NACHWEISAPP / VERSION 1.4

Überprüfbare Originalaufnahmen

Technisches Whitepaper

Für Unternehmen, Auftraggeber und technische Entscheider.

NachweisApp verbindet Foto- und Videodokumentation mit kryptografischen Signaturen, einem aufnahmebezogenen Herkunftsbeleg und vertraulicher Übergabe. Empfänger können die erhaltene Datei selbst prüfen und das Ergebnis ihrem Vorgang zuordnen.

Diese Fassung erklärt das Zusammenspiel der Schutzfunktionen vom Auslösen bis zur Ablage. Neu aufgenommen sind bewusst freigegebene Fotoanfragen, geschützter Empfang, präzise Zertifikatangaben und die Weiterentwicklung der Serverdienste.

> **Eine nachvollziehbare Kette**
>
> Aufnehmen und signieren · Herkunft bestätigen · Vertraulich übergeben · Inhalt selbst prüfen · Zum Vorgang ablegen

Stand: 14. November 2026 · Version 1.4

Herausgeber: KI-Shield UG (haftungsbeschränkt)

nachweisapp.de · Öffentlicher Dateiprüfer

02 / TECHNISCHES WHITEPAPER

Dokumentation, die Empfänger prüfen können

Ein Foto wird wertvoller, wenn sein Inhalt, seine Herkunft und seine Zuordnung zum Vorgang nachvollziehbar bleiben.

Bei einer Fahrzeugübergabe, einem Schaden oder einer Bauabnahme zählt neben dem Motiv die verlässliche Dokumentation. NachweisApp ergänzt die Aufnahme um Prüfdaten. Der Empfänger kann kontrollieren, ob die vorliegende Datei zu den signierten Angaben und zum Herkunftsbeleg gehört.

Einsatz	Praktischer Nutzen
Übergaben und Abnahmen	Zustand und Details erfassen, Nachweise weitergeben und gemeinsam mit dem Protokoll aufbewahren.
Schadensdokumentation	Übersichts- und Detailaufnahmen einem Vorgang zuordnen und ihren technischen Prüfstatus festhalten.
Angeforderte Fotos	Eine konkrete Anfrage bewusst annehmen und die Antwort anhand ihrer signierten Anfragebindung zuordnen.
Zusammenarbeit mit Empfängern	Originaldateien in der App oder kostenlos im Browser prüfen, ohne für die Browserprüfung ein Konto anzulegen.

Was das positive Prüfergebnis bedeutet

„Original bestätigt“ steht für das Zusammenpassen des geschützten Medieninhalts, der erforderlichen Signaturen und des aufnahmebezogenen Herkunftsbelegs. Bei einer unterstützten Schwärzung bestätigt der Prüfer die Bindung der sichtbaren Bereiche an das Original. Vorhandene Zeitstempel fließen mit ihrem eigenen Prüfstatus ein.

Diese technischen Ergebnisse ergänzen die fachliche Bewertung des dokumentierten Vorgangs. Unternehmen erhalten eine klar gegliederte Grundlage für Rückfragen, Übergaben und die spätere Bearbeitung.

Orientierung im Dokument

Architektur und Dateibindung: Seiten 3-4 · Herkunft und Signaturen: Seiten 5-6 · Übergabe und Fotoanfragen: Seiten 7-8 · Schwärzung und Zertifikat: Seiten 9-10 · Betrieb und Versionsstand: Seiten 11-12 · Unternehmen und Quellen: Seiten 13-14

03 / TECHNISCHES WHITEPAPER

Vom Auslösen bis zur Prüfung

Die App sichert den Inhalt. Der Herkunftsdienst bestätigt einen gebundenen App-Vorgang. Der Empfänger prüft die erhaltene Datei.



Herkunftsprüfung: technische Belege, keine Bildpixel.

Dateiübergabe: gesonderter, auf dem Gerät verschlüsselter Transport.

1. Aufnahme und Kontext verbinden

Die App berechnet aus dem Medium und ausgewählten Kontextdaten kryptografische Hashwerte. Gerätesignaturen binden diese Angaben aneinander. Unterstützte Bilder erhalten zusätzlich eine signierte Kachelstruktur für selektive Schwärzungen.

