BRANDING, PRIVACY-LINK AND AUTHENTICATION WARNING · CLOUD CLIENTS AND AUTHENTICATION

Google-branded apps. Privacy promises contradicted by shipped code.

A Google Photos client promises not to request full Google Drive access, yet a shipped sign-in branch passes that very permission to Google. Gmail, Docs and Photos also ship app-controlled Google login paths that conflict with Google's browser policy; alongside buyer refund complaints and Google-associated branding, these findings warrant urgent Apple review.

Apple developer account examined: **滿 李 / MAN LI · Shield Apps · 1653727587**

By Alex Kleber · Published 2026-11-19 · Updated 2026-11-19

VISUAL EVIDENCE

Google colours can suggest a Google product. This seller is Shield Apps.

The current Gmail and Photos icons use Google-associated colours alongside Google product names. Compare the originals: the icons are not exact copies. Docs has changed since our earlier capture; Drive and Dropbox use generic cloud icons.

Independent client · Shield Apps



Shield Apps Gmail client. Original current Apple artwork; diagonal red, yellow, green and blue bands. E1; E2.

Official reference · Google

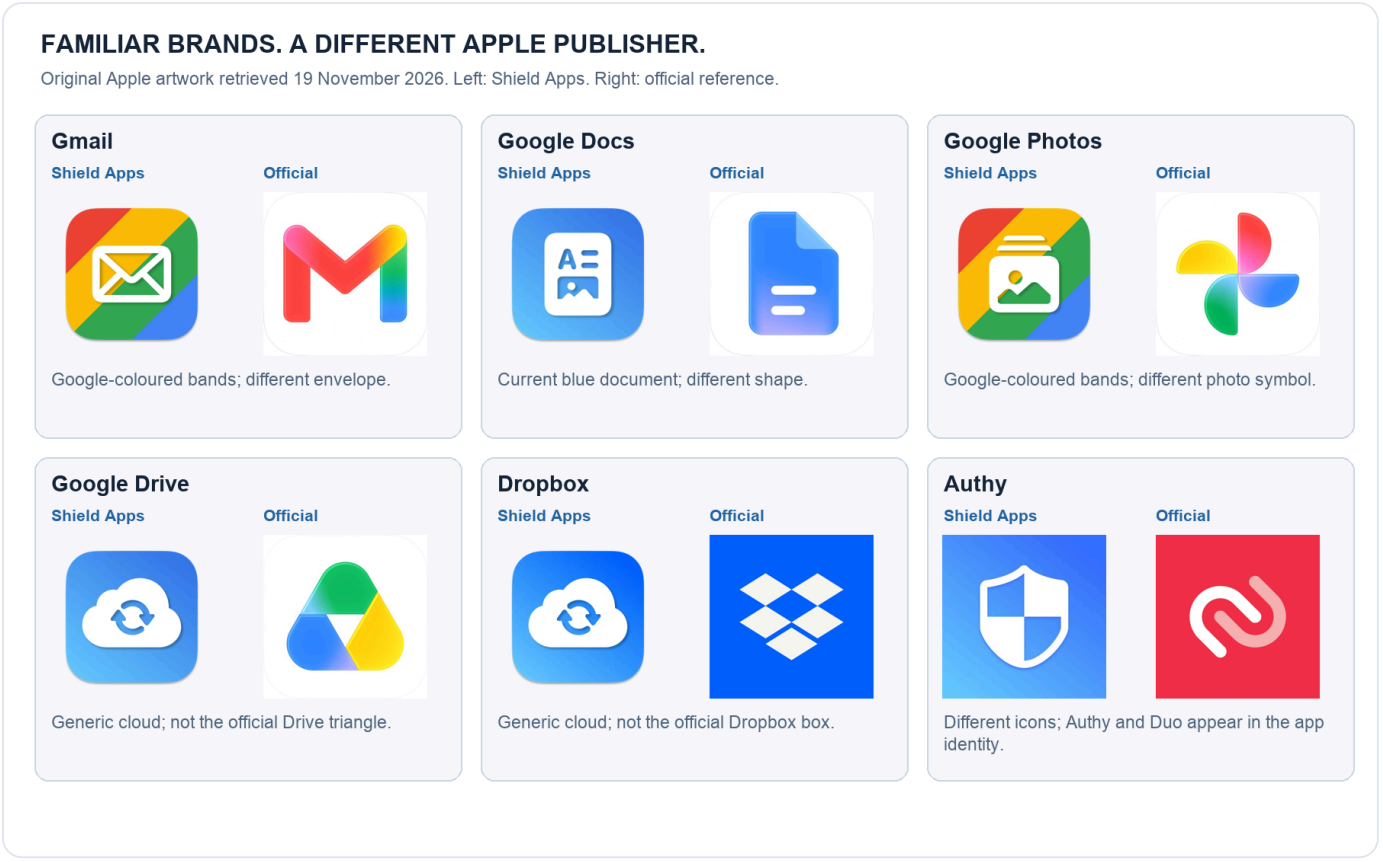


Official Gmail by Google. Original current Apple artwork: the multicolour M, visibly different from the client icon. E17.

Compare the branding before deciding what was copied.

The same seller uses different kinds of branding. Gmail and Photos use the Google palette; the current Docs icon is blue. The authenticator's name carries Authy, while its recorded subtitle adds Duo. Drive and Dropbox use a shared generic cloud icon, not the official product symbols.

The current Dropbox promotion also displays the Dropbox mark and a #1 Dropbox App badge. No market, date or ranking source is stated in that image. That is a specific promotional claim for Apple to substantiate, separate from the generic cloud icon.



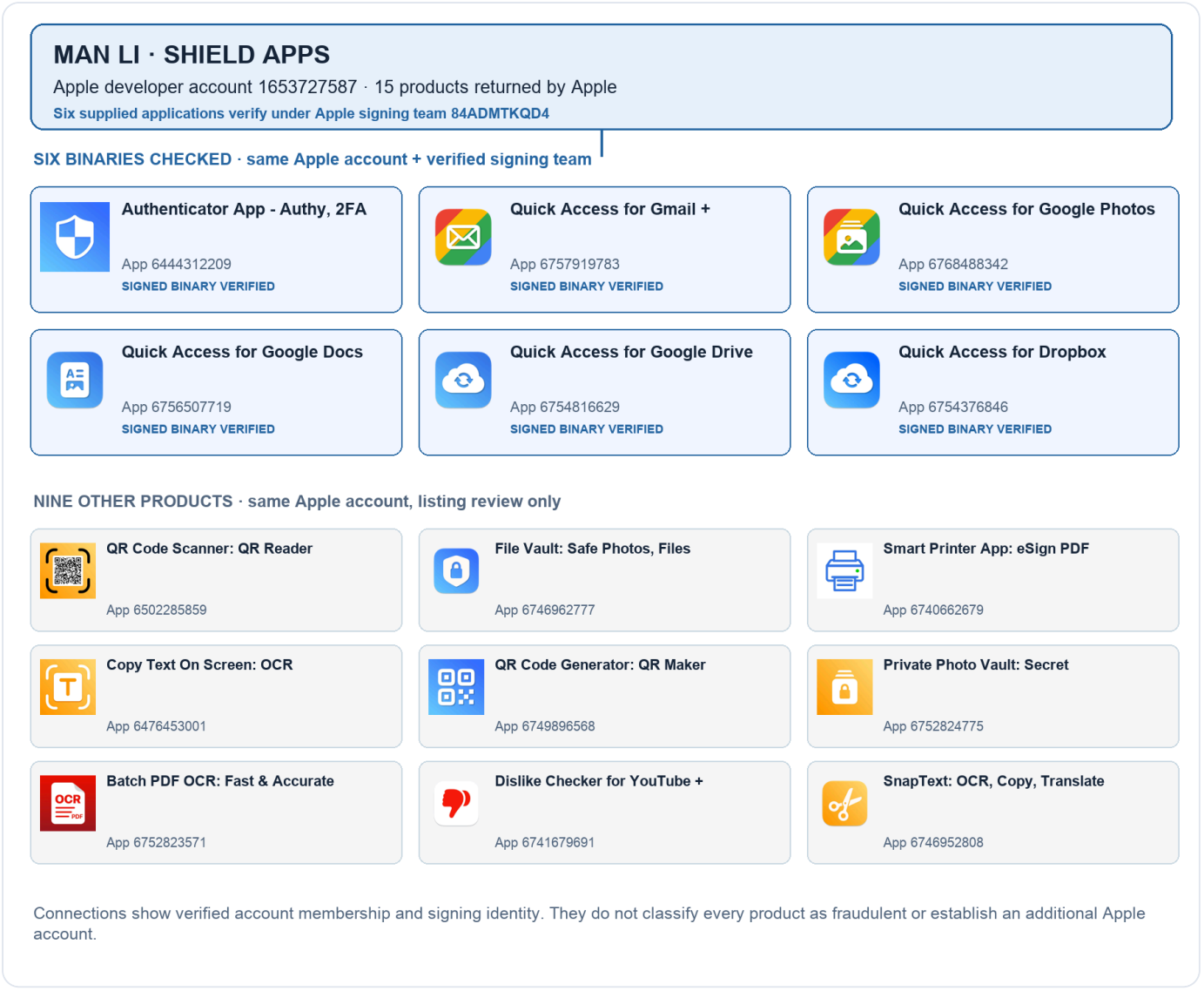
Editorial comparison composed from original current Apple icons. Six independent Shield Apps products on the left of each pair; verified official references on the right. Similar colours, exact names and visibly different icon shapes are distinguished. E1; E17; E51.

E1; E17; E21; E22; E51.

One Apple account connects all 15 products.

The account membership is direct: Apple gives every product the same numeric publisher ID. The supplied six binaries add a second check: their Apple signatures validate under the same signing team. There is no need to infer this connection from similar colours or a shared free website.

Nine other utilities were reviewed at listing level. They belong on the account map, but this investigation does not label every QR, OCR, printer or vault tool an impersonation app. No additional Apple account was established by the binary comparison.



Original product icons and exact app IDs. Blue cards mark the six supplied binaries verified under team 84ADMTKQD4; grey cards identify nine further products returned by the same Apple publisher catalog. This is account membership, not a blanket fraud classification. E1; E31–E36; E52.

Open MAN LI / Shield Apps Apple account 1653727587

E1; E31–E36; E52.

What Apple should review, and why.

Apple should urgently examine the Photos permission promise against the shipped sign-in argument, and the three app-controlled Google login paths against Google's explicit browser rule. These are specific code and disclosure issues. The branding assessment, buyer complaints and unsupported ranking badge add separate grounds for review.

Current Apple rules mapped to specific evidence

Apple rule	Evidence and assessment
5.1.1 / 2.3 · Privacy and accurate metadata	Photos policy denies full Drive access, while one shipped SDK sign-in branch passes that scope. Review the reachable production branch and disclosures. E40; E49.
5.2.2 · Third-Party Sites/Services	Gmail, Docs and Photos ship app-owned Google OAuth window paths that conflict with Google's secure-browser rule. Gmail and Docs additionally promise Google security best practices. Verify the production route and applicable service authorization. E19; E37–E39; E41; E47.
5.1.1(i) · Privacy policies	Gmail's App Store Privacy Policy link uses a non-resolving .cc hostname. The working .top page does not repair that actual button. Directly reproduced link failure. E2; E24; E47.
2.3.7 · App names, keywords and subtitles	Authy in the authenticator name plus Duo/Authy in its dated Mac subtitle; current Dropbox promotion has an unqualified #1 Dropbox App badge. Review keyword presentation and substantiate that ranking claim. E1; E4; E51.
4.1 / 5.2.1 · Copycats and intellectual property	Assess Google-associated colours, product names and reproduced marks in promotions together with the existing disclaimers. Different original icon shapes and legitimate compatibility references are preserved. E17; E21; E22.
2.3.2 · In-app purchase disclosure	The Drive reviews include objections to the upgrade presentation. A transaction and checkout reproduction would be needed to establish the exact purchase flow; a paid client alone is not a violation. E25.

