BRANDING AND PRIVACY WARNING · AUTHENTICATION UTILITIES

A new icon after launch. A Microsoft-like identity for a paid Mac authenticator.

VISUAL EVIDENCE

This paid Mac app beside the original Microsoft Authenticator

Left: Authenticator App for Desktop by Muhammad Basit. Right: Microsoft Authenticator by Microsoft Corporation. The shared Authenticator wording reinforces the resemblance of the blue lock, shield-like outline and cyan gradients. Together, the name and icon can misleadingly suggest an official Microsoft desktop product. The white tick and panel design differ from Microsoft's person symbol. The earlier purple icon and dated change evidence are preserved below.

This Mac app · Muhammad Basit



Original Apple artwork for app 6826168444, independently retrieved on 10 November; matches the supplied record.

Original · Microsoft Authenticator



Original Apple artwork for Microsoft Authenticator, app 983156458, retrieved 10 November. The official reference is a mobile app.

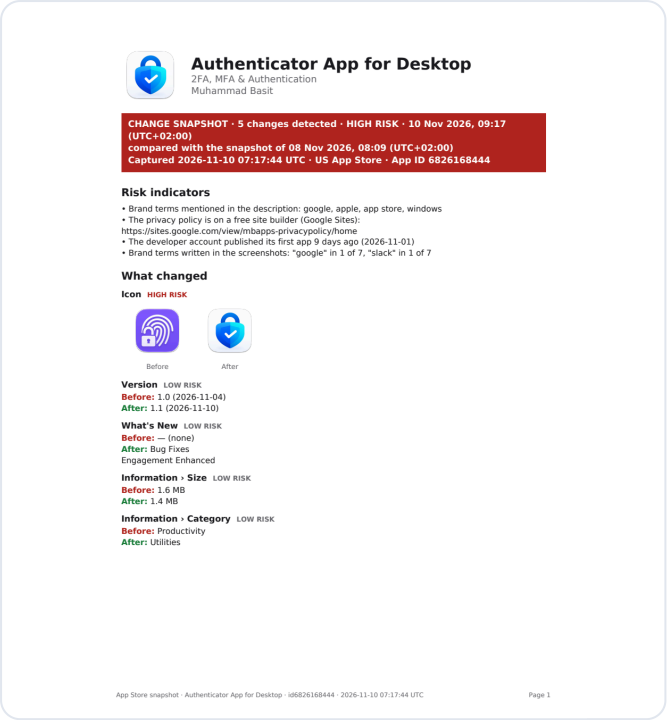
Another suspected scam pattern has reached Apple's storefront from a seller declaring Pakistan: a generic-looking identity first, then an update adopting familiar third-party branding. This case adds documented evidence of a Microsoft-like icon reaching the Mac App Store despite App Review. Muhammad Basit's Authenticator App for Desktop changed from a purple fingerprint on 8 November to a blue lock-and-shield by 10 November. App Scam DB assesses the combination of the prominent Authenticator name and the Microsoft-like icon as misleading: buyers may mistake this independent paid Mac app for an official Microsoft Authenticator desktop product. The sequence also raises a possible review-evasion concern, alongside mismatched privacy documents. The visible records establish the branding change and the seller's declared location; they do not reveal what reviewers were shown or prove deliberate deception.

By Alex Kleber · Published 2026-11-10 · Updated 2026-11-10

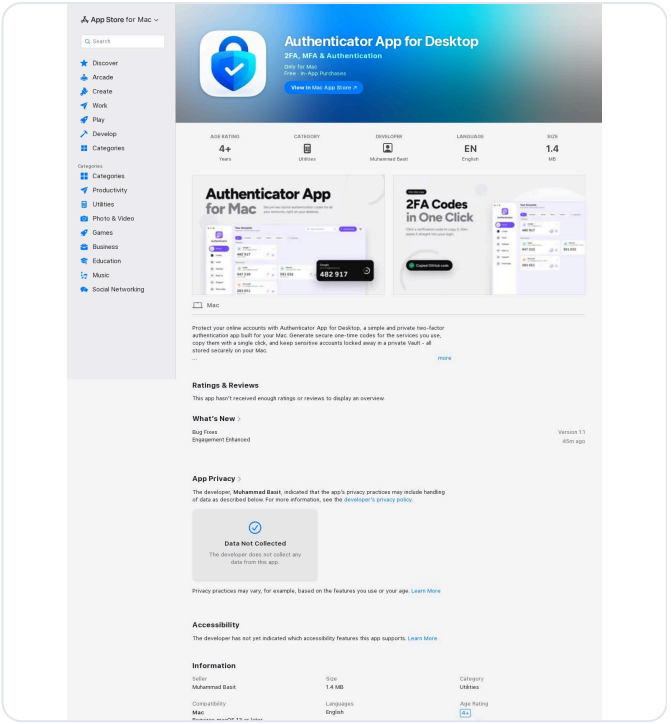
LOOK FOR YOURSELF

The screenshots tell the story.

The dated monitoring page establishes the icon change. The native Apple capture and seven original promotions show what the new listing advertises. They are listing evidence, not screenshots of an independently installed or tested app.

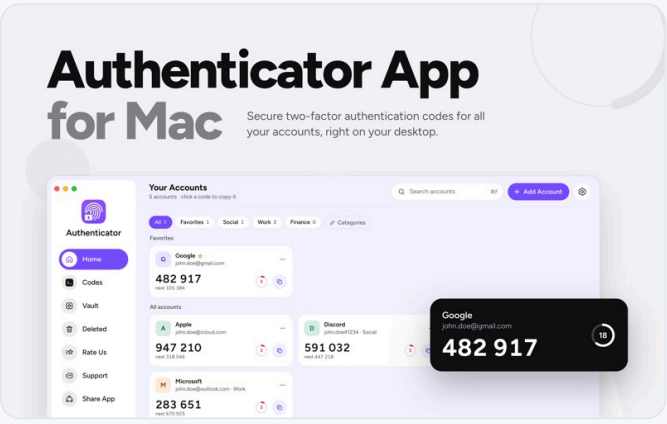


Supplied change record, page 1: 8 November 06:09 UTC compared with 10 November 07:17:44 UTC. The monitor's risk labels are source annotations, not findings of fraud.

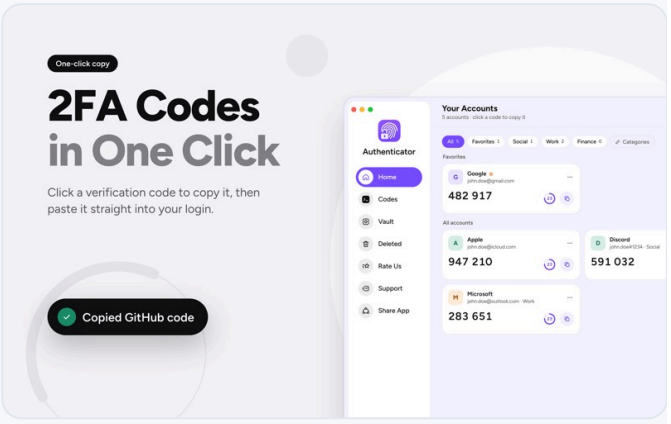


Native US Apple-page capture embedded in source PDF page 9, captured 10 November 07:17 UTC. New storefront icon, earlier purple identity still visible inside promotions.

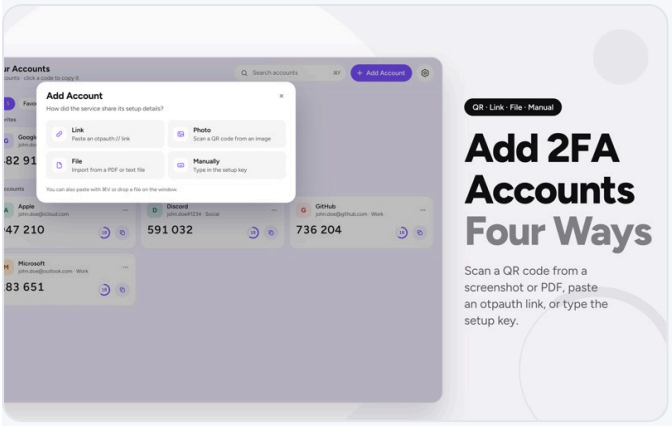
▼ See all 7 additional screenshots



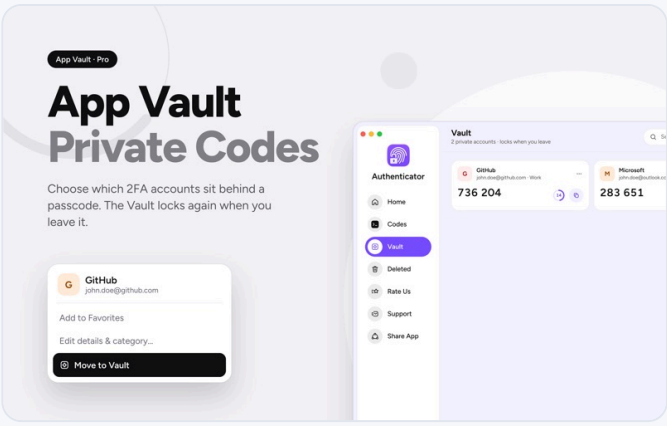
Original Apple promotion 1, retrieved 10 November; also in source page 5. Purple in-product identity contrasts with the new blue storefront icon.