2. App-Herkunft bestätigen

Eine kurzlebige Serveranfrage verbindet das Nachweismanifest mit Apple App Attest beziehungsweise Google Play Integrity. Der Dienst prüft die Belege nach seiner Freigaberichtlinie und stellt einen signierten, an die Aufnahme gebundenen Herkunftsbeleg aus. [4, 5]

3. Vollständigen Nachweis übergeben

Die Mediendatei trägt die zugehörigen Nachweisdaten. Im PNG-Format liegen diese im XMP-Metadatenblock. Ein Exportpaket kann außerdem ein Manifest, ein PDF-Zertifikat und eine Prüfanleitung enthalten. Die verschlüsselte Übergabe ist ein eigener Verarbeitungsschritt.

4. Inhalt beim Empfänger kontrollieren

Der Prüfer berechnet die relevanten Werte aus der erhaltenen Datei neu und kontrolliert Signaturen, Herkunftsbindung und vorhandene Zeitbelege. Ein Registertreffer unterstützt die Zuordnung; die inhaltliche Prüfung erfolgt an der Mediendatei.

04 / TECHNISCHES WHITEPAPER

Dateibindung und geschützte Ablage

Die technische Prüfung beginnt beim tatsächlich vorliegenden Inhalt. Ein gespeicherter Nachweis behält seine Zuordnung zur richtigen Datei.

Inhalt und Signaturen gehören zusammen

Der Medienhash ist der kryptografische Fingerabdruck des geschützten Inhalts. Der Prüfer berechnet ihn neu und vergleicht ihn mit den signierten Angaben. Zusätzlich kontrolliert er die klassischen und Postquantum-Signaturen, den signierten Kontext und die Bindungen des Herkunftsbelegs.

Fingerabdruck	Aufgabe
Medienhash	Bindet das Medium an die Signaturen. Beim beschriebenen PNG-Format umfasst die Berechnung die Dateibytes ohne den XMP-Nachweisblock.
Dateihash	Erfasst sämtliche Bytes der fertigen Exportdatei und dient dem Abgleich einer vollständig identischen Kopie.

Originale und empfangene Nachweise

Eigene Originalaufnahmen und eingehende Nachweise werden getrennt verwaltet. Beim Empfang wird die Zuordnung von Eintrag und Datei inhaltlich abgesichert. Eine vorhandene Aufnahme behält ihre Datei; weitere empfangene Fassungen werden anhand ihrer tatsächlichen Inhalte zugeordnet.

Unter Android werden zusammengehörige Speichervorgänge durch eine gemeinsame Zugriffssperre koordiniert. Dateien werden zunächst vollständig geschrieben und anschließend atomar übernommen. Inhaltsvergleiche begleiten die Ablage; auch das lokale Postfach wird atomar gespeichert.

Nutzen für die Vorgangsakte

Die Prüfung bezieht sich auf die erhaltene Datei. Die Ablage erhält die Verbindung zwischen dieser Datei, ihrem Eintrag und den zugehörigen Nachweisen. So bleibt die Dokumentation auch bei wiederholtem Empfang nachvollziehbar.

05 / TECHNISCHES WHITEPAPER

Herkunft pro Aufnahme

Ein eigener Herkunftsbeleg verbindet das konkrete Nachweismanifest mit einem serverseitig geprüften App-Vorgang.

Das Manifest verknüpft unter anderem Nachweiskennung, Medientyp, Medienhash, Fingerabdrücke der Geräteschlüssel und Kontextdaten. Bei unterstützten Bildern gehört auch die Kachelwurzel dazu. Der Herausgeber signiert den Herkunftsbeleg mit Ed25519 und ML-DSA-65.