Apple App Review Guidelines **Google OAuth policies · Use secure browsers**

E19; E20. No Apple enforcement decision or legal infringement judgment is claimed.

The strongest evidence: promises versus shipped code.

The Photos finding concerns access to a person's files, not just an app icon. Its policy rules out full Drive access, while an actual SDK call in the supplied executable includes that permission. Google describes this as permission to view and manage all Drive files. Whether a real user reaches and approves that branch still needs a controlled production check.

The Gmail and Docs policies also say their authorization follows Google's security best practices. Their shipped app-controlled login paths conflict with Google's express ban on embedded authorization browsers. The same architecture was traced in Photos. This establishes a concrete implementation and disclosure mismatch; it does not establish password theft.

What is promised, what is evidenced, and why it matters

Claim or presentation	Verified evidence	Consequence for the user
Photos: no full Google Drive access requested.	A shipped Google Sign-In branch passes the full Drive scope. E40; E49; E53.	If used and granted, the permission reaches Drive files beyond the Photos upload feature.
Gmail / Docs: Google security best practices.	Their own embedded OAuth controllers load Google's authorization request; Photos has an equivalent path. E19; E37–E39; E41; E47.	The app controls the login browser. Google explicitly prohibits this authorization architecture.
Dropbox promotion: "#1 Dropbox App".	Original Apple artwork has that badge without a market, period or ranking source. E4.	An unsupported apparent ranking can influence trust and purchase decisions.
Drive purchase experience.	A dated Apple review reports paying about $20 and requests a refund. Other negative and positive reviews are retained. E25.	The buyer complaint warrants checking the actual upgrade and refund flow; it is not a transaction we reproduced.

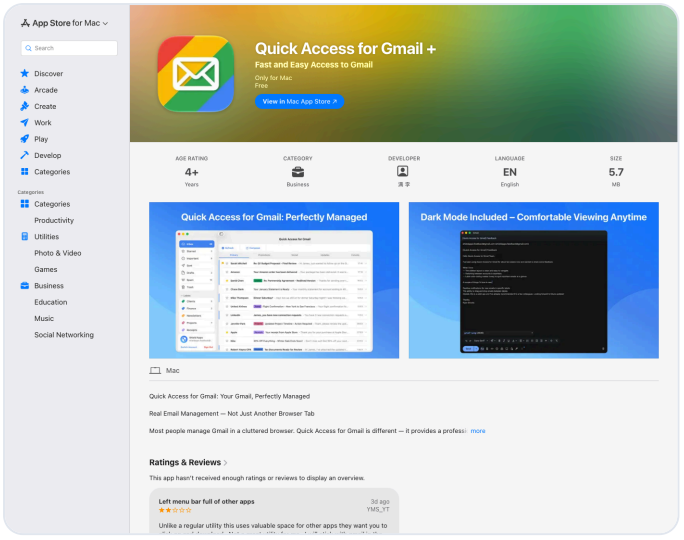
Photos policy: section 2, Google permissions **Google: use secure browsers** **Google: the full Drive scope**

E4; E19; E25; E37–E41; E47; E49; E53. Compiled code, retained developer policies and attributed Apple reviews are distinct evidence types.

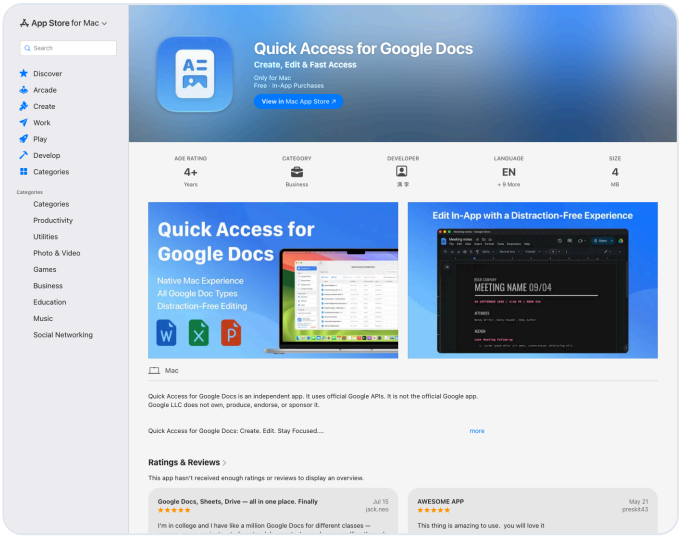
LOOK FOR YOURSELF

The screenshots tell the story.

Original Apple product artwork and dated captures support the branding assessment. The code images are explicitly labelled extraction panels; they are not screenshots of an app we ran.

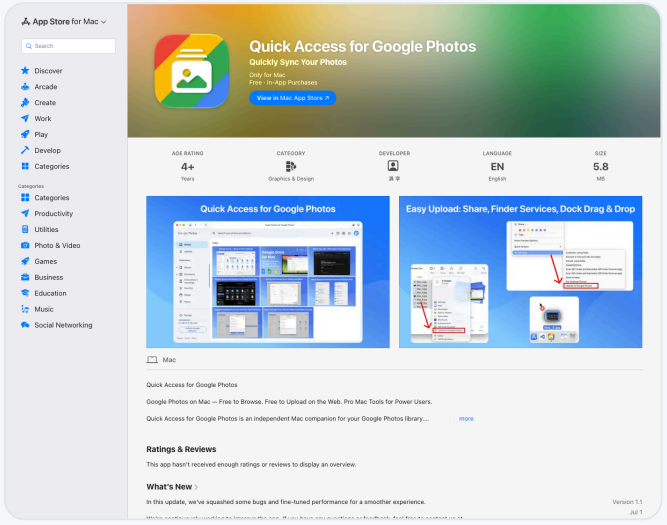


Apple public listing rendered from the successful retained 19 November HTML response, with original external artwork. This is the developer's public presentation, not a running-app test. 6757919783.

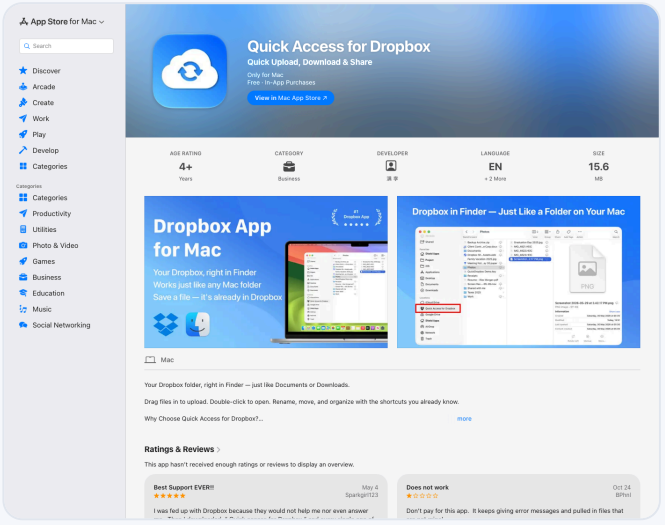


Apple public listing rendered from the successful retained 19 November HTML response, with original external artwork. This is the developer's public presentation, not a running-app test. 6756507719.

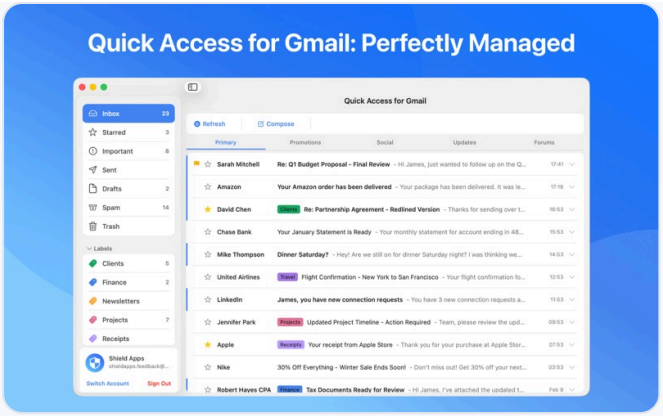
▼ See all 17 additional screenshots



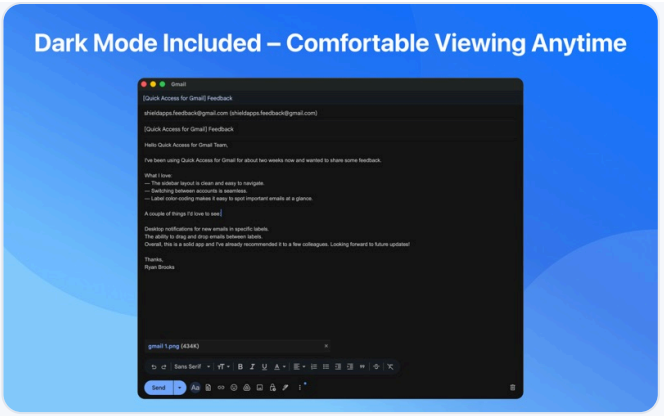
Apple public listing rendered from the successful retained 19 November HTML response, with original external artwork. This is the developer's public presentation, not a running-app test. 6768488342.



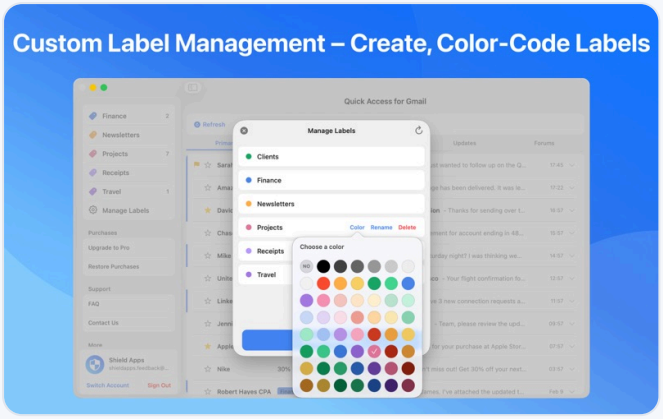
Apple public listing rendered from the successful retained 19 November HTML response, with original external artwork. This is the developer's public presentation, not a running-app test. 6754376846.



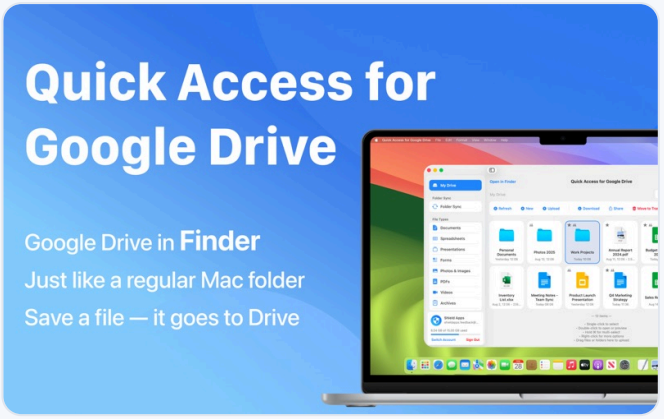
Quick Access for Gmail + · original Apple promotional image 1, retrieved 19 November 2026. Developer-supplied marketing; not an independently tested feature.



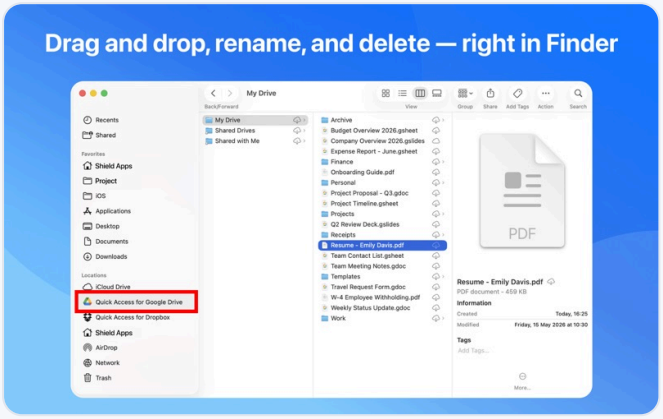
Quick Access for Gmail + · original Apple promotional image 2, retrieved 19 November 2026. Developer-supplied marketing; not an independently tested feature.



