System and Organization Controls (SOC) 3 Report

Report on the Google Firebase System

Relevant to Security, Availability, and Confidentiality

For the Period 1 May 2018 to 30 April 2019

Google LLC
1600 Amphitheatre
Parkway
Mountain View, CA, 94043

650 253-0000 main
Google.com

Management's Report of its Assertion 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) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal 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 principal service commitments and system requirement
- 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 2018 to 30 April 2019, to provide reasonable assurance that the principal 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
26 June 2019

Building a better
working world

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 Assertion on the Effectiveness of Its Controls over the Google Firebase System Based on the Trust Services Principles and Criteria for Security, Availability and Confidentiality" (Assertion), that Google's controls over the Google Firebase System (System) were effective throughout the period 1 May 2018 through 30 April 2019, to provide reasonable assurance that its principal 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 Responsibilities

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

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

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. 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.

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 principal 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 2018 through 30 April 2019, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

Ernst + Young LLP

26 June 2019
San Jose, CA

Attachment A – Google Firebase System

Google Overview

Google LLC ("Google" or "the Company") 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) offered by Google with an integrated, unified software development kit (SDK), hereafter described collectively as (Firebase). Firebase provides developers with a rich suite of tools and resources to develop and manage high quality apps, for growing their user base, and to monetize the platform. It consists of complementary features that work independently, or can be mix-and-matched as needed.

Leveraging Google's cloud environment, Firebase can be accessed from virtually 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:

- Cloud Firestore
- Cloud Functions for Firebase
- Cloud Storage for Firebase
- Firebase A/B Testing
- Firebase Authentication
- Firebase Cloud Messaging
- Firebase Console
- Firebase Dynamic Links
- Firebase Hosting
- Firebase In-App Messaging
- Firebase Invites
- Firebase Performance Monitoring
- Firebase Predictions
- Firebase Realtime Database
- Firebase Remote Config
- Firebase Test Lab
- Google Analytics for Firebase
- ML Kit for Firebase

Cloud Firestore

Cloud Firestore is a fully managed, scalable, serverless NoSQL document database for mobile, web, and server development. It provides query capabilities, strong consistency, live synchronization and offline support. It also provides integrations with both Firebase and Google Cloud Platform (GCP).

Cloud Functions for Firebase

Cloud Functions for Firebase are developer tools used for development and deployment of Google Cloud Functions. Cloud Functions enable developers to run their own backend code that executes automatically based on HTTP requests and Firebase and Google Cloud Platform events. Developers functions are stored in Google's cloud and run in a managed Node.js environment.

Cloud Storage for Firebase

Cloud Storage for Firebase adds customizable Google security (via Firebase Security Rules for Cloud Storage) to file uploads and downloads for Firebase apps. Cloud Storage for Firebase is backed by Google Cloud Storage, a service for storing and accessing data on Google's infrastructure.

Firebase A/B Testing

Firebase A/B Testing allows developers to make data-driven decisions about changes to their apps. 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 Authentication

Firebase Authentication is a fully managed user identity and authentication system providing backend services enabling sign-in and sign-up experiences for an application or service.

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 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 (plus project and app management APIs) 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 Dynamic Links

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

Firebase Hosting

Firebase Hosting is developer-focused web hosting for modern front-end web applications. Using Firebase Hosting, developers can deploy SSL-enabled web apps with static content and microservices to a global content-delivery network from a single command.

Firebase In-App Messaging

Firebase 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 Invites

Building on Firebase Dynamic Links, Firebase Invites provides developers with tools to enable their users to send content to their friends, over both SMS and email and ensures that referral codes, recipe entries, or other shared content gets passed along with the invitation.

Firebase Performance Monitoring

Firebase Performance Monitoring is a service that helps developers to gain insight into the performance characteristics of their iOS and Android apps. 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, and A/B Testing.

Firebase Realtime Database

The Firebase Realtime Database is a cloud-hosted, NoSQL database. Data can be synchronized in realtime to every connected client. Developers can build cross-platform apps 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 user segments, 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 Test Lab

Firebase Test Lab provides cloud-based infrastructure for testing apps on physical and virtual devices. Developers can test their apps across a wide variety of devices with Firebase Test Lab.

Google Analytics for Firebase

Google Analytics for Firebase is an app measurement solution that provides businesses with insights on app usage and user engagement, and provides marketers with information on the efficacy of their advertising spend.

ML Kit for Firebase

ML Kit for Firebase blends 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.

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. Customer 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 all data centers for physical security to help protect production and corporate 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 a dashboard that provides 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.

Firebase Hosting and Firebase Realtime Database backups are periodically performed to support the availability of user entity data. Firebase Hosting and Firebase Realtime Database data restore tests are periodically performed to confirm the ability to recover customer data. Critical data is replicated to at least two (2) data centers and provides high availability by dynamically load balancing across those sites.

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. Data traffic is encrypted between Google production facilities.

Google follows a formal process to grant or revoke employee 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 semi-annual basis under the direction of the group administrators.

Change Management

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

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 employees are required to complete these training programs annually. All product feature launches that include new collection, processing, or sharing of user data are required to go through an internal design review process. Google has also established incident response processes to report and handle events related to confidentiality. Google establishes agreements, including non-disclosure 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 employees on the Company’s intranet. The intranet provides drill-down functionality for identifying employees 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 - Principal Service Commitments and System Requirements

Service Commitments

Commitments are declarations made by management to customers regarding the performance of Google Firebase System. Commitments to customers are communicated via Terms of Service, Google Firebase System Service Level Agreements, and Data Processing Addendums.

System Requirements

Google has established internal policies and processes to support the delivery of Google Firebase System products to customers. These internal policies are developed in consideration with legal and regulatory obligations, to define Google's organizational approach and system requirements. The delivery of Google Firebase System services depends upon the appropriate functioning of system requirements.

The following processes and system requirements function to meet Google's contractual commitments to customers with respect to 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 all Google Applications, Systems, and Services.
- Incident Management: Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.
- Data Management: Google complies with any obligations applicable to it with respect to the processing of personal data. Google processes data in accordance with the customer instructions and complies with applicable regulations.
- Data Security: Google implements and maintains technical and organizational measures to protect user data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.
- Third Party Risk Management: Google conducts routine inspections of sub-processors to evaluate control conformance. Google defines security and privacy practices that must be applied to the processing of data and obtains contractual commitments from sub-processors to comply with these practices.