STEIMER
STRATEGIE · GOVERNANCE · TECHNOLOGIE
TRANSFORMATION FÜR JUSTIZ, SICHERHEIT UND VERWALTUNG

David Steimer
Breitengässli 4 · 3800 Unterseen
david@steimer.ch · steimer.ch

KONZEPT / STUDIE

Standardisierte Metadaten für die Aktenbildung

Zielarchitektur für den Polizei- und Justizkontext

ADRESSAT	eCH-Fachgruppe Polizei/Justiz
GEGENSTAND	Fachkatalog Aktenobjekt-Metadaten
STATUS	Diskussionsgrundlage
STAND	29. September 2026
ANTRAGSTELLER	David Steimer
VERSION	0.4

KERNAUSSAGE
Nicht die Aktenordnung wird vereinheitlicht. Vereinheitlicht wird ein kleiner, belastbarer semantischer Kern pro Aktenobjekt. Aktenordnungen werden dadurch zu versionierten Sichten auf dieselben Objekte.

Unabhängiger Fachbeitrag. Keine Verbindung zur Staatsanwaltschaft des Kantons Bern.

Dokumentsteuerung

Feld	Festlegung
Zweck	Fachliche und technische Entscheidgrundlage
Dokumenttyp	Arbeitsentwurf · Version 0.4
Normative Sprache	«MUSS», «SOLL» und «KANN» im Antrags- und Modellteil bezeichnen vorgeschlagene Anforderungen
Prüfbasis	Beilagen des Auftraggebers sowie offizielle Quellen von eCH, Bundesamt für Justiz, ISO, HIS Schweiz, Justitia 4.0, W3C und IETF
Wesentliche offene Quelle	Der Arbeitsentwurf und die XSD von eCH-0303 sollen Ende 2026 beziehungsweise Anfang 2027 verfügbar werden. Der Feld- und Schemaabgleich ist unmittelbar danach vorzunehmen

ENTWURF · VERSION 0.4

CC BY 4.0 · © 2026 David Steimer

Inhaltsübersicht

Dokumentsteuerung 1
Inhaltsübersicht 2
1 Management Summary 3
2 Ausgangslage, Hauptthesen und Abgrenzung 4
2.1 Ausgangslage 4
2.2 Hauptthesen 4
2.3 Abgrenzung 5
3 Prüfung des Lösungskonzepts 5
3.1 Was für das Konzept zentral ist 5
3.2 Wichtige Präzisierungen 5
3.3 Der eigentliche Harmonisierungsgegenstand 6
4 Zielbild und Architektur 6
4.1 Grundsätze 6
4.2 Logisches Objektmodell 7
5 Vorgeschlagener Metadatenkatalog 7
5.1 Obligatorischer Kern 7
5.2 Fachliche Zuordnungen 8
5.3 Codelisten 8
5.4 Personen- und Organisationsdaten 9
6 Anwendbarkeit auf Beweismittel 9
6.1 Digitale Beweismittel 9
6.2 Physische Beweismittel 10
6.3 Gemeinsames und Trennendes 10
6.4 Chain of Custody als Querschnittsanforderung 10
7 Technische Umsetzungsvariante 12
7.1 Empfohlenes Paketmuster 12
7.2 Bindungsmodell 12
7.3 Beispiel eines XML-Manifests 13
7.4 XSD-Struktur 13
7.5 Konformitätsstufen 14
7.6 Abgrenzung und mögliche Weiterentwicklung: Referenzierung innerhalb von Aktenstücken 14
8 Einpassung in die Standardlandschaft 15
8.1 Bewertung eCH-0039 16
8.2 Bewertung eCH-0051 16
8.3 Bewertung eCH-0303 16
8.4 Bewertung eCH-0160 16
8.5 Bewertung der Chain-of-Custody-Standards 16
9 Verbesserungen und Einsparpotenzial 17
9.1 Erwartete Verbesserungen 17
9.2 Einsparmodell 17
9.3 Pilot-Messplan 17
10 Risiken und Stolpersteine 18
10.1 Recht und Informationssicherheit 19
11 Umsetzungsvariante und Vorgehensplan 19
11.1 Mögliche Zusammensetzung einer Arbeitsgruppe 19
11.2 Lieferobjekte (Entwurf) 20
11.3 Abnahmekriterien (Entwurf) 20
12 Begründung 20
12.1 Ziel und Geltungsbereich 20
12.2 Vorgeschlagene normative Inhalte 21
12.3 Abhängigkeiten und Koordination 21
12.4 Lieferobjekte und Qualitätssicherung 22
12.5 Risiken des Vorhabens 22
12.6 Erwarteter Nutzen 22
13 Quellen und Prüfbasis 22
13.1 Nachweis der zentralen Ableitungen 23
14 Schlussfolgerung 24

1 Management Summary

Ein standardisierter Metadatensatz kann die Aktenbildung und das Beweismittelhandling teilweise automatisieren, ohne eine schweizweit einheitliche Aktenordnung vorauszusetzen. Der Nutzen entsteht vor allem beim Erfassen, Übernehmen, Prüfen, Ordnen, Suchen und Weitergeben von Aktenobjekten. Die Aktenordnung wird dabei nicht abgeschafft. Sie wird als organisations- und verfahrensspezifische, versionierte Sicht auf einen gemeinsamen Objektbestand behandelt.

Für jedes Aktenobjekt soll ein obligatorisches, transportneutrales XML-Statement bestehen, das Nutzdateien und physische Objekte über persistente Identifikatoren referenziert und digitale Inhalte über kryptografische Prüfsummen bindet. Bei Dokumenten, die eine Behörde in einer Fachapplikation erzeugt, stehen die massgebenden Metadaten regelmässig vor der Signatur fest. Sie sollen deshalb zusätzlich vor dem Signieren strukturiert in das Dokument eingebettet werden, sofern das Dokumentformat dies zuverlässig und standardkonform erlaubt. Das XML-Statement bleibt für Austausch, Validierung und nicht einbettungsfähige Objekte die verbindliche Referenz.

Das Argument der Datensparsamkeit ist in diesem Bereich differenziert zu betrachten. Dossiernummern, Namen, Rollen, Verfahrenshandlungen und Dokumentdaten sind regelmässig bereits im Nutzinhalt enthalten. Standardisierte Metadaten machen sie in erster Linie zuverlässig maschinenlesbar. Der Standard soll deshalb nicht bloss Schlüssel übermitteln. Insbesondere Beteiligte sind mit einem verwendbaren strukturierten Basisdatensatz abzubilden. Empfänger ohne entsprechende Berechtigung benötigen gleichwohl strukturierte Namen, Rollen und weitere für die Zuordnung erforderliche Angaben.

Für Beweismittel reicht eine Kombination aus UUID, Prüfsumme und allgemeiner Provenienz nicht aus. Der Standard muss von Beginn an eine organisationsübergreifend übertragbare Chain of Custody unterstützen. Dazu gehören unveränderliche Ereignisdatensätze für Sicherung, Übernahme, Übergabe, Untersuchung, Kopie, Transformation, Öffnung, Neuversiegelung, Rückgabe und Vernichtung. ISO 22095:2020 kann dafür Begriffe und generische Modelle liefern. Für den Polizei- und Justizkontext sind jedoch insbesondere ISO 21043-2 für physische Gegenstände und ISO/IEC 27037 für digitale Beweismittel fachnäher. Eine belastbare Konformitätsaussage setzt die Auswertung der vollständigen Normtexte voraus und wird deshalb als zwingendes Arbeitspaket vor der Schemafreigabe vorgesehen.

> **Take-Away**
> Weiterverfolgen als «Fachkatalog Aktenobjekt-Metadaten» und dabei die Standards eCH-0039 und eCH-0051 wiederverwenden (sowie später eCH-0303).
> Die Unterstützung einer normgerechten Chain of Custody muss von Beginn an in das Modell.
> Die formatübergreifende Passagenreferenzierung wird als abgegrenzte Weiterentwicklung vorbereitet.

