approov
API THREAT PROTECTION

WHITE PAPER

The Security and Compliance of the Approov Solution

This document describes the security aspects of the Approov solution and best-practices for integrating the solution into your own security and compliance framework. It is intended to be shared with the security and compliance teams in your organization as part of the evaluation process.

Overall Architecture of the Solution

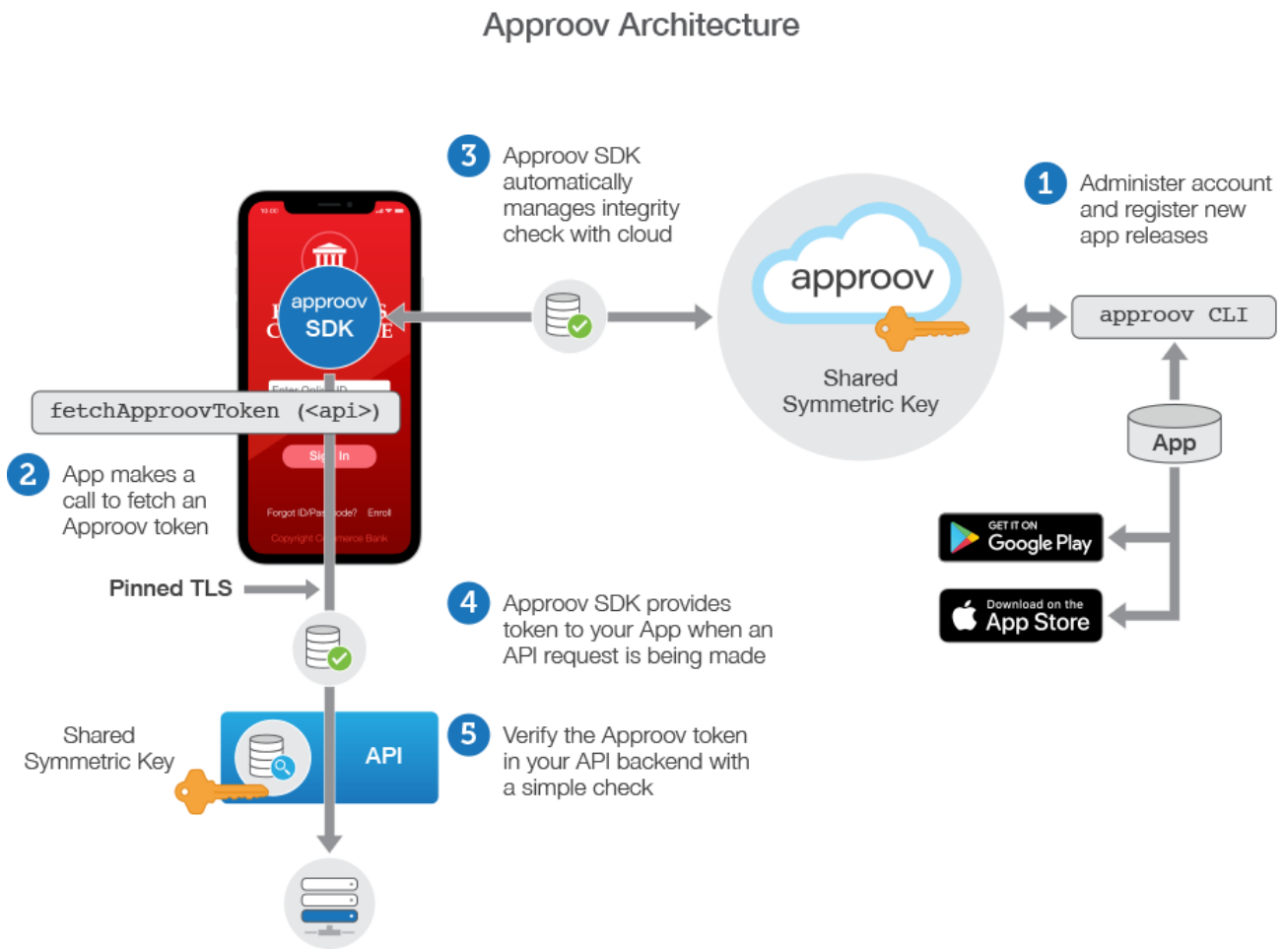
The Approov CLI tool is downloaded to your development environment. This tool is used to administer the properties of your account using the approov command line tool and Approov account access you were issued upon sign up. This tool is also used to register new apps that are to be released to the app store. The approov tool analyzes the app (in either .apk, .aab or .ipa format) and adds its signature to a database in the Approov cloud service for your account. No application code is stored or uploaded to the Approov service. The particular build of the app then becomes recognized as being official, allowing valid Approov tokens to be generated for calls from that app.