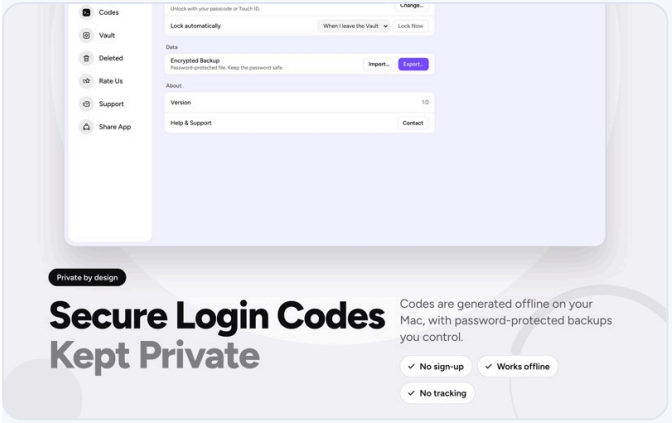
Original Apple promotion 2, retrieved 10 November. Example codes and service labels are marketing content.



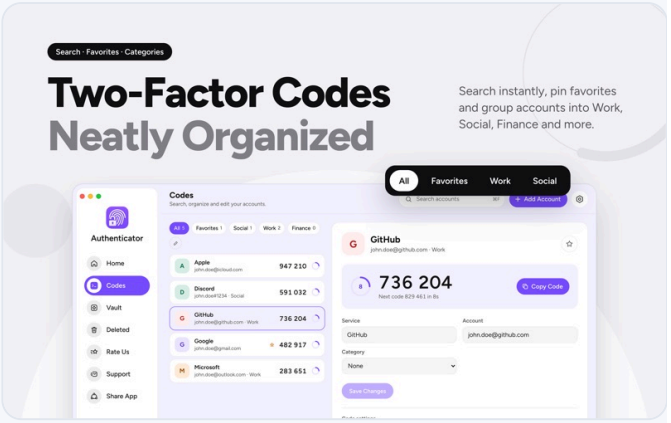
Original Apple promotion 3, retrieved 10 November. No real account secret was entered during this investigation.



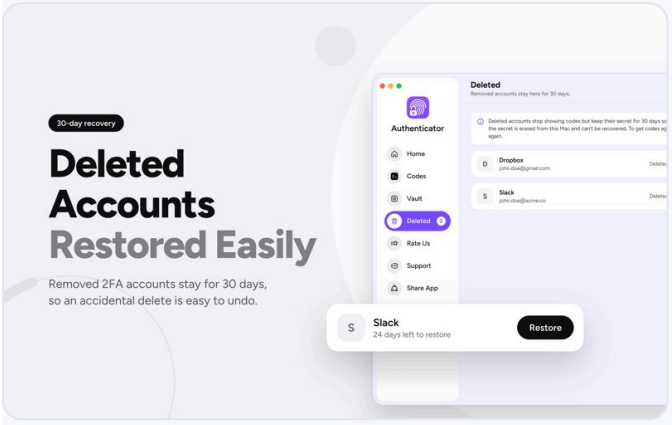
Original Apple promotion 4, retrieved 10 November. The vault protection is a developer claim, not a verified security property.



Original Apple promotion 5, retrieved 10 November: local storage and password-protected backup claims.



Original Apple promotion 6, retrieved 10 November.



Original Apple promotion 7, retrieved 10 November. Recognisable service labels can describe compatibility; they do not by themselves establish endorsement or copying.

WHAT YOU NEED TO KNOW

A security product needs a clear identity and app-specific privacy promises.

01

The icon changed after the app was already available

The supplied comparison records a purple fingerprint on 8 November and a blue lock-and-shield on 10 November under the same app ID. Version 1.1 has brief bug-fix and engagement release notes. Apple independently records its release at 06:32:12 UTC on 10 November. This supports scrutiny of post-launch presentation changes; it does not reveal what the reviewer saw or the developer's private review notes.

E1 page 1; E2/E3.

E1 E2 E3

02

The Authenticator name and look-alike icon reinforce each other

App Scam DB assesses the combined name and icon as misleading presentation: Authenticator App for Desktop shares the prominent Authenticator wording with Microsoft's product and pairs it with a similar blue lock-and-shield icon. That combination can make an independent paid Mac app look like an official Microsoft desktop counterpart. Apple identifies Muhammad Basit as seller. Microsoft's own support page says Microsoft Authenticator is not available for PC or Mac. This assessment concerns the combined presentation; it does not establish exclusive rights over the descriptive word Authenticator or prove that buyers were actually confused.

Visual assessment of original icons; E2/E4/E5.

E2 E4 E5

03

Local-only claims meet an unrelated AI policy

The listing says account secrets stay on the Mac, with Keychain storage and no server upload. Its Data Not Collected label sits beside a policy allowing technical collection and describing transmission of text, files or audio to AI providers. It does not explain which of those clauses apply to authenticator secrets, recovery data or backups. This is a disclosure mismatch, not evidence that any secret was actually transmitted.

E1 pages 3, 6 and 13–15; E3/E7.

E1 E3 E7

04

A second sensitive-data app shares the same account and documents

Esignature-Sign Any Document is on the same Apple developer ID and links exactly the same privacy and terms URLs. Both apps received version 1.1 releases on 10 November, twenty seconds apart. These are direct same-publisher connections. No second Apple account, prior suspension or hidden common operator was established.

E2/E6/E8; Apple exact-ID timestamps.

E2 E6 E8

WHAT IT COSTS

Free download, with monthly, yearly and lifetime purchases

These amounts are displayed by Apple in the US and Irish listings, checked on 10 November and consistent with the supplied PDF. Twelve monthly renewals at an unchanged price total $95.88, about 4.8 times the listed $19.99 yearly option; in Ireland, €107.88 versus €22.99, about 4.7 times. The listing describes auto-renewing monthly/yearly access and a one-time lifetime option. Feature equivalence, purchase flow and actual charges were not tested. Price alone is not proof of deception.

Prices displayed in the saved listing

Purchase option	United States	Ireland
Monthly Pro	$7.99 per month	€8.99 per month
Yearly Pro	$19.99 per year	€22.99 per year
Lifetime Pro	$29.99 one-time	€34.99 one-time

WHO IS BEHIND IT?

The name on the listing.

App name

Authenticator App for Desktop

Developer / seller

Muhammad Basit

Developer country · App ID 6826168444

Pakistan · Apple-declared trader business location: Faisalabad; not nationality.

E1 page 3 and freshly checked DE/IE provider disclosures, E3, 10 November 2026.

App Store listing ↗

▼ **App ID, version and other identifiers**

App Store ID

6826168444

Bundle identifier

com.mb.authenticator.app

Version

1.1 · 10 November 2026

First released

3 November 2026 · Apple release field

The warning pattern: change the identity after release

An already-listed app can acquire a much more recognisable visual identity through an update. That is the relevant consumer and review concern here: a generic-looking fingerprint gives way to an icon reminiscent of an established security product while the app retains its store identity. App Scam DB assesses this as a suspicious post-launch branding change deserving Apple's review.

An earlier App Scam DB investigation documented another Pakistan-declared seller changing a generic study chatbot into a Claude-branded listing. It is a comparison of the observed post-launch marketing technique, not a connection between those developers. The repeated concern is that familiar third-party branding reaches an already-live listing through updates; the evidence does not establish that the initial submissions were deceptive or that reviewers were deliberately bypassed.

The earlier observation is 8 November, five days after Apple's first-release field. It is not proof of the launch-day icon, an entirely infringement-free initial submission, a rejected or bypassed review, or a change in the app's actual code. The version-history entry dates 1.0 to 4 November while Apple's first-release field says 3 November; both fields are retained rather than silently reconciled.

The current promotional images still show the purple fingerprint inside the app. That supports a mismatch between storefront artwork and the advertised interface, but does not prove that all screenshots changed in the update. Only the five fields recorded by the source monitor are presented as observed changes.



Before · observed 8 November 2026. Original purple fingerprint icon from the supplied change record, page 1.



After · observed 10 November 2026. Original blue lock-and-shield icon under the same app ID.

Earlier generic-to-Claude rebranding investigation

E1 pages 1–7; E2/E3; E14 for the separately identified comparison case. All times are UTC unless expressly stated otherwise.

Recognisable security branding has consequences

The comparison preserves the differences: Microsoft's icon contains a cyan person inside a dark-blue shield-like padlock; Basit's uses overlapping blue/cyan panels and a white tick. The shared arched-lock silhouette, colour family and security-product context are the basis for the editorial resemblance assessment. No automated similarity percentage is used.

Microsoft's official support material directs users to mobile stores and explicitly rules out a PC or Mac version of Microsoft Authenticator. A third-party TOTP app can be a legitimate product, but compatibility with authentication services does not make it Microsoft's desktop product. The Apple seller field is essential to distinguishing them.

Microsoft's brand guidance restricts use of its product icons and misleading implied affiliation. The side-by-side comparison supports a request to review confusing presentation; this investigation has no licence agreement, Microsoft enforcement notice or legal determination establishing infringement.

Microsoft's official download guidance Official Microsoft Authenticator listing

E4/E5/E10. Brand guidance is relevant context, not evidence of an enforcement outcome.

A 2FA vault linked to AI-service paperwork

The listing describes TOTP generation, QR/setup-key import, a passcode or Touch ID vault, Keychain storage, encrypted local backups and thirty-day deleted-account recovery. Those features involve sensitive authentication material. They require clear disclosure of where that material goes and who can access it.

The linked MB Apps privacy policy, dated 20 October 2026, instead describes inputs sent to OpenAI, Anthropic, Google and xAI; possible AWS/Firebase hosting; payment providers; and analytics or diagnostics. These are the policy's statements, not independently detected dependencies. Its references to AI inputs do not identify an actual AI feature in the advertised authenticator.

The live page also retains an editorial note headed Important before publishing, telling its publisher to check whether the described providers and processing match the implementation. That is visible published drafting residue, not evidence identifying who wrote the document or whether AI was used to write it.

The Terms of Use link leads to an MB Apps page titled Term & Conditions, but its body is headed Privacy Policy and carries a different effective date, 29 April 2026. It repeats AI-provider and data-processing material and ends with a Before publishing instruction. It does not provide a clear, app-specific explanation of the lifetime entitlement or termination conditions in its displayed body.

The policy also excludes children under nine while Apple rates the app 4+. A store content rating is not a privacy consent rule, so this is a documentation inconsistency requiring explanation rather than proof of unlawful processing. No app binary was supplied or installed, and no network traffic or real authentication secret was tested.


MB Apps

Privacy Policy

Privacy Policy

Effective Date: October 20, 2026

A Note About Your Privacy

We believe your privacy matters. Our app is designed to provide useful features while collecting as little personal information as possible. This Privacy Policy explains what information may be collected, how it is used, and how we protect it.

1. Information We Collect

We aim to minimize the amount of information we collect.

Depending on how you use the app, we may collect limited technical information, such as:

- App version and device type.
- Crash reports and diagnostic logs.
- Anonymous usage statistics that help us understand how features are used.

We do not:

- Sell your personal information to third parties.
- Track your activity across other apps or websites.
- Collect sensitive personal information unless it is necessary for a specific feature and appropriately disclosed.

Information you enter into the app, such as notes, text, or other inputs, generally remains on your device unless a feature requires processing by an external service. Where applicable, the relevant data handling practices are explained in this policy.

2. How We Use Information

Any information we collect is used for legitimate operational and improvement purposes, including:

- Identifying and fixing bugs or crashes.
- Improving app performance, stability, and reliability.
- Understanding feature usage to improve the overall user experience.

We do not use collected information for purposes unrelated to operating, maintaining, or improving the app, except where otherwise disclosed or required by law.

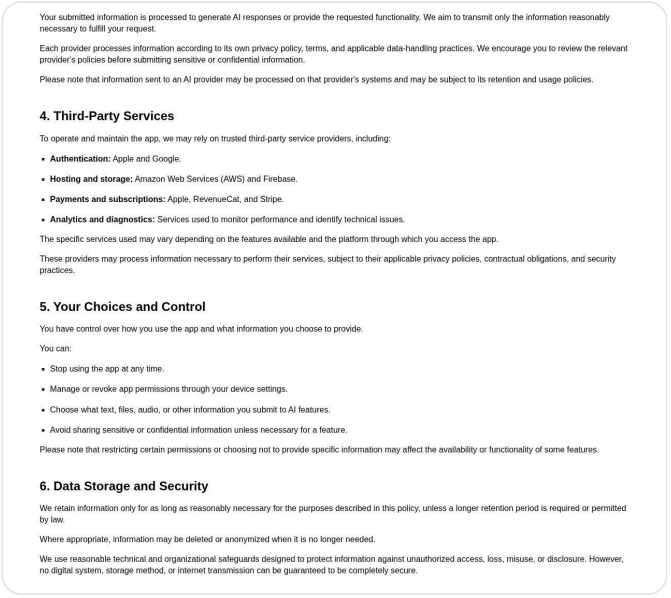
3. AI Models and Third-Party Processing

Our app provides access to advanced artificial intelligence (AI) models operated by third-party providers.

Depending on the features you use and the AI model you select, information you submit, including text, files, or audio, may be transmitted to the relevant provider to process your request. These providers may include:

- OpenAI
- Anthropic (Claude)
- Google (Gemini)
- xAI (Grok)

Source PDF page 13, original native policy capture. The security app's linked document describes AI services and possible data collection.


Your submitted information is processed to generate AI responses or provide the requested functionality. We aim to transmit only the information reasonably necessary to fulfill your request.

Each provider processes information according to its own privacy policy, terms, and applicable data-handling practices. We encourage you to review the relevant provider's policies before submitting sensitive or confidential information.

Please note that information sent to an AI provider may be processed on that provider's systems and may be subject to its retention and usage policies.

4. Third-Party Services

To operate and maintain the app, we may rely on trusted third-party service providers, including:

- **Authentication:** Apple and Google.
- **Hosting and storage:** Amazon Web Services (AWS) and Firebase.
- **Payments and subscriptions:** Apple, RevenueCat, and Stripe.
- **Analytics and diagnostics:** Services used to monitor performance and identify technical issues.

The specific services used may vary depending on the features available and the platform through which you access the app.

These providers may process information necessary to perform their services, subject to their applicable privacy policies, contractual obligations, and security practices.

5. Your Choices and Control

You have control over how you use the app and what information you choose to provide.

You can:

- Stop using the app at any time.
- Manage or revoke app permissions through your device settings.
- Choose what text, files, audio, or other information you submit to AI features.
- Avoid sharing sensitive or confidential information unless necessary for a feature.

Please note that restricting certain permissions or choosing not to provide specific information may affect the availability or functionality of some features.

6. Data Storage and Security

We retain information only for as long as reasonably necessary for the purposes described in this policy, unless a longer retention period is required or permitted by law.

Where appropriate, information may be deleted or anonymized when it is no longer needed.

We use reasonable technical and organizational safeguards designed to protect information against unauthorized access, loss, misuse, or disclosure. However, no digital system, storage method, or internet transmission can be guaranteed to be completely secure.

Unscaled crop from the native capture in source page 14, x=0, y=0, width=1280, height=1140. Contact details outside this detail are preserved in the complete source appendix.

What the linked documents explain, and what remains unclear

Record	Published position	Issue for this product
Apple privacy label	Data Not Collected	Not reconciled with the linked policy's conditional collection clauses
App description	On-device secrets, Keychain, no server upload	Policy does not map those promises to its external-processing clauses
Privacy page	AI inputs and multiple third-party providers	No authenticator-specific applicability explanation
Terms route	Privacy Policy body, separate effective date	No clear product-specific terms in the displayed document

Linked MB Apps privacy policy Linked MB Apps terms route

E1 pages 6–7 and 13–15; E3/E7/E8. Current drafting notes were read in the freshly retrieved page text; they are not claimed to appear in the earlier embedded source captures.

Muhammad Basit, MB Apps and the second app

Apple developer ID 6824482366 currently lists two apps. The individual seller is Muhammad Basit; MB Apps is the label on the shared legal pages and copyright. No incorporated company, beneficial-owner record or verified social profile was established for this publisher. A common personal name or studio abbreviation is insufficient to merge it with unrelated people or businesses.

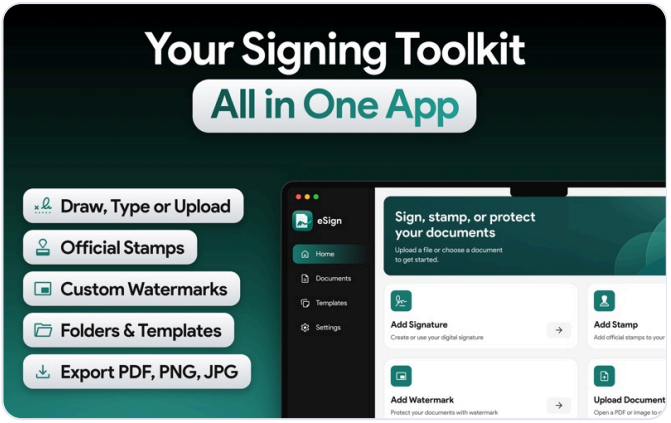
German and Irish disclosures identify the authenticator seller as a trader and declare Faisalabad, Pakistan. The Esignature listing repeats the same trader contact fields. This is app-specific declared business-location evidence, not a nationality claim and not evidence of wrongdoing.

Esignature-Sign Any Document, bundle com.mb.esignature.app, advertises signatures, stamps, document templates and watermarks. Its description links the same two legal pages used by the authenticator. Reuse of a generic AI policy is therefore relevant to both a security utility and a document-handling utility. The reviewed signing promotions do not establish an additional copied-brand allegation.

Apple's exact-ID records timestamp Esignature 1.1 at 06:31:52 UTC and Authenticator 1.1 at 06:32:12 UTC on 10 November. The twenty-second interval is a concrete same-account release association. It is not a link to another publisher, proof of fraudulent coordination, or the date the Apple account was created.



Original Apple icon for Esignature-Sign Any Document, app 6825320157. Same developer ID 6824482366; independently retrieved 10 November.



Original Apple Esignature promotion 1, retrieved 10 November. Product context for the shared-policy finding.

Current apps on the same verified Apple developer account

App	App ID / bundle	First-release field	Current version release
Esignature-Sign Any Document	6825320157 / com.mb.esignature.app	1 November 2026	1.1 · 10 November 06:31:52 UTC
Authenticator App for Desktop	6826168444 / com.mb.authenticator.app	3 November 2026	1.1 · 10 November 06:32:12 UTC

Muhammad Basit's Apple developer account Esignature-Sign Any Document

E2/E6/E9; current developer-software lookup and native Apple catalog. Two current apps is a checked storefront observation, not an all-time total.

Connections: one confirmed account, no verified wider network

The strongest connection is direct: the two apps share Apple's numeric developer ID, seller identity, paired legal URLs and trader contact information. Their bundle identifiers also share the com.mb prefix. Exact identifier and contact searches did not establish a separate Apple account, an earlier removed portfolio, a corporate shell or a prior enforcement case.

The previously reported Google-look authenticator under Mubashir Iqbal and the Authy-name report concerning Ahmad Waheed are relevant comparisons of presentation and disclosure risks. Their different sellers, app IDs and legal infrastructure do not connect them to Muhammad Basit. Pakistan, Gmail, Google Sites, a similar app category and a common name are not evidence of common control.

The Google Sites pages resolve and contain substantial text. The concern is their inadequate fit to the two products and the absence of a separate listed product/support website, not the fact that a hosted website builder was used. No custom domain, historic hosting provider or meaningful domain-registration trail was identified from the checked listing links.

Strength of the observed associations

Association	Evidence	Assessment
Authenticator ↔ Esignature	Same Apple developer ID and seller	Confirmed same publisher account
Both apps ↔ MB Apps pages	Exact matching legal URLs and contact fields	Confirmed shared published documents
Two 1.1 updates	Release timestamps twenty seconds apart	Confirmed timing; no separate-account inference
Other reviewed authenticator sellers	Similar product category or country only	No verified operator connection

Earlier Google-look authenticator investigation Earlier Authy-name investigation

E2/E6–E9/E12. Exact public contact values were checked privately and are not reproduced in the narrative.

The concrete questions for Apple

Apple should review the new icon against its copycat and intellectual-property rules, the consistency of the storefront identity and promotional imagery, and whether the linked documents accurately describe this app's handling of authentication material. Rules 2.3, 4.1, 5.2.1 and 5.1.1 are relevant; the paid options also require clear subscription disclosures under 3.1.2.

Public release notes are not the private Notes for Review. Their generic wording cannot establish that the developer concealed the artwork change from reviewers. The supplied chronology does establish that the new identity reached a live listing after release. No Apple ban, enforcement reason, verified consumer loss or credential theft is established by these records.

Buyers should check the seller before interpreting familiar security artwork as official affiliation. An app holding authentication secrets warrants clear product-specific documentation; this listing's mismatched documents do not provide that clarity.

E3/E7/E8/E10/E11. Editorial consumer warning based on the documented presentation and disclosure issues.

THE FULL RECORD

What else changed?

Five changed fields recorded by the supplied monitor. Earlier observation: 8 November 2026, 06:09 UTC (minute precision). Current capture: 10 November 2026, 07:17:44 UTC. Source risk labels are replaced here with descriptive review priorities.

▼ Compare all 5 recorded changes

▼ Icon BRANDING CONCERN

BEFORE	AFTER
Purple fingerprint with small lock	Blue padlock and layered shield with white tick

E1 page 1; new artwork independently matched to E2.

▼ Version RECORDED CHANGE

BEFORE	AFTER
1.0 · version-history entry 4 November 2026	1.1 · 10 November 2026

E1 pages 1 and 7; E2.

▼ Release notes RECORDED CHANGE

BEFORE	AFTER
No notes recorded	Bug Fixes; Engagement Enhanced

E1 page 1; current Apple listing. Not the private review submission notes.

▼ Size RECORDED CHANGE

BEFORE	AFTER
1.6 MB	1.4 MB

E1 page 1; displayed sizes, not a binary analysis.

▼ Category RECORDED CHANGE

BEFORE	AFTER
Productivity	Utilities

E1 page 1; E3.

▼ View the dates and timeline

1 November 2026

Esignature first-release field

Earliest current app on the checked developer account; not the date the account was opened.

3 November 2026

Authenticator first-release field

Apple exact-ID releaseDate; the separate 1.0 version-history entry is dated 4 November.

8 November 2026 · 06:09 UTC

Earlier purple icon observed

Minute precision as printed in the source comparison; original time 08:09 UTC+02.

10 November 2026 · 06:31:52 UTC

Esignature 1.1 released

Apple currentVersionReleaseDate.

10 November 2026 · 06:32:12 UTC

Authenticator 1.1 released

Apple currentVersionReleaseDate; twenty seconds after the related app.

10 November 2026 · 07:17:44 UTC

New blue identity captured

Supplied monitor detects five changed fields under the existing app ID.

10 November 2026 · 15:36 UTC onward

Independent checks

US, DE and IE listings, original Apple assets, developer catalog, legal pages and Microsoft reference checked; wider identity searches did not establish a second account.

CHECK THE SOURCES

The records behind this report.

The dossier combines this independent investigation with all 15 original source pages, including dated icons, Apple captures and the linked-policy captures. Additional original Apple artwork and promotions were retrieved independently. No binary was supplied, installed or tested, no purchase made, and no real account secret imported. The supplied file's visible source material remains intact; the source monitor's automated risk labels and comparison scores are not adopted as legal or fraud findings.

▼ Open source files, archive links and checksums

E1 / Complete supplied 15-page change report

Captured 10 November 2026, 07:17:44 UTC. Page 1 before/after; pages 2–4 identity, trader and portfolio; page 5 seven promotions; pages 6–7 description, version history and sources; page 8 continuation; pages 9–12 native Apple captures; pages 13–15 native privacy capture. All pages preserved in the appended source section. Original-source hash independently calculated.

`SHA-256: 35abff9f073905155b933e36cc54b5cf6cedf791ebd63b626f1c18b400096590`

E2 / Apple exact-ID and developer-software records

Retrieved 10 November 2026, 15:36 UTC. App IDs, names, seller/developer IDs, bundle IDs, release timestamps, original artwork and screenshot URLs. Developer lookup with entity=software returns artist and the same two software records; the macSoftware-filtered request returned only the artist record and is not used to imply an empty catalog.

Open source ↗

E3 / Fresh US, German and Irish authenticator listings

All three exact-ID pages returned HTTP 200 on 10 November at 15:36 UTC. Name/subtitle, blue icon, seven promotions, subscriptions, Data Not Collected label, exact legal links. DE and IE declare Muhammad Basit as trader in Faisalabad, Pakistan, consistent with source E1.

Open source ↗

E4 / Official Microsoft Authenticator and original icon

Retrieved 10 November 2026, 15:36 UTC; HTTP 200. Seller Microsoft Corporation, app ID 983156458, bundle com.microsoft.azureauthenticator. Original 512px Apple-hosted artwork downloaded independently, separate from the reviewed Mac product.

Open source ↗

E5 / Microsoft official download guidance

Checked 10 November 2026. Explicitly describes a mobile app and says Microsoft Authenticator is not available for PC or Mac. Used to distinguish an independent Mac product from an official desktop edition.

Open source ↗

E6 / Current Muhammad Basit Apple catalog

Retrieved 10 November 2026; HTTP 200. Two current app links: 6825320157 and 6826168444. Exact numeric developer identity corroborated by software lookup. No historic ban or additional developer account verified.

Open source ↗

E7 / Linked MB Apps privacy policy

Retrieved 10 November 2026, 15:36 UTC; HTTP 200. Effective date 20 October 2026. Full visible text read, including conditional technical collection, AI-provider transmission, third-party hosting/payment/analytics, under-nine clause and a published pre-publication editorial note. Original morning native capture also preserved in E1.

Open source ↗

E8 / Linked MB Apps terms route

Retrieved 10 November 2026, 15:36 UTC; HTTP 200. Site navigation says Term & Conditions; document body says Privacy Policy, effective 29 April 2026, with AI-services content and a pre-publication instruction. Both app descriptions link this exact route.

Open source ↗

E9 / Esignature-Sign Any Document — related app

Retrieved 10 November 2026, 15:36 UTC; HTTP 200. Same developer ID, individual seller, trader contact fields, copyright and exact two legal URLs. Original icon and five promotions inspected. App-specific document features recorded; no additional brand-copy allegation established.

Open source ↗

E10 / Microsoft trademark and brand guidance

Retrieved 10 November 2026; HTTP 200. Addresses product icons, permission and misleading affiliation. Used as relevant review context; no permission document or adjudication obtained.

Open source ↗

E11 / Apple App Review Guidelines

Retrieved 10 November 2026; HTTP 200. Accurate metadata 2.3, copycats 4.1, intellectual property 5.2.1, privacy 5.1.1 and subscriptions 3.1.2 checked. Private Notes for Review distinguished from public release notes.

Open source ↗

E12 / Exact-identifier searches and historical checks

Checked 10 November 2026. Exact app/developer IDs, support contact, policy slugs and bundle IDs searched against public search results and existing structured report corpus. No supported second-account, prior suspension or corporate ownership connection found. Archive discovery endpoint returned HTTP 503; source-record archive links are retained separately and not claimed independently replayed.

Open source ↗

E13 / Source-recorded Apple archive capture

Archive URL printed in source page 7. Not independently replayed during this investigation. Dated icon comparison relies on the supplied monitoring record, not this replay.

Open source ↗

E14 / Earlier documented generic-to-branded update pattern

Existing App Scam DB investigation, dated 22 October 2026. Saved 13/22 October records show a generic study chatbot changing to Claude/Anthropic wording and coral artwork; seller Anam Shehzadi declares Faisalabad, Pakistan. Used solely as a documented pattern comparison, not evidence of common ownership or confirmed App Review evasion.

Open source ↗

Authenticator App for Desktop

2FA, MFA & Authentication
Muhammad Basit

CHANGE SNAPSHOT · 5 changes detected · HIGH RISK · 10 Nov 2026, 09:17 (UTC+02:00)
compared with the snapshot of 08 Nov 2026, 08:09 (UTC+02:00)
Captured 2026-11-10 07:17:44 UTC · US App Store · App ID 6826168444

Risk indicators

• Brand terms mentioned in the description: google, apple, app store, windows
• The privacy policy is on a free site builder (Google Sites): https://sites.google.com/view/mbapps-privacypolicy/home
• The developer account published its first app 9 days ago (2026-11-01)
• Brand terms written in the screenshots: "google" in 1 of 7, "slack" in 1 of 7

What changed

Icon HIGH RISK



Before



After

Version LOW RISK

Before: 1.0 (2026-11-04)
After: 1.1 (2026-11-10)

What's New LOW RISK

Before: — (none)
After: Bug Fixes
Engagement Enhanced

Information › Size LOW RISK

Before: 1.6 MB
After: 1.4 MB

Information › Category LOW RISK

Before: Productivity
After: Utilities

App details (US App Store)

App name	Authenticator App for Desktop
Subtitle	2FA, MFA & Authentication
Developer	Muhammad Basit (ID 6824482366)
Seller	Muhammad Basit
Developer website	— (none listed on the App Store)
Privacy Policy	https://sites.google.com/view/mbapps-privacypolicy/home
Developer page	https://apps.apple.com/us/developer/muhammad-basit/id6824482366
Bundle ID	com.mb.authenticator.app
Category	Productivity, Utilities
Price	Free
Ratings	— (not enough ratings)
First released	2026-11-03
App Store link	https://apps.apple.com/us/app/authenticator-app-for-desktop/id6826168444?mt=12
App ID	6826168444

Pages linked from the listing

Privacy Policy

Link	https://sites.google.com/view/mbapps-privacypolicy/home
Status	working · page title: MB Apps
Hosted on	Google Sites (a free site builder)
Emails on the page	ipadapple058@gmail.com

Latest update

Version	1.1
Released	2026-11-10

What's New

Bug Fixes
Engagement Enhanced

EU App Store (IE) — provider / trader

App name	Authenticator App for Desktop
Provider	Muhammad Basit
Trader	Yes — identified as a trader
Statement	Muhammad Basit has identified itself as a trader for this app and confirmed that this product or service complies with European Union law.
Address	H 39 Tahir Town H203 R.B Manawala Faisalabad 38000 Pakistan
Phone Number	+92 3087130883
Email	ipadapple058@gmail.com
Store link	https://apps.apple.com/ie/app/authenticator-app-for-desktop/id6826168444?mt=12

Information that differs on the IE store

In-App Purchases	Yes Lifetime Pro: €34.99 Monthly Pro: €8.99 Yearly Pro: €22.99

Information

Seller	Muhammad Basit
Size	1.4 MB
Category	Utilities
Compatibility	Mac Requires macOS 13 or later.
Languages	English
Age Rating	4+
In-App Purchases	Yes Lifetime Pro: $29.99 Monthly Pro: $7.99 Yearly Pro: $19.99
Copyright	© 2026 @ mb apps

App Privacy

Data Not Collected

Icon compared with the official apps of the brands it mentions

	**This app**	
	Google Drive by Google official google app · App ID 507874739	**32%** different
	Slack by Slack Technologies, Inc. official slack app · App ID 618783545	**16%** different
	Apple Music by Apple official apple app · App ID 1108187390	**1%** different

The brands are those named in the listing (name, subtitle, description, text in the screenshots); the official app of a brand is the App Store app with the brand in its name and the most ratings. Similarity is an automatic estimate; from 52% the icons count as similar.

Developer account

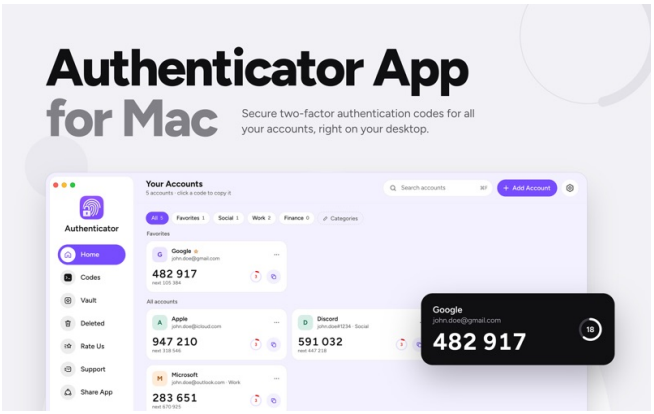
Developer	Muhammad Basit (ID 6824482366)
Apps on the US App Store	2
First app published	2026-11-01 (9 days ago)
Published in the last 90 days	2

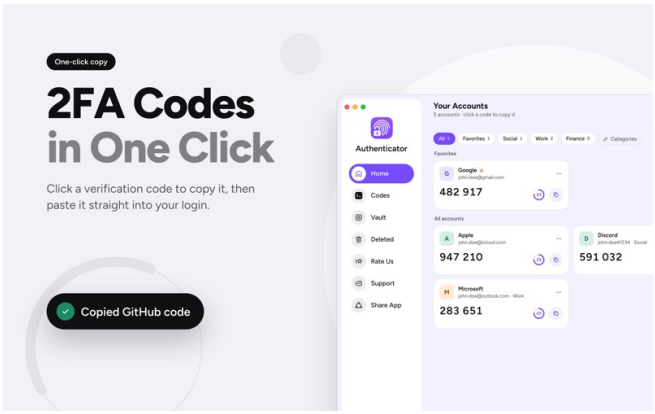
Apps of this developer account (oldest first)

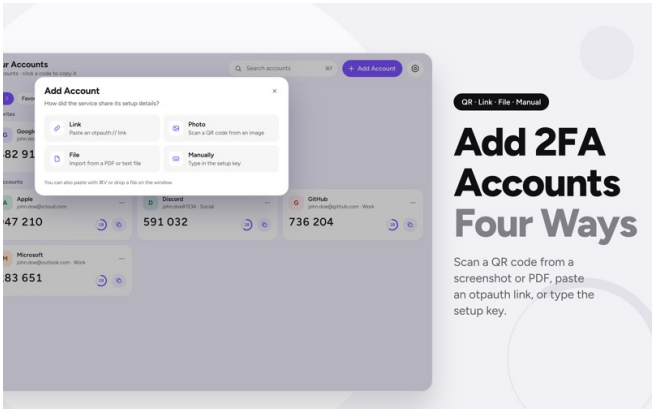
- Esignature-Sign Any Document · 2026-11-01 · 0 ratings · App ID 6825320157
- Authenticator App for Desktop · 2026-11-03 · 0 ratings · App ID 6826168444

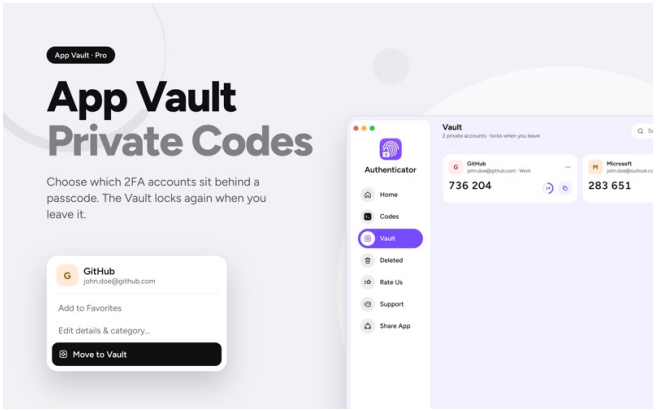
Screenshots

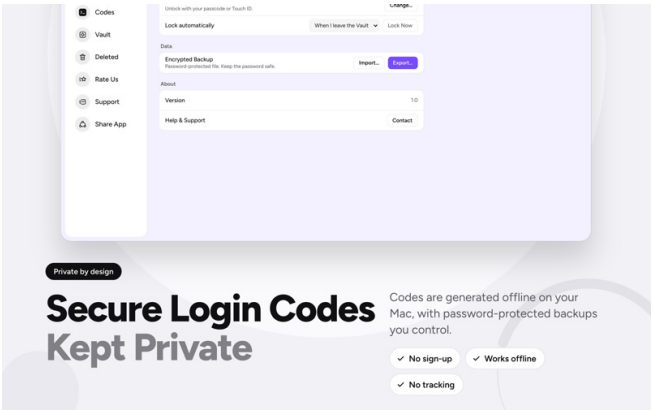
Mac (7)

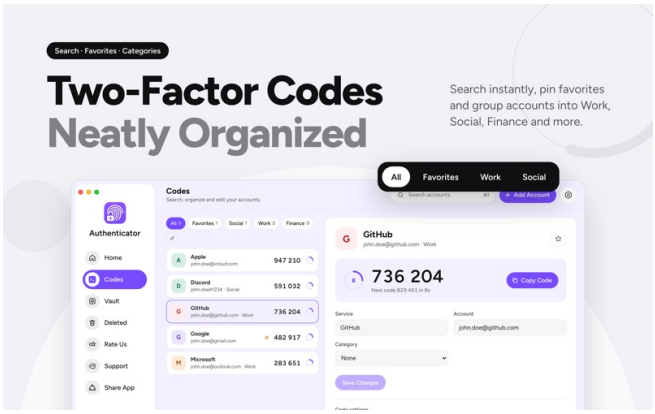


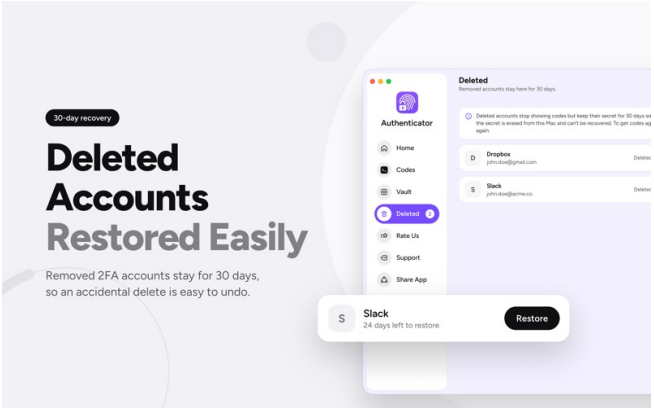












Description

Protect your online accounts with Authenticator App for Desktop, a simple and private two-factor authentication app built for your Mac. Generate secure one-time codes for the services you use, copy them with a single click, and keep sensitive accounts locked away in a private Vault - all stored securely on your Mac.

Whether you're signing in to email, social media, banking, work tools, or developer accounts, Authenticator gives you fast access to your verification codes without reaching for your phone.

Everything You Need for Two-Factor Authentication

Add Accounts in Seconds
Set up two-factor authentication your way. Paste a setup link, scan a QR code from a screenshot or photo, find a QR code inside a PDF or image file, or simply type in the setup key. You can even paste or drag and drop a QR image straight onto the window. Moving from another authenticator? Import transfer links to bring several accounts across at once.

One-Click Codes
Your codes are always front and center. Each account shows a large, easy-to-read code with a live countdown, so you know exactly how long it's valid. Click any code to copy it instantly, and see the next code before the current one expires. Copied codes are automatically cleared from your clipboard for extra privacy.

Keep Private Accounts in the Vault
Move your most sensitive accounts — like banking or work admin — into the Vault. Vault accounts are hidden from your main list and search, and their codes only appear after you unlock the Vault with your passcode or Touch ID.

Stay Organized
Pin favorites to the top, sort accounts into categories, and find any account instantly with search. Edit service names, account details, and categories at any time from the Codes view.

Secure, On-Device Storage
Your secrets never leave your Mac. Accounts are stored in the macOS Keychain, and codes are generated entirely on your device. No sign-up, no account, and nothing uploaded to a server.

Encrypted Backups
Create password-protected backups of all your accounts, including your Vault, and restore them whenever you need — perfect when moving to a new Mac.

Recover Deleted Accounts
Deleted something by mistake? Removed accounts stay in Deleted for 30 days, so you can restore them with a click.

Designed for Mac
Enjoy a clean, native Mac experience with Light and Dark mode, a compact sidebar for smaller windows, and handy keyboard shortcuts: ⌘N to add, ⌘F to search, ⌘1–9 to copy a code, and ⌘V to paste a setup link or QR image.

Key Features
• Generate time-based (TOTP) two-factor codes
• Add accounts by link, QR image, PDF, file, or setup key
• One-click copy with live countdown and next code preview
• Private Vault protected by passcode or Touch ID
• Favorites, categories, and instant search
• Secure storage in the macOS Keychain
• Password-protected encrypted backups
• 30-day recovery for deleted accounts
• Light and Dark mode with keyboard shortcuts

Authenticator Premium
Upgrade to Premium for unlimited accounts, an unlimited Vault, custom categories, and bulk import.

Premium is available as a monthly or yearly auto-renewing subscription, or as a one-time lifetime purchase.

Payment will be charged to your Apple ID account at confirmation of purchase. Subscriptions automatically renew unless canceled at least 24 hours before the end of the current period. Your account will be charged for renewal within 24 hours prior to the end of the current period. You can manage and cancel your subscriptions in your App Store account settings after purchase. Any unused portion of a free trial period will be forfeited when you purchase a subscription.
here are the links:
Privacy Policy: https://sites.google.com/view/mbapps-privacypolicy/home
Terms of Use: https://sites.google.com/view/mbapps-terms-conditions/home

Version history

1.1 · 2026-11-10
Bug Fixes
Engagement Enhanced

1.0 · 2026-11-04
—

Evidence and integrity

Captured (UTC)	2026-11-10 07:17:44 UTC
Source: US App Store page	https://apps.apple.com/us/app/authenticator-app-for-desktop/id6826168444?mt=12
Source: IE App Store page	https://apps.apple.com/ie/app/authenticator-app-for-desktop/id6826168444?mt=12
Source: privacy policy linked from the listing	https://sites.google.com/view/mbapps-privacypolicy/home
Web archive: US App Store page	https://web.archive.org/web/20261110071836/https://apps.apple.com/us/app/authenticator-app-for-desktop/id6826168444?mt=12
Web archive: IE App Store page	not archived yet (web.archive.org was busy; the bot tries again later and lists the link in the dossier)
Web archive: privacy policy linked from the listing	https://web.archive.org/web/20261110071855/https://sites.google.com/view/mbapps-privacypolicy/home

SHA-256 of the raw files captured for this snapshot

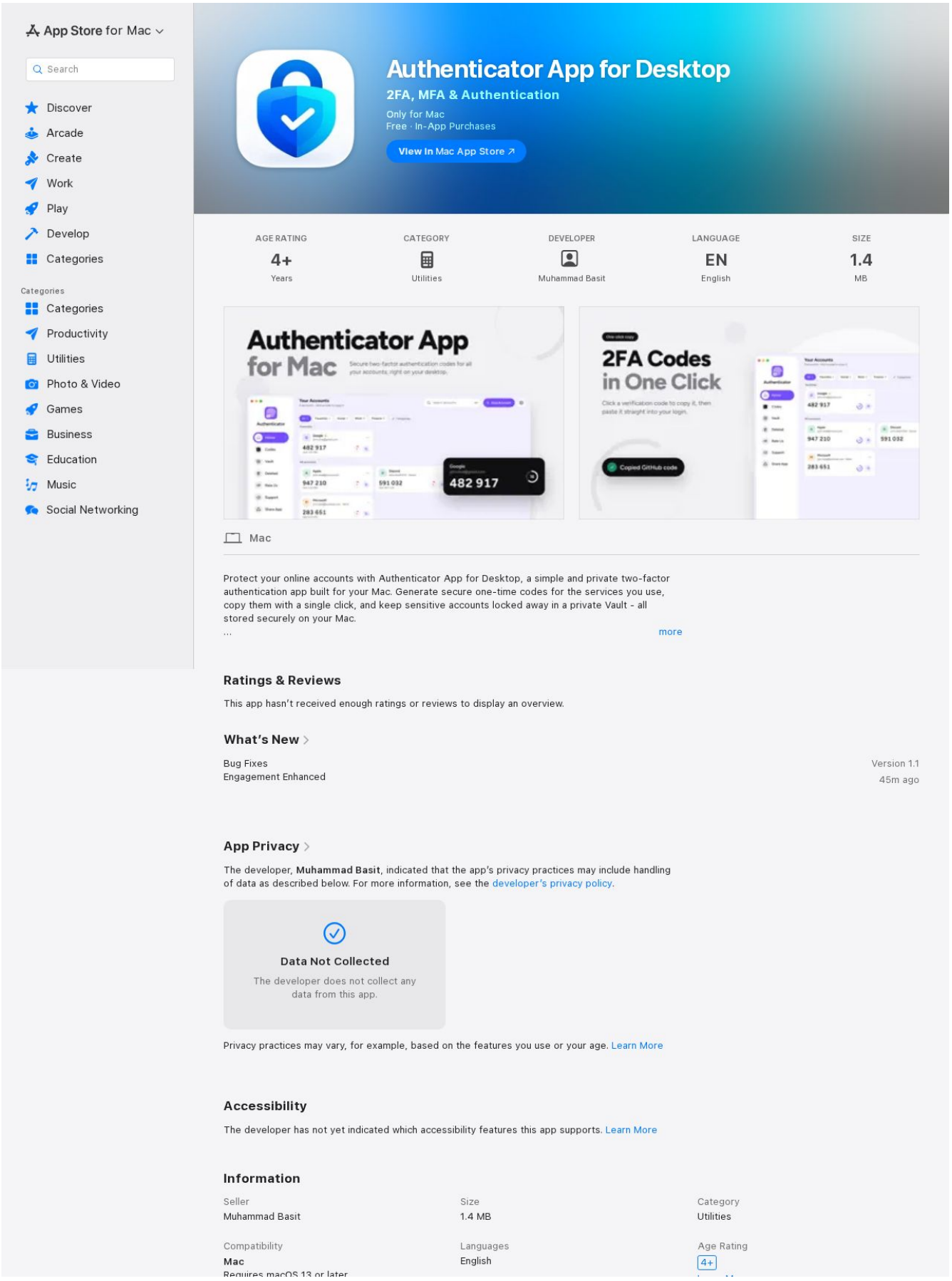
capture_ie.png	`42027f1016c5d1e1bd3415780903d9f838a671dc543d30e39e0519b15ba7ecb4`
capture_site-privacy-policy.png	`85d40a99ebd56aa7982378e613e5f5c34a1d72162d18427255159817cebdce5d`
capture_us.png	`41ee00fc11400032e2639d88d4ce33d1b0ee62b25b6fa75d18c686a689765c7a`
lookup_ie.json	`6e65ceeb05c5e0cb7be451c4bc9724fa9f2e353567f464eba69648f0eb69ad25`
lookup_us.json	`432d87fb51a617cb82543aff13a6d5eda869567b8c54a5a78d6a7fd28a2f5139`
page_ie.html	`a9dcf8b87ce3df504b43aff675ba33d3ccc0def401f085fa4aaa708bdcfa9792`
page_us.html	`cedeb6d83ef966f0dc95077f9b3e121356de8178d33502701bf8a00c7786ed1f`
site_privacy-policy.html	`11319bc9148d6da344ae2a5c04cc529ab8e6f71844e37e2a0052a9b0d13974f7`

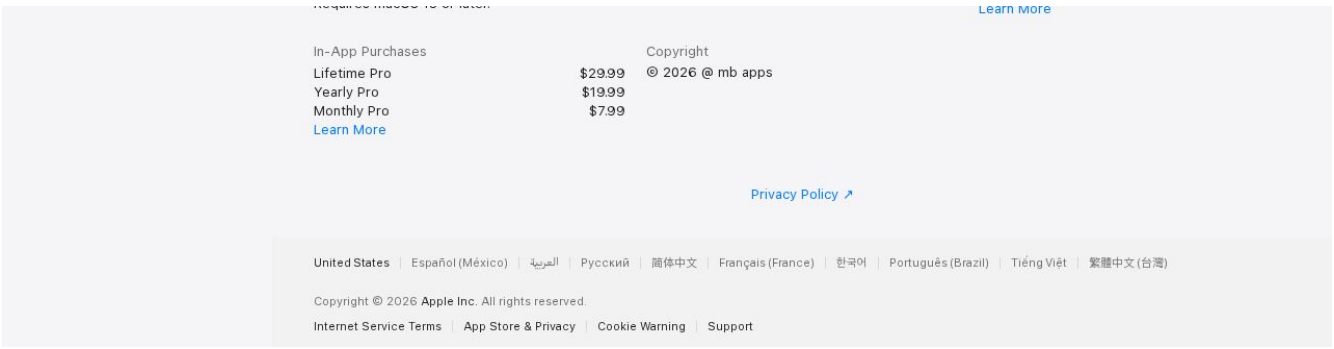
The raw answers from Apple, the page captures and the images are kept in the evidence archive that has the same name as this PDF. The SHA-256 of this PDF is written in that archive (SHA256SUMS.txt) and in the Telegram message that

delivered it.

Appendix — the US App Store page as displayed

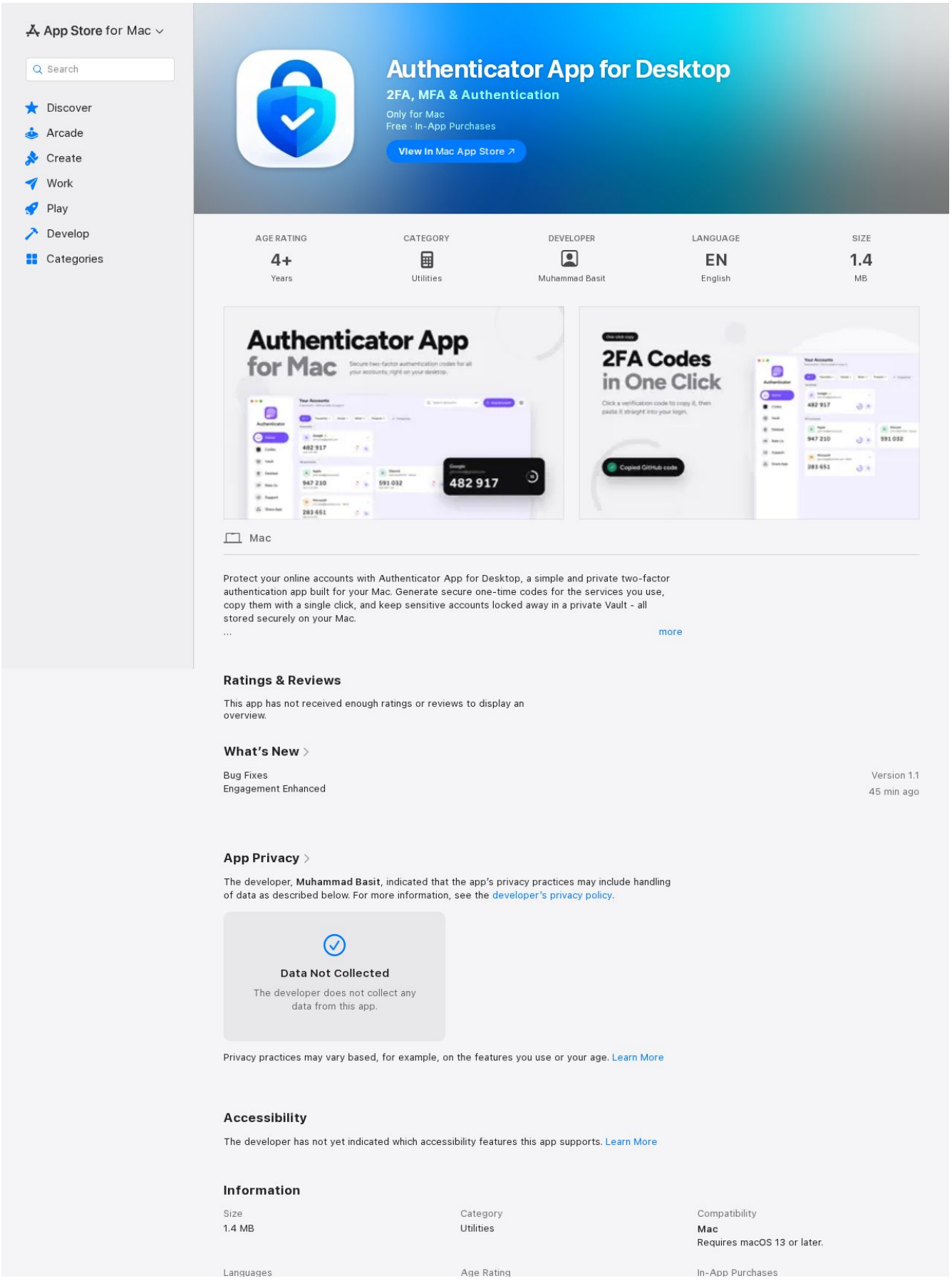
Full-page browser capture of https://apps.apple.com/us/app/authenticator-app-for-desktop/id6826168444?mt=12, taken 2026-11-10 07:17:44 UTC.




Learn More
In-App Purchases
Lifetime Pro $29.99
Yearly Pro $19.99
Monthly Pro $7.99
Learn More
Copyright
© 2026 @ mb apps
Privacy Policy ↗
United States | Español (México) | العربية | Русский | 简体中文 | Français (France) | 한국어 | Português (Brazil) | Tiếng Việt | 繁體中文 (台灣)
Copyright © 2026 Apple Inc. All rights reserved.
Internet Service Terms | App Store & Privacy | Cookie Warning | Support

Appendix — the IE App Store page as displayed

Full-page browser capture of https://apps.apple.com/ie/app/authenticator-app-for-desktop/id6826168444?mt=12, taken 2026-11-10 07:17:44 UTC.



English

4+
Learn More

Lifetime Pro €34.99
Yearly Pro €22.99
Monthly Pro €8.99
Learn More

Provider
Muhammad Basit has identified itself as a trader for this app and confirmed that this product or service complies with European Union law.

Address
H 39 Tahir Town
H203 R.B
Manawala
Faisalabad 38000
Pakistan

Phone Number
+92 3087130883

Email
ipadapple058@gmail.com

Copyright
© 2026 @ mb apps

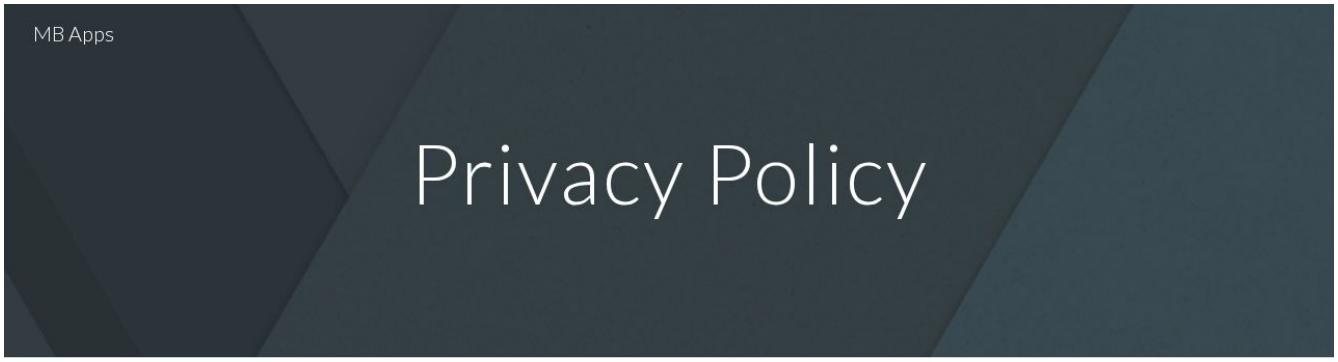
Privacy Policy ↗

Ireland

Copyright © 2026 Apple Inc. All rights reserved.
Internet Service Terms | App Store & Privacy | Cookie Warning | Support

Appendix — the privacy policy linked from the listing as displayed

Full-page browser capture of https://sites.google.com/view/mbapps-privacypolicy/home, taken 2026-11-10 07:17:44 UTC. Cookie-consent overlays (the host's, not the page's content) were hidden before the capture, and Google pages were opened in English.



Privacy Policy

Effective Date: October 20, 2026

A Note About Your Privacy

We believe your privacy matters. Our app is designed to provide useful features while collecting as little personal information as possible. This Privacy Policy explains what information may be collected, how it is used, and how we protect it.

1. Information We Collect

We aim to minimize the amount of information we collect.

Depending on how you use the app, we may collect limited technical information, such as:

- App version and device type.
- Crash reports and diagnostic logs.
- Anonymous usage statistics that help us understand how features are used.

We do not:

- Sell your personal information to third parties.
- Track your activity across other apps or websites.
- Collect sensitive personal information unless it is necessary for a specific feature and appropriately disclosed.

Information you enter into the app, such as notes, text, or other inputs, generally remains on your device unless a feature requires processing by an external service. Where applicable, the relevant data handling practices are explained in this policy.

2. How We Use Information

Any information we collect is used for legitimate operational and improvement purposes, including:

- Identifying and fixing bugs or crashes.
- Improving app performance, stability, and reliability.
- Understanding feature usage to improve the overall user experience.

We do not use collected information for purposes unrelated to operating, maintaining, or improving the app, except where otherwise disclosed or required by law.

3. AI Models and Third-Party Processing

Our app provides access to advanced artificial intelligence (AI) models operated by third-party providers.

Depending on the features you use and the AI model you select, information you submit, including text, files, or audio, may be transmitted to the relevant provider to process your request. These providers may include:

- OpenAI
- Anthropic (Claude)
- Google (Gemini)
- xAI (Grok)

Your submitted information is processed to generate AI responses or provide the requested functionality. We aim to transmit only the information reasonably necessary to fulfill your request.

Each provider processes information according to its own privacy policy, terms, and applicable data-handling practices. We encourage you to review the relevant provider's policies before submitting sensitive or confidential information.

Please note that information sent to an AI provider may be processed on that provider's systems and may be subject to its retention and usage policies.

4. Third-Party Services

To operate and maintain the app, we may rely on trusted third-party service providers, including:

- **Authentication:** Apple and Google.
- **Hosting and storage:** Amazon Web Services (AWS) and Firebase.
- **Payments and subscriptions:** Apple, RevenueCat, and Stripe.
- **Analytics and diagnostics:** Services used to monitor performance and identify technical issues.

The specific services used may vary depending on the features available and the platform through which you access the app.

These providers may process information necessary to perform their services, subject to their applicable privacy policies, contractual obligations, and security practices.

5. Your Choices and Control

You have control over how you use the app and what information you choose to provide.

You can:

- Stop using the app at any time.
- Manage or revoke app permissions through your device settings.
- Choose what text, files, audio, or other information you submit to AI features.
- Avoid sharing sensitive or confidential information unless necessary for a feature.

Please note that restricting certain permissions or choosing not to provide specific information may affect the availability or functionality of some features.

6. Data Storage and Security

We retain information only for as long as reasonably necessary for the purposes described in this policy, unless a longer retention period is required or permitted by law.

Where appropriate, information may be deleted or anonymized when it is no longer needed.

We use reasonable technical and organizational safeguards designed to protect information against unauthorized access, loss, misuse, or disclosure. However, no digital system, storage method, or internet transmission can be guaranteed to be completely secure.

7. Children's Privacy

This app is not intended for children under the age of 9. We do not knowingly collect personal information from children under 9.

If you believe a child has provided personal information through the app, please contact us at **ipadapple058@gmail.com** so we can review the matter and take appropriate action.

8. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes to the app, our services, or applicable legal requirements.

Any updates will be published on this page, along with a revised effective date where appropriate. If a change significantly affects how information is handled, we will make reasonable efforts to communicate that change.

We encourage you to review this page periodically to stay informed about our privacy practices.

9. Contact Us

If you have any questions, concerns, or requests regarding this Privacy Policy or how your information is handled, please contact us:

Email: ipadapple058@gmail.com

We will review your inquiry and respond as appropriate.

Our Privacy Commitment

We aim to collect as little information as possible, use it responsibly, protect it with reasonable safeguards, and never sell your personal information.

Important before publishing: This version is professionally rephrased, but make sure it accurately describes your actualapp. In particular, verify which AI providers and third-party services you use, whether user inputs are stored ortransmitted, and your data-retention practices. The policy should reflect your implementation rather than promise privacyprotections your app does not provide.