Frage	Befund	Konsequenz
Einheitliche Aktenordnung?	Nicht realistisch und nicht erforderlich	Nur Semantik und Bindung standardisieren
Metadaten direkt im Dokument?	Als alleinige Lösung zu fragil, bei behördlich erzeugten Dokumenten aber regelmässig vor der Signatur möglich	XML-Statement obligatorisch, strukturierte Einbettung vor Signatur soweit technisch möglich
eCH-0039?	Enthält Dossier-, Dokument- und Dateibasistypen	Profilieren und referenzieren, nicht duplizieren
eCH-0051?	Liefert Basistypen und Modulsystem. Handlungen gehören in Fachkataloge	Neuer Fachkatalog importiert eCH-0051
eCH-0303?	Passender Pilot und späterer Nutzer. Entwurf wird Ende 2026 beziehungsweise Anfang 2027 erwartet	Integrationsanhang unmittelbar nach Verfügbarkeit finalisieren
Beweismittel?	Anwendbar, aber Dokumentfelder reichen nicht	Erweiterungen für Herkunft, Integrität und Gewahrsam
Einsparung?	Plausibel, noch nicht empirisch belegt	Vor Normierung mit messbarem Pilot quantifizieren
Chain of Custody?	Von Beginn an zwingend unterstützbar. ISO 22095 allein ist für forensische Beweismittel zu allgemein	Ereignismodell und Evidenzprofile an ISO 21043-2 und ISO/IEC 27037 spiegeln. Volltexte vor Schemafreigabe auswerten
Paginierung und Passagenreferenz?	Eine dossierabhängige fortlaufende Pagina ist im dynamischen digitalen Dossier nicht stabil	Nicht normativer Bestandteil von V1. Optionalen Lokator-Erweiterungspunkt vorsehen und später ein hybrides Referenzmodell ausarbeiten

2 Ausgangslage, Hauptthesen und Abgrenzung

2.1 Ausgangslage

eCH-0051 V3.0.0 stellt einen modularen Basis-Datenkatalog für Polizei und Justiz bereit. eCH-0280 zeigt bereits, wie ein fachlicher Austauschstandard eCH-0039, eCH-0051 und eCH-0058 kombiniert. eCH-0303 soll den strukturierten Datenaustausch zwischen Polizeiorganen und Staatsanwaltschaften beziehungsweise Verwaltungsstrafbehörden standardisieren. Keines dieser Vorhaben normiert eine allgemeine Aktenordnung.

Diese Lücke ist nicht zwingend ein Fehler. Aktenordnungen bilden unterschiedliche Rechtsgebiete, Organisationsmodelle, Prozessphasen und lokale Arbeitsweisen ab. Selbst die beigezogene bernische Weisung zeigt eine mehrdimensionale Ordnung nach Personen, Sachverhalten, Verfahrenshandlungen und Dokumentarten. Eine einzige starre Hierarchie kann diese Dimensionen nur unvollständig ausdrücken.

Rechtlich bleibt die Aktenführung zentral. Art. 100 StPO verlangt für jede Strafsache ein Aktendossier. Die VEKJ konkretisiert im Entwurf vor allem Formate, Quittungen, Prüfsummen und die Digitalisierung physischer Unterlagen. Die Vernehmlassung zur VEKJ endete am 22. Juni 2026. Das Inkrafttreten der übrigen BEKJ-Bestimmungen ist derzeit auf den 1. Juli 2027 geplant. Der Termin ist als Planungsannahme und nicht als bereits feststehende Tatsache zu behandeln.

2.2 Hauptthesen

- Ein kleiner semantischer Kern kann organisationsübergreifend harmonisiert werden, auch wenn die lokale Ablage verschieden bleibt.
- Die meisten Kernmetadaten können bei systemerzeugten Aktenobjekten aus bestehenden Fachapplikationsdaten abgeleitet werden.
- Ein obligatorisches XML-Statement gewährleistet die transportneutrale Bindung. Bei behördlich erzeugten Dokumenten verbessert eine zusätzliche Einbettung vor der Signatur die Interoperabilität.

- Dokumente, digitale Beweismittel und physische Beweismittel benötigen ein gemeinsames Grundmodell und unterschiedliche Fachprofile.
- Die Unterstützung einer überprüfbaren Chain of Custody ist keine nachgelagerte Zusatzfunktion. Sie beeinflusst Identitäten, Ereignismodell, Versionierung, Integritätsnachweise, Signaturen, Empfängerbestätigungen und Tests und muss deshalb bereits im Grundmodell angelegt werden.

2.3 Abgrenzung

Der vorgeschlagene Standard regelt ausdrücklich nicht:

- eine schweizweit einheitliche Aktenordnung oder Faszikelstruktur
- die materiellrechtliche Frage, was zu den Akten gehört oder offengelegt werden muss
- Zugriffsberechtigungen, Geheimnisschutz oder Löschfristen als alleinige Rechtsgrundlage
- die Beweiswürdigung oder die Echtheit eines Objekts
- ein neues Transportprotokoll, eine Übermittlungsplattform oder ein Archiv-SIP
- die vollständige Verwaltung eines Asservatenlagers oder eines forensischen Labors
- die normative Festlegung einer schweizweiten Paginierung oder einer formatübergreifenden Referenzierung einzelner Passagen in der ersten Version. Das Datenmodell enthält jedoch einen optionalen Lokator-Erweiterungspunkt, damit eine spätere Lösung keine neue Objektidentität oder inkompatible Parallelstruktur benötigt.

Nicht abgegrenzt wird die fachliche Unterstützung einer Chain of Custody. Abgegrenzt bleibt lediglich der Betrieb eines vollständigen Asservaten-, Labor- oder Forensiksystems. Der Standard muss die beweisrelevanten Ereignisse, Nachweise und Beziehungen systemübergreifend transportieren können.

3 Prüfung des Lösungskonzepts

3.1 Was für das Konzept zentral ist

- Mehrdimensionale Semantik statt starrer Ordnerlogik. Ein Objekt kann gleichzeitig einer Person, einer Verfahrenshandlung, einem Sachverhalt und einer Dokumentart zugeordnet sein.
- Lokale Autonomie bleibt erhalten. Jede Behörde kann eine eigene Sicht definieren, solange die Ableitungsregeln transparent und versioniert sind.
- Metadaten entstehen nahe an der Quelle. Fachapplikationen kennen Fallnummer, Beteiligte, Rolle, Handlung, Ersteller und Zeitpunkt meist bereits.
- Die Nutzbarkeit überlebt Systemwechsel und Übermittlungen, sofern Inhalt, Identität, Metadatenversion und Integritätsnachweis gemeinsam transportiert werden.
- Der Ansatz passt zum Baukastenprinzip der eCH-Standards und lässt sich in bestehende Nachrichtenstandards einhängen.

3.2 Wichtige Präzisierungen

Ausgangsannahme	Kritik	Verbesserte Festlegung
Metadaten befinden sich direkt im Aktenstück	Als einzige Ablage ungeeignet für fremde Originale, grosse Binärdaten und physische Objekte	Obligatorisches XML-Statement. Bei behördlich erzeugten Dokumenten strukturierte Einbettung vor der Signatur als zusätzliche, gleichlautende Projektion
UUID genügt als Schlüssel	Eine UUID belegt weder Identität noch Inhalt noch Version	UUID plus Objektart, Metadatenversion, Prüfsumme, Provenienz und Relationsmodell
Dossier ist ein einfaches Feld	Aktenobjekte können mehrere Verfahren, Teilverfahren oder Bezugsrollen haben	Wiederholbare Fallreferenzen mit Behörde, lokaler Nummer und Bezugsrolle
Beteiligte werden nur über eine ID referenziert	Empfänger ohne Zugriff auf das Quellsystem oder ohne Berechtigung zur Nutzung einer Spezial-ID erhalten keine verwendbaren strukturierten Parteidaten	ID und strukturierter Basisdatensatz gemeinsam übermitteln. AHVN13 und andere beschränkte Identifikatoren nur im zulässigen Empfängerprofil

Ausgangsannahme	Kritik	Verbesserte Festlegung
Datensparsamkeit verlangt möglichst wenige Metadaten	Die meisten Angaben stehen bereits im Nutzinhalt und werden durch die Standardisierung primär maschinenlesbar	Den interoperablen Mindestbedarf vollständig strukturieren. Zusätzliche Offenlegung, Indexierbarkeit und Empfängerkreis gezielt begrenzen
Aktenordnung lässt sich vollständig ableiten	Ausnahmen, richterliche Entscheide und lokale Regeln bleiben	Teilautomatisierung mit Validierungs- und Ausnahmeprozess
Beweismittel sind Dokumente	Herkunft, Gewahrsam und Repräsentationen fehlen	Spezialisierte Evidenzprofile unter demselben Grundtyp
Prüfsumme und Provenienz genügen für Beweismittel	Sie belegen weder lückenlose Obhut noch Übergabe, Zustand, Siegelwechsel oder verantwortliche Stelle	Eigenes, unveränderliches Chain-of-Custody-Ereignismodell mit Verknüpfung, Empfangsbestätigung und Integritätsnachweisen
Eine Pagina kann die kanonische Referenz bilden	Eine dossier- oder ordnungsabhängige Nummer verliert bei Umordnung, Teilakten, Versionen und anderen Darstellungen ihre Stabilität	Kanonische Referenz auf Objekt, Repräsentationsstand und Selektor. Kurze menschliche Zitierform und ePagina nur als auflösbare Darstellung

3.3 Der eigentliche Harmonisierungsgegenstand

Die Harmonisierung der Aktenordnung wird nicht beseitigt, sondern auf eine realistischere Ebene verschoben. Zu harmonisieren sind Begriffe, Identifikatoren, Beziehungen, Codelisten und Mindestqualitäten. Besonders anspruchsvoll sind Dokumentarten, Verfahrenshandlungen und Beteiligtenrollen. Diese Codelisten brauchen Eigentümer, Versionierung, Übersetzungen, Änderungsverfahren und Regeln für lokale Erweiterungen.

