consider the matters stated including the basis of our consent to disclosure and their ability to rely on this report. This report is not to be used by anyone other than these specified parties.

This report does not restrict use by customers on the basis that those customers remain responsible for their own decisions and consideration of this report and for evaluating the evidence presented by our report and for determining its effect on their usage of ExpressVPN's TrustedServer services.

Any party other than ExpressVPN who obtains access to this report or a copy and chooses to use and rely on this report (or any part of it) will therefore do so at its own risk. To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than ExpressVPN, for our work, for this report, or for the opinions we have formed.

Yours faithfully

DocuSigned by:
KPMG LLP
9F04C487613C4C6...

KPMG LLP

2. Management Statement

We have prepared the description of ExpressVPN's TrustedServer services provided to ExpressVPN's customers ("Description") as at 12 December 2023. The Description is intended to provide customers, who have a sufficient understanding to consider the Description, with information about the TrustedServer services, particularly system controls intended to achieve the company's service commitments and system requirements relating to its Privacy Policy. We confirm that:

(a) The accompanying Description at pages 6 to 33 fairly presents the controls system applicable to the TrustedServer services provided to ExpressVPN's customers as at 12 December 2023. The criteria used in making this statement were that the accompanying Description:

(i) Presents how the system was designed and implemented, including:

- The types of services provided;
- The components of the controls system ("system") used to provide the services:
  - Software: the programs and operating software of the system (systems, applications, and utilities);
  - People: the personnel involved in the operation and use of the system (developers, operators, users, and managers);
  - Procedures: the automated and manual procedures involved in the operation of the system; and
  - Data: the information used and supported by the system (transaction streams, files, databases, and tables).
- The boundaries or aspects of the system covered by the Description;
- How the system captures and addresses significant events and conditions;
- Relevant control objectives and controls designed to achieve those objectives;
- Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to provision of the TrustedServer services.

(ii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the Description is prepared to meet the common needs of a broad range of customers using ExpressVPN's TrustedServer services and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular circumstances.

(b) The controls related to the control objectives stated in the accompanying Description were suitably designed as at 12 December 2023. The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified; and

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.

DocuSigned by:
Aaron Engel
94AFC1176C9F448...

Aaron Engel

Chief Information Security Officer

3. Management's System Description

The following section describes:

1. ExpressVPN's service offering
2. ExpressVPN's Privacy Policy as it relates to its VPN service
3. ExpressVPN TrustedServer technology
4. How ExpressVPN operates in compliance with its Privacy Policy

3.1. Background

Founded in 2009, ExpressVPN is one of the world's largest providers of VPN services, enabling users to protect their privacy and security online with just a few clicks. The company has since expanded to a suite of privacy and security tools and hardware products, in addition to its core VPN service. Today, ExpressVPN enables millions of users in over 180 countries to access the free and open internet, and to do so privately and securely.

3.2. Overview

ExpressVPN is committed to protecting our customers' privacy. Our privacy policy, which is publicly available, explains what information we collect, what we don't collect, and how we collect, use, and store information. ExpressVPN's guiding principle toward data collection is to collect only the minimal data required to operate a reliable, privacy-focused VPN service at scale.

3.3. Scope of the report

This report provides detailed descriptions of how our system is implemented, and describes a set of verifiable controls that ExpressVPN has developed to uphold our Privacy Policy. These controls cover the full software development lifecycle to verify that code we write, build and deploy maintains its integrity, describes the operational constraints that are in place to help ensure that this remains true throughout TrustedServer's operational lifecycle, and that it is not possible for any logs to be collected for user activity.

3.4. Privacy Policy

Excerpts of the relevant sections from the ExpressVPN Privacy Policy as at 12 December, located on ExpressVPN's website:

> *"We want you to understand what information (including Personal Data) we collect in connection with your use of our Services and/or access to our Site; for what purpose such information is collected; how we collect, use, and store such information; to whom it may be disclosed; and how you can exercise your rights and access your information, verify its accuracy, correct and/or have it erased.*

Equally, we want you to know what information we do not collect under any circumstances.

In addition, this Privacy Policy outlines what security measures we take to safeguard your information and who you can contact if you have any queries or complaints about the contents of this Privacy Policy.

Our guiding principle toward data collection is to collect only the minimal data required to operate world-class Services at scale. We designed our systems (and strive to constantly improve them) to not have sensitive data about our customers. We cannot disclose, misuse, or abuse, even when compelled, data that we do not possess. We do not collect logs of your online activity while you are connected to our Services, including no logging of browsing history, traffic destination, data content, or DNS queries. We also never store connection logs, meaning no logs of your IP address, your outgoing VPN IP address, connection timestamp, or session duration.

Usage Statistics Data and App Diagnostic Data

We ensure that Usage Statistics Data and App Diagnostic Data never include any sensitive information, in line with our overall commitment to never logging browsing history, traffic destination, data content, IP addresses, or DNS queries.

With regard to VPN Usage Statistics, our principle of minimal data collection means that:

- *We do not know which user ever accessed a particular website or service.*
- *We do not know which user was connected to the VPN at a specific time or which VPN server IP addresses they used.*
- *We do not know the set of original IP addresses of any given user's computer.*

Should anyone try to compel ExpressVPN to release user information based on any of the above, ***we cannot supply this information because the data does not exist****.*

Apps and Apps versions

We collect information related to which Apps and Apps version(s) you have activated in order to use our Services. Knowing your current version of the Apps allows our Support Team to troubleshoot technical issues you may encounter.

Successful connection

As you use the App, we collect information about whether you have successfully established a VPN connection on a particular day (but not a specific time of the day), to which VPN location (but not your assigned outgoing IP address), and from which country/ISP (but not your source IP address). This minimal information assists us in providing technical support, such as identifying connection problems,

providing country-specific advice about how to best use our Services, and enabling ExpressVPN engineers to identify and fix network issues.

Aggregate sum of data transferred (in MB)

We collect information regarding the total sum of data transferred by a given user. Although we provide unlimited data transfer, if we notice that a single user pushes more traffic than thousands of others combined, thereby affecting the quality of Services for other ExpressVPN users, we may contact that user for an explanation.

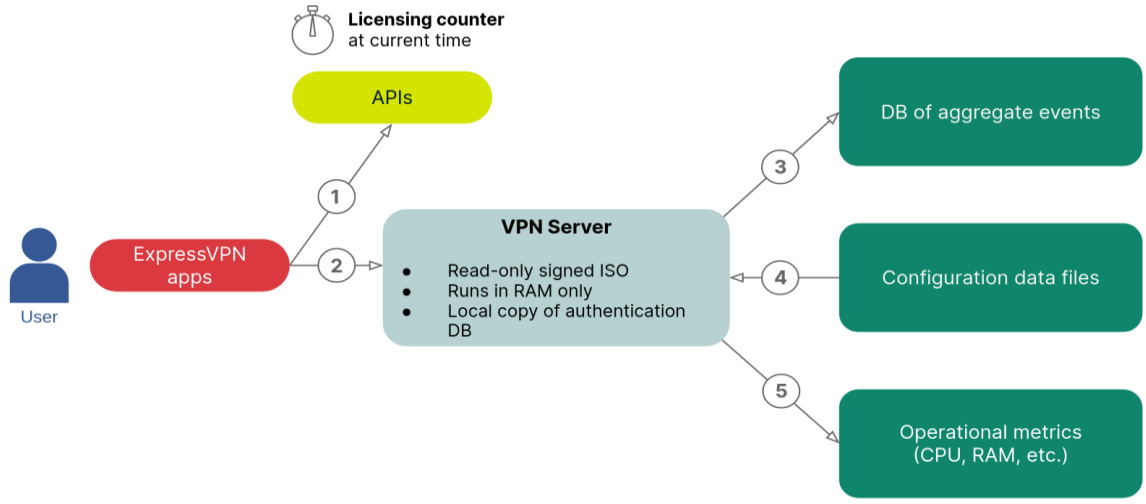
Usage Statistics Data summary

In summary, we collect minimal usage statistics to maintain our quality of service. We may know, for example, that our customer John had connected to our New York VPN location on Tuesday and transferred an aggregate of 823 MB of data across a 24-hour period. John can't be uniquely identified as responsible for any specific online behaviour because his usage pattern overlaps with thousands of other ExpressVPN customers who also connected to the same location on the same day.

We've engineered our systems to categorically eliminate storage of sensitive data. We may know THAT a user has used ExpressVPN, but we are unable to single out the user and we never know HOW they have utilised our Service. We stand by our firm commitment to our users' privacy by not possessing any data related to a user's online activities."

3.5. How ExpressVPN's servers comply with our Privacy Policy

System Overview



System Overview

Notes to explain the diagram above:

1. Only if the user chooses to use the ExpressVPN apps: The apps call Application Programming Interfaces (APIs) operated by ExpressVPN (See “Apps and Apps versions” in the Privacy Policy excerpts). If the user chooses to manually configure the Virtual Private Network (VPN) in their operating system, these API calls do not happen. The types of API calls are:
    a. Authenticate the user, retrieve credentials to connect to the VPN, and discover the set of available VPN infrastructure. This generates an event saved to a database with the Operating System (OS) and app version used.
    b. Check whether the user’s license has reached its limit on the number of simultaneous connections. This system keeps counters of simultaneous connections per license only at the current moment in time. It does not keep historical records. Also, while an app is connected to the VPN, it sends a periodic heartbeat through the VPN to keep the simultaneous-connection counter accurate. Upon disconnect or absence of heartbeats, the counter resets within five minutes.
2. The user connects to VPN servers operated by ExpressVPN (See “Successful connection” in the Privacy Policy excerpts).
    a. Authentication is done with a username and password. Both credentials are generated randomly for each customer at the time of signup, and they are unrelated to the credentials used to login to the ExpressVPN website. Each VPN server has a local copy of the authentication database and authorises the user without making additional network calls.
    b. The VPN servers are designed and configured to prevent logging of anything about what the user does with the VPN. No connection logs, no activity logs (even of Domain Name System (DNS) lookups), or other types of logs that would contradict our Privacy Policy.
3. The VPN server writes exactly one event per connection. The VPN server uses the user’s IP address to make a GeoIP lookup using a locally stored GeoIP database. The event is sent to a database. The event does NOT include the user’s IP address or the outgoing IP address that the server used to route the user’s traffic. The fields in the event are (See “Successful connection” in the Privacy Policy excerpts):
    a. the current date (not time).
    b. a salted and hashed version of the VPN username (which itself is randomly generated, unrelated to the user’s email address or other personally identifiable information) that performed the event.
    c. the Country and Internet Service Provider (ISP) GeoIP attributes of the connection.
    d. the aggregate amount of data transferred in and out through the VPN tunnel, in megabytes, for the now completed session. (See Aggregate sum of data transferred (in MB) in the privacy policy excerpts)

e. an ID representing the VPN location. This does not identify the specific server used, but rather the group of servers corresponding to the location that the user selected.

f. an ID representing the VPN protocol used, such as OpenVPN or Lightway.

4. Immediately on first activation, and then subsequently every 15 minutes, each VPN server downloads the latest configuration data files, including the authentication database and a specification of the server's expected configuration.

5. Each VPN server sends operational infrastructure metrics every minute to:

   a. a cloud-hosted Prometheus database. This data does not contain any personally identifiable information (PII). They are operational metrics such as Central Processing Unit (CPU), Random Access Memory (RAM), network utilisation metrics, and the version-identifier of the TrustedServer image running on this server.

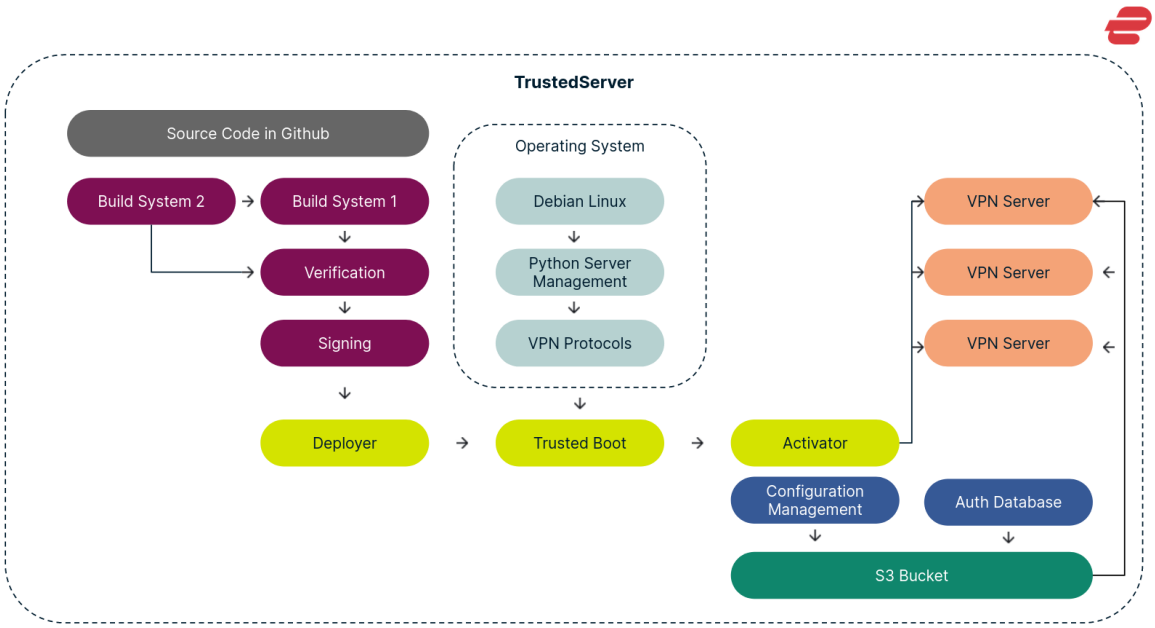
   b. a cloud-hosted Icinga infrastructure-monitoring system. This data does not contain any PII. They are uptime heartbeats commonly used in operating Linux servers.

3.5.1. TrustedServer Architecture

ExpressVPN VPN servers are operated on the "ExpressVPN TrustedServer" RAM-only architecture as described below. This represents all users and traffic, both using the ExpressVPN applications and manual configuration. No other VPN server platform is available in the ExpressVPN service offering.

Our TrustedServer technology is built upon a Linux-based operating system. It utilises a combination of open-source technologies, Ansible playbooks for Deployment, and in-house developed orchestration tooling to manage VPN servers end-to-end service lifecycle in an automated and secure manner.

The architecture broadly consists of the following:

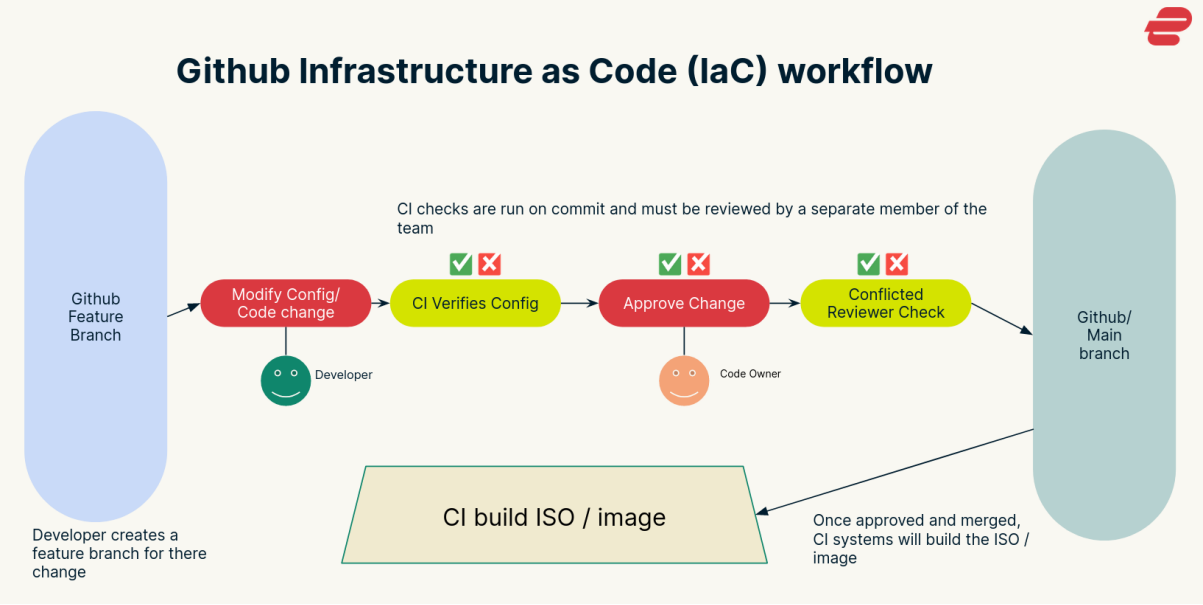


On an ExpressVPN TrustedServer:

1. The entire OS is defined as code in a version-controlled repository. These codebases have automated change management controls in place, which helps to ensure a single developer acting alone cannot modify the source code.
2. The servers run in RAM only. Trusted Boot is our bootloader system that is executed on the server hardware. In turn it loads a read-only ISO image from our CDN that is built from our version-controlled codebase and digitally signed by ExpressVPN. The ISO contains the entire Debian operating system compiled by ExpressVPN as well as all applications in it. A server cannot boot without a valid signature on the ISO, which in turn validates that the content of the ISO is unchanged.
3. Within the booted OS, any files written to system locations are written to an OverlayFS that resides in memory only.
4. With every reboot, the servers reset themselves to their standardised state (specifically, TrustedBoot, where they await verification) based on the read-only ISO image, therefore any data that might have accumulated during operations are lost.
5. The ISO image is generic. No server-specific configuration or secrets are shipped inside the ISO image. A separate “activator” validates the running OS before pushing or generating secrets.
6. No PII, such as users’ IP addresses, are logged on the server, or exported from the server in any form.

3.5.2. TrustedServer Workflows

Code changes



To help ensure that our servers remain compliant with our Privacy Policy, we follow workflows to protect ourselves from accidental or malicious changes. The key points are:

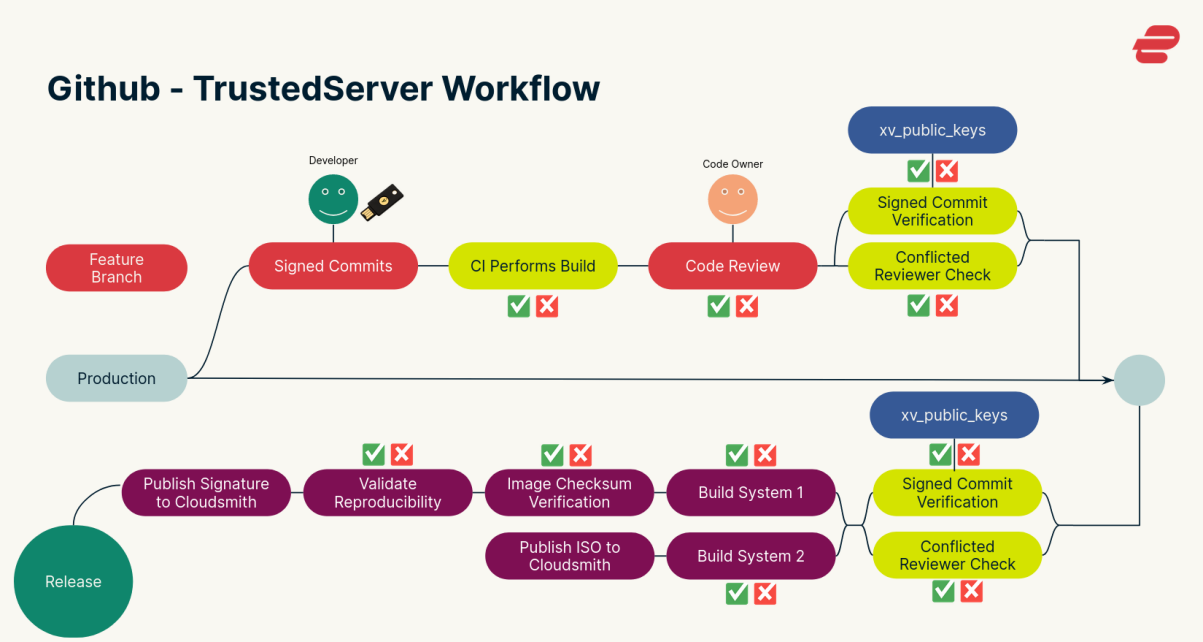
1. Everything running on TrustedServer, starting with the bootloader (TrustedBoot) that boots into the TrustedServer OS, all the way up to the applications we build and run, is defined in source code and stored in git. That source code is compiled into a single ISO that defines all code and runs on TrustedServer.
2. No one can push source-code changes to the production branch directly. Instead, changes are made in a feature branch.
3. Commits are cryptographically signed using hardware-backed signing keys that are securely generated and stored on the device, the public keys to which are validated against a version-controlled source of truth that is maintained by our internal IT team (known as xv_public keys).
4. Automated unit tests include checks that verify that the configuration remains in a no-logging state. Tests automatically fail if code-coverage is below 95%. Failing tests automatically prevent the merging of code into the production branch.
5. Feature branches require review and approval from one or more reviewers, at least one of whom must be a Code Owner, before they can be merged into the production branch.
6. With every change to the production branch, automated tests are run again.

This multi-person code review workflow policy is also defined in code, which is subjected to the same workflow.

Automatic Security Scanning

Third-party dependencies included within the codebase are continually scanned for active security alerts against Common Vulnerabilities and Exposures (CVE) using automatic dependency vulnerability checking tools. The ability to merge code changes from a feature branch is automatically disabled until any active security alerts are resolved.

Reproducible Builds



TrustedServer employs the practice of Reproducible Builds for the OS and application stack that is shipped as an ISO image. We do this by building the OS image from the same source of truth (the source code) on at least two independently operated Build Systems, which both produce the final ISO image. These ISO images are then compared using cryptographic hashes of their contents to help ensure they are bit-for-bit identical.

The images being identical asserts that both build systems took identical source code, dependencies, OS base, software versions, and configuration files and that they have not been modified throughout the build process.

This process protects TrustedServer against build pipeline attacks. Once the TrustedServer OS image is verified reproducible, the ISO image is cryptographically signed for release after comparing checksums from each build system. The image is signed via OpenSSL certificates that are managed by ExpressVPN and verified during deployment. The source of truth for verified signing certificates are maintained in a version-controlled repository, itself having all of the above described protections.

The purpose of cryptographically signing at this stage is to achieve the following:

1. Signed - The image has been verified reproducible.
2. Sealed - The contents of the image have not been changed since signing.

3. Delivered - The image can be shipped to our servers which can digitally verify the image has been delivered unaltered.

The signed TrustedServer image is then published to Cloudsmith, which acts as a backend artifact store. Our VPN server fleet then connects to our CDN frontend servers to request the image, allowing the fleet to perform automatic upgrades. These upgrades are managed by our global orchestration tooling, preventing customer impact during the upgrade cycle. This process repeats every 7 days.

Signature Verification

The signature of the TrustedServer image is validated at multiple stages along the deployment pipeline, using multiple unique and version-controlled sources of truth. This helps ensure that no discrepancies make their way into TrustedServer through its lifecycle.

Activation

Since no server or service-specific secrets are stored inside the TrustedServer ISO, we generate them on-server and/or push them from a secure source once the OS is running. That is performed by the Activator, an external service that is able to validate the security of the running TrustedServer instance before generating and pushing secrets.

Some entropy-related secrets are automatically generated on-server (such as Diffie-Hellman parameters for OpenVPN), and others are pushed to the server (such as per-server VPN keys and authentication credentials for downstream systems) once the system's integrity has been validated.

Upon the completion of activation, where a server enters "production" ready to pass users' traffic, remote access to the server via Secure Shell Protocol (SSH) is disabled by default. Additionally, the Activator revokes its access to the server as the last step. Neither the Activator nor ExpressVPN staff can access the server using SSH after this stage.

4. Control objectives, related controls, and tests of design and implementation

4.1. Test of the control environment

The control environment represents the collective effect of various elements in establishing, enhancing, or mitigating the effectiveness of specific controls. Tests of the control environment included the following procedures, to the extent we considered necessary:

1) Reviews of ExpressVPN organisational structure, including policy statements, policies, and the segregation of functional responsibilities within each team to carry out assigned activities;
2) Discussions with management, operations, administrative, and other personnel who are responsible for developing, ensuring adherence to, and applying controls;
3) Observations of personnel in the performance of their assigned duties; and
4) Discussion with management regarding the risk, operational, and compliance management process.

The control environment was considered in determining the nature, timing, and extent of the testing of controls relevant to achievement of the control objectives.

4.2. Description of tests performed

Tests performed to determine the design and implementation of the controls detailed in this section are described below:

Test Procedure	Description
Enquiries	Enquired of appropriate ExpressVPN personnel. Enquiries were used to obtain, among other things, knowledge and additional information about the control.
Inspection	Read documents, reports, and electronic files that contain an indication of performance of the control. This includes, among other things, examining management reports, operational logs, and other relevant documentation.
Observation	Observed the application of a specific control by ExpressVPN personnel. Observations are primarily performed where there is no documentary evidence of the implementation of the controls.

4.3. Control objectives, related controls and tests performed

4.3.1. Control objective 1 – Logging of users' activity

Controls provide reasonable assurance that the ExpressVPN TrustedServer does not collect logs of users' activity, including no logging of browsing history, traffic destination, data content, DNS queries, or specific connection logs.

Ref	Control activity specified by ExpressVPN	Tests performed by KPMG LLP	Results of testing
C1.1.1	User-facing services are configured to automatically prevent exposing internal state containing: - users' activity; - browsing history; - traffic source and destination; - data content; - DNS queries via error; - output; or - outputting of log file.	On a selected day, inspected the system configuration of a selected user-facing service and noted that it had been configured to automatically prevent exposing internal state containing: - users' activity; - browsing history; - traffic source and destination; - data content; - DNS queries via error; - output; or - outputting of log file.	No exceptions noted.
C1.1.2	Service managers for user-facing services are configured to automatically prevent leaked data from the process' error, output or logging facility from being logged, and send them instead to a special device (/dev/null) which discards the data.	On a selected day, inspected the system configuration of a service manager for a selected user-facing service and noted that it had been configured to: - automatically prevent leaked data from the process' error, output or logging facility from being logged; and - send them instead to a special device (/dev/null/) which discarded the data.	No exceptions noted.

Ref	Control activity specified by ExpressVPN	Tests performed by KPMG LLP	Results of testing
C1.2.1	The TrustedServer OS is configured to run only on an in-memory file system, OverlayFS such that files written to the root filesystem are allowed to exist in memory only and are lost on server reboot.	On a selected day, inspected the configuration of the OS and noted that it had been configured to run only on an in-memory file system, OverlayFS. For a selected file written to the root filesystem, inspected the output of the server reboot and noted that files written to the root filesystem had existed in memory only and had been lost on server reboot.	No exceptions noted.
C1.3.1	Version control on the change management system is configured to automatically disable changes being pushed directly to production branches.	On a selected day, inspected the configuration of version control on the change management system and noted that it had been configured to automatically disable changes being pushed directly to production branches. For a selected change, inspected the change records on the change management system and noted that the system automatically disabled the change from being pushed directly to the production branch.	No exceptions noted.

Ref	Control activity specified by ExpressVPN	Tests performed by KPMG LLP	Results of testing
C1.4.1	The change management system is configured to run continuous integration tests on code changes to validate that no logging configuration has been enabled. Version control on the change management system is configured to automatically disable merging of a code change to the production branch when the validation fails.	On a selected day, inspected the configuration of the change management system and noted that it had been configured to run continuous integration tests on code changes to validate that no logging configuration had been enabled. On a selected day, inspected the configuration of version control on the change management system and noted that it had been configured to automatically disable merging of the code change to the production branch when the validation failed. For a selected change, inspected the change records on the change management system and noted that: - continuous integration tests had been run on the change to validate that no logging configuration had been enabled; and - when the validation failed, the version control on the change management system disabled merging the change to the production branch.	No exceptions noted.

Ref	Control activity specified by ExpressVPN	Tests performed by KPMG LLP	Results of testing
C1.4.2	The change management system is configured to automatically disable merging of the change to the production branch until a minimum of two people have reviewed and approved code changes in the form of Pull Requests, one of whom is a Code Owner.	On a selected day, inspected the configuration on the change management system and noted that it had been configured to automatically disable merging of the change to the production branch until a minimum of two people had reviewed code changes in the form of Pull Requests, one of whom was a Code Owner. For a selected change, inspected the change record on the change management system and noted that: - a minimum of two people had reviewed the code change in the form of a Pull Request, one of whom had been a Code Owner. - merging of the change to the production branch had been automatically disabled until the change had been approved.	No exceptions noted.

Ref	Control activity specified by ExpressVPN	Tests performed by KPMG LLP	Results of testing
C1.4.3	The change management system is configured to automatically disable merging of a change to the production branch if: - the code reviewers for the change are not different from code contributors; or - a code contributor is the sole reviewer, even where the contributor is the Code Owner.	On a selected day, inspected the configuration of the change management system and noted that it had been configured to automatically disable merging of a change to the production branch if: - the code reviewers are not different from the code contributors; or - the code contributor is the sole reviewer even where the contributor is the Code Owner. For a selected change request, inspected the change record on the change management system and noted that: - the code reviewers for the change had been different from the code contributors; - the code contributor had not been the sole reviewer; and - merging of the change to the production branch had been automatically disabled until the validation of the segregation of reviewers had passed.	No exceptions noted.

Ref	Control activity specified by ExpressVPN	Tests performed by KPMG LLP	Results of testing
C1.4.4	The change management system is configured to only allow changes to the Code Owners group membership if a minimum of two people have reviewed and approved the change, one of whom is a Code Owner.	On a selected day, inspected configuration of the changes to Code Owners group on the change management system and noted that it had been configured to only allow changes to the Code Owners group membership if a minimum of two people had reviewed and approved the change, one of whom was a Code Owner. For a selected change to the Code Owners group on the change management system that had not been reviewed and approved by a minimum of two people including at least one Code Owner, inspected the change management system and noted that it had rejected the change.	No exceptions noted.
C1.5.1	The change management system is configured to only allow changes to configuration of the version control system if the change is approved by a separate team, unrelated to TrustedServer, overseeing the security posture of ExpressVPN's source code repositories.	On a selected day, inspected the configuration of the change management system and noted that it had been configured to only allow changes to configuration of the version control system if the change had been approved by a separate team that was unrelated to TrustedServer and had oversight of the security posture of ExpressVPN's source code repositories.	No exceptions noted.

Ref	Control activity specified by ExpressVPN	Tests performed by KPMG LLP	Results of testing
C1.6.1	The TrustedServer OS image or boot process is configured to automatically fail verification steps for changes made to it such that the changed image is prevented from being used for production.	On a selected day, inspected the configuration of the TrustedServer OS image or boot process and noted that it had been configured to automatically fail verification steps for changes made to it such that the changed image is prevented from being used for production. For an attempted change made to the TrustedServer OS image, inspected the results of the change and the verification steps and noted that: - the verification steps had failed; and - the changed image had been prevented from being used for production.	No exceptions noted.
C1.7.1	The configuration for TrustedServer VPN credentials only allows pseudo-random, automatically generated, unpredictable username and password strings.	On a selected day, inspected the configuration for TrustedServer VPN credentials and noted that it had been configured to only allow pseudo-random, automatically generated, unpredictable username and password strings. Inspected the creation of a TrustedServer VPN user and noted that credentials allowed to be used by the system had been random, automatically generated username and password strings.	No exceptions noted.

4.3.2. Control objective 2– Usage analytics data

Controls provide reasonable assurance that usage analytics data are collected in line with ExpressVPN's privacy policy, including VPN location, aggregate data transfer per connection but not the source, or length of connection.

Ref	Control activity specified by ExpressVPN	Tests performed by KPMG LLP	Results of testing
C2.1.1	Guidelines for collection of usage analytics including VPN location, aggregate data transfer per connection but not the source, or length of connection is documented within the Privacy Policy as published on ExpressVPN's website. The Privacy Policy is reviewed and approved for distribution by ExpressVPN's Chief Communications Officer, Legal Department, and Data Protection Officer on an annual basis at a minimum.	Inspected the Privacy Policy, ExpressVPN website, and the email correspondence from approvers and noted that the Privacy Policy: - contained guidelines for collection of usage analytics including VPN location, aggregate data transfer per connection but not the source, or length of connection; - had been published on ExpressVPN's website; and - had been reviewed and approved for distribution within the last twelve months by ExpressVPN's Chief Communications Officer, Legal Department, and Data Protection Officer.	No exceptions noted.

Ref	Control activity specified by ExpressVPN	Tests performed by KPMG LLP	Results of testing
C2.1.2	Prior to the event leaving the server, the Usage Analytics system automatically verifies the schema of the generated event, filtering out invalid keys and values. Valid keys and values are maintained by the TrustedServer team in version-controlled source code.	On a selected day for a selected event submission, inspected the record in the Usage Analytics system and noted that prior to the event leaving the server, the Usage Analytics system had automatically verified the schema of the generated event, filtering out invalid keys and values. On a selected day, inspected the records in the version control system and noted that valid keys and values had been maintained by the TrustedServer team in version-controlled source code.	No exceptions noted.
C2.1.3	When a data set is received from the VPN servers by the analytics pipeline, automated schema validation is performed. On schema failure, the failing field is automatically removed from the data set before being stored in the database.	For a selected data set, inspected record in the system and noted that when the data set was received from the VPN servers by the analytics pipeline, automated schema validation had been performed. For a selected schema failure, inspected the record in the system and noted that the failing field had been automatically removed from the data set before being stored in the database.	No exceptions noted.

Ref	Control activity specified by ExpressVPN	Tests performed by KPMG LLP	Results of testing
C2.2.1	The networking applications do not contain log lines to prevent traffic source and destination being logged. Changes to this configuration are stored in version-controlled source code, and failed unit tests automatically prevents merging of the code into the production branch should the word "log" appear in the configurations.	On a selected day, inspected configuration of the network applications and noted that the networking applications had not contained log lines to prevent traffic source and destination being logged. On a selected day, inspected the version control system and noted that changes to networking applications had been stored in version-controlled source code and configured such that failing unit tests automatically disable merging of the code into the production branch should the word "log" appear in the configurations.	No exceptions noted.
C2.3.1	The TrustedServer analytics event data is configured to only include the date and to automatically generate a timestamp of 00:00:00. The data analysis pipeline consumer filters the date field to convert the datestamp to an ISO formatted string without a time portion.	On a selected day, inspected the configuration of the TrustedServer and noted that: - the TrustedServer analytics event data had been configured to only include the date and to automatically generate a timestamp of 00:00:00; and - the data analysis pipeline consumer had filtered the date field to convert the datestamp to an ISO formatted string without a time portion.	No exceptions noted.

Ref	Control activity specified by ExpressVPN	Tests performed by KPMG LLP	Results of testing
C2.3.2	Usage analytics are stored such that the length of a connection cannot be determined retrospectively. This is achieved via technical implementation to only store sanitised disconnect events, without any corresponding connect events.	On a selected day, inspected the configuration of the technical implementation of the usage analytics system and noted that usage analytics had been stored such that the length of a connection could be determined retrospectively and only sanitised disconnect events, without any corresponding connect events had been stored For a selected data event, inspected the record in the Usage Analytics System and noted that only sanitised disconnect event had been stored without any corresponding connect event.	No exceptions noted.

4.3.3. Control objective 3 – Third-party software as a service (SaaS) platforms

Controls provide reasonable assurance that ExpressVPN protects its customers from the compromise of ExpressVPN's selected third-party SaaS platforms involved in the TrustedServer build process.

Ref	Control activity specified by ExpressVPN	Tests performed by KPMG LLP	Results of testing
C3.1.1	A commit signed with an unauthorised key, or an unsigned commit results in the automatic disabling of the code change from being merged.	On a selected day, inspected the configuration of the change management system and noted that it had been configured to automatically disable the code from being merged for commits with an unauthorised key, or unsigned commits. For a selected commit, with an unauthorised key, inspected the change management system and noted that it had resulted in the automatic disabling of the code change from being merged. For a selected unsigned commit, inspected the change management system and noted it had resulted in the automatic disabling of the code change from being merged.	No exceptions noted.

Ref	Control activity specified by ExpressVPN	Tests performed by KPMG LLP	Results of testing
C3.2.1	Reproducible builds of the OS Image result in the following verification of multiple builds: - automatically by cross checking SHA-512 checksums from each build system in Github Actions; and - signature file only generated on success of cross check.	On a selected day, inspected the configuration of the record in the system and noted that reproducible builds of the OS Image had resulted in multiple builds being verified: - by automatically cross checking SHA512 checksums from each build system in Github Actions; and - by generating the signature file only on the success of the cross check.	No exceptions noted.

4.3.4. Control objective 4 – Individual VPN servers protection

Controls provide reasonable assurance that ExpressVPN protects its customers from the cross-compromise of any individual VPN server.

Ref	Control activity specified by ExpressVPN	Tests performed by KPMG LLP	Results of testing
C4.1.1	VPN Servers, Config Management, CDN and monitoring tools are configured at the firewall level to accept incoming management connections from specific ExpressVPN controlled sources, and to drop other connection requests.	On a selected day, inspected the VPN Servers, Config Management, CDN and monitoring tools and noted that the system had been configured at the firewall level to accept incoming management connections from specific ExpressVPN controlled sources, and to drop other connection requests. For a selected accepted incoming connection, inspected the record in the system and noted that the firewall level had been configured to accept incoming management connections from specific ExpressVPN controlled sources, and to drop other connection requests.	No exceptions noted.
C4.1.2	Authentication to VPN servers is performed using hardware-backed SSH keys, provisioned by a central IT team with known-good keys stored in a version-controlled repository.	On a selected day for a selected authentication session, inspected the configuration of the system and noted that authentication to VPN servers had been performed using hardware-backed SSH keys, provisioned by a central IT team with known-good keys stored in a version-controlled repository.	No exceptions noted.

Ref	Control activity specified by ExpressVPN	Tests performed by KPMG LLP	Results of testing
C4.1.3	SSH agent forwarding is disabled in the SSH configuration, which is maintained in version-controlled source code.	On a selected day, inspected the configuration of the system and noted that the SSH agent forwarding had been disabled in the SSH configuration, which had been maintained in version-controlled source code.	No exceptions noted.
C4.1.4	A VPN server configuration does not record the details of other VPN servers.	For a selected server session, inspected the record in the system and noted that VPN server configuration had not recorded the details of other VPN servers.	No exceptions noted.
C4.1.5	Before a server enters production state, SSH access is automatically disabled by default.	On a selected day, inspected the configuration of the server and noted that SSH access had been automatically disabled by default before the server entered production state.	No exceptions noted.

4.3.5. Control objective 5 – Build pipeline protection

Controls provide reasonable assurance that ExpressVPN protects its build pipeline from dependency injection attacks.

Ref	Control activity specified by ExpressVPN	Tests performed by KPMG LLP	Results of testing
C5.1.1	The TrustedServer team maintains a version controlled repository of the versions and unique cryptographic hashes for external Python dependencies. The packages downloaded at build time are automatically verified against this repository of cryptographic hashes, with any mismatches resulting in failure to build.	On a selected day, inspected the configuration of the system and noted that the TrustedServer team had maintained a version controlled repository of the versions and unique cryptographic hashes for external Python dependencies. For a selected package, inspected the record in the system and noted that: - the packages downloaded at build time had been automatically verified against the repository of cryptographic hashes; and - any mismatches had resulted in failure to build.	No exceptions noted.

Ref	Control activity specified by ExpressVPN	Tests performed by KPMG LLP	Results of testing
C5.1.2	A third-party security scanning tool is configured to automatically and continuously validate Python and Ruby dependency files against known vulnerable versions, raising alerts should one be found. If there are outstanding security alerts for dependencies, merging of new code is automatically disabled and the TrustedServer team subsequently resolves the outstanding security alert.	On a selected day, inspected the configuration of third party security scanning tool and noted that it had been configured to automatically and continuously validate Python and Ruby dependency files against known vulnerable versions, raising alerts should one be found. For a selected outstanding security alert for dependencies, inspected the record in the system and noted that the merging of new code had been automatically disabled and the outstanding security alert had been resolved subsequently by the TrustedServer team.	No exceptions noted.
C5.2.1	The TrustedServer OS Image is built from open source repositories, with updates and security fixes automatically incorporated into each release of TrustedServer.	On a selected day, inspected the configuration of the change management system and noted that TrustedServer OS Image had been configured to be built from open source repositories, with updates and security fixes automatically incorporated into each release of TrustedServer. For a selected pull request, inspected the pull request record and noted that the TrustedServer OS image had been built from open source repositories, with updates and security fixes automatically incorporated into the release.	No exceptions noted.

Ref	Control activity specified by ExpressVPN	Tests performed by KPMG LLP	Results of testing
C5.2.2	Third-party package source signatures are automatically verified against version-controlled, vendor published, GNU Privacy Guard (GPG) keys. These keys are maintained by the TrustedServer team as evidenced by the inclusion of keys alongside repository configuration in version-controlled source code. An invalid or modified key results in automatic failure of OS build.	On a selected day, inspected the configuration of the TrustedServer for a selected package, and noted that it had been configured to: - automatically verify the third-party package source signatures against version-controlled, vendor published, GPG keys maintained by the TrustedServer team; - include the keys alongside repository configuration in version-controlled source code as evidence of signature verification; and - automatically fail the OS build for invalid or modified keys.	No exceptions noted.
C5.2.3	ExpressVPN provided Debian Server packages that are consumed by TrustedServer are cryptographically signed, with signatures validated at build time. A failing signature verification results in automatic build failure of the OS.	For a selected ExpressVPN provided Debian Server package that is consumed by TrustedServer, inspected the record in the system and noted that it had been cryptographically signed, with signatures validated at build time. For a selected ExpressVPN provided Debian Server package that is consumed by TrustedServer, inspected the record in the system and noted that a failed signature verification had resulted in automatic build failure of the OS.	No exceptions noted.

5. Other information

Appendix – Glossary

Term	Description
Activator	A server that is responsible for setting sensitive credentials on target servers and setting the target servers to a production ready state or close to production ready state.
Ansible playbook	A set of predefined instructions to be executed on target servers.
Booted OS	A running operating system.
Bootloader	A small program that loads the operating system into memory and boots (starts running) it.
Build system	A software system that takes source code as input and produces deployable artefacts, e.g. binary files and configuration files.
CDN	Acronym for content delivery network. It is a network of servers likely to be geographically close to the end users such that the data only needs to traverse a short distance and the response time is shorter as a result.
Cryptographic hash	A hash function is any function that can be used to map data of arbitrary size to fixed-size values. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes. A Cryptographic hash is a hash where it is mathematically extremely difficult to deduce the original data from the hash and to find two data source that will result in the same hash.
Cryptographic signature	Using public and private key cryptography to help ensure data integrity and authenticity. One can use the signature to verify that the target data has not been tampered with and is signed by a specific entity.
CVE	Acronym for Common Vulnerabilities and Exposures. CVE are publicly available list of existing security flaws.
ISO image	A kind of computer filesystem format that is widely supported. It is commonly used for CD-ROM or operating system distribution.
Licensing counter	A software counter that counts concurrent logged in session against users' licenses.
Manual configuration	A means to connect to ExpressVPN VPN services without using the ExpressVPN client applications.
Operational metrics	Metrics that are useful for monitoring stability of servers, e.g. CPU usage, available RAM, network load, etc.

Term	Description
Orchestration tooling	A centralised tool for updating server configuration in a controlled and safe manner.
OverlayFS	A filesystem that stores changes and results of file system operation in RAM and not on hard disk or any device that persist data across boot.
PII	Acronym for Personally identifiable information. It is any data that can be used to identify an individual.
Production branch/Feature branch	A set of version of source code marked for production use (production branch) or development-in-progress (feature branch).
Ram-only infrastructure	Operating system that run entirely on RAM only, i.e. the hard disk is irrelevant and can be absent.
SHA-512	512-bit cryptographic hash function used to generate checksums for reproducible builds.
SSH	Acronym for secure shell. It is a protocol for secure remote login from one computer to another computer.
Version-controlled repository	Source code management system that records each changeset to the source code.
VPN server	Servers running our TrustedServer technology that handle the VPN traffic workload. User devices connect to our VPN servers and establish secure tunnels, i.e. the VPN tunnels, which encrypt the data passing through. The servers may be located in different countries/regions from the connecting users.
Yubikey	A hardware security device that allows the use of private key for encryption/authentication without the possibility of extracting the private key from the device.