The Approov SDK must be integrated with your app, for example by using Android Studio or iOS Xcode, configured and initialized. See a later section in this document about how the Approov SDK is protected. The app then must make a call to either the `fetchApproovToken` or `fetchApproovTokenAndWait` methods in the SDK. Note that these calls must only be made after having initialized the Approov SDK. If this is the first call to obtain an Approov token, then it will initiate an integrity measurement process inside the SDK that requires communication with the Approov cloud service. Once an Approov token has been obtained it is cached by the SDK for up to 5 minutes so that subsequent fetch calls do not require additional network communication. However certain events (e.g. evidence of an instrumentation framework being attached) can trigger a new token fetch during this period.

The integrity check process requires the SDK and the Approov cloud service to work together. The SDK analyzes the runtime environment of the app and the authenticity of the app that is being measured. These checks are implemented in hardened code and communications are protected both by TLS, certificate pinning and also by a secondary level of request integrity signing. The app gathers and passes data and measurements to the Approov service. The Approov cloud service performs analysis on the data provided by the SDK and makes a decision based on this and the security policy criteria you set for your account. If the criteria are met then the Approov cloud service provides a short lived token signed with a symmetric secret allocated randomly during your account sign up. If the criteria are not met then a token is still issued, but it is not signed with the correct secret. Options are also available to use other secrets or other signing algorithms, including those with asymmetric keys.

The obtained Approov token is added by the Approov Service to every backend API request as an additional header, such as `Approov-Token`, but the name used is configurable. It is important that all communications made by these APIs are pinned so that no Man-in-the-Middle (MitM) interception is possible that could make a copy of the short lived token. Pinning TLS connections is managed automatically by the Approov dynamic pinning functionality.

The customer backend API is able to check the validity of the Approov token by checking if it has been correctly signed and has not expired. If it is, then you know that the



API request is really coming from an official registered version of your app; it is not being spoofed by some other entity. Moreover, a valid Approov token also indicates that the checks on the runtime environment have passed, as controlled by the security policy you have set in your account. Since the signing key is never put inside the app, an attacker cannot reverse engineer it in order to create their own signed Approov tokens.

How the CLI Tool is protected

Administration API endpoints require management tokens for access. There is a hierarchy of tokens for different operations: admin, dev and automation etc. Management tokens will be typically password protected. Sessions last one hour normally, after which time the password must be re-entered. See later section on passwords and user authentication.

How the mobile SDK is protected

The following techniques are employed in the Approov SDK to prevent attempts to spoof the measurement algorithm or to enable the measurement algorithm to be executed in a different environment without detection:

- **Obfuscated Native Code:** All of the integrity measurement calculations are performed in highly obfuscated native code, rendering decompilation and analysis extremely difficult.
- **No Memory State Reliance:** The integrity measurement is performed in a standalone way as an atomic execution blob without reliance on input memory state that could be tampered with in any way.
- **No Reliance on External Libraries:** The core integrity measurement process has no reliance on any external system library that could be tampered with.
- **Self Measurement:** The integrity measurement includes both the app package and the integrity measurement algorithm itself. Thus any change to the measurement algorithm will be detected.
- **Runtime Address Integration:** Runtime addresses generated by the running of the measurement algorithm are bound into the measurement calculation, making the reproduction of the results from

anything other than the original unmodified binary code extremely difficult.

- **Root and Debug Detection:** The SDK checks for rooted devices or debug attachment so that suspicious devices can be detected and rejected. The detections are included in the core algorithms and their code and generated results are subject to the measurement to avoid any tampering.
- **Framework Detection:** The SDK checks the memory map of the running process for the presence of instrumentation frameworks that might be being used by attackers to gain insight into the operation of the algorithm.

How Communication Between the CLI and the Approov Service is Protected

Communication between the Approov CLI and the Approov cloud service is always conducted using TLS, and the security of this is subject to the certificate trust store installed on your local machine. Ordinarily if this were to be compromised then it would be possible for a Man-in-the-Middle (MITM) attacker to intercept, modify and then spoof requests to the Approov cloud service. The password mechanism provides protection from such compromises, as it provides an additional level of message integrity over and above TLS. It employs asymmetrically encrypted integrity tokens with a proof of password possession protocol to transmit this information, ensuring that an attacker cannot spoof these integrity tokens without knowledge of the password.

If a CLI command is issued that uses a password protected role, then the user will be invited to provide the password before they can continue. Once the password is correctly entered this initiates an active session that lasts for one hour. During that time it is not necessary to enter the password again in order to issue CLI commands. The current session information is stored in a .approov file in your home directory.

Access to Approov: User Authentication and Authorization in Approov

Activating your account grants access to your Approov account from your machine via a time limited onboarding code.