> **LEITPRINZIP**
> Standardisieren, was interoperabel verstanden werden muss. Lokal lassen, was nur die Präsentation oder Arbeitsorganisation betrifft.

4 Zielbild und Architektur

Das Zielbild trennt Nutzinhalt, fachliche Metadaten, Transport und Sichtbildung. Dadurch kann dasselbe Aktenobjekt über eCH-0039, eine eCH-0303-Nachricht, eine Plattform nach BEKJ oder eine andere zulässige Lösung übertragen werden, ohne dass sein fachlicher Kern neu erfunden wird.

SICHTEN	Aktenordnung A	Aktenordnung B / Akteneinsicht / Archivsicht
REGELN	Versionierte Zuordnungsregeln	Codelisten und Ausnahmeentscheide
METADATEN	Aktenobjekt-Manifest	UUID, Fallbezug, Handlung, Rolle, Art, Provenienz, Integrität, Gewahrsam und optionaler Lokator
INHALT	Digitale Repräsentationen	Physisches Objekt mit persistenter Kennzeichnung
TRANSPORT	eCH-0039 / eCH-0303 / VEKJ	Dateiablage, Paket, Referenz oder Plattform

4.1 Grundsätze

- Obligatorisches XML-Statement. Jedes Aktenobjekt verfügt über eine transportneutrale, maschinenlesbare Metadatenrepräsentation.
- Einbettung vor Signatur. Bei behördlich erzeugten Dokumenten werden die Metadaten soweit formattechnisch möglich zusätzlich vor der Signatur in das Dokument eingebettet.
- Persistente Identität. Die UUID eines logischen Aktenobjekts bleibt bei Übermittlungen erhalten.

- Explizite Versionen. Inhalt, Repräsentation, Metadaten und Klassifikationsschema werden getrennt versioniert.
- Mehrfachzuordnung. Ein Objekt kann mehreren Dossiers, Personen, Handlungen und Ordnungssichten zugeordnet sein.
- Provenienz. Jedes automatisch erzeugte oder geänderte Metadatum muss Herkunft, Zeitpunkt und Erzeugungsart nachvollziehbar machen.
- Interoperabler Mindestumfang. Der obligatorische Kern enthält alle Angaben, die ein Empfänger ohne Zugriff auf fremde Register zur fachlichen Zuordnung benötigt.
- Kontrollierte Redundanz. Schlüssel und strukturierte Sachdaten dürfen gemeinsam geführt werden. Ihre Herkunft, ihr Stand und ihre Version müssen erkennbar sein.
- Erweiterbarkeit. Lokale Felder liegen in eigenen Namensräumen und dürfen die Kernbedeutung nicht verändern.
- Technologieoffenheit. XML ist normative Referenzdarstellung. Eine JSON-Abbildung kann zusätzlich spezifiziert und gegen XML getestet werden.
- Ereignisbasierte Chain of Custody. Beweisrelevante Vorgänge werden als unveränderliche, typisierte und untereinander verknüpfte Ereignisse erfasst. Korrekturen überschreiben kein Ereignis, sondern referenzieren es mit einem neuen Korrektur- oder Aufhebungsereignis.

4.2 Logisches Objektmodell

Der abstrakte Typ «Aktenobjekt» bildet die gemeinsamen Eigenschaften. «Dokument», «digitales Beweismittel» und «physisches Beweismittel» spezialisieren ihn. Eine digitale Repräsentation ist nicht mit dem logischen Dokument gleichzusetzen. Ein Einvernahmeprotokoll kann etwa als signiertes PDF/A, als bearbeitbare Quelle und als OCR-Derivat vorliegen.

Entität	Zweck	Zentrale Beziehungen
Aktenobjekt	Logische, verfahrensrelevante Einheit	gehört zu Fall, betrifft Beteiligte, entstand aus Handlung
Repräsentation	Konkrete digitale Datei oder physische Ausprägung	repräsentiert Aktenobjekt, ist Version oder Derivat
Fallreferenz	Verknüpfung zu Dossier oder Verfahren	Behörde, lokale Nummer, Bezugsrolle
Beteiligtenbezug	Verknüpfung zu Person oder Organisation mit strukturiertem Basisdatensatz	Identifikatoren, Namen, Rolle, Gültigkeit und Datenstand
Verfahrenshandlung	Fachliches Ereignis, das Objekt erzeugt oder betrifft	Art, Zeitpunkt, ausführende Stelle
Klassifikationszuordnung	Einordnung in eine konkrete Aktenordnung	Schema, Version, Knoten, Gültigkeit, Methode
Integritätsnachweis	Bindung der digitalen Bytes	Algorithmus, Prüfsumme, Grösse, Zeitpunkt
Gewahrsamsereignis	Nachvollzug von Obhut, Kontrolle und beweisrelevanter Verarbeitung	Vorgängerereignis, Objekt und Repräsentation, Übergabe und Empfang, Person oder Stelle, Zeit, Ort, Zustand, Siegel, Hash und Attestation
Lokator	Optionaler Erweiterungspunkt für eine spätere Referenz auf Seiten, Passagen, Zeitabschnitte oder Bildbereiche	Aktenobjekt, Repräsentationsstand, Selektor, menschliche Zitierform und Resolver-URI

5 Vorgeschlagener Metadatenkatalog

5.1 Obligatorischer Kern

Feldgruppe	Vorgeschlagene Kardinalität	Inhalt und Begründung
recordObjectId	1	UUID des logischen Aktenobjekts. Bei Übernahme unverändert

Feldgruppe	Vorgeschlagene Kardinalität	Inhalt und Begründung
objectCategory	1	Dokument, digitales Beweismittel oder physisches Beweismittel
title	1..n	Kurzbezeichnung mit Sprachangabe. Übernimmt die Titelidee aus eCH-0039
caseReference	1..n	Behörde, lokale Fallnummer, Bezugsrolle und optional Teilverfahren
provenance	1	Quellsystem oder Quellstelle, Erzeugungszeit, Erzeugungsart und verantwortliche Stelle
metadataVersion	1	Versionsnummer, Zeitstempel und Status des Metadatensatzes
representation	0..n	Dateireferenz oder physische Kennzeichnung. Bei digitalem Inhalt mit MIME-Typ, Grösse und Prüfsumme
relation	0..n	Typisierte Beziehungen wie Beilage zu, Version von, abgeleitet aus, ersetzt oder Duplikat von
custodyEvent	0..n, im Evidence-Profil 1..n	Unveränderliche, verknüpfte Ereignisse zu Sicherung, Obhut, Übergabe, Empfang, Untersuchung, Kopie, Transformation, Siegel und Abschluss
locator	0..n, in V1 optional	Vorbereiteter Erweiterungspunkt für Objekt-, Repräsentations- und Passagenreferenzen. Selektorsemantik wird erst in einer Weiterentwicklung normiert

5.2 Fachliche Zuordnungen

Feld	Kardinalität	Hinweis
proceduralAction	0..n	Code der Verfahrenshandlung, Bezeichnung, Zeitpunkt oder Zeitraum, ausführende Stelle
documentKind	0..n	Dokumentart. Nicht mit Verfahrenshandlung gleichsetzen
participant	0..n	Identifikatoren, strukturierter Basisdatensatz, Verfahrensrolle, Gültigkeit und Beziehung zum Objekt
subjectMatter	0..n	Sachverhalt, Delikt, Gegenstand oder Themenreferenz
createdAt / receivedAt / registeredAt	0..1 je Feld	Verschiedene Zeitpunkte nicht in ein einziges «Datum» pressen
creator / issuer / owner	0..n	Rollen explizit benennen
classificationAssignment	0..n	Schema-ID, Schemaversion, Positionscode, Gültigkeit, Zuweisungsmethode
confidentialityMarking	0..n	Hinweis für Weiterverarbeitung. Ersetzt keine Berechtigungsprüfung

5.3 Codelisten

Codelisten dürfen nicht unkontrolliert in jeder Fachapplikation entstehen. Der Standard soll das eCH-0051-Muster aus Domäne, Kategorie und Wert übernehmen. Für dynamische Listen ist eine versionierte externe Publikation zweckmässig. Der XML-Schema-Kern sollte keine häufig ändernden Fachwerte fest einbauen.