Prüfschritt	iOS	Android
App-Prüfung	Apple App Attest: Registrierung und Assertion	Google Play Integrity: serverseitig ausgewerteter Token
Aufnahmebindung	Registrierte Schlüssel, Manifest und Challenge	Manifest, Schlüsselbesitz und gebundener requestHash
Frische	Kurzlebige Challenge und Assertion-Zähler	Kurzlebige Challenge und Prüfung der Tokenfrische
Freigabe	Explizite Build-Richtlinie	App-Zertifikat, zugelassene Version und Geräteverdict

Vertrauensanker beim Empfänger

Der Empfänger prüft den Herkunftsbeleg mit fest hinterlegten Herausgeberschlüsseln. Der Beleg muss zur Aufnahme, zu ihren Schlüsseln und zum signierten Kontext passen. Diese Bindung bleibt bei der Weitergabe der vollständigen Nachweisdatei erhalten.

Koordinierte Verarbeitung

Challenges, Zähler und die Erzeugung des Herkunftsbelegs werden im Serverprozess zusammengeführt. Datenbanktransaktionen sichern zusammengehörige Zustandsänderungen. Die zeitliche Begrenzung der Challenges und die Prüfung der Anfragebindung unterstützen die eindeutige Zuordnung eines Vorgangs.

Apple und Google stellen die Plattformverfahren bereit; NachweisApp wertet sie im eigenen Herkunftsprotokoll aus und stellt den aufnahmebezogenen Beleg aus. [4, 5]

06 / TECHNISCHES WHITEPAPER

Zwei Signaturverfahren, ein Inhalt

Ed25519 und ML-DSA-65 binden dieselbe Aufnahme mit unterschiedlichen kryptografischen Verfahren. Beide Prüfungen ergänzen sich.

Verfahren	Rolle im Nachweis
Ed25519	Klassisches Signaturverfahren aus der EdDSA-Familie nach RFC 8032. [2]
ML-DSA-65	Gitterbasiertes Postquantum-Signaturverfahren nach NIST FIPS 204. Es ergänzt die klassische Signatur mit einer anderen mathematischen Grundlage. [1]
SHA-256	Kryptografischer Fingerabdruck für definierte Inhalte und die Bindung der zugehörigen Nachweisdaten.

Doppelte Signierung in der Nachweiskette

Die ML-DSA-65-Signatur bindet einen Kontext ein, der den Medienhash und weitere Nachweisangaben enthält. Auch der Herkunftsbeleg des Dienstes trägt klassische und Postquantum-Signaturen. Der Prüfer kontrolliert die jeweils erforderlichen Signaturen zusammen mit der tatsächlichen Dateibindung.

Langfristige Dokumentation

ML-DSA wurde für den Schutz auch gegenüber leistungsfähigen Quantencomputern entwickelt. Die Verwendung von ML-DSA-65 ermöglicht, Nachweise bereits heute mit diesem zusätzlichen Signaturverfahren auszustatten. Die Standardangabe bezieht sich auf das eingesetzte Signaturverfahren. [1]

Schlüsselverwaltung auf dem Gerät

Die iOS-Implementierung verwendet für ML-DSA-65 die Secure-Enclave-Schnittstelle von CryptoKit. Unter Android werden die Signaturverfahren in Software ausgeführt; gespeicherte Schlüssel sind durch Keystore-gestützte Verschlüsselung geschützt. Die Prüfung verwendet die jeweils zugehörigen öffentlichen Schlüssel. [6]

Für die Aufbewahrung

Die vollständige Originaldatei mit ihren Nachweisdaten bildet die Grundlage späterer Prüfungen. Prüferstand und verwendete Vertrauensanker können zusammen mit dem Vorgang dokumentiert werden.

07 / TECHNISCHES WHITEPAPER

Vertrauliche Übergabe und lokale Prüfung

Der Inhalt wird auf dem Gerät verschlüsselt. Der Empfänger entschlüsselt die Übergabe und prüft die Nachweisdatei lokal.

Übergabeweg	Technisches Prinzip
Direkter Link-Versand	Frischer Schlüssel und AES-256-GCM. Der Schlüssel steht im Fragment der Linkadresse.
Antwort auf eine Anfrage	Das NWS2-Verfahren kombiniert X25519 und ML-KEM-768 zur Schlüsselableitung und verschlüsselt den Inhalt mit ChaCha20-Poly1305. [3]

Verschlüsselung vor dem Upload

Beim direkten Versand erhält der Transferdienst den verschlüsselten Datenblock. Der Schlüssel befindet sich hinter dem Fragmentzeichen der Linkadresse und wird beim normalen HTTP-Abruf nicht an den Webserver übertragen. Der vollständige Link wird deshalb gezielt an die berechtigten Empfänger weitergegeben.