You will normally be invited to choose a password for your access to Approov. If your onboarding included a dev role then this will be automatically selected for subsequent uses of the Approov CLI. You will be invited to type in the password again on first usage, and after every one hour session expires.

Note that you are also provided with a PIN number. You should make a note of this somewhere private and secure, it will be needed if you ever need to recover access to your account via email. The PIN provides an additional level of protection for your Approov account in case access to your email account is compromised.

User and Password Management

When a new account is created the account holder is issued with dev and admin roles. One the capabilities of the admin role is the ability to add new users, with specific roles.

In a larger organization where multiple personnel need to interact with the Approov service, we expect that there will be some internal control of the access to Approov. We recommend that only a single individual, or small restricted group, should have access to the admin role. We suggest that dev roles are created for each of the individuals that are involved in the development of the apps that use the Approov service. These tokens allow access to all of the facilities required for app development, without more dangerous privileges that might allow an accidental detrimental impact to apps that are live in production in the account. The dev user roles can be issued to named individuals, preferably for a timescale that represents their likely involvement. Access can be revoked by the administrator at any time.

More info here

Application End User Data Stored by Approov and How it is Protected

No data (PII or other) that your application creates or captures from your users, or is accessible via your service APIs, is stored or used by Approov.

When a client signs up for an Approov account, we collect and process information about their end users; specifically, a unique app instance identifier (Install ID) and a (non-reversible) IP address. Note that Install ID is referred to as Device ID in the Approov documentation. Install IDs and IP addresses are masked to afford data subjects reasonable anonymity and to assure their rights to privacy are bal-

anced with the legitimate business interest of our clients to protect their assets through our software and services. If you use an app that is using the Approov service, then we will retain the above data as long as the Approov account, with which the app is registered, is active. We will also continue to retain this personal data after the account is terminated if it is necessary for tax and financial reporting purposes or to comply with our legal obligations. See here for the full Approov privacy policy.

Service Performance Data Stored by Approov and How its Protected

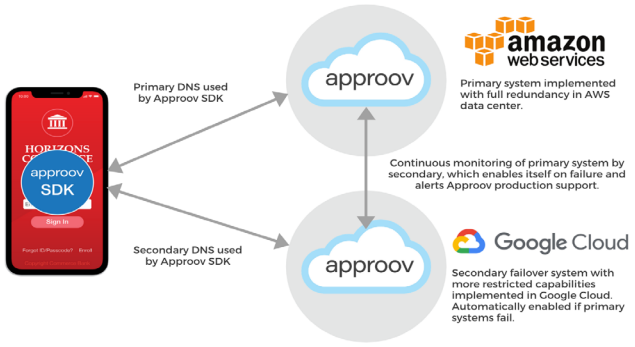
All data stored by Approov is encrypted at rest and in transit.

Approov stores data which is required to operate the service and provide reporting about the performance of the service. The following customer data is stored:

- **Application signatures:** The Approov tool analyzes the app (in either .apk, .aab or .ipa format) and adds its signature to a database in the Approov cloud service for your account. The particular build of the app then becomes recognized as being official, allowing valid Approov tokens to be generated for calls from that app. No app code is stored or used by Approov.
- **Service Performance data:** Data about the operation of the service is stored and processed by Approov in order to present analytics and provide performance dashboards to each Approov customer about the operation of their service. All access to such data is via signed JWT management tokens with a different signing secret for each Approov account holder. Tokens provide an account holder field and the tokens only provide rights to access data associated with that account holder. Approov uses agglomerated data only for monitoring overall system health status via aggregated metrics and these are only used internally and accessible only to accredited Approov personnel.

Cloud Server Redundancy

To enable a highly reliable Approov service, the backend is implemented in two different cloud service providers, as illustrated below:



When an Approov token fetch is requested, the initial transmission is sent to the primary token service hosted in the AWS cloud. This primary service has multiple frontend servers deployed across the availability zones of a region and is set up to automatically scale with the service load. The particular geographic data center utilized is allocated upon sign up. Some accounts may also have support in multiple different geographic data centers to lower latencies in different parts of the world and to offer further enhanced redundancy.

If communication cannot be established with the primary service (or errors are continually returned) then the SDK attempts to make contact with the secondary (aka failover) system. This is available on a different domain name using a different TLD (Top Level Domain) to further enhance redundancy. The secondary failover system is implemented in Google Cloud to provide complete isolation from any large scale failures that may occur in AWS. The failover system only provides a subset of the full analysis capability of the primary system, but it will ensure your apps should continue to receive valid Approov tokens in the event of a catastrophic primary system failure.

The failover system only serves Approov tokens if it is enabled. It continually checks the primary system on a minute-by-minute basis and automatically enables itself if a primary failure is detected, with no need for any manual intervention in the switch over process.