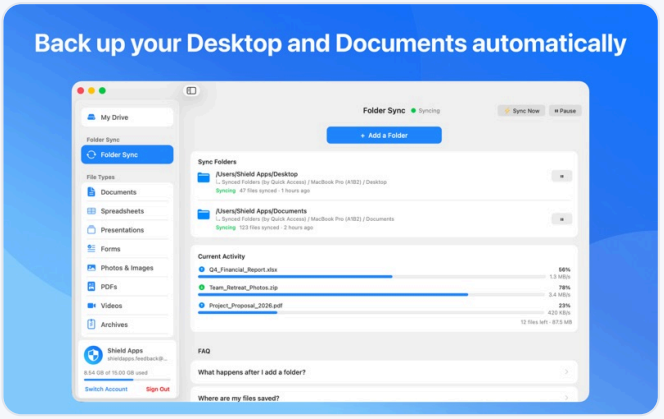
Quick Access for Gmail + · original Apple promotional image 3, retrieved 19 November 2026. Developer-supplied marketing; not an independently tested feature.



Quick Access for Google Drive · original Apple promotional image 1, retrieved 19 November 2026. Developer-supplied marketing; not an independently tested feature.



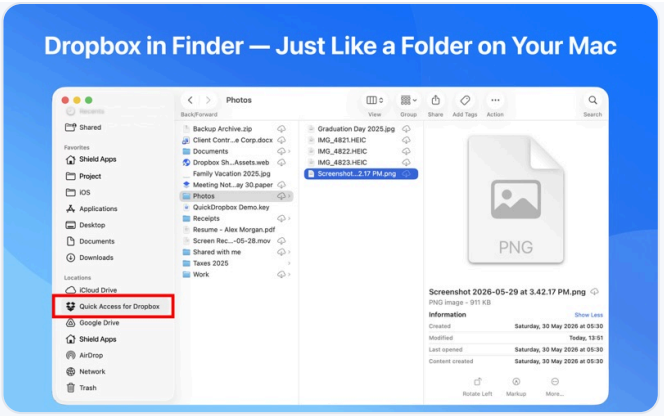
Quick Access for Google Drive · original Apple promotional image 2, retrieved 19 November 2026. Developer-supplied marketing; not an independently tested feature.



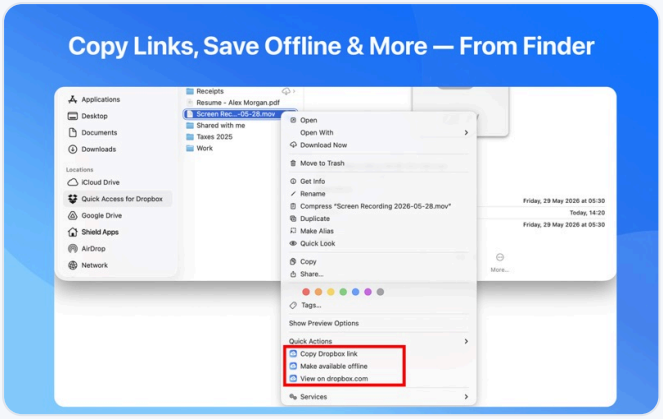
Quick Access for Google Drive · original Apple promotional image 3, retrieved 19 November 2026. Developer-supplied marketing; not an independently tested feature.



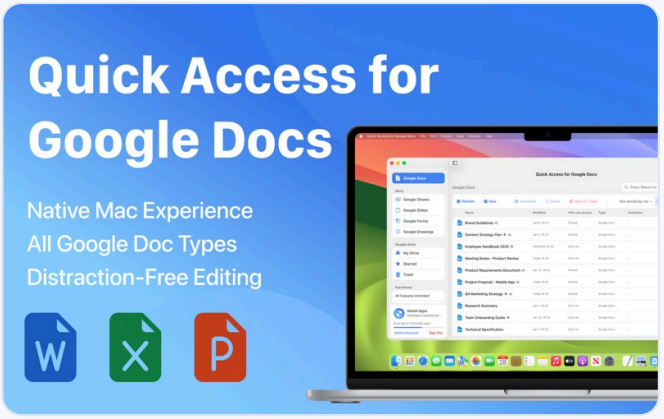
Quick Access for Dropbox · original Apple promotional image 1, retrieved 19 November 2026. Developer-supplied marketing; not an independently tested feature.



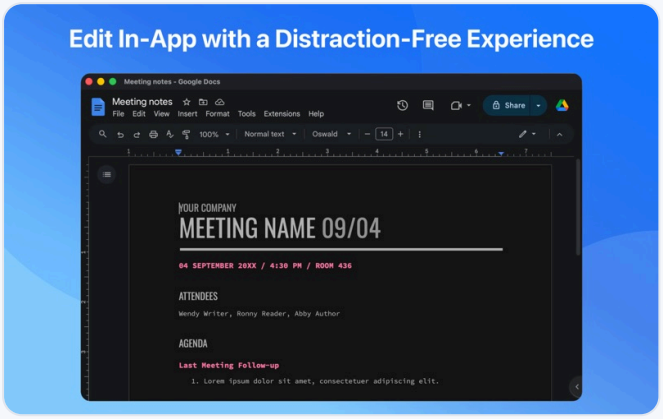
Quick Access for Dropbox · original Apple promotional image 2, retrieved 19 November 2026. Developer-supplied marketing; not an independently tested feature.



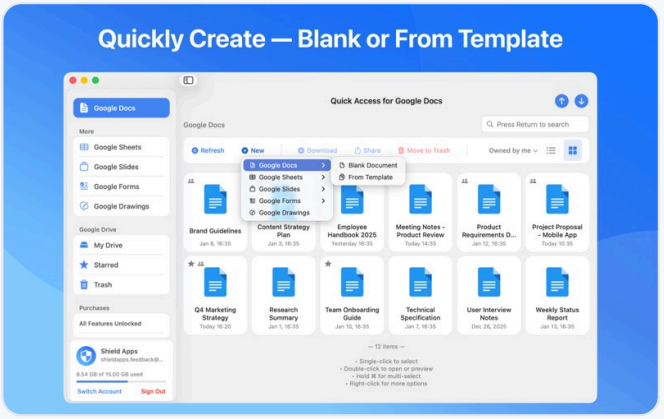
Quick Access for Dropbox · original Apple promotional image 3, retrieved 19 November 2026. Developer-supplied marketing; not an independently tested feature.



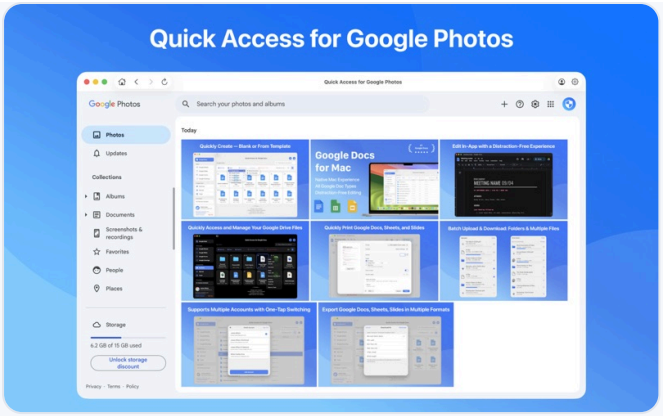
Quick Access for Google Docs · original Apple promotional image 1, retrieved 19 November 2026. Developer-supplied marketing; not an independently tested feature.



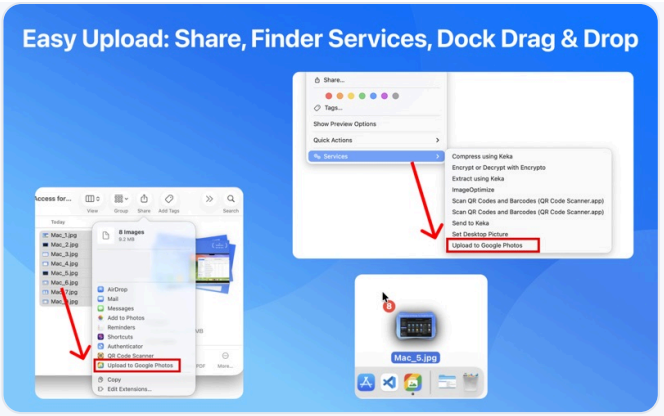
Quick Access for Google Docs · original Apple promotional image 2, retrieved 19 November 2026. Developer-supplied marketing; not an independently tested feature.



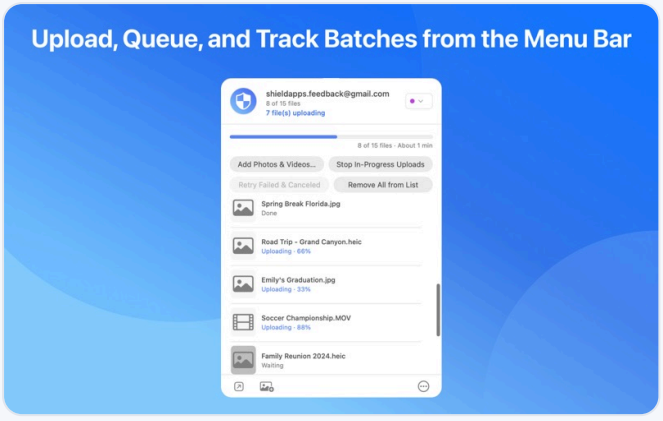
Quick Access for Google Docs · original Apple promotional image 3, retrieved 19 November 2026. Developer-supplied marketing; not an independently tested feature.



Quick Access for Google Photos · original Apple promotional image 1, retrieved 19 November 2026. Developer-supplied marketing; not an independently tested feature.



Quick Access for Google Photos · original Apple promotional image 2, retrieved 19 November 2026. Developer-supplied marketing; not an independently tested feature.



Quick Access for Google Photos · original Apple promotional image 3, retrieved 19 November 2026. Developer-supplied marketing; not an independently tested feature.

WHAT YOU NEED TO KNOW

A familiar name is not a substitute for knowing who controls the software.

01

Photos promises limited access. A shipped sign-in branch asks for all of Drive.

The Photos privacy policy expressly denies requesting full Google Drive access. QuickPhotos 1.1 passes the full Drive permission into a Google Sign-In SDK call. If that route is used and the permission granted, it covers files across Drive, far beyond uploading photos. A separate narrow Photos route also exists; live route selection and user consent were not observed.

E40; E49; E53

E40 E49 E53

02

Three shipped Google login paths conflict with Google’s browser rule.

Gmail, Docs and Photos each contain an app-owned OAuthWebViewController that loads Google’s authorization request into WKWebView. Google prohibits directing its authorization request to an embedded browser controlled by the app. The Gmail and Docs policies nevertheless promise authentication following Google’s security best practices. The compiled paths are verified; a completed login and captured passwords are not.

E19; E37–E39; E41; E47

E19 E37 E38 E39 E41 E47

03

A Drive buyer reports an unwanted $20 purchase and asks for a refund.

The 14 November Apple review describes paying about $20, difficulty using the app and a refund request. Other Drive reviewers describe upgrade prompts or functionality problems. These are concrete consumer complaints to investigate, with positive reviews also retained; the investigation did not reproduce a charge or establish payment fraud.

E25; E26; E28; E29; E30

E25 E26 E28 E29 E30

04

Four independent Google-named apps present a misleading-branding concern.