Liste	Governance-Vorschlag	Umgang mit lokalen Werten
Objektkategorie	Klein und normativ im Standard	Keine lokalen Alternativen, nur definierte Erweiterungspunkte
Verfahrenshandlung	Fachgruppe Polizei/Justiz mit Fachkatalogverantwortlichen	CodeOrFreetext mit Domain und Version
Dokumentart	Gemeinsamer Kern plus domänenspezifische Ergänzungen	Lokaler Namespace und Mapping auf Oberkategorie

Liste	Governance-Vorschlag	Umgang mit lokalen Werten
Verfahrensrolle	Abgleich mit bestehenden Fachkatalogen und Rollenmodellen	Zeitlich gültige lokale Rolle mit Oberrollen-Mapping
Relationstyp	Klein und normativ	Erweiterung nur bei dokumentierter Semantik
Klassifikationsschema	Je Behörde oder Fachbereich	Schema-ID und Version obligatorisch

5.4 Personen- und Organisationsdaten

Eine reine Schlüsselstrategie genügt für den organisationsübergreifenden Austausch nicht. Der Empfänger kann einen fremden Schlüssel möglicherweise nicht auflösen. Zudem darf er einen besonderen Identifikator wie die AHVN13 je nach Rechtsgrundlage und Empfängerkonstellation nicht systematisch verwenden. Der Standard soll deshalb neben zulässigen Identifikatoren einen strukturierten Basisdatensatz übermitteln, der für Anzeige, Suche und fachliche Zuordnung ausreicht. Dazu gehören namentlich Name beziehungsweise Firma, Verfahrensrolle, soweit erforderlich Geburtsdatum oder Sitz sowie der fachlich relevante Gültigkeits- und Datenstand.

Dies ist keine unkontrollierte Verdoppelung. Die Angaben sind im Akteninhalt regelmässig bereits vorhanden und werden für die Interoperabilität strukturiert wiedergegeben. Der Standard muss jedoch Herkunft, Erhebungs- oder Bestätigungszeitpunkt und Empfängerprofil kenntlich machen. Welche Applikation bei Abweichungen den Schlüssel auflöst, den mitgelieferten Datenstand übernimmt, beide Stände vergleicht oder eine fachliche Prüfung verlangt, ist eine Frage der darstellenden beziehungsweise empfangenden Anwendung. Der Standard muss den Konflikt erkennbar machen, aber keine allgemeine Vorrangregel für alle Verfahren und Systeme vorgeben.

DATENSPARSAMKEIT RICHTIG EINORDNEN
Zu minimieren sind vor allem zusätzliche Offenlegung, unnötige Spezialidentifikatoren und zu breite Empfängerkreise. Nicht sachgerecht wäre ein so schmaler Metadatensatz, dass berechtigte Empfänger den bereits im Dokument enthaltenen Sachverhalt nicht strukturiert nutzen können.

6 Anwendbarkeit auf Beweismittel

6.1 Digitale Beweismittel

Das Grundmodell ist anwendbar, wenn das digitale Beweismittel nicht auf eine einzelne Datei reduziert wird. Ein Mobiltelefonabzug, eine forensische Image-Datei, ein Export, eine Arbeitskopie und ein Bericht sind unterschiedliche Repräsentationen oder Aktenobjekte mit expliziten Beziehungen.

- Erwerbs- oder Sicherungsereignis mit Zeitpunkt, Stelle, Rechtsgrund und Quelle
- Quellgerät oder Quellmedium mit möglichst stabiler Referenz
- Werkzeug, Version und Methode der Akquisition, soweit beweisrelevant
- Prüfsumme des Originals und jeder relevanten Repräsentation
- Repräsentationsrolle wie Original, forensisches Abbild, Arbeitskopie, Export oder Derivat
- Gewahrsams- und Übergabeereignisse
- Verknüpfung zwischen Beweismittel, Auswertungsauftrag, Ergebnis und Bericht

WICHTIG
Originalformate werden nicht in PDF/A umgewandelt, nur um sie in eine Akte einzufügen. Original, forensische Sicherung und lesbare Derivate werden getrennt referenziert und kryptografisch gebunden.

6.2 Physische Beweismittel

Auch physische Beweismittel können dem abstrakten Aktenobjektmodell folgen. Das XML befindet sich naturgemäss nicht im Gegenstand. Auf dem Gegenstand oder der Verpackung befindet sich eine persistente maschinen- und menschenlesbare Kennzeichnung, etwa QR-Code und Klartext-ID. Der kanonische Metadatensatz wird als obligatorisches XML-Statement geführt und im führenden System verwaltet.

- persistente Asservat- oder Objekt-ID
- Beschreibung, Menge, Einheit, Zustand und gegebenenfalls Gefahrenhinweise
- Verpackungs- und Siegel-ID sowie Siegelzustand
- aktueller Lagerort mit Ereignishistorie
- Sicherstellung, Eingang, Untersuchung, Übergabe, Öffnung, Neuversiegelung und Herausgabe als Ereignisse
- Verknüpfte Fotos, Scans, Protokolle und Berichte als eigene Aktenobjekte

Das Ereignisprofil bildet die für den organisationsübergreifenden Austausch erforderlichen Teile der Chain of Custody ab. Es ersetzt weder die physische Sicherung noch das führende Asservatenmanagement. Die beigezogene bernische Weisung verlangt bei separat gelagerten Gegenständen bereits eine eindeutige Auflistung im Dossier. Der vorgeschlagene Standard verbindet diese Referenz mit Zustand, Verpackung, Siegel, Lagerung und Übergaben und macht sie systemübergreifend prüfbar.

6.3 Gemeinsames und Trennendes

Aspekt	Dokument	Digitales Beweismittel	Physisches Beweismittel
Persistente ID	Ja	Ja	Ja, zusätzlich Kennzeichnung
Fall- und Rollenbezug	Ja	Ja	Ja
Dateiprüfsumme	Für digitale Repräsentationen	Zentral	Nur für digitale Abbilder
Gewahrsamskette	Bei gewöhnlichen Dokumenten nur bei Bedarf. Im Evidence-Profil obligatorisch	Im Evidence-Profil ab Identifikation oder Akquisition obligatorisch	Im Evidence-Profil ab Sicherung obligatorisch
Original unverändert	Bei signierten oder beweisrelevanten Dateien	Zwingend	Physischer Zustand dokumentiert
Speicherort	Paketpfad oder URI	Repository, Forensikspeicher oder Paket	Lagerort und Behältnis

6.4 Chain of Custody als Querschnittsanforderung

Provenienz, Integrität und Chain of Custody sind getrennte, miteinander verbundene Konzepte. Provenienz beschreibt Herkunft und Entstehung. Ein Hashwert erlaubt den Vergleich digitaler Bytes. Die Chain of Custody dokumentiert dagegen, wer oder welche Stelle wann die Kontrolle über ein Objekt oder eine Repräsentation hatte, was damit geschah und in welchem Zustand es weitergegeben wurde. Keines dieser Elemente ersetzt die beiden anderen.

Das Modell soll ereignisbasiert und systemübergreifend sein. Ein Gewahrsamsereignis wird nach seiner Bestätigung nicht geändert. Fehler werden durch ein neues, verknüpftes Korrekturereignis berichtigt. Übergaben erhalten eine gemeinsame transferId und bestehen mindestens aus Übergabe und Empfang oder aus einer beidseitig bestätigten Transaktion. Das ermöglicht den Abgleich auch dann, wenn unterschiedliche Organisationen eigene führende Systeme verwenden.

Ein vollständiger Ereignisauszug kann im Austauschpaket mitgeführt werden. Alternativ kann auf ein autoritatives Register verwiesen werden, sofern der mitgegebene Stand kryptografisch gebunden, für den berechtigten Empfänger auflösbar und langfristig nachweisbar ist. Eine Blockchain ist dafür weder erforderlich noch generell zweckmässig. Entscheidend sind unveränderliche Ereignisse, überprüfbare Identitäten, nachvollziehbare Korrekturen und eine belastbare Bindung an Objekt und Repräsentation.

Feldgruppe	Mindestinhalt	Zweck
Ereignisidentität	eventId, eventType, predecessorEventId und bei Korrekturen correctedEventId	Reihenfolge und spätere Berichtigungen nachvollziehen
Bezugsobjekt	recordObjectId, optional representationId, Version und Prüfsumme	Ereignis eindeutig an Gegenstand oder digitale Ausprägung binden
Übergabe	transferId, fromCustodian, toCustodian sowie Übergabe- und Empfangsstatus	Organisationsgrenzen ohne stillschweigende Lücken überbrücken
Zeit und Ort	occurredAt, recordedAt, Zeitzone, Ort und gegebenenfalls vertrauenswürdiger Zeitnachweis	Chronologie auch bei abweichenden Systemuhren bewerten
Vorgang	Zweck, Rechts- oder Auftragsbezug, Methode, Werkzeug und Ergebnis	Sicherung, Untersuchung, Kopie oder Transformation fachlich einordnen
Zustand	Zustand vor und nach dem Vorgang, Verpackung, Siegel und Gefahrenhinweise	Physische Veränderungen und Öffnungen belegen
Integrität	Hash vor und nach digitalen Vorgängen, Algorithmus, Grösse und gegebenenfalls Signatur	Unveränderte oder bewusst transformierte Repräsentationen unterscheiden
Verantwortung	handelnde Person oder Stelle, Quellsystem, Erfassungsart, Attestation und Validierungsstatus	Urheberschaft und Verlässlichkeit des Ereignisses prüfen

NORMEN-GATE

Vor der Freigabe des Evidence-Schemas sind die vollständigen Fassungen der einschlägigen ISO-Normen auszuwerten und in einer Konformitätsmatrix auf Datenfelder, Prozessanforderungen und Tests abzubilden. Bis dahin darf der Entwurf Unterstützung vorsehen, aber keine Normkonformität behaupten.

7 Technische Umsetzungsvariante

7.1 Empfohlenes Paketmuster

Ein Austauschpaket enthält ein obligatorisches XML-Statement als Manifest und die zugehörigen Inhalte. Bei grossen oder besonders geschützten Daten kann das Statement stattdessen auf einen kontrollierten Speicher verweisen. Die Referenz muss auf dem Übertragungsweg auflösbar und über Prüfsumme, Grösse und Medienart prüfbar sein. Enthält ein Dokument eine eingebettete Metadatenprojektion, tragen XML-Statement und Dokument dieselbe Objekt-ID und Metadatenversion.

```
package/
  metadata/
    record-manifest.xml
  content/
    550e8400-e29b-41d4-a716-446 655 440 000/
      interview.pdf
    9c42dcae-2540-4cd8-a623-b130 736afdb9/
      image.E01
  validation/
    validation-report.xml
  signatures/
    package-seal.p7s
```

7.2 Bindungsmodell

1. Das logische Aktenobjekt erhält eine UUID.
2. Jede digitale Repräsentation erhält eine eigene Identität, Dateibezeichnung, MIME-Angabe, Grösse und kryptografische Prüfsumme.
3. Das obligatorische XML-Statement referenziert die Repräsentation über relativen Paketpfad oder kontrollierte URI.
4. Bei behördlich erzeugten Dokumenten wird eine gleichlautende Metadatenprojektion soweit möglich in das Dokument eingebettet, bevor die Dokumentensignatur angebracht wird. Damit erfasst die Signatur auch die eingebetteten Metadaten.
5. Eine detached Signatur oder ein Plattform-Siegel bindet zusätzlich das XML-Statement beziehungsweise die Hashliste. Die VEKJ-Mechanismen für Quittung, Hashwerte und Siegel können dafür genutzt werden.
6. Änderungen an Metadaten erzeugen eine neue Metadatenversion. Ein bereits signiertes Dokument wird deswegen nicht verändert. Die neue Version wird im XML-Statement geführt und mit der im Dokument eingebetteten Version vergleichbar gehalten.
7. Bei widersprüchlichen Ständen weist die empfangende Applikation den Konflikt aus. Ob sie den Schlüssel auflöst, eigene Stammdaten verwendet, den Dokumentstand übernimmt oder eine fachliche Entscheidung verlangt, bestimmt ihr fachliches Regelwerk.
8. Gewahrsamsereignisse werden append-only geführt und über eventId sowie predecessorEventId verknüpft. Übergaben über Organisationsgrenzen verwenden eine gemeinsame transferId und eine nachweisbare Empfangsbestätigung.
9. Bei digitalen Vorgängen referenziert jedes Ereignis die betroffene Repräsentation und dokumentiert je nach Vorgang Hashwerte vor und nach der Verarbeitung. Eine Transformation erzeugt eine neue Repräsentation mit Beziehung zum Ausgangsobjekt.

7.3 Beispiel eines XML-Manifests

Die eCH-Nummer und konkreten Typnamen sind Platzhalter. Das Beispiel zeigt die Trennung zwischen Kern, fachlichen Zuordnungen und Repräsentation.

```
<am:recordManifest
 xmlns:am="https://www.ech.ch/xmlns/eCH-0xxx/1"
 xmlns:ech0039="http://www.ech.ch/xmlns/eCH-0039/3"
 xmlns:ech0051="http://www.ech.ch/xmlns/eCH-0051/3">
 <am:recordObject>
  <am:recordObjectId>550e8400-e29b-41d4-a716-446 655 440 000</am:recordObjectId>
  <am:objectCategory>document</am:objectCategory>
  <am:title language="de">Einvernahme vom 14.07.2026</am:title>
  <am:caseReference>
   <am:authorityCode domain="CH-PJ">STA-BE</am:authorityCode>
   <am:caseNumber>BA.2026.1234</am:caseNumber>
   <am:referenceRole>leadingCase</am:referenceRole>
  </am:caseReference>
  <am:proceduralAction>
   <am:actionCode domain="CH-PJ-ACTION">interview</am:actionCode>
   <am:occurredAt>2026-07-14T09:00:00+02:00</am:occurredAt>
  </am:proceduralAction>
  <am:participantReference>
   <am:participantId>urn:uuid:…</am:participantId>
   <am:participantSnapshot>
    <am:familyName>Muster</am:familyName>
    <am:givenName>Anna</am:givenName>
    <am:dataConfirmedAt>2026-07-14</am:dataConfirmedAt>
   </am:participantSnapshot>
   <am:proceduralRole domain="CH-PJ-ROLE">accusedPerson</am:proceduralRole>
  </am:participantReference>
  <am:classificationAssignment>
   <am:schemeId>urn:example:aktenordnung:sta-be</am:schemeId>
   <am:schemeVersion>2026-01</am:schemeVersion>
   <am:nodeCode>05.02</am:nodeCode>
   <am:assignmentMethod>ruleBased</am:assignmentMethod>
  </am:classificationAssignment>
  <am:representation>
   <am:path>content/550e8400-e29b-41d4-a716-446 655 440 000/interview.pdf</am:path>
   <am:mimeType>application/pdf</am:mimeType>
   <am:size unit="byte">482 771</am:size>
   <am:checksum algorithm="SHA-256">…</am:checksum>
  </am:representation>
 </am:recordObject>
</am:recordManifest>
```

7.4 XSD-Struktur

Der neue Namespace importiert eCH-0039 und eCH-0051. Er definiert keine Kopien von UUID-, Datei-, Fallnummer- oder Basistypen, wenn ein geeigneter Typ bereits besteht. Wo eCH-0039 eine zu grosse oder technisch ungünstige Struktur vorgibt, wird eine explizite Mapping-Regel dokumentiert, statt die Bedeutung stillschweigend zu verändern.

```
<xs:schema
 targetNamespace="https://www.ech.ch/xmlns/eCH-0xxx/1"
 xmlns:xs="http://www.w3.org/2001/XMLSchema"
 xmlns:ech0039="http://www.ech.ch/xmlns/eCH-0039/3"
 xmlns:ech0051="http://www.ech.ch/xmlns/eCH-0051/3"
 elementFormDefault="qualified">
 <xs:import namespace="http://www.ech.ch/xmlns/eCH-0039/3"
            schemaLocation="eCH-0039-3-1.xsd"/>
 <xs:import namespace="http://www.ech.ch/xmlns/eCH-0051/3"
            schemaLocation="eCH-0051-3-0-0.xsd"/>
 <!-- recordManifestType, recordObjectComponentType,
      evidence extensions and conformance constraints -->
</xs:schema>
```