How Real-time Operation of the Service is Protected

Only Approov account holders are able to generate SDK configurations that are signed for that account holder, so only they are able to generate SDK configurations that are valid.

The JWT for the SDK configuration is signed using asymmetric Elliptic Curve Cryptography (ECC). The public key is in the configuration, but the private key is held securely in the Approov cloud service. This means that only the Approov cloud service is able to generate valid configurations. They cannot be manually modified as any tampering will be detected. The public key is transmitted by the SDK to the Approov cloud service, so any attempt to modify the public key and re-sign the configuration will also be detected.

In addition to the use of standard TLS encryption to protect your traffic from prying eyes, you will automatically benefit from using the Approov built-in dynamic certificate pinning service to implement, manage and maintain certificate pinning for you. This provides continuous protection against bad actors reading/modifying your transactions, while also addressing any concerns that you have not implemented pinning correctly or that you may block your the users of the mobile app when certificates are rotated in the API server. Approov dynamic certificate pinning leverages the built-in Approov dynamic configuration to keep your mobile app up to date with the latest pins from your API server certificates. More information about the pinning approach is provided in Public Key Pinning.

In order to support over-the-air dynamic updates to the configuration, the Approov cloud service can send an update if API domains or their pins (or some other parameter) is changed. Updates are also signed using ECC and the signature is checked against the public key provided in the initial base configuration. This prevents any tampering of the configuration in the communication channel.

The normal lifetime for an Approov token is 5 minutes, plus a grace period, from the point of issue by the Approov cloud service. The grace period of a few seconds is added to allow a valid token to be propagated and checked within a backend API system. If a particular device is identified as being risky in some way (such as it being rooted or jailbroken), then, independently of the overall security rejection policy that is set, it will receive a shorter lived 2 minute token instead of a 5 minute one. This forces the device to make more frequent checks as it receives tokens.

The app itself should never cache Approov tokens that it gets from the Approov SDK. Instead, a fresh call to `fetchApproovToken` or `fetchApproovTokenAndWait` should be made each time an Approov token is required.

If a token has already been fetched, and is not yet expired, then it will be returned immediately. However, each fetch call does some basic app environment checking and, if issues are discovered, performs a complete attestation check to fetch a new token. Thus an Approov token lifetime should be considered to be *up* to 5 minutes, since any cached token may be discarded at any point.

How Approov can be integrated into your Compliance Reporting

Metrics graphs provide both live and longer term summary information about your account usage. They can be used to see the total number of devices that have requested Approov tokens over a time period (and therefore what the usage related costs will be) and also show the failures where particular devices have been denied valid Approov tokens. The graphs provide information about the reasons for any such failures.

Approov provides facilities that allow monitoring of the status of your account. A healthcheck API endpoint is supported, along with monthly or daily summaries of usage and notification emails if there is a certificate problem with one of your endpoints.

The Approov cloud service is able to monitor your API endpoints to ensure that they are both accessible and that the certificates presented match one or more of the pins you have set in your account. The endpoints are checked every 15 minutes, and a notification email is sent if a problem is detected. This will list each of the monitored API domains that are experiencing an issue.

Applying end-user device policies: Approov provides fundamental checks regarding the integrity of the app itself, so that valid Approov tokens are only issued to valid app instances. Additionally, various other runtime integrity checks are also performed and the results transmitted to the Approov cloud server in a secure manner. Whether these checks should result in an invalid Approov token or not is determined by the security policies that are selected.

This gives you the flexibility to permit or block access according to your risk assessments and the characteristics of your user base. For instance, if you develop a banking app, you may take the view that no rooted device should receive a valid Approov token. However, other consumer apps, deployed to certain markets or demographics, may require rooted devices to be accepted. Thus the security stance must be informed by the characteristics

of the app's user base and the particular threats that Approov is being used to defend against.

Approov Compliance and Certifications

As a company which provides security solutions, Approov ensures compliance with industry and regulatory standards while conforming to leading security benchmarks.

Approov monitors the industry for regulatory developments and changes that may impact our organization and services. This allows us to proactively plan for upcoming compliance requirements and take the appropriate steps to ensure our adherence to these requirements.

Approov is committed to offering services that are compliant with the E.U. General Data Protection Regulation ("GDPR"). Data that a customer or its users send to us is only processed in accordance with the customer's instructions and our GDPR-updated data processing agreements. See here for the full Approov privacy policy.

The Approov service is deployed in AWS and Google Cloud which both meet the requirements of an extensive list of global security standards such as SOC, PCI, HIPAA, FedRAMP, HITRUST. Learn about AWS Compliance here and Google Cloud here. No data is stored on-premises by Approov.

We use a PCI DSS Level 1 certified service provider to handle all sensitive customer billing data.