In our assessment, the four Google clients’ names and presentation can mislead users about Google endorsement. Gmail and Photos use Google’s familiar colour palette; Docs previously used a multicolour icon and now uses blue. The current Drive and Docs icons differ from Google’s originals. The assessment considers the combined presentation, including the developer’s independence disclaimers.

E1–E5; E12; E17; E21; E51

E1 E2 E3 E5 E12 E17 E21 E51

05

The Dropbox promotion uses an unqualified “#1 Dropbox App” claim.

The original promotion reproduces the Dropbox mark and claims #1 Dropbox App without stating a market, period or ranking source. This is a concrete marketing claim for review, not a verified chart position. The app’s independence disclaimer elsewhere is preserved.

E1; E4; E22

E1 E4 E22

06

A broken privacy button is a directly reproduced problem.

Apple's Gmail privacy button points to www.shieldapps.cc, which currently returns a DNS non-existence result. The working policy is on shieldapps.top. A buyer using the App Store button cannot read that policy through the linked address.

E2; E24; E47

E2 E24 E47

07

Authy/Duo keywords and Google-coloured marketing deserve review.

The independent authenticator uses Authy in its title and Duo in its recorded subtitle. Gmail and Photos combine Google service names with the Google palette. These can suggest familiar brands; original comparisons and existing independence disclaimers are shown rather than treating all icons as identical copies.

E1; E2; E12; E17; E21; E51

E1 E2 E12 E17 E21 E51

08

One verified account, not a discovered second account.

All 15 products share Apple developer 1653727587. All six supplied apps have signing team 84ADMTKQD4. A comparison against 36 distinct older executables found no matching team, support identity, domain or extracted OAuth-client identifiers outside this case.

E1; E31; E32; E33; E34; E35; E36; E52

E1 E31 E32 E33 E34 E35 E36 E52

WHAT IT COSTS

What the paid listings actually show

Listed US purchases, not completed charges. A paid third-party client is not automatically fraudulent. Lifetime here is an app licence; no claim is made that it funds an external metered AI service. No weekly offer is recorded for these six apps.

Prices displayed in the saved listing

Purchase option	United States	Ireland
Google Drive · listed in current catalog description	$14.99 yearly; $19.99 lifetime	Not freshly checked
Google Docs · current US page	$14.99 yearly; $19.99 lifetime	Not freshly checked
Google Photos · current US page	$14.99 yearly; $19.99 lifetime	Not freshly checked

Purchase option	United States	Ireland
Dropbox · current US page	$4.99 monthly; $9.99 yearly; $19.99 lifetime	Not freshly checked
Gmail · current US page	Free; no purchase table displayed	Not freshly checked
Authenticator · earlier Mac purchase table, 13 November	$4.99 monthly; $9.99 / $14.99 yearly; $29.99 / $39.99 lifetime	Earlier record; no new checkout test

WHO IS BEHIND IT?

The name on the listing.

App name

Quick Access for Google Drive, Gmail, Docs, Photos and Dropbox; Authenticator App - Authy, 2FA

Developer / seller

满 李 / MAN LI / Shield Apps

Developer country · App ID 6754816629

Unknown · No app-specific registered business country established

The prior EU provider panels do not give an address. The publisher domain has a CN / Hubei registry indicator, which is kept separate from an Apple business-country attribution.

Developer country · App ID 6757919783

Unknown · No app-specific registered business country established

The prior EU provider panels do not give an address. The publisher domain has a CN / Hubei registry indicator, which is kept separate from an Apple business-country attribution.

Developer country · App ID 6756507719

Unknown · No app-specific registered business country established

The prior EU provider panels do not give an address. The publisher domain has a CN / Hubei registry indicator, which is kept separate from an Apple business-country attribution.

Developer country · App ID 6768488342

Unknown · No app-specific registered business country established

The prior EU provider panels do not give an address. The publisher domain has a CN / Hubei registry indicator, which is kept separate from an Apple business-country attribution.

Developer country · App ID 6754376846

Unknown · No app-specific registered business country established

The prior EU provider panels do not give an address. The publisher domain has a CN / Hubei registry indicator, which is kept separate from an Apple business-country attribution.

Developer country · App ID 6444312209

Unknown · No app-specific registered business country established

The prior EU provider panels do not give an address. The publisher domain has a CN / Hubei registry indicator, which is kept separate from an Apple business-country attribution.

App Store listing ↗

▼ App ID, version and other identifiers

App Store ID

6754816629 / 6757919783 / 6756507719 / 6768488342 / 6754376846 / 6444312209

Bundle identifier

Six exact bundle IDs are listed in the binary table.

Version

First released

Six supplied versions: Drive 3.5.4; Gmail 1.3; Docs 1.5; Photos 1.1; Dropbox 2.2.2; authenticator Mac 3.7.8	**Different per app; no neutral-launch-to-branding sequence established here.**

Do these apps use APIs, web pages or both?

The four Google clients combine real compiled API request paths with embedded web interfaces. We traced Drive and Docs constructing file-list queries, Gmail constructing message-list queries, and calls that submit those queries with completion handlers. Photos builds an upload request, attaches its body and starts the fetch; it also has a media-item creation request. An API is a service connection used by software; a WebView is a browser built into an app.

Google OAuth is also implemented as executable request logic. In all four clients, code builds a request to Google's token endpoint, sets a request body, creates a network task and starts it. The authorization code also contains PKCE, a protection used during the exchange. These are compiled implementation findings. A successful Google response, a completed user login and Google verification status were not observed.

The branding assessment and the engineering findings are separate. Genuine API integration does not make an app an official Google product or establish permission to imply endorsement. The specific Google-policy issue is the app-controlled embedded OAuth path traced in Gmail, Docs and Photos; using a WebView for ordinary document editing is not that same finding.

What the supplied code supports — static inspection, not a completed service test

Application	API integration	Embedded web content	Authorization
Quick Access for Google Drive	Drive file-list query construction and executeQuery call sites; native file management and Finder extensions. E33; E55.	Docs, Sheets, Slides and related Google web editors.	Google OAuth endpoints, token management and Google sign-in components. An equivalent custom embedded OAuth controller was not established for this app.
Quick Access for Google Docs	Drive file-list query construction, fields/filter configuration and executeQuery call sites. E32; E55.	Google Docs and related document editors.	Google OAuth with token/PKCE code; an app-owned OAuthWebViewController path was traced.
Quick Access for Gmail +	Gmail message-list query construction, filtering and executeQuery call sites. E35; E55.	Gmail website views.	Google OAuth with token/PKCE code; an app-owned OAuthWebViewController path was traced.
Quick Access for Google Photos	Photos upload and media-item creation requests: request body is attached and beginFetch is called. E36; E55.	Google Photos website.	Google OAuth with token/PKCE code; embedded authorization and an alternative full-Drive SDK scope branch are separately documented.
Quick Access for Dropbox	Dropbox v2 and SwiftyDropbox.	Browser components are also present.	Dropbox authorization components; this is not a Google-client identity.
Authenticator App - Authy, 2FA	Local one-time-password and cryptographic components.	A web-view class is present; core OTP code is local.	No Google account OAuth login implementation was established for this app. It is not one of the four Google clients.

E31–E40; E54; E55. Compiled API and OAuth call sites are verified; service responses and live route selection were not observed.

The API calls found in the supplied code.

The locations below let a reviewer check the actual instructions in the supplied signed executables. The first three rows resolve the query class, its configuration and the executeQuery selector within one compiled function. Photos uses explicit requests and a fetcher. All addresses refer to the ARM64 program in memory; they are not byte positions in the ZIP.

The code also constructs token-exchange requests to https://oauth2.googleapis.com/token and schedules them for transmission. The table identifies request and task instructions, without publishing client secrets, tokens or a user's account data.

Application code paths: API request construction and submission

App	Request construction	Submission evidence
Drive 3.5.4 / 558	FilesList class reference 0x1002b7288; query, page size, fields and filter are configured.	executeQuery selector 0x1002b7ed0, within function 0x1002b6e28–0x1002b7f48.
Docs 1.5 / 214	FilesList class reference 0x10000fee8; query, page size, fields and filter are configured.	executeQuery selector 0x1000100f8, within the same compiled function.
Gmail 1.3 / 121	UsersMessagesList class reference 0x10003b888; user, maximum results and filter are configured.	executeQuery selector 0x10003bb0c, within function 0x10003b4a8–0x10003bbc4.
Photos 1.1 / 49	Upload endpoint 0x10007f524; body data 0x10007f6d4. Batch-create endpoint 0x10008091c; body data 0x100080ebc.	beginFetch selectors 0x10007f770 and 0x100080f58.

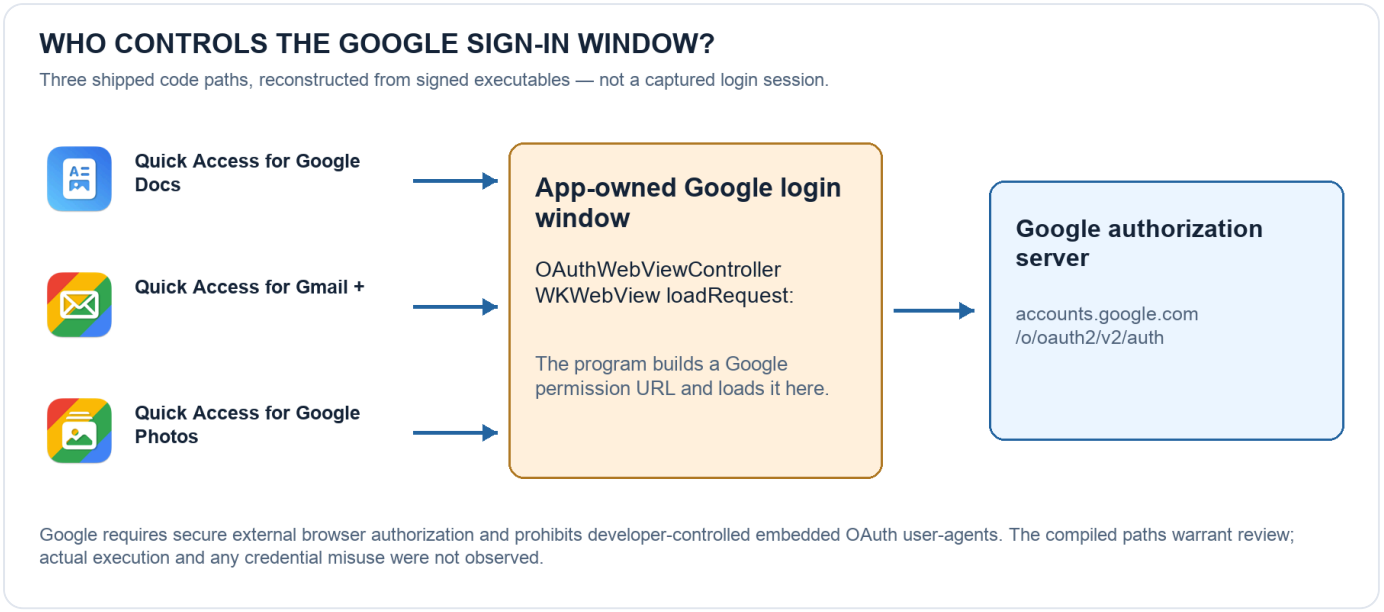
E55; signed executable hashes and versions are listed in the binary record. Selector references are analyst-resolved from original metadata; no runtime service success is claimed.

The Google sign-in window is part of the app’s code.

OAuth is the permission process used to connect an app to a Google account. We found the app’s own window controller building Google’s authorization address and loading the request into an embedded WebKit browser. For Gmail, its class lifecycle and browser construction are independently resolved; Docs and Photos have equivalent compiled controller paths.

The Gmail and Docs privacy policies promise Google Sign-In and OAuth authorization following Google’s security best practices. Google’s published policy specifically prohibits sending its authorization request through an app-controlled embedded browser. The compiled controllers therefore contradict that security assurance at the implementation level.

This matters because the application controls the embedded browsing environment. The finding identifies the architecture and an apparent policy mismatch; it does not establish captured passwords, a completed login or stolen data. Separate Google Sign-In SDK code also exists.



Static source-derived flow using original app icons. Gmail, Docs and Photos contain compiled app-owned Google authorization window paths. Arrows are code relationships, not a captured network exchange. E19; E37–E39.

EVIDENCE EXTRACT · 19 NOVEMBER 2026

The Google login request is loaded into an app-owned web view.

A concrete path in the shipped Gmail client; equivalent controller paths were found in Docs and Photos.

```
File: QuickEmail.app/Contents/MacOS/QuickEmail
Version 1.3 / build 121
Bundle: com.shieldapps.quickemail
SHA-256: 38c5e696fe5c8d4e778b5a1414170e6f74f71192ced745fe2b39d093dfe89aaf

Class metadata:
_TtC10QuickEmail22OAuthWebViewController
viewDidLoad implementation: 0x100088170
viewDidAppear implementation: 0x1000881dc

Google authorization URL loaded by this controller:
0000000100088a60        adrp    x8, 361 ; 0x1001f1000
0000000100088a64        add     x8, x8, #0x430 ; literal pool for: "https://accounts.google.com/o/oauth2/v2/auth"

Compiled request-loading call:
0000000100088f54        adrp    x8, 502 ; 0x10027e000
0000000100088f58        ldr     x1, [x8, #0x2f8] ; resolved selector: loadRequest:
0000000100088f5c        mov     x0, x19
0000000100088f60        mov     x2, x20
0000000100088f64        bl      0x1001cd148 ; Objc message: _objc_msgSend

Browser construction in viewDidLoad helper:
0x100089af0 loads class reference 0x100283c28
dyld fixups identify that reference as WebKit/_OBJC_CLASS_$_WKWebView
0x100089b14 sends initWithFrame:configuration:
```

Read-only class metadata, ARM64 disassembly and Apple dyld fixups. The “resolved selector” annotation is added by our pointer resolver; instruction addresses and operands remain unchanged. This is rendered extraction output, not a live app screenshot. E37–E39.

Exact read-only Gmail evidence: source-relative executable path, SHA-256, app-specific class, URL reference, resolved loadRequest selector and WKWebView class binding. Selector annotations are analyst-added and labelled. No app interface or successful login is simulated. E35; E37.

Where the three embedded authorization paths were found

Signed app / version	Executable inside the .app	ARM64 code references
Gmail 1.3 · build 121	QuickEmail.app/Contents/MacOS/QuickEmail	Google URL 0x100088a64; loadRequest selector 0x100088f58; invocation 0x100088f64. E37.
Docs 1.5 · build 214	QuickDocs.app/Contents/MacOS/QuickDocs	Google URL 0x1000ae2a8; loadRequest selector 0x1000ae79c; invocation 0x1000ae7a8. E38.
Photos 1.1 · build 49	QuickPhotos.app/Contents/MacOS/QuickPhotos	Google URL 0x1000298ac; loadRequest selector 0x100029da0; invocation 0x100029dac. E39.

E19; E35–E39; E41; E47. ARM64 values are virtual code addresses, not universal-file byte offsets.

Photos: the privacy policy and a shipped SDK branch disagree.

The developer's Photos policy describes a narrow upload permission and says full Google Drive access is not requested. In QuickPhotos 1.1, a separate Google Sign-In SDK function prepares an additional-scope array containing the full Drive scope and passes it into the sign-in call. Google classifies this scope as restricted access covering all Drive files.

Full Drive permission is not limited to photos selected for upload. Google's scope reference describes access to view and manage all Drive files. If a user is taken through that branch and approves it, the authorization is broader than this product's published promise.

This is not a conclusion drawn from finding a spare text string. The one-element Swift array at 0x1001ea388 is decoded, bridged to an Objective-C array, and passed through register x4 as additionalScopes at invocation 0x10006c89c. Another compiled function calls this SDK route.

The binary also contains a narrower Photos append-only route. We did not observe which route a real user reaches or what appears on Google's consent screen. The supported finding is a shipped policy/code discrepancy requiring production-path verification.

EVIDENCE EXTRACT · 19 NOVEMBER 2026

The Photos policy and one shipped sign-in branch disagree.

The full Drive scope is passed to the Google Sign-In SDK in compiled code, beyond a standalone text match.

```
QuickPhotos policy, section 2:
“We do not request full Google Drive access for this product.”

Shipped executable: QuickPhotos.app/Contents/MacOS/QuickPhotos
Version 1.1 / build 49
SHA-256: d1bfe53009ea2f96b1acefc9a78193cf7739519d1bc91c11c182b4564e644442

SDK sign-in branch:
000000010006c798        adrp    x8, 252 ; 0x100168000
000000010006c79c        add     x8, x8, #0x930 ; literal pool for: "https://www.googleapis.com/auth/drive"
000000010006c7d4        adrp    x1, 382 ; 0x1001ea000
000000010006c7d8        add     x1, x1, #0x388
000000010006c7e8        bl      0x1001552f8 ; symbol stub for: _$sSa10FoundationE19_bridgeToObjectiveCSo7NSArrayCyF

Static Swift array at 0x1001ea388:
Element count: 1
Decoded first element: https://www.googleapis.com/auth/drive

Array is passed as additionalScopes (register x4):
000000010006c880        adrp    x8, 370 ; 0x1001de000
000000010006c884        ldr     x1, [x8, #0x460] ; resolved selector:
signInWithPresentingWindow:hint:additionalScopes:completion:
000000010006c894        mov     x4, x25
000000010006c89c        bl      0x100155fac ; Objc message: _objc_msgSend
```

A separate, narrower Photos append-only path also exists. Runtime branch selection and a real Google consent screen were not observed. This supports a policy/code review issue, not a claim that every user grants Drive access. E40; E49.

Developer policy excerpt beside independently decoded QuickPhotos SDK scope argument. The raw scope is supplied to a sign-in function; a narrower route also exists. No live consent, credential misuse or account access was observed. E40; E49.

Read the exact Photos privacy policy Google's scope reference

E40; E49; E53. Runtime selection of the SDK branch was not observed.

The Gmail privacy button takes users to a domain that does not exist.

The successful current Apple page contains three visible privacy links to www.shieldapps.cc, including the main Privacy Policy button. Google Public DNS returns NXDOMAIN for that hostname. The app binary and description point to the working .top policy instead.

These are different addresses. The existence of the working developer policy is preserved, while the broken App Store entry remains a directly testable privacy-access problem.



Exact current Apple link destination and independently retained public-DNS response, with the working in-app policy URL shown separately. Labelled extraction output, not a fabricated browser error page. E2; E24; E47.

E2; E24; E35; E47.

What buyers actually wrote.

The original US Apple review feed for Drive returns nine entries: six one-star and three five-star reviews. This is the returned feed sample, not the app's overall rating. A 14 November reviewer reports paying about $20 and asks for a refund; other entries describe upgrade objections or functionality problems.

The Dropbox feed includes an October complaint about errors and unfamiliar displayed files, alongside a strongly positive support review. The Gmail feed includes a November complaint about cross-promoting other apps in the interface. These statements are attributed to reviewers. They do not prove a payment transaction, a data breach or deliberate fraud.

Static strings include sample/test data and fictional-looking account records. That can be ordinary screenshot/test material. We did not establish why the Dropbox reviewer saw unfamiliar files and do not turn that complaint into a claim that other customers' files leaked.

EVIDENCE EXTRACT · 19 NOVEMBER 2026

Buyers describe refund requests and malfunction.

Selected Apple RSS reviews; these are user accounts, not transactions reproduced by this investigation.

```
GOOGLE DRIVE · app 6754816629
One star · 14 November 2026
“I paid $20 when I didn’t have to.”
The same reviewer requests a refund and reports difficulty using the app.

DROPBOX · app 6754376846
One star · 24 October 2026
The reviewer reports errors and says the displayed files were not theirs.

GMAIL · app 6757919783
Two stars · 16 November 2026
The reviewer criticises the space used for cross-promoting other apps.

COUNTEREVIDENCE
The same Apple feeds also contain positive Drive, Docs, Dropbox and
authenticator reviews. These excerpts are not a claim that all users report problems.
```

Source: original US Apple customer-review RSS responses, fetched 19 November 2026. Full responses are retained privately; exact endpoint links are in the source register. E25–E30.

Short selected Apple RSS excerpts and summaries. The feeds also contain positive entries; complete retained responses and exact source URLs are available in the evidence register. E25–E30.

US Apple review feeds returned on 19 November 2026

Product	Returned entries	What can be said
Drive	9 · six one-star, three five-star	Refund/payment and functionality complaints, plus favourable experiences. E25.
Gmail	1 · two-star	Cross-promotion and interface-space complaint. E26.
Photos	No entries returned	No invented customer-confusion allegation. E27.
Docs	2 · five-star	Both returned entries are positive. E28.
Dropbox	3 · two one-star, one five-star	Error/incorrect-files allegation and favourable support account. E29.
Authenticator	4 · two favourable, two low-rated	Ease-of-use opinions; no Authy-confusion complaint from the separate Appios app is imported here. E30.

E25–E30. The zero rating-count values in some software API records are not treated as proof of zero Mac reviews.

The Docs icon changed between the two captures.

Our retained 13 November Docs icon used diagonal Google-coloured bands. The current 19 November Apple icon is a blue document-style design. These two original files belong to the same app ID. This is an observed visual change; the available records do not establish why it changed or a neutral launch followed by impersonation.



Before: original Docs client icon retained by the earlier investigation, 13 November 2026. E51.



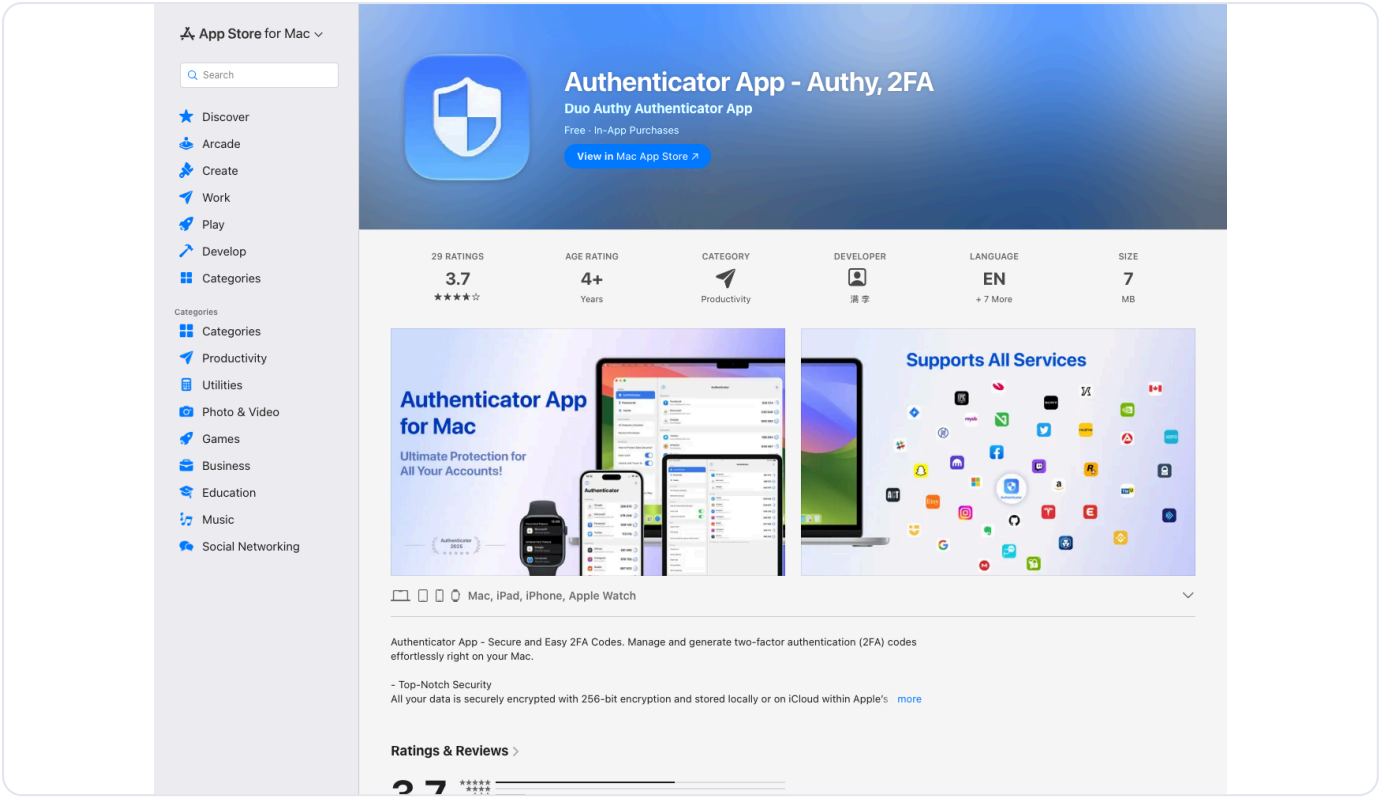
Current: original Apple Docs client icon, retrieved 19 November 2026. Blue design replaces the earlier multicolour bands. E1.

E1; E51.

The authenticator uses Authy and Duo wording, not their official publisher.

Apple's current catalog names the product Authenticator App - Authy, 2FA under this seller. The retained native Mac capture from 13 November also shows Duo Authy Authenticator App in the subtitle.

The independent app's blue shield is visibly different from official Authy's symbol. The issue here is the combination of trusted product names in the app's identity, not an invented claim that these icons are identical. The signed app contains real OTP, cryptographic and local-authentication components; their presence is not evidence of secret theft.



Earlier original native Apple Mac page, 13 November 2026: Authy in the title, Duo/Authy in the subtitle, and the independent publisher. Dated evidence, not a fresh successful 19 November page capture. E51.



Shield Apps authenticator: current original Apple icon. Different from the official Authy reference. E1.



Official Twilio Authy by Authy Inc. Current original Apple artwork; independent comparison reference. E17.

E1; E6; E17; E31; E51.

All 15 apps, with the scope of each check.

Six core apps were inspected as signed binaries and listings. Nine other utilities were checked from Apple's catalog and successful listing responses where available. Their shared account identity is verified; no specific impersonation finding is invented for a generic QR, OCR or vault icon.

Apple developer 1653727587 · exact product inventory

Product / App ID	Bundle ID	Review scope and supported issue
Quick Access for Gmail + / 6757919783	com.shieldapps.quickemail	Binary + listing: Google palette/name; current App Store privacy button fails DNS; embedded authorization path.
Quick Access for Google Drive / 6754816629	com.shieldapps.googledrive	Binary + listing: Generic cloud icon; real Drive API/native integration code; refund and functionality complaints.
Quick Access for Dropbox / 6754376846	com.shieldapps.dropboxy	Binary + listing: Same generic cloud design as Drive; Dropbox branding in promotions; mixed customer reports.
Quick Access for Google Docs / 6756507719	com.shieldapps.quickdocs	Binary + listing: Icon changed from multicolour to blue; real API and embedded authorization code.
Authenticator App - Authy, 2FA / 6444312209	com.maxapps.authenticator	Binary + listing: Authy title and recorded Duo/Authy subtitle; different official icon.
QR Code Scanner: QR Reader / 6502285859	com.shieldapps.qrscanner	Catalog/listing only: Generic utility presentation. No specific impersonated official product established.
File Vault: Safe Photos, Files / 6746962777	com.shieldapps.vaultbox	Catalog/listing only: Generic utility presentation. No specific impersonated official product established.
Smart Printer App: eSign PDF / 6740662679	com.shieldapps.printer	Catalog/listing only: Printer compatibility claims; generic printer icon, not a verified manufacturer-logo copy.
Copy Text On Screen: OCR / 6476453001	com.shield.textsnapper	Catalog/listing only: Generic utility presentation. No specific impersonated official product established.
QR Code Generator: QR Maker / 6749896568	com.shieldapps.qrgenerator	Catalog/listing only: Generic utility presentation. No specific impersonated official product established.
Quick Access for Google Photos / 6768488342	com.shieldapps.quickphotos	Binary + listing: Google palette/name; embedded authorization and full-Drive SDK scope discrepancy.
Private Photo Vault: Secret / 6752824775	com.shieldapps.photovault	Catalog/listing only: Generic utility presentation. No specific impersonated official product established.
Batch PDF OCR: Fast & Accurate / 6752823571	com.shieldapps.pdfocr	Catalog/listing only: Generic utility presentation. No specific impersonated official product established.
Dislike Checker for YouTube + / 6741679691	com.shieldapps.dislikes	Catalog/listing only: Thumb-down utility; no copied YouTube play icon established.
SnapText: OCR, Copy, Translate / 6746952808	com.shieldapps.snaptext	Catalog/listing only: Generic utility presentation. No specific impersonated official product established.

Quick Access for Gmail + · 6757919783 **Quick Access for Google Drive · 6754816629** **Quick Access for Dropbox · 6754376846**

Quick Access for Google Docs · 6756507719 **Authenticator App - Authy, 2FA · 6444312209**

QR Code Scanner: QR Reader · 6502285859 **File Vault: Safe Photos, Files · 6746962777** **Smart Printer App: eSign PDF · 6740662679**

Copy Text On Screen: OCR · 6476453001 QR Code Generator: QR Maker · 6749896568 Quick Access for Google Photos · 6768488342

Private Photo Vault: Secret · 6752824775 Batch PDF OCR: Fast & Accurate · 6752823571 Dislike Checker for YouTube + · 6741679691

SnapText: OCR, Copy, Translate · 6746952808

E1–E16; E31–E36.

All original account icons.

These are the original current Apple images, preserved separately from the comparison plates and diagrams. Select any image to open the source-resolution copy.

▼ Show all 15 original Apple icons



Quick Access for Gmail + · 6757919783. Original Apple artwork from the exact developer catalog. E1.



Quick Access for Google Drive · 6754816629. Original Apple artwork from the exact developer catalog. E1.



Quick Access for Dropbox · 6754376846. Original Apple artwork from the exact developer catalog. E1.



Quick Access for Google Docs · 6756507719. Original Apple artwork from the exact developer catalog. E1.



Authenticator App - Authy, 2FA · 6444312209. Original Apple artwork from the exact developer catalog. E1.



QR Code Scanner: QR Reader · 6502285859. Original Apple artwork from the exact developer catalog. E1.



File Vault: Safe Photos, Files · 6746962777. Original Apple artwork from the exact developer catalog. E1.



Smart Printer App: eSign PDF · 6740662679. Original Apple artwork from the exact developer catalog. E1.



Copy Text On Screen: OCR · 6476453001. Original Apple artwork from the exact developer catalog. E1.



QR Code Generator: QR Maker · 6749896568. Original Apple artwork from the exact developer catalog. E1.



Quick Access for Google Photos · 6768488342. Original Apple artwork from the exact developer catalog. E1.



Private Photo Vault: Secret · 6752824775. Original Apple artwork from the exact developer catalog. E1.



Batch PDF OCR: Fast & Accurate · 6752823571. Original Apple artwork from the exact developer catalog. E1.



Dislike Checker for YouTube + · 6741679691. Original Apple artwork from the exact developer catalog. E1.



SnapText: OCR, Copy, Translate · 6746952808. Original Apple artwork from the exact developer catalog. E1.

E1. Catalog membership does not establish wrongdoing.

The official reference icons, separately preserved.

These are the official publishers' current Apple icons used in the comparison plate. Each opens at its original delivered resolution. They are references, not accused apps.

▼ Show all six official reference icons



Twilio Authy · official Apple publisher reference, app 494168017. Original source-resolution artwork retrieved 19 November 2026; not an investigated Shield Apps product. E17.



Gmail · official Apple publisher reference, app 422689480. Original source-resolution artwork retrieved 19 November 2026; not an investigated Shield Apps product. E17.



Google Drive · official Apple publisher reference, app 507874739. Original source-resolution artwork retrieved 19 November 2026; not an investigated Shield Apps product. E17.



Google Docs · official Apple publisher reference, app 842842640. Original source-resolution artwork retrieved 19 November 2026; not an investigated Shield Apps product. E17.



Google Photos · official Apple publisher reference, app 962194608. Original source-resolution artwork retrieved 19 November 2026; not an investigated Shield Apps product. E17.



Dropbox · official Apple publisher reference, app 327630330. Original source-resolution artwork retrieved 19 November 2026; not an investigated Shield Apps product. E17.

E17. Official publisher and exact app ID checked.

The six original signed applications.

Every supplied app passed macOS deep strict signature verification under team 84ADMTKQD4. Inspection covered archive members, main executables, signing entitlements, library dependencies, embedded property lists, strings, app-specific class metadata, original instruction output and privacy manifests.

The binaries contain real Google/Dropbox API and native application components alongside embedded browser code. No Firebase project configuration was recovered from the six packages. Generic Google App Check SDK references are not evidence of a Firebase analytics project. No private OpenAI key, AWS access-key identifier or private-key block was found by the recorded pattern scans. These scans do not prove the absence of every possible secret or runtime behaviour.

The apps were not launched. No real Google/Dropbox account was connected, authentication code imported, purchase made, receipt used or developer endpoint queried with a credential. The static findings and reviewer allegations are identified separately.

Exact supplied versions, Apple team and executable hashes

App / version / build	Bundle ID	Main executable SHA-256
Authenticor App.app · 3.7.8 / 573	com.maxapps.authenticator	7c4dfacd349edf3ce1249958dd12bb0018f9f1dffbc764c0d856d1a0468abd70
QuickDocs.app · 1.5 / 214	com.shieldapps.quickdocs	63a65f37a6b6076be0b7586b92178350a3373761e5b279095593e17470aa9467
QuickDrive.app · 3.5.4 / 558	com.shieldapps.googledrive	eff1f32898b4fc2c109e3d7ecfa8a2d9e99461b13560132ab60403a76a2b0189
QuickDropbox.app · 2.2.2 / 279	com.shieldapps.dropboxy	f664d6532598d7df57d9e2179fba3c94ed83ecd4d6e4d0693cb1aa3045bdb66a
QuickEmail.app · 1.3 / 121	com.shieldapps.quickemail	38c5e696fe5c8d4e778b5a1414170e6f74f71192ced745fe2b39d093dfe89aaf
QuickPhotos.app · 1.1 / 49	com.shieldapps.quickphotos	d1bfe53009ea2f96b1acefc9a78193cf7739519d1bc91c11c182b4564e644442

E31–E40. Untouched archives and raw binary research remain private.

Who is behind the public account?

Apple identifies the seller as 满 李; the earlier EU records render MAN LI, and the authenticator's legal pages use LI MAN. The product site, support identity and six signed binaries tie this portfolio together. No verified shareholders, corporate registration number or second current Apple account was recovered.

The domain registry gives shieldapps.top a CN / Hubei registrant indicator, through Alibaba Cloud, with an 18 November 2025 registration date. This is stronger than guessing from a name, but it is a domain-registration record. It is not an Apple-verified company address or a nationality finding; the app-specific business country remains Unknown.

The earlier German and Irish panels said the provider had not identified as a trader. That dated commercial-status issue was already documented in the prior report. It is not a finding that this account has been banned.

Shield Apps product site **Official registry response** **Earlier Authy/Shield Apps investigation**

E18; E23; E31–E36; E51; E52.

THE FULL RECORD

What else changed?

One independently observed Docs icon difference between the retained 13 November artwork and the 19 November current Apple artwork; no launch history is invented.

▼ Compare all 1 recorded changes

▼ Docs app icon · exact app ID 6756507719 OBSERVED ICON CHANGE

BEFORE

13 November: original document symbol on multicolour diagonal bands.

AFTER

19 November: current blue document-style app icon.

Original 13 November Docs artwork from E51 compared with current 19 November Apple artwork in E1. The same numeric app ID is retained.

▼ View the dates and timeline

2026-11-13

Earlier branding investigation

Original Docs multicolour icon, native authenticator naming and EU provider records retained.

2026-11-14

Drive buyer requests a refund

Dated one-star Apple RSS entry reports paying about $20 and asks for a refund.

2026-11-16

Gmail buyer criticises cross-promotion

Two-star Apple RSS entry objects to interface space used for promoting other apps.

2026-11-19

Six signed binaries examined

15-product catalog corroborated; six signatures verify; three embedded sign-in paths, a Photos scope discrepancy and the broken Gmail privacy button recorded.

CHECK THE SOURCES

The records behind this report.

Independent static inspection of six original signed application archives; current exact-ID Apple catalog for all 15 products; retained successful Apple pages, original artwork, Apple review feeds, working developer policies, DNS and registry responses, and official Apple/Google/Dropbox rules. Earlier 13 November evidence is labelled separately. Screenshots of extraction output are labelled; no real account was logged in and no purchase was performed.

▼ **Open source files, archive links and checksums**

E1 / Apple account catalog: all 15 products

Exact artist ID 1653727587 on all 15 returned software records. The macSoftware-only request returns no products and is not used as an availability verdict.

Open source ↗

SHA-256: 24c67daffce1452252c366786b6ef93eaaca3245028057e5e50a364f59a80a14

E2 / Quick Access for Gmail + — US App Store

Current primary response retained. Successful pages support original wording, privacy links and displayed purchases. Access-limited pages are not treated as readable or removed; the independent catalog identifies the product. HTTP 200.

Open source ↗

SHA-256: c1ed4f3119f019ca6614fd6424c2b4e1423f424cc2ff16a5bfbdf6282f58fec9

E3 / Quick Access for Google Drive — US App Store

Current primary response retained. Successful pages support original wording, privacy links and displayed purchases. Access-limited pages are not treated as readable or removed; the independent catalog identifies the product. HTTP 429.

Open source ↗

SHA-256: 3566293e9fc367806a9551a795f324cf3bbcbff7e660bfef99af0d4ccd53df74

E4 / Quick Access for Dropbox — US App Store

Current primary response retained. Successful pages support original wording, privacy links and displayed purchases. Access-limited pages are not treated as readable or removed; the independent catalog identifies the product. HTTP 200.

Open source ↗

SHA-256: 8117066ea84fa0ca44cf47f6deda8c7304805d1cd8938de6a231ff663f879b41

E5 / Quick Access for Google Docs — US App Store

Current primary response retained. Successful pages support original wording, privacy links and displayed purchases. Access-limited pages are not treated as readable or removed; the independent catalog identifies the product. HTTP 200.

Open source ↗

SHA-256: 7d0251aa5be0297f8e67f3e642e36e1921692431d32c05dad75d3090ec4e4dcc

E6 / Authenticator App - Authy, 2FA — US App Store

Current primary response retained. Successful pages support original wording, privacy links and displayed purchases. Access-limited pages are not treated as readable or removed; the independent catalog identifies the product. HTTP 429.

Open source ↗

SHA-256: 3566293e9fc367806a9551a795f324cf3bbcbff7e660bfef99af0d4ccd53df74

E7 / QR Code Scanner: QR Reader — US App Store

Current primary response retained. Successful pages support original wording, privacy links and displayed purchases. Access-limited pages are not treated as readable or removed; the independent catalog identifies the product. HTTP 429.

Open source ↗

SHA-256: 3566293e9fc367806a9551a795f324cf3bbcbff7e660bfef99af0d4ccd53df74

E8 / File Vault: Safe Photos, Files — US App Store

Current primary response retained. Successful pages support original wording, privacy links and displayed purchases. Access-limited pages are not treated as readable or removed; the independent catalog identifies the product. HTTP 200.

Open source ↗

SHA-256: 72917a7b6d7201396e8ef41309c3de11eb63a21cf59ec9da0d7c2c01157db182

E9 / Smart Printer App: eSign PDF — US App Store

Current primary response retained. Successful pages support original wording, privacy links and displayed purchases. Access-limited pages are not treated as readable or removed; the independent catalog identifies the product. HTTP 429.

Open source ↗

SHA-256: 3566293e9fc367806a9551a795f324cf3bbcbff7e660bfef99af0d4ccd53df74

E10 / Copy Text On Screen: OCR — US App Store

Current primary response retained. Successful pages support original wording, privacy links and displayed purchases. Access-limited pages are not treated as readable or removed; the independent catalog identifies the product. HTTP 200.

Open source ↗

SHA-256: 3976bb321cc672eb127b08639bad377348ac54d34f6e3bb5916d16052db9a548

E11 / QR Code Generator: QR Maker — US App Store

Current primary response retained. Successful pages support original wording, privacy links and displayed purchases. Access-limited pages are not treated as readable or removed; the independent catalog identifies the product. HTTP 200.

Open source ↗

SHA-256: 1317a34100683a84136ab6646f5e6f990c03f528a4160556e188bd1603e571ee

E12 / Quick Access for Google Photos — US App Store

Current primary response retained. Successful pages support original wording, privacy links and displayed purchases. Access-limited pages are not treated as readable or removed; the independent catalog identifies the product. HTTP 200.

Open source ↗

SHA-256: 2f43ef1de43a4af30bbbef541ba73b14e5cf9e14cb56721713193b6225c2c5a0

E13 / Private Photo Vault: Secret — US App Store

Current primary response retained. Successful pages support original wording, privacy links and displayed purchases. Access-limited pages are not treated as readable or removed; the independent catalog identifies the product. HTTP 200.

Open source ↗

SHA-256: 4f30b2ec83de3b21b40d8f4f6ec201e2fc9e0887b3baf043b16d0d5c09665be5

E14 / Batch PDF OCR: Fast & Accurate — US App Store

Current primary response retained. Successful pages support original wording, privacy links and displayed purchases. Access-limited pages are not treated as readable or removed; the independent catalog identifies the product. HTTP 200.

Open source ↗

SHA-256: be3f7f38d8456ed77eefb35ec06edb677913ba62bc9a90831f434f405183aef6

E15 / Dislike Checker for YouTube + — US App Store

Current primary response retained. Successful pages support original wording, privacy links and displayed purchases. Access-limited pages are not treated as readable or removed; the independent catalog identifies the product. HTTP 200.

Open source ↗

SHA-256: f45f60bb6a094eaa12e28e3bb3902a40c333d18b5830102e1608474a2975a84a

E16 / SnapText: OCR, Copy, Translate — US App Store

Current primary response retained. Successful pages support original wording, privacy links and displayed purchases. Access-limited pages are not treated as readable or removed; the independent catalog identifies the product. HTTP 200.

Open source ↗

SHA-256: 419bba737893853b88f11e60b7919b41a6cbc193e1ec1b18093a80b4b03f1b63

E17 / Official Authy, Gmail, Drive, Docs, Photos and Dropbox references

Official Apple IDs and publisher identities checked; original Apple artwork retrieved separately. HTTP unavailable.

Open source ↗

SHA-256: b4625427aae1638e2109e63f3684ed1f0772a6b1dd89c906a47d9131fbe6ed82

E18 / Shield Apps product website

The product site uses Shield Apps branding and links its apps. It is a working independent site, not a free Google Sites page. HTTP 200.

Open source ↗

SHA-256: 7a49364d7c8cc5bf53f3b81d1c722a016382644f5db7ad4c558627003b9a81a2

E19 / Google OAuth policies: secure browser requirement

Current official policy prohibits directing Google authorization to developer-controlled embedded user-agents. HTTP 200.

Open source ↗

SHA-256: d4fc4efdfc605225755320aa736b68b1e42196a9061e9c1f0c630a1c744d74fe

E20 / Apple App Review Guidelines

Current official provisions read: 2.3, 2.3.7, 4.1, 5.1.1(i), 5.2.1 and 5.2.2. Assessment is editorial, not an Apple decision. HTTP 200.

Open source ↗

SHA-256: 68b3d39c8e9a0c8d12cc0d7c46fdabcb9c0bdae3a7d77f2e450c542a8f795323

E21 / Google brand guidance

Current guidance on misleading affiliation and use of Google brand elements. HTTP 200.

Open source ↗

SHA-256: 0b5c61b13ee49baa94ec1542246058cd1c5af2510aec00224fd8101a0d591c49

E22 / Dropbox brand guidance

Current guidance read; descriptive compatibility and false affiliation are separate questions. HTTP 200.

Open source ↗

SHA-256: 227643b229648b0b6ae510b81c514d8877228937c8937392b9af0a33a254fd8c

E23 / Official .top registry record for shieldapps.top

Registrant country CN, region hu bei; registered 18 November 2025 through Alibaba Cloud. This is domain-registration context, not an Apple-verified business address. HTTP 200.

Open source ↗

SHA-256: b3d68648adee061fdad7d91ec85fd9fffc8a9f6b08623ecc1c8a548bc6a2d7bd

E24 / Gmail App Store privacy domain: DNS failure

Google Public DNS returned Status 3 / NXDOMAIN for www.shieldapps.cc. Exact broken anchors were extracted from current successful Apple Gmail HTML. HTTP 200.

Open source ↗

SHA-256: d342c642da8fddf9c44de1ed167960437e8b6108cd50a7755185bdc7895f5428

E25 / Quick Access for Google Drive — original US Apple customer reviews

Original Apple RSS, including positive and negative entries where returned. Review statements are attributed allegations, not reproduced transactions or a forensic finding of theft. HTTP 200.

Open source ↗

SHA-256: 0fe68a4ea574b862133b3c9a78bf3ea01e7f76eb87e3c13f462882a74bc5b2c2

E26 / Quick Access for Gmail + — original US Apple customer reviews

Original Apple RSS, including positive and negative entries where returned. Review statements are attributed allegations, not reproduced transactions or a forensic finding of theft. HTTP 200.

Open source ↗

SHA-256: 3f1cc3ee13b16d165fb6a5d705d944d8f843a1a427c1d8de1072d7502c9f928b

E27 / Quick Access for Google Photos — original US Apple customer reviews

Original Apple RSS, including positive and negative entries where returned. Review statements are attributed allegations, not reproduced transactions or a forensic finding of theft. HTTP 200.

Open source ↗

SHA-256: e00161ccbae9436f9b1c38a52b255260bb1610f4ae31e103e11b244a73684187

E28 / Quick Access for Google Docs — original US Apple customer reviews

Original Apple RSS, including positive and negative entries where returned. Review statements are attributed allegations, not reproduced transactions or a forensic finding of theft. HTTP 200.

Open source ↗

SHA-256: 8d0dd38dc668959e208a3cd85de1bfc7ed23c4e414bcc4a92f1476e575f8d8bf

E29 / Quick Access for Dropbox — original US Apple customer reviews

Original Apple RSS, including positive and negative entries where returned. Review statements are attributed allegations, not reproduced transactions or a forensic finding of theft. HTTP 200.

Open source ↗

SHA-256: cccea4b025107bd121a38693cf8d90bcb04ada32cf16e09f727a15d8d2e6d2c8

E30 / Authenticator App - Authy, 2FA — original US Apple customer reviews

Original Apple RSS, including positive and negative entries where returned. Review statements are attributed allegations, not reproduced transactions or a forensic finding of theft. HTTP 200.

Open source ↗

SHA-256: 5eab5e918814a4505aa012d70b34a6e7993dc34c1451a1dd961e293ac8e99cde

E31 / Authenticor App.app — supplied signed binary

Static read-only inspection of Authenticor App.zip. Bundle com.maxapps.authenticator; version 3.7.8 / build 573; Apple signing team 84ADMTKQD4. Deep strict signature verification passed. Main executable SHA-256 7c4dfacd349edf3ce1249958dd12bb0018f9f1dffbc764c0d856d1a0468abd70. No app launched, receipt used, credentials submitted or purchase performed.

SHA-256: f0c7d5c7f54253f1ba3cc7a545948abff789971498d9800e3511c3c43d519305

E32 / QuickDocs.app — supplied signed binary

Static read-only inspection of QuickDocs.zip. Bundle com.shieldapps.quickdocs; version 1.5 / build 214; Apple signing team 84ADMTKQD4. Deep strict signature verification passed. Main executable SHA-256 63a65f37a6b6076be0b7586b92178350a3373761e5b279095593e17470aa9467. No app launched, receipt used, credentials submitted or purchase performed.

SHA-256: 9b793b97890f68357006b972b6248a0c0a1aa1372f61b6914a62146cac52fa49

E33 / QuickDrive.app — supplied signed binary

Static read-only inspection of QuickDrive.zip. Bundle com.shieldapps.googledrive; version 3.5.4 / build 558; Apple signing team 84ADMTKQD4. Deep strict signature verification passed. Main executable SHA-256 eff1f32898b4fc2c109e3d7ecfa8a2d9e99461b13560132ab60403a76a2b0189. No app launched, receipt used, credentials submitted or purchase performed.

SHA-256: 18e2df2b303170e0572b47d0a879a6e94f82c967007ae8112267c595dd468763

E34 / QuickDropbox.app — supplied signed binary

Static read-only inspection of QuickDropbox.zip. Bundle com.shieldapps.dropboxy; version 2.2.2 / build 279; Apple signing team 84ADMTKQD4. Deep strict signature verification passed. Main executable SHA-256 f664d6532598d7df57d9e2179fba3c94ed83ecd4d6e4d0693cb1aa3045bdb66a. No app launched, receipt used, credentials submitted or purchase performed.

SHA-256: f9664218343d3796d6f7146ad2bc1b33372116f6d14e8d2bcd7eb71bf71812ef

E35 / QuickEmail.app — supplied signed binary

Static read-only inspection of QuickEmail.zip. Bundle com.shieldapps.quickemail; version 1.3 / build 121; Apple signing team 84ADMTKQD4. Deep strict signature verification passed. Main executable SHA-256 38c5e696fe5c8d4e778b5a1414170e6f74f71192ced745fe2b39d093dfe89aaf. No app launched, receipt used, credentials submitted or purchase performed.

SHA-256: 55a5fc7cb5ea53d98f57c6e7adc913c4ebbf4c36164df7ca78ff25323a03a995

E36 / QuickPhotos.app — supplied signed binary

Static read-only inspection of QuickPhotos.zip. Bundle com.shieldapps.quickphotos; version 1.1 / build 49; Apple signing team 84ADMTKQD4. Deep strict signature verification passed. Main executable SHA-256 d1bfe53009ea2f96b1acefc9a78193cf7739519d1bc91c11c182b4564e644442. No app launched, receipt used, credentials submitted or purchase performed.

SHA-256: 4611abbb6a65ffc3abe246ea6cea83b103d2d54e0f0c7cf28f6b642c371aef9f

E37 / QuickEmail.app — app-owned Google sign-in path

Main executable: QuickEmail.app/Contents/MacOS/QuickEmail. App-specific OAuthWebViewController class metadata, Google authorization URL at 0x100088a64, and loadRequest selector reference at 0x100088f58 independently located in ARM64 code. Read-only pointer resolution adds explicitly labelled selector annotations to preserved original disassembly. Runtime execution was not observed.

SHA-256: 38c5e696fe5c8d4e778b5a1414170e6f74f71192ced745fe2b39d093dfe89aaf

E38 / QuickDocs.app — app-owned Google sign-in path

Main executable: QuickDocs.app/Contents/MacOS/QuickDocs. App-specific OAuthWebViewController class metadata, Google authorization URL at 0x1000ae2a8, and loadRequest selector reference at 0x1000ae79c independently located in ARM64 code. Read-only pointer resolution adds explicitly labelled selector annotations to preserved original disassembly. Runtime execution was not observed.

SHA-256: 63a65f37a6b6076be0b7586b92178350a3373761e5b279095593e17470aa9467

E39 / QuickPhotos.app — app-owned Google sign-in path

Main executable: QuickPhotos.app/Contents/MacOS/QuickPhotos. App-specific OAuthWebViewController class metadata, Google authorization URL at 0x1000298ac, and loadRequest selector reference at 0x100029da0 independently located in ARM64 code. Read-only pointer resolution adds explicitly labelled selector annotations to preserved original disassembly. Runtime execution was not observed.

SHA-256: d1bfe53009ea2f96b1acefc9a78193cf7739519d1bc91c11c182b4564e644442

E40 / QuickPhotos: full Drive scope passed to a Google Sign-In SDK branch

QuickPhotos 1.1 build 49; ARM64 function 0x10006c600. Static Swift array at 0x1001ea388 contains one item, https://www.googleapis.com/auth/drive. It is bridged to NSArray and passed as register x4 / additionalScopes in signInWithPresentingWindow:hint:additionalScopes:completion: at call 0x10006c89c. A direct caller exists at 0x10006e0d4. A separate narrower Photos append-only route also exists; active route selection was not observed.

SHA-256: d1bfe53009ea2f96b1acefc9a78193cf7739519d1bc91c11c182b4564e644442

E41 / quickdocs legal 64

Working developer legal page, directly retrieved. Independence disclaimers are preserved. Photos policy says it does not request full Drive access; the shipped alternative SDK path is separately recorded. HTTP 200.

Open source ↗

SHA-256: 706fb2b25c4c21b1a67d6979516d0bb25d3f436859f0398fb8bc2570fd40746a

E42 / quickdocs legal 65

Working developer legal page, directly retrieved. Independence disclaimers are preserved. Photos policy says it does not request full Drive access; the shipped alternative SDK path is separately recorded. HTTP 200.

Open source ↗

SHA-256: 56d4d8c230f837771857e71482a6c6860a4d4f6970715de43f166e1f4d63bab6

E43 / quickdrive legal 68

Working developer legal page, directly retrieved. Independence disclaimers are preserved. Photos policy says it does not request full Drive access; the shipped alternative SDK path is separately recorded. HTTP 200.

Open source ↗

SHA-256: 68a06f8d68cdd05e51b7a6d5e0de16229b48323892ce9912192b5e7ebdb69dd6

E44 / quickdrive legal 69

Working developer legal page, directly retrieved. Independence disclaimers are preserved. Photos policy says it does not request full Drive access; the shipped alternative SDK path is separately recorded. HTTP 200.

Open source ↗

SHA-256: 875ba0864cb66d9f64ce4a8c094f05d743923a4c1c69219b0cc38f5ce5c85d97

E45 / quickdropbox legal 26

Working developer legal page, directly retrieved. Independence disclaimers are preserved. Photos policy says it does not request full Drive access; the shipped alternative SDK path is separately recorded. HTTP 200.

Open source ↗

SHA-256: 722dfecba7bdf42b3bee680c5bd58b9eea4847b387085417826f5c04827299a2

E46 / quickdropbox legal 27

Working developer legal page, directly retrieved. Independence disclaimers are preserved. Photos policy says it does not request full Drive access; the shipped alternative SDK path is separately recorded. HTTP 200.

Open source ↗

SHA-256: 9289ceba52313d9c9bf6ffd7c66d41f792fd42322616a8aa732ee731c63d54b9

E47 / quickemail legal 54

Working developer legal page, directly retrieved. Independence disclaimers are preserved. Photos policy says it does not request full Drive access; the shipped alternative SDK path is separately recorded. HTTP 200.

Open source ↗

SHA-256: 797348a4e85bc26c292dd9b72d0a25f4de1ee3e0e0a7d05ff8dd18c5086ddf69

E48 / quickemail legal 55

Working developer legal page, directly retrieved. Independence disclaimers are preserved. Photos policy says it does not request full Drive access; the shipped alternative SDK path is separately recorded. HTTP 200.

Open source ↗

SHA-256: c90a2d04c9b5d932ae129839fed8358a7375b825f0037d2ed7d13216170a8fc6

E49 / quickphotos legal 40

Working developer legal page, directly retrieved. Independence disclaimers are preserved. Photos policy says it does not request full Drive access; the shipped alternative SDK path is separately recorded. HTTP 200.

Open source ↗

SHA-256: 6c6c17b015d50ba97b3e1d8d21ad130be986e5babcf9e8fb081522aba92ac140

E50 / quickphotos legal 41

Working developer legal page, directly retrieved. Independence disclaimers are preserved. Photos policy says it does not request full Drive access; the shipped alternative SDK path is separately recorded. HTTP 200.

Open source ↗

SHA-256: 6e012aadb66afefb165fe61e477fb6cf81759c62ea19ec1098ea37ae13edb649

E51 / Earlier report and dated original Docs/Authy artwork

Published investigation from 13 November 2026. Its original Docs icon has Google-coloured diagonal bands; current 19 November Apple artwork is blue. Its native Mac authenticator capture shows Authy in the name and Duo Authy in the subtitle. Earlier review complaints about the separate Appios Authly app are not attributed to Shield Apps here.

Open source ↗

E52 / Cross-case binary comparison

Compared all 12 prior Case 1–7 ZIP archives, including one nested archive level: 36 distinct main executables, no read errors. No match for this signing-team string, support mailbox, publisher domain or extracted OAuth-client identifiers. This scope does not cover every app ever published.

E53 / Google Drive official scope reference

Google classifies https://www.googleapis.com/auth/drive as a restricted scope that permits viewing and managing all Drive files. Current official scope table read; no live account consent was performed.

Open source ↗

SHA-256: 80f177e162bc07e55bddf14c73e31e63516704edfb2631700c46594936d8a640

E54 / Six-app API, embedded-browser and authorization architecture

Static comparison of the supplied signed main executables, dependencies, application classes, routes and OAuth configuration. Drive: custom Drive v3 file/upload routes and embedded Docs editing. Docs: GTLRDriveService and drive/v3 routes plus embedded Docs web UI. Gmail: generated Gmail v1 query routes/classes plus mail.google.com views. Photos: photoslibrary.googleapis.com uploads/batchCreate plus photos.google.com UI. Dropbox: SwiftyDropbox and Dropbox v2 routes. Authenticator: local OTP/cryptographic components. Four Google clients contain configured Google OAuth endpoints, token-management code and SDK components; custom embedded OAuth paths were traced in Gmail/Docs/Photos. No live end-to-end login, Google consent verification or server authorization was established.

E55 / Compiled API query execution and Google token-request call sites

Read-only ARM64 trace with LC_FUNCTION_STARTS boundaries and class/selector references resolved from retained Objective-C metadata. Drive: GTLRDriveQuery_FilesList reference 0x1002b7288 and executeQuery selector 0x1002b7ed0 in the same compiled function. Docs: FilesList reference 0x10000fee8 and executeQuery 0x1000100f8 in the same function. Gmail: UsersMessagesList reference 0x10003b888 and executeQuery 0x10003bb0c in the same function. Photos: uploads endpoint 0x10007f524, request construction, setBodyData 0x10007f6d4 and beginFetch selector 0x10007f770; batchCreate endpoint 0x10008091c, setBodyData 0x100080ebc and beginFetch selector 0x100080f58. All four also construct a Google token-endpoint request with a body, dataTaskWithRequest and resume. This proves shipped implementation call sites, not successful transactions, Google approval or live branch selection.