7.5 Konformitätsstufen

Stufe	Mindestumfang	Zweck
Core	Identität, Objektkategorie, Titel, Fallbezug, Provenienz, Version	Breite Interoperabilität
Content-bound	Core plus Repräsentation, MIME-Typ, Grösse und Prüfsumme	Verlustfreie digitale Übergabe
Filing	Core plus Handlung, Dokumentart, strukturierter Beteiligtenbezug und Klassifikationszuordnung	Teilautomatisierte Aktenbildung
Evidence	Content-bound plus Erwerb oder Sicherung, obligatorische Chain-of-Custody-Ereignisse, Original/Derivat, Zustand, Siegel sowie digitale Integritätsnachweise	Nachweisbare Behandlung digitaler und physischer Beweismittel über System- und Organisationsgrenzen

7.6 Abgrenzung und mögliche Weiterentwicklung: Referenzierung innerhalb von Aktenstücken

Die heutige Pagina ist eine Sichtreferenz. Sie setzt eine bestimmte Aktenordnung und Reihenfolge voraus. Sobald dieselben Aktenobjekte nach einer anderen Ordnung dargestellt, nur teilweise offengelegt, in ein anderes Dossier übernommen oder neu versioniert werden, kann dieselbe Stelle eine andere Pagina erhalten. Eine fortlaufende Dossierpagina eignet sich deshalb weiterhin für eine unveränderliche Papierakte oder einen eingefrorenen Export, nicht aber als dauerhafte kanonische Identität einer Passage.

Das Konzept ePagina löst einen wichtigen Teil des Problems für hybride Akten. Es kombiniert Behörden-, Akten- und Dokumentkontext mit einer Seitenreferenz und kann diese maschinenlesbar, etwa als QR-Code, auf Dokumenten darstellen. Das Konzept bezeichnet weitergehendes Deep Linking selbst als späteren Anwendungsfall. Offen bleiben namentlich die stabile Referenz auf Zeilen oder Textpassagen, die Bindung an einen bestimmten Repräsentationsstand, der Umgang mit OCR-Korrekturen, Versionen, Aufteilungen und Zusammenführungen sowie medienfremde Ziele wie Zeitabschnitte in Audio- oder Videodateien.

Variante	Referenzprinzip	Stärke	Grenze und Einordnung
a) Sichtpagina oder ePagina	Dossier- und Dokumentkontext plus Seite, optional mit QR-Code	Für Menschen vertraut und für hybride Akten gut sichtbar	Von Sicht, Reihenfolge und teilweise vom Dossier abhängig. Als Alias geeignet, nicht als alleinige kanonische Referenz
b) Unveränderliche Repräsentation	Kurzer Objektcode plus Repräsentationsversion, Seite und autoritative Zeile	Gut sprech- und zitierbar. Beispiel: «Akt 7K4M-2F9Q, Fassung 3, Seite 12, Zeilen 15 bis 27»	Erfordert eine eingefrorene Repräsentation und eine standardisierte, hashgebundene Text- und Zeilenebene
c) Struktur- oder Inhaltsanker	Objekt und Repräsentationsstand plus Absatz-, Satz-, Zeichen-, Textzitat- oder Koordinatenselektor	Unabhängig von der Dossierordnung und für Text, Bilder sowie Binärbereiche erweiterbar	Bei OCR-Fehlern und Inhaltsänderungen anspruchsvoll. Für gesprochene Zitate ist eine kurze Menschenform nötig
d) Hybrider Resolver	Kanonische URI oder URN auf Objekt, Repräsentation und Selektor. Ein Resolver erzeugt Link und zitierfähigen Alias	Verbindet Maschinenlesbarkeit, Klickbarkeit und gesprochene Sprache. Medienprofile können Seiten, Zeitcodes oder Bildbereiche unterstützen	Benötigt Governance, Zugriffsschutz, dauerhafte Auflösung und Regeln für veraltete oder ersetzte Repräsentationen

EMPFEHLUNG

Als Zielbild eignet sich Variante D mit den Mechanismen aus B und C.

Kanonisch ist die Referenz auf Objekt, Repräsentationsstand und Selektor.

ePagina oder eine andere Sichtpagina wird als auflösbarer Alias geführt.

Die erste Standardversion normiert die Selektoren noch nicht, reserviert aber den Lokator mit targetObjectId, targetRepresentationId, Repräsentationsversion oder Digest, selectorType, selectorValue, humanCitation, resolverUri, snapshotId und supersedes.

Für PDF kann ein späteres Profil Seiten, benannte Ziele, Strukturanker, Koordinaten und eine autoritative Zeilenabbildung kombinieren. W3C Web Annotation stellt unter anderem Fragment-, Textpositions-, Textzitat-, XPath-, Datenpositions- und SVG-Selektoren bereit. RFC 8118 kennt für PDF Seiten, benannte Ziele, Strukturelemente und Ansichtsbereiche. Für Audio und Video sind Zeitcodes vorzusehen. Eine sichtbare Zeilennummer darf nur dann normativ zitiert werden, wenn die zugrunde liegende Text- und Zeilenabbildung Bestandteil des gebundenen Repräsentationsstands ist.

Der Resolver darf durch eine Referenz nicht offenlegen, ob ein geschütztes Aktenobjekt existiert. Auflösung und Anzeige unterstehen weiterhin Authentisierung, Berechtigung und Protokollierung. Die menschenlesbare Kurzform benötigt einen kollisionssicheren Objektcode mit Prüfziffer oder vergleichbarer Fehlererkennung. Die UUID bleibt im Hintergrund die vollständige Identität.

8 Einpassung in die Standardlandschaft

Standard / Erlass	Vorhandene Funktion	Rolle des neuen Fachkatalogs	Integrationsregel
eCH-0003	Qualitäts- und Genehmigungsprozess	Bestimmt Form, Prüfkriterien und Beilagen	Aktuelle Vorlage, UML, XSD, Tests und Fachgruppenfreigabe
eCH-0039 V3.1	Austausch von Dossiers, Dokumenten, Dateien und Geschäftskontext	Fachliche Spezialisierung der Aktenobjekte	UUID, dossierType, documentType und fileType wiederverwenden oder eindeutig mappen
eCH-0051 V3.0.0	Modularer Basis-Datenkatalog Polizei/Justiz	Basistypen und Konventionen	Direkte Abhängigkeit. Handlungen und Fachstrukturen im neuen Fachkatalog
eCH-0280 V1.0.0	Strafanzeigen im öffentlichen Verkehr	Möglicher Nutzer des Metadatenprofils	Spätere Version referenziert Manifest, keine Duplikatfelder
eCH-0303 V1.0.0	Datenaustausch Polizei und Staatsanwaltschaft, in Arbeit. Entwurf Ende 2026 beziehungsweise Anfang 2027 erwartet	Erster Pilot und Integrationsprofil	Nach Veröffentlichung Feld-für-Feld-Abgleich und Kollisionsprüfung
eCH-0160 V1.3.0	Archivische Ablieferungsschnittstelle	Ziel-Mapping für Langzeitaufbewahrung	Kein Ersatz-SIP. Separates Mapping für Dossier, Dokument, Datei und Metadaten
VEKJ-Entwurf	Formate, Digitalisierung, Quittungen, Hashwerte und Siegel	Fachmetadaten oberhalb der Transportregeln	Hashbindung und zulässige Formate berücksichtigen
BEKJ / StPO	Rechtsrahmen für elektronische Aktenführung und Strafakten	Technische Unterstützung, keine materielle Neudefinition	Rechtskonformität je Anwendungsfall prüfen
ISO 22095:2020 mit Amd 1:2026	Generische Terminologie und Modelle für Chain of Custody von Materialien und Produkten	Begrifflicher und architektonischer Referenzrahmen	Nicht als alleiniger forensischer Konformitätsmassstab verwenden
ISO 21043-2:2018	Anforderungen an Erkennen, Erfassen, Sammeln, Transport und Lagerung forensisch relevanter Gegenstände	Referenz für physische Beweismittel und deren Zustands- und Gewahrsamsereignisse	Laufende Revision beobachten und vollständigen Normtext in Konformitätsmatrix auswerten
ISO/IEC 27037:2012	Leitlinien für Identifikation, Sammlung, Akquisition und Erhaltung digitaler Beweismittel	Referenz für digitale Sicherung, Akquisition, Repräsentationen und Integrität	Evidence-Profil und Tests am vollständigen Normtext spiegeln

8.1 Bewertung eCH-0039

eCH-0039 ist die naheliegende Grundlage für den Austauschcontainer. Der Standard kennt UUIDs für Dossiers und Dokumente sowie Dateien mit Pfad, MIME-Typ, Version und Hashangaben. Er erlaubt fachspezifische Nachrichten und zusätzliche Metadaten. Seine generischen Felder reichen aber nicht für Verfahrenshandlung, zeitabhängige Rollen, mehrere Klassifikationssichten oder Chain of Custody. Diese Lücke füllt der Fachkatalog.

Technisch ist Zurückhaltung bei XML-Ableitungen angezeigt. eCH-0039 weist selbst auf Probleme mit Restriction und Extension hin. Für das neue Schema ist deshalb ein klarer Kompositions- oder Referenzansatz mit automatisierten Validierungstests vorzuziehen.

8.2 Bewertung eCH-0051

eCH-0051 ist eine direkte Abhängigkeit. Der Standard unterscheidet Basistypen, Codes und Komponenten und verlangt modulare, gerichtete Abhängigkeiten. Er hält zugleich fest, dass Handlungen beziehungsweise Prozessverben nicht in den Basiskatalog gehören. «Einvernahme», «Vorladung» oder «Sicherstellung» sind daher sachgerecht im neuen Fachkatalog zu modellieren. Allgemein wiederverwendbare atomare Typen können später über einen separaten Änderungsantrag in eCH-0051 aufgenommen werden.

8.3 Bewertung eCH-0303

eCH-0303 ist als erste praktische Integration besonders geeignet, weil bei der Übergabe Polizei–Staatsanwaltschaft viele Aktenobjekte, Rollen, Handlungen und Beweismittel zusammenkommen. Die öffentliche eCH-Seite enthält per 24. Juli 2026 nur Beschreibung und Status. Hauptdokument und XSD sind noch nicht publiziert. Nach der Projektplanung soll der Entwurf Ende 2026 beziehungsweise Anfang 2027 zur Verfügung stehen. Aussagen zur kollisionsfreien Feld- und Namespace-Integration bleiben bis dahin vorläufig.

ZEITLICHE KOORDINATION
Die konzeptionelle Arbeit am gemeinsamen Metadatenkern kann sofort beginnen. Der definitive Feld-, Typ- und Namespace-Abgleich ist für Ende 2026 beziehungsweise Anfang 2027 einzuplanen, sobald der eCH-0303-Entwurf und seine XSD verfügbar sind.

8.4 Bewertung eCH-0160

eCH-0160 stützt die empfohlene Trennung. Der Archivstandard unterscheidet eingebettete und separate Metadaten und weist darauf hin, dass eingebettete Metadaten bei Formatumwandlungen verloren gehen können. Metadaten, die Archivprozesse überleben müssen, werden separat in metadata.xml geführt und den Primärdaten zugeordnet. Der neue Fachkatalog soll diese Logik aufnehmen, ohne die archivische Ablieferungsschnittstelle nachzubauen.

8.5 Bewertung der Chain-of-Custody-Standards

ISO 22095:2020 definiert einen generischen Rahmen, harmonisierte Begriffe und verschiedene Chain-of-Custody-Modelle für Materialien und Produkte. Die Norm weist selbst darauf hin, dass sie allein keine Eigenschaften oder entsprechenden Behauptungen verifiziert. Sie ist deshalb nützlich für Begriffe, Systemgrenzen, Verantwortlichkeiten und Modellwahl, aber für forensische Beweismittel nicht hinreichend spezifisch. Seit Januar 2026 besteht zudem Amendment 1:2026.

Für physische Gegenstände ist ISO 21043-2:2018 fachnäher. Sie betrifft Erkennen, Erfassen, Sammeln, Transport und Lagerung von Gegenständen mit potenziellem forensischem Wert. Die Norm befindet sich in Revision. Für die Wiedergewinnung von Daten aus digitalen Speichermedien verweist sie ausdrücklich auf ISO/IEC 27037:2012. Diese behandelt Identifikation, Sammlung, Akquisition und Erhaltung potenzieller digitaler Beweismittel. Für spätere Analyseprofile sind zusätzlich ISO/IEC 27041 bis 27043 zu prüfen.

Aus diesen Normen folgt für das Vorhaben nicht zwingend ein einziges übergreifendes Zertifikat. Erforderlich ist vielmehr eine normative Zuordnung zwischen fachlichen Anforderungen, Datenfeldern, Prozessereignissen, Nachweisen und Testfällen. Der Standard muss festlegen, welche Norm, Fassung und welches Profil für welchen Objekttyp gilt. Sie muss zudem unterscheiden zwischen «kann normkonforme Prozesse transportieren», «erfüllt definierte Datenanforderungen» und einer weitergehenden Konformitäts- oder Zertifizierungsaussage.

9 Verbesserungen und Einsparpotenzial

9.1 Erwartete Verbesserungen

Wirkung	Mechanismus	Messgrösse
Automatische Einordnung	Regelbasierte Zuordnung nach Handlung, Rolle, Art und Datum	Anteil ohne manuelle Umklassierung
Schnellere Übergabe	Keine Neuerfassung vorhandener Kontextdaten	Bearbeitungszeit pro importiertem Objekt
Bessere Vollständigkeit	Regeln prüfen Pflichtobjekte, Prüfsummen und Beziehungen	Fehler je Dossierübergabe
Bessere Suche	Strukturierte, organisationsübergreifende Filter	Zeit bis zum Auffinden eines Aktenobjekts
Mehrere Sichten	Lokale Ordnung, Akteneinsicht und Archivsicht aus demselben Bestand	Zeit zur Erstellung einer Dossiersicht
Weniger Herstellerbindung	Explizite Semantik und offenes Schema	Aufwand für Migration und Systemwechsel
Nachvollziehbare Evidenz	Provenienz, Original oder Derivat sowie unveränderliche Gewahrsams-, Übergabe- und Empfangsereignisse	Lücken, widersprüchliche Übergaben, ungeklärte Siegel- oder Hashwechsel und manuelle Nachfragen

9.2 Einsparmodell

Seriöse Frankenbeträge lassen sich ohne Mengengerüst und Zeitmessung nicht angeben. Das Potenzial kann mit einer einfachen, transparenten Formel pilotiert werden:

Jährliche Nettozeit = Anzahl Aktenobjekte × (manuelle Basiszeit − Validierungs- und Ausnahmezeit)

Illustration, nicht Prognose: Bei 100 000 neu übernommenen Aktenobjekten und einer netto vermiedenen manuellen Bearbeitungszeit von 30 bis 60 Sekunden ergibt sich ein Potenzial von rund 833 bis 1 667 Arbeitsstunden pro Jahr. Hinzu kommen vermiedene Nacharbeit, schnellere Übergaben und bessere Datenqualität. Der Pilot muss prüfen, ob diese Annahmen in realen Prozessen erreicht werden.

9.3 Pilot-Messplan

Kennzahl	Basis	Zielrichtung
Zeit pro Objekt bei Eingang	Zeitmessung heutiger manueller Prozess	deutlich tiefer
Automatisch korrekt zugeordnet	0 oder heutige Heuristik	hoch, getrennt nach Dokumentart
Ausnahmequote	heutige Rückfragen und Umordnungen	sinkend und fachlich erklärbar
Fehlzuordnungen	Stichprobe vor Übergabe	keine Verschlechterung gegenüber manueller Ordnung
Vollständigkeitsmängel	Beanstandungen pro Dossier	tiefer
Metadatenübernahme ohne Neuerfassung	heutiger Wert	hoch
Technische Validierung	Schema-, Hash- und Referenzfehler	nahe null

Kennzahl	Basis	Zielrichtung
Chain of Custody vollständig übernommen	Heutige Medienbrüche, Nacherfassung und fehlende Ereignisse	Alle Pflichtschritte maschinenlesbar. Jede Lücke oder widersprüchliche Übergabe wird erkannt
Korrekte Ereignisvalidierung	Testfälle mit fehlender Empfangsbestätigung, Siegelwechsel, Hashabweichung und abweichender Systemzeit	Fehler werden reproduzierbar erkannt und fachlich verständlich ausgewiesen

10 Risiken und Stolpersteine

Risiko	Auswirkung	Gegenmassnahme
Scheinharmonisierung	Uneinheitliche Codes trotz gleichem XML	Begriffsmodell, Codelist-Governance, Konformitätstests
Metadatenfehler durch Automatik	Falsche Aktenordnung oder falsche Beteiligtenbezüge	Provenienz, Validierungsstatus, Ausnahmequeue, fachliche Stichproben
Rollen ändern über die Zeit	Historisch falsche Sicht	Rolle mit Gültigkeit und Bezugsquelle modellieren
Einbettung zum falschen Zeitpunkt	Nachträgliche Änderungen machen Signaturen und Hashwerte ungültig	Einbettung bei behördlicher Erzeugung vor Signatur. Signierte oder fremde Originale nicht nachträglich verändern
Verlust eingebetteter Daten	Migration oder Formatkonversion entfernt Metadaten	Obligatorisches XML-Statement, Versionsabgleich und Exporttests
Personendaten in Metadaten	Erhöhte Auffindbarkeit und Offenlegungsrisiken	Empfängerprofile, beschränkte Identifikatoren nur bei Zulässigkeit, Verschlüsselung, Logging und Berechtigungsprüfung
Versionskonflikte bei Personen- oder Falldaten	Abweichende Anzeige oder fehlerhafte automatische Zuordnung	Quelle, Datenstand und Version mitführen, Konflikt ausweisen, Entscheidung dem fachlichen Regelwerk der Anwendung überlassen
UUID-Duplikate oder Neunummerierung	Beziehungen brechen	Vergaberegeln, Unveränderlichkeit und Kopie-/Duplikatsemantik
Lokale Erweiterungsflut	Interoperabilität sinkt	Kernkonformität, Namespace-Regeln und Mappingpflicht
Aktenordnungen ändern	Alte Zuordnung nicht reproduzierbar	Schema-ID, Version, Gültigkeit und Regelversion speichern
Mehrfachdossiers	Ein Objekt wird kopiert oder widersprüchlich geführt	Viele-zu-viele-Fallreferenz und führende Bezugsrolle
Hash wird mit Echtheit verwechselt	Falsche Beweissicherheit	Hash nur als Integritätsnachweis. Provenienz, Signatur und Gewahrsam separat
Grosse digitale Evidenz	Pakete werden unhandlich	Referenzmodus, Chunking und mediengerechter Transfer
Abhängigkeit vom eCH-0303-Entwurf	Nachträgliche Schemakollision	Früher Feldabgleich und gemeinsamer Pilot
Fehlende organisatorische Verantwortung	Standard bleibt technisch, wird aber nicht gepflegt	Product Owner, Codelist-Verantwortliche und geregelter Änderungsprozess
Chain-of-Custody-Daten werden nachträglich überschrieben	Gewahrsamskette ist nicht mehr beweisbar	Append-only-Ereignisse, Korrekturereignisse, Signatur oder Siegel und revisionssichere Protokollierung
Übergabe und Empfang passen nicht zusammen	Lücke an der Organisationsgrenze	Gemeinsame transferId, Gegenbestätigung, Statusmodell und Ausnahmeprozess
Unklare Identitäten oder Zeitstempel	Verantwortung und Reihenfolge bleiben zweifelhaft	Verifizierte Stellen- und Systemidentitäten, occurredAt und recordedAt, Zeitzone, Sequenz sowie optional vertrauenswürdiger Zeitnachweis

Risiko	Auswirkung	Gegenmassnahme
Vorschnelle Behauptung von ISO-Konformität	Falsche Sicherheit und angreifbare Spezifikation	Volltexte lizenzkonform auswerten, Konformitätsmatrix und Prüfnachweise als Gate vor Schemafreigabe
Instabile Passagenreferenzen	Zitate führen nach Umordnung, Versionierung oder OCR-Korrektur zur falschen Stelle	Objekt und Repräsentationsstand kryptografisch binden, Selektor typisieren, alte Stände auflösbar halten und Menschenform nur als Alias verwenden

10.1 Recht und Informationssicherheit

Metadaten können besonders schützenswerte Personendaten und verfahrensstrategische Informationen leichter auffindbar und auswertbar machen. Dieser Effekt ist sicherheitsrelevant, auch wenn die betreffenden Angaben regelmässig bereits im Nutzinhalt stehen. Das Gebot der Datensparsamkeit rechtfertigt deshalb keinen auf blosse Schlüssel reduzierten Standard. Es verlangt vielmehr, den interoperablen Zweck, die erforderlichen strukturierten Angaben, die zulässigen Identifikatoren und den Empfängerkreis sauber zu bestimmen. Der Standard muss Zweckbindung, Vertraulichkeitskennzeichnung und sichere Verarbeitung adressieren, darf aber kein organisationsspezifisches Berechtigungsmodell normieren.

Die automatische Einordnung darf die verantwortliche Verfahrensleitung nicht von der Pflicht entbinden, Vollständigkeit, Aktenrelevanz, Akteneinsicht und Aussonderung zu beurteilen. Eine technisch plausible Klassifikation ist keine rechtliche Entscheidung.

11 Umsetzungsvariante und Vorgehensplan

Phase	Inhalt	Ergebnis / Gate
0. Scope	Standardisierungsumfang, Arbeitsgruppe, Quellenzugang	Genehmigter Auftrag und Abgrenzung
1. Discovery	Drei Aktenordnungen, zwei Übergaben, bestehende Codelisten und Chain-of-Custody-Prozesse vergleichen. Vollständige ISO-Normen auswerten und Anschlussstellen für eCH-0303 vorbereiten	Gemeinsamer semantischer Kern und freigegebene Normen- und Konformitätsmatrix
2. Minimalmodell	UML, Datenwörterbuch, XSD, Codelisten, Evidence- und Chain-of-Custody-Profil, Lokator-Erweiterungspunkt, Beispielpaket und Mapping eCH-0039/eCH-0051	Technischer Entwurf V0.1
3. Abgleich und Pilot	Ab Ende 2026 beziehungsweise Anfang 2027 eCH-0303 abgleichen. Danach Polizei–Staatsanwaltschaft sowie je einen digitalen und physischen Evidenzfall über eine Organisationsgrenze pilotieren. Fehlerfälle gezielt einspeisen	Messwerte, Fehlerkatalog, überarbeitetes Modell
4. eCH-Entwurf	Dokument gemäss aktueller eCH-Vorlage, normative Regeln und Testverfahren	Fachgruppenfreigabe zur öffentlichen Konsultation
5. Einführung	Referenzvalidator, Implementierungsleitfaden, Mappings und Schulung	Mindestens zwei unabhängige Implementierungen

11.1 Mögliche Zusammensetzung einer Arbeitsgruppe

- Polizei, Staatsanwaltschaft, Gerichte und Verwaltungsstrafbehörden
- Programm Justitia 4.0 beziehungsweise Plattform- und BEKJ-Umsetzung
- Fachverantwortliche eCH-0039, eCH-0051, eCH-0303 und relevante Fachkataloge
- Records Management/GEVER und Digitale Archivierung
- Forensik, Asservatenmanagement und Informationssicherheit
- Hersteller von Polizei-, Staatsanwaltschafts-, Gerichts- und Dokumentenmanagementsystemen
- Datenschutz- und Verfahrensrechtsexpertise
- Fachpersonen mit nachgewiesener Kenntnis der massgebenden Chain-of-Custody- und Forensiknormen

11.2 Lieferobjekte (Entwurf)

- normatives UML-Informationsmodell und Datenwörterbuch
- XSD mit versioniertem Namespace und automatisiert prüfbaren Regeln
- normative Codelisten oder verbindliche Codelist-Referenzregeln
- Beispielmanifeste für Dokument, digitales und physisches Beweismittel
- Mappingtabellen zu eCH-0039, eCH-0051, eCH-0280, eCH-0303 und eCH-0160
- Konformitätsstufen, Testdaten und Referenzvalidator
- Implementierungsleitfaden mit Paket-, Hash-, Signatur- und Fehlerregeln
- Pilotbericht mit Nutzenmessung und Datenschutzfolgen
- Normen- und Konformitätsmatrix für ISO 22095, ISO 21043-2, ISO/IEC 27037 und gegebenenfalls weitere forensische Normen
- normatives Chain-of-Custody-Ereignismodell samt Zustands-, Korrektur-, Übergabe- und Empfangsregeln

11.3 Abnahmekriterien (Entwurf)

- Zwei unabhängige Systeme können dasselbe Manifest erzeugen und verarbeiten.
- Eine empfangende Anwendung kann mindestens zwei unterschiedliche Aktenordnungen aus demselben Testbestand ableiten.
- Alle digitalen Repräsentationen sind über UUID, Pfad oder URI, MIME-Typ, Grösse und Prüfsumme eindeutig gebunden.
- Metadatenänderungen und automatische Ableitungen sind nachvollziehbar versioniert.
- Der Pilot umfasst mindestens einen digitalen und einen physischen Beweismittelfall.
- Die Übergabe in ein eCH-0160-konformes Ablieferