System and Organization Controls (SOC) 3

Report over the Google Firebase System

Relevant to Security, Availability, and Confidentiality

For the Period 1 May 2021 to 30 April 2022

Google LLC
1600 Amphitheatre
Parkway
Mountain View, CA, 94043

650 253-0000 main
Google.com

Management's Report of Its Assertions on the Effectiveness of Its Controls Over the Google Firebase System Based on the Trust Services Criteria for Security, Availability, and Confidentiality

We, as management of Google LLC ("Google" or "the Company") are responsible for:

- Identifying the Google Firebase System (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our service commitments and system requirements
- Identifying the risks that would threaten the achievement of its service commitments and system requirements that are the objectives of our System, which are presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the service commitments and system requirements
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the System were effective throughout the period 1 May 2021 to 30 April 2022, to provide reasonable assurance that the service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

Very truly yours,

Google LLC
13 June 2022

Ernst & Young LLP
303 Almaden Boulevard
San Jose, CA 95110

Tel: +1 408 947 5500
Fax: +1 408 947 5717
ey.com

Report of Independent Accountants

To the Management of Google LLC:

Scope

We have examined management's assertion, contained within the accompanying "Management's Report of its Assertions on the Effectiveness of Its Controls Over the Google Firebase System Based on the Trust Services Criteria for Security, Availability, and Confidentiality" (Assertion), that Google's controls over the Google Firebase System (System) were effective throughout the period 1 May 2021 to 30 April 2022, to provide reasonable assurance that its service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

Management's Responsibilities

Google's management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the System and describing the boundaries of the System
- Identifying the service commitments and system requirements and the risks that would threaten the achievement of the service commitments and system requirements that are the objectives of the System
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the service commitments and system requirements

Our Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA"). 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 Google's relevant security, availability, and confidentiality 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 to provide a reasonable basis for our opinion.

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

We are required to be independent of Google LLC and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the *Preface: Applicable to All Members* and *Part 1 – Members in Public Practice of the Code of Professional Conduct* established by the AICPA. We have complied with such independence and other ethical requirements and applied the AICPA's *Statements on Quality Control Standards*.

Inherent limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Google's service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. 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.

Opinion

In our opinion, Google's controls over the system were effective throughout the period 1 May 2021 to 30 April 2022, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.

Ernst & Young LLP

13 June 2022
San Jose, CA

Attachment A - Google Firebase System

Overview

Google LLC ("Google" or "the Company"), an Alphabet subsidiary, is a global technology service provider focused on improving the ways people connect with information. Google's innovations in web search and advertising have made Google's website one of the most viewed Internet destinations and its brand among the most recognized in the world. Google maintains one of the world's largest online index of websites and other content and makes this information freely available to anyone with an Internet connection. Google's automated search technology helps people obtain nearly instant access to relevant information from their vast online index.

Firebase is a mobile app platform (platform as a service or PaaS) developed by Google with an integrated, unified software development kit (SDK), hereafter described collectively as (Google Firebase or Firebase). Firebase provides developers with a suite of tools and resources to develop and manage high quality mobile and web applications for growing their business. It consists of complementary products, solutions, and extensions that enable developers to independently manage their projects and mix-and-match services as needed.

Leveraging Google's cloud environment, Firebase can be accessed from any location with internet connectivity. This means every developer and each user they work with can be productive from anywhere, using any device with an internet connection.

The Firebase services covered in this system description consist of the following:

- Firebase A/B Testing
- Firebase App Check
- Firebase App Distribution
- Firebase Cloud Messaging
- Firebase Console
- Firebase Crashlytics
- Firebase Dynamic Links
- Firebase Hosting
- Firebase In-App Messaging
- Firebase Machine Learning
- Firebase Performance Monitoring
- Firebase Predictions
- Firebase Realtime Database
- Firebase Remote Config
- Firebase User Segmentation Storage

Firebase A/B Testing

Firebase A/B Testing allows developers to make data-driven decisions about changes to their applications. Developers can run controlled experiments with Firebase Remote Config parameters to compare alternative scenarios and see which one performs better in reaching their goals.

Firebase App Check

App Check helps protect backend resources from abuse, such as billing fraud and phishing. It works with both Firebase services and customer backends to keep resources safe. With App Check, devices running customer applications will use an application or device attestation provider that attests to the authenticity of the request.

Firebase App Distribution

Firebase App Distribution allows users to distribute pre-release versions of their iOS and Android apps to trusted testers before releasing to production

Firebase Cloud Messaging

Firebase Cloud Messaging (FCM) is a cross-platform messaging solution that allows developers to send messages to devices. Using FCM, developers can notify a client app that a new email or other data is available to sync. Developers can send notification messages to drive user re-engagement and retention.

Firebase Console

Firebase Console is the central web interface for application management used by developers to enable and configure their Firebase products, as well as a common interface through which users can interact with individual Firebase products.

Firebase Crashlytics

Firebase Crashlytics is a lightweight, real-time crash reporter that helps developers track, prioritize, and fix stability issues that erode app quality. Crashlytics reduces troubleshooting time by grouping crashes and highlighting the circumstances that lead up to them.

Firebase Dynamic Links

Firebase Dynamic Links is a service that allows developers to create and manage smart URLs sending users to any location within their iOS, Android, or web application. Firebase Dynamic Links persists during the application install process, so new users see the content they are looking for when they open the app for the first time.

Firebase Hosting

Firebase Hosting is a fully-managed hosting service for static and dynamic content as well as microservices. Using Firebase Hosting, developers can deploy Secure Sockets Layer (SSL)-enabled web applications with static content and microservices to a global content-delivery network from a single command.

Firebase In-App Messaging

In-App Messaging enables developers to drive engagement by sending customized, targeted messages to their users, without any engineering effort, from the Firebase Console.

Firebase Machine Learning

Firebase Machine Learning provides on-device and cloud APIs to give developers solutions to problems without requiring deep knowledge of machine learning, neural networks, or model optimization. Developers are also able to use this service to train and dynamically serve and update mobile optimized custom models to their users.

Firebase Performance Monitoring

Firebase Performance Monitoring is a service that helps developers to gain insight into the performance characteristics of their iOS and Android applications. Developers can use Performance Monitoring to collect performance data from their applications, and then review and analyze that data in the Firebase Console. Performance Monitoring helps developers understand where and when the performance of their applications can be improved so that they can use that information to fix performance issues.

*Firebase Predictions**

Firebase Predictions applies machine learning to a developer's analytics data to create dynamic user groups based on their user's predicted behavior. These predictions are automatically available for use with Firebase Remote Config, the Notification composer which is a feature in the Firebase Console, Firebase In-App Messaging and A/B Testing.

Firebase Realtime Database

The Firebase Realtime Database is a cloud-hosted, NoSQL database. Data can be synchronized in real-time to every connected client. Developers can build cross-platform applications where clients share one Realtime Database instance and automatically receive updates with the newest data.

Firebase Remote Config

Firebase Remote Config allows developers to customize how their app renders for different users. Developers can change the app's look and feel, roll out features gradually, run A/B tests, deliver customized content to certain users, or make other updates without deploying a new version – all from the Firebase Console.

Firebase User Segmentation Storage

Firebase User Segmentation Storage stores developer-created audience lists to provide targeting information to other Firebase services that use them.

* Firebase Predictions was deprecated on February 21, 2022

Data Centers

The above products are serviced from data centers operated by Google around the world. Below is a list of Google's production data center locations that host the above products and operations for Google Firebase:

North America, South America

- Arcola (VA), United States of America
- Ashburn (1) (VA), United States of America
- Ashburn (2) (VA), United States of America
- Ashburn (3) (VA), United States of America

- Atlanta (1) (GA), United States of America
- Clarksville (TN), United States of America
- Columbus (OH), United States of America
- Council Bluffs (1) (IA), United States of America
- Council Bluffs (2) (IA), United States of America
- Henderson (NV), United States of America
- Las Vegas (NV), United States of America
- Leesburg (VA), United States of America
- Lenoir (NC), United States of America
- Los Angeles (1) (CA), United States of America
- Los Angeles (2) (CA), United States of America
- Midlothian (TX), United States of America
- Moncks Corner (SC), United States of America
- Montreal, Quebec, Canada
- New Albany (OH), United States of America
- Osasco, Brazil
- Papillion (NE), United States of America
- Pryor Creek (OK), United States of America
- Quilicura, Santiago, Chile
- Reno (NV), United States of America
- Salt Lake City (1) (UT), United States of America
- Salt Lake City (2) (UT), United States of America[+]
- The Dalles (1) (OR), United States of America
- The Dalles (2) (OR), United States of America
- Toronto, Ontario, Canada
- Vinhedo, Brazil
- Widows Creek (AL), United States of America

Europe, Middle East, and Africa

- Dublin, Ireland
- Eemshaven, Groningen, the Netherlands
- Frankfurt (1), Hesse, Germany
- Frankfurt (2), Hesse, Germany
- Frankfurt (4), Hesse, Germany
- Frankfurt (5), Hesse, Germany
- Frankfurt (6), Hesse, Germany
- Frankfurt (7), Hesse, Germany[+]
- Fredericia, Denmark
- Ghlin, Hainaut, Belgium
- Hamina, Finland
- London (1), United Kingdom
- London (2), United Kingdom
- London (3), United Kingdom
- London (4), United Kingdom

- London (5), United Kingdom
- London (6), United Kingdom
- Madrid (1), Spain$^+$
- Madrid (2), Spain$^+$
- Middenmeer, Netherlands
- Milan (1), Italy$^+$
- Milan (2), Italy$^+$
- Paris (1), France$^+$
- Paris (2), France$^+$
- Paris (3), France$^+$
- Warsaw (1), Poland
- Warsaw (2), Poland
- Zurich, Switzerland

Asia Pacific

- Changhua, Taiwan
- Delhi, India
- Hong Kong (1), Hong Kong
- Hong Kong (2), Hong Kong
- Hong Kong (3), Hong Kong
- Jakarta, Indonesia
- Koto-ku (1), Tokyo, Japan
- Koto-ku (2), Tokyo, Japan
- Koto-ku (3), Tokyo, Japan
- Lok Yang Way, Singapore
- Melbourne, Victoria, Australia
- Mumbai, India
- Osaka, Japan
- Seoul (1), South Korea
- Seoul (2), South Korea$^+$
- Sydney (1), NSW, Australia
- Sydney (2), NSW, Australia
- Sydney (3), NSW, Australia
- Wenya, Singapore

$^+$ Indicates data centers in scope only for the period 1 November 2021 through 30 April 2022

Infrastructure

Google Firebase runs in a multi-tenant, distributed environment. Rather than segregating user entity data to one machine or set of machines, data from all user entities is distributed amongst a shared infrastructure. For Google Firebase, this is achieved through a Google distributed file system designed to store extremely large amounts of data across many servers. User entity data is then stored in large, distributed databases, built on top of this file system.

Data Centers and Redundancy

Google maintains consistent policies and standards across its data centers for physical security to help protect production servers, network devices and network connections within Google data centers.

Redundant architecture exists such that data is replicated in real-time to at least two (2) geographically dispersed data centers. The data centers are connected through multiple encrypted network links and interfaces. This provides high availability by dynamically load balancing across those sites. Google uses monitoring mechanisms that provide details such as resource footprint, central processing unit capacity, and random-access memory availability to monitor resource availability across their data centers and to validate that data has been replicated to more than one location.

Authentication and Access

Strong authentication and access controls are implemented to restrict access to Google Firebase production systems, internal support tools, and customer data. Machine-level access restriction relies on a Google-developed distributed authentication service based on Transport Layer Security (TLS) certificates, which helps to positively identify the resource access requester. This service also offers transport encryption to enhance data confidentiality in transit. Google uses encryption to secure user data in transit between Google production facilities.

Google follows a formal process to grant or revoke employee, temporary worker, contractor or vendor access to Google resources. Lightweight Directory Access Protocol (LDAP), Kerberos, and a Google proprietary system which utilizes Secure Shell (SSH) and TLS certificates help provide secure and flexible access mechanisms. These mechanisms are designed to grant access rights to systems and data only to authorized users.

Both user and internal access to customer data is restricted through the use of unique user account IDs. Access to sensitive systems and applications requires two-factor authentication in the form of a unique user account ID, strong passwords, security keys and/or certificates. Periodic reviews of access lists are implemented to help ensure access to customer data is appropriate and authorized. Access to production machines, network devices and support tools is managed via an access group management system. Membership in these groups must be approved by respective group administrators. User group memberships are reviewed on a semiannual basis under the direction of the group administrators.

Change Management

Change Management policies, including code reviews, are in place, and procedures for tracking, testing, approving, and validating changes are documented and implemented appropriately. Changes are developed and deployed utilizing source code management systems and release workflow automation tools to manage source code, documentation, release labeling and other functions. Google requires all production-impacting code changes to be reviewed and approved by a separate technical resource, other than the developer, to evaluate quality and accuracy of changes. Further, all application and configuration changes are tested prior to migration to the production environment. Following a successful pass of tests, multiple binaries are then grouped into a candidate and deployed to production through a release.

Data

Google provides controls at each level of data storage, access, and transfer. Google has established training programs for privacy and information security to support data confidentiality. All Google personnel, including employees, temporary workers, vendors and contractors are required to complete these training programs at the time of joining the organization and annually thereafter. All new products and product feature launches that include collection, processing, or sharing of user data are required to go through an internal design review process that defines retention and deletion timelines. This review is performed by legal and privacy teams. In addition to the preventative controls, Google has also established detective measures like incident response processes to report and handle events related to security. Google establishes agreements, including nondisclosure agreements, for preserving confidentiality of information and software exchange with external parties.

Network Architecture and Management

The Google Firebase system architecture utilizes a fully redundant network infrastructure. Google has implemented perimeter devices to protect the Google network from external attacks. Network monitoring mechanisms are in place to prevent and disconnect access to the Google network from unauthorized devices.

People

Google has implemented a process-based service quality environment designed to deliver the Google Firebase products to customers. The fundamentals underlying the services provided are the adoption of standardized, repeatable processes; the hiring and development of highly skilled resources; and leading industry practices. Google has established internal compliance teams utilizing scalable processes to efficiently manage core infrastructure and product-related security, availability, and confidentiality controls.

Formal organizational structures exist and are available to Google personnel on the Company’s intranet. The intranet provides drill-down functionality for identifying personnel in the functional operations team. Google has developed and documented formal policies, procedures, and job descriptions for operational areas including data center operations, security administration, system and hardware change management, hiring, training, performance appraisals, terminations, and incident escalation. These policies and procedures have been designed to segregate duties and enforce responsibilities based on job functionality. Policies and procedures are reviewed and updated as necessary.

Attachment B - Service Commitments and System Requirements

Service Commitments

Commitments are declarations made by management to customers regarding the performance of the Google Firebase System. Commitments to customers are communicated via Terms of Service, Google Firebase Service Level Agreements, and/or Data Processing Agreements. Data Processing Agreements define the security and privacy obligations which the processors must meet to satisfy the organization's obligations regarding the processing and security of customer data.

System Requirements

Google has implemented a process-based service quality environment designed to deliver the Google Firebase System products to customers. These internal policies are developed in consideration of legal and regulatory obligations, to define Google's organizational approach and system requirements.

The delivery of these services depends upon the appropriate internal functioning of system requirements defined by Google to meet customer commitments.

The following processes and system requirements function to meet Google's commitments to customers with respect to the terms governing the processing and security of customer data:

- Access Security: Google maintains data access and logical security policies, designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Access to systems is restricted based on the principle of least privilege
- Change Management: Google requires standard change management procedures to be applied during the design, development, deployment, and maintenance of Google applications, systems, and services
- Incident Management: Google monitors internal communication channels, audit logs and signals to determine the validity of security threats. Confirmed threats, including threats related to security, are escalated to the appropriate team including incident management. Google's dedicated security personnel will react promptly to potential and known incidents
- Data Management: Google complies with any obligations applicable to it with respect to the processing of Customer Personal Data. Google processes data in accordance with Google Firebase Terms of Service and/or Data Processing Agreements, and complies with applicable regulations
- Data Security: Google maintains data security policies and implements technical and organizational measures to protect customer data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. Google takes appropriate steps to ensure compliance with the security measures by its employees, contractors and vendors to the extent applicable to their scope of performance
- Third-Party Risk Management: Google conducts an assessment of the security practices of third-party suppliers to ensure they provide a level of security appropriate to their access to data and the scope of the services they are engaged to provide. Google conducts routine inspections of subprocessors to ensure their continued compliance with the agreed upon

security and privacy requirements. Google defines security practices that must be applied to the processing of data and obtains contractual commitments from suppliers to comply with these practices