Prüfung ohne Upload des Fotos

Nach dem vollständigen Laden der Prüfmodule läuft die Dateiprüfung im Browser lokal. Das ausgewählte Foto wird dabei nicht an den Prüfserver übertragen. Der Prüfer berechnet den Inhalt selbst neu und prüft die mitgelieferten Signaturen und Belege.

Eine gezielt ausgelöste Registerabfrage ist ein gesonderter Onlinevorgang. Sie dient der Zuordnung des Nachweises. Herkunftsprüfung und optionaler Transfer bleiben ebenfalls getrennt: Für den Herkunftsbeleg verarbeitet der Dienst technische Nachweisdaten wie öffentliche Schlüssel und Manifesthashes, keine Bildpixel.

Gezielt weitergeben und ablegen

Sensible Bildbereiche können vor der Weitergabe mit der vorgesehenen Schwärzungsfunktion verdeckt werden. Empfänger übernehmen erfolgreich erhaltene Nachweisdateien in ihre eigene Vorgangsablage. Der Transferdienst verwendet zeitlich begrenzte Aufbewahrung und kontrollierte Abrufabläufe.

08 / TECHNISCHES WHITEPAPER

Fotoanfragen mit bewusster Freigabe

Eine Anfrage führt zu einer gezielten Aufnahme. Annahme, sichtbare Zuordnung und Prüfung der Antwort bilden einen zusammenhängenden Ablauf.

Schritt	Verhalten in den beschriebenen App-Versionen
1. Entscheiden	Der Empfänger der Anfrage kann sie ausdrücklich annehmen oder ablehnen.
2. Zuordnung sehen	Eine aktive Anfrage bleibt in der Kamera sichtbar und kann beendet werden.
3. Gezielt aufnehmen	Die Freigabe gilt für das nächste Foto innerhalb von 15 Minuten. Beim Auslösen wird die Zuordnung zum Anforderer festgehalten.
4. Antwort prüfen	Eine Antwort wird anhand ihrer Nachweise geprüft und über ihre signierte Anfragebindung dem Vorgang zugeordnet.

Ein klar begrenzter Aufnahmeauftrag

Die Frist wird mit einer monotonen Uhr gemessen. Dadurch bleibt ihre Laufzeit von Änderungen der eingestellten Geräteuhr getrennt. Nach Ablauf endet die aktive Zuordnung. Dieser Ablauf unterstützt die bewusste Entscheidung, welche Aufnahme als Antwort auf welche Anfrage erstellt wird.

Verifizierter Empfang

Die Empfangsverarbeitung verbindet die Prüfung der Nachweisdatei mit der Kontrolle des signierten Anfragebezugs. Die Antwort wird dem passenden Vorgang zugeordnet und mit ihrer Datei gespeichert. Getrennte Ablage und Inhaltsvergleich schützen die Zuordnung bereits vorhandener Nachweise.

Beispiel: dokumentierter Fahrzeugzustand

Ein Auftraggeber fordert ein aktuelles Detailfoto an. Die Person vor Ort nimmt die Anfrage an, sieht den aktiven Auftrag in der Kamera und erstellt die Aufnahme. Beim Auftraggeber wird die geprüfte Antwort dem zugehörigen Vorgang zugeordnet.

Technischer Bezugsstand: iOS 1.1.3 (108) und Android 1.0.8 (152).

09 / TECHNISCHES WHITEPAPER

Selektive Schwärzung

Sensible Bereiche bleiben verdeckt. Für die sichtbaren Bildbereiche bleibt die Bindung an das Original technisch überprüfbar.

Signierte Kacheln statt eines bloßen Vorschaubildes

Ein unterstütztes Bild wird in ein Raster mit 20 mal 20 Kacheln aufgeteilt. Aus den Pixelwerten jeder Kachel und einem zufälligen Zusatzwert entsteht ein Hash. Ein Merkle-Baum fasst die Kacheln zu einer gemeinsamen Wurzel zusammen, die signiert und an den übrigen Nachweis gebunden ist.

Prüfung der sichtbaren Bereiche

Bei der Schwärzung werden ausgewählte Kacheln deckend schwarz ausgegeben. Für die verdeckten Bereiche werden die benötigten ursprünglichen Blatthashes mitgegeben. Die sichtbaren Kacheln berechnet der Prüfer aus dem erhaltenen Bild neu. So lässt sich die signierte Wurzel rekonstruieren, während die ursprünglichen verdeckten Pixel beim Ersteller bleiben.

Prüfgegenstand	Bedeutung
Vollständiges Original	Medienhash und erforderliche Signaturen passen zum vorliegenden Inhalt.
Geschwärzte Ableitung	Die sichtbaren Kacheln passen zur signierten Struktur des Originals. Der Prüfer kennzeichnet das Ergebnis als „Schwärzung bestätigt“.
Farbdarstellung	Unterstützte Farbprofile und Darstellungsmetadaten werden auf Konsistenz geprüft und in die Inhaltskontrolle einbezogen.

Konsistente Bildinterpretation

Für den Vergleich der sichtbaren Kacheln verwendet die Farbprüfung farbverwaltete sRGB-Pixel. Sie kontrolliert die unterstützten PNG-Farbangaben einschließlich ihrer Reihenfolge, Einmaligkeit und Konsistenz. Die Verarbeitung eingebetteter Farbprofile ist begrenzt. Dadurch beruht der Kachelvergleich auf einer definierten Interpretation der Bilddaten.

Die fachliche Auswahl der zu verdeckenden Bereiche erfolgt im dokumentierten Vorgang. Nach der Schwärzung wird die abgeleitete Nachweisdatei weitergegeben und geprüft.

10 / TECHNISCHES WHITEPAPER

Zeitbeleg und verständliches Zertifikat

Ein Zeitstempel ordnet das Vorliegen des Medienhashs zeitlich ein. Das PDF macht den ermittelten Prüfstatus für die Vorgangsakte lesbar.

Lokale Prüfung des Zeitbelegs

Webprüfer und native Apps prüfen vorhandene RFC-3161-Tokens kryptografisch. Dazu gehören Signatur, Medienhash, Zertifikatsbindung und die Kette zu hinterlegten Vertrauensankern. Die Apps kontrollieren beim Anfordern zusätzlich, ob die Antwort zur ursprünglichen Anfrage passt. [7]

Die von NachweisApp betriebene Zeitstempelstelle bestätigt, wann der Medienhash dort vorlag. Das Zertifikat weist die Ausstellungszeit eines erfolgreich geprüften Tokens in UTC aus. Signierte Aufnahmeangaben und der Zeitbeleg bleiben nachvollziehbar zugeordnet.

Angabe im Export	Nutzen für den Empfänger
Herkunftsstatus	Wird aus der Prüfung der zugehörigen Nachweisdatei übernommen.
Aufnehmendes Gerät	Die Gerätezeile bezieht sich auf das Gerät, mit dem die Aufnahme erstellt wurde.
Zeitstempelstatus	Zeigt an, ob ein gültiger Zeitbeleg vorliegt, nur lokale Zeitangaben vorhanden sind oder die Zeitprüfung kein positives Ergebnis liefert.
Datei- und Nachweisbezug	Verbindet das lesbare Zertifikat mit der zugehörigen Mediendatei und ihren Prüfdaten.

Plattformübergreifend dokumentieren

Empfangene iPhone-Aufnahmen einschließlich ihrer Bewegungsprüfungsdaten lassen sich in der beschriebenen Android-Version als Zertifikat aufbereiten. Der Herkunftsstatus und die Angaben zum aufnehmenden Gerät bleiben dabei an die ursprüngliche Aufnahme gebunden.

PDF und Original gemeinsam aufbewahren

Das PDF unterstützt die lesbare Dokumentation. Die vollständige technische Inhaltsprüfung erfolgt an der zugehörigen Mediendatei. Beide gehören zusammen in die Vorgangsakte.

11 / TECHNISCHES WHITEPAPER

Koordinierte Serverdienste

Die Serverdienste verbinden Herkunftsprüfung, Registrierung und Übergabe mit klaren Eingaberegeln und abgestimmter paralleler Verarbeitung.

Formatgeprüfte Registerdaten

Das Register prüft Kennungen, Hashes und Signaturfelder auf die vorgesehenen Formate. Für vollständige ML-DSA-65-Nachweise steht eine zusätzliche serverseitige Signaturprüfung zur Verfügung; ihr Ergebnis wird zum Eintrag dokumentiert. Das Register unterstützt die Zuordnung, während die vollständige Nachweisprüfung an der Mediendatei erfolgt.

Geregelte Anfrageverarbeitung

Adressbezogene Kontingente und ein übergreifendes Budget steuern Android-Herkunftsanfragen. Die adressbezogenen Regeln werden vor dem gemeinsamen Kontingent ausgewertet. Größenprüfungen begrenzen eingehende Anfragen früh im Verarbeitungsweg.

Abgestimmte Benachrichtigungen

Die Anmeldung von Benachrichtigungsgeräten wird pro Anfrage transaktional koordiniert. Die Grenze von fünf Geräten je Anfrage bleibt auch bei parallelen Anmeldungen wirksam. Push-Zustellungen erfolgen außerhalb der gehaltenen Datenbankverbindung.

Zeitstempel, Anker und Aufbewahrung

Zeitstempel- und Arweave-Verarbeitung werden außerhalb der zentralen Ereignisschleife ausgeführt. Der Zeitstempeldienst erzeugt frische Seriennummern. Die Aufbewahrungsverwaltung bestätigt eine Löschung nach erfolgreicher Ausführung und kann ausstehende Bereinigungen im regulären Ablauf erneut bearbeiten.

Die Upload-Verarbeitung bereinigt nicht abgeschlossene Dateiablagen. Die Portalprüfung berücksichtigt den aktuellen Freigabestatus des Zugangs. Zusammen unterstützen diese Maßnahmen die konsistente Verwaltung der Nachweis- und Übergabevorgänge.

Veröffentlichter Serverstand

Die beschriebenen Serverergänzungen sind seit dem 13. November 2026 veröffentlicht. Sie ergänzen die Schutzfunktionen der beschriebenen App-Versionen.

12 / TECHNISCHES WHITEPAPER

Qualität und technischer Bezugsstand

Gezielte Prüfungen begleiten die Entwicklung vom Dateiformat über die App bis zur parallelen Datenbankverarbeitung.

Komponente	Beschriebener Stand	Schwerpunkte
Webprüfer	0.4.5	Dateibindung, doppelte Signaturprüfung, Farbe, Schwärzung und lokale Zeitstempelprüfung.
iOS	1.1.3 (108)	Geschützter Empfang, bewusste Fotoanfragen und präzise Zertifikatangaben.
Android	1.0.8 (152)	Geschützter Empfang, atomare Ablage, Fotoanfragen und plattformübergreifender PDF-Export.
Serverdienste	13. November 2026	Eingabeprüfung, Anfragekontingente, koordinierte Geräteanmeldungen und entkoppelte Zusatzverarbeitung.

Die App-Funktionen in dieser Fassung beziehen sich auf die genannten Versionen. Die Bereitstellung erfolgt über die jeweiligen Stores. Maßgeblich für das eingesetzte Gerät ist die dort verfügbare und installierte Version.

Prüfungen entlang des tatsächlichen Ablaufs

Die projektinternen Prüfungen umfassen Originaldateien, Signatur- und Inhaltsabgleich, unterstützte Farbprofile, Schwärzungen, Zeitbelege, Import, Anfragezuordnung, Zertifikatexport und Speicherabläufe. Dabei werden die einzelnen Schutzfunktionen und ihr Zusammenspiel betrachtet.

Für die jüngsten Serverergänzungen wurden ergänzend 19 gezielte Modelltests und 12 Tests mit PostgreSQL erfolgreich ausgeführt. Die Datenbanktests prüfen insbesondere parallele Registrierungen und das Zusammenwirken mit den Kontingenten. Diese Angaben beschreiben den jeweiligen Testumfang.

Abgleich vor und nach Veröffentlichung

Zur Serververöffentlichung wurden Paket- und Laufzeitdateien abgeglichen. Nach dem Ausrollen wurden Dienstzustand, Datenbankanbindung und öffentliche Erreichbarkeit geprüft. Versionierte Pakete und Sicherungen ermöglichen eine nachvollziehbare Zuordnung des veröffentlichten Stands.

Die technischen Projektbelege werden beim Anbieter geführt.

13 / TECHNISCHES WHITEPAPER

Für prüfbare Nachweise.

NachweisApp wird von der KI-Shield UG (haftungsbeschränkt) entwickelt. Unser Ziel ist eine nachvollziehbare Dokumentation vom Ersteller bis zum Empfänger.



Johanna und René Bringezu mit dem TRIP Full Ticket für KI-Shield UG am 11. November 2026.

Die TRIP-Jury hat sich für uns entschieden

Am 11. November 2026 haben Johanna und René Bringezu bei StartYourTRIP ein **Full Ticket für KI-Shield UG** erhalten. Die Jury hat uns für das Accelerator-Programm ausgewählt. Das ist ein wichtiger Meilenstein für unser Unternehmen und für die Arbeit hinter NachweisApp.

TRIP ist der Thüringer Startup-Accelerator der **Stiftung für Technologie, Innovation und Forschung Thüringen (STIFT)** im Rahmen von ThEx innovativ. Das Programm begleitet innovative Teams bei der Entwicklung ihres Geschäftsmodells und Unternehmens. [8]

Wir freuen uns über das Vertrauen der Jury und die Zusammenarbeit mit der STIFT, dem TRIP-Team und den anderen ausgewählten Teams.

NachweisApp im eigenen Ablauf kennenlernen: nachweisapp.de/kontakt.html

14 / TECHNISCHES WHITEPAPER

Einsatz und Quellen

Eine vollständige Nachweisdatei, ein verständliches Prüfergebnis und die fachliche Zuordnung bilden gemeinsam die Vorgangsakte.

Ein klarer Ablauf im Unternehmen

1. Zweck festlegen. Vorgang, benötigte Ansichten und Beteiligte bestimmen.
2. Aufnehmen und übergeben. Nachweisdatei vollständig exportieren, bei Bedarf sensible Bereiche schwärzen und vertraulich versenden.
3. Als Empfänger prüfen. Originaldatei im aktuellen Prüfer öffnen und das Ergebnis dem Vorgang zuordnen.
4. Gemeinsam ablegen. Mediendatei, PDF, Kontext, Prüfzeitpunkt und Prüferstand aufbewahren.

Öffentliche technische Grundlagen

[1] NIST FIPS 204: ML-DSA

[2] RFC 8032: Ed25519 / EdDSA

[3] NIST FIPS 203: ML-KEM

[4] Apple: Establishing your app’s integrity

[5] Google: Play Integrity API

[6] Apple CryptoKit: SecureEnclave.MLDSA65.PrivateKey

[7] RFC 3161: Time-Stamp Protocol

[8] STIFT: Thüringer Startup-Accelerator TRIP

Technische Dokumentationsbasis

Diese Fassung baut auf Whitepaper 1.3 vom 10. November 2026 und den dokumentierten Produktquellen auf. Ergänzt wurden die App-Umsetzung vom 12./13. November, die zugehörigen Releasebelege, die isolierten Datenbankprüfungen sowie die bestätigte Serververöffentlichung vom 13. November 2026. Die Projektbelege liegen beim Anbieter vor.

Die Abschnitte zu Verfahren erläutern die eingesetzten technischen Standards. Die Produktabschnitte beschreiben ihre Umsetzung in den genannten Versionen. Der TRIP-Abschnitt dokumentiert die Juryentscheidung für die Teilnahme am Accelerator-Programm.

KI-Shield UG (haftungsbeschränkt)
nachweisapp.de · Datei prüfen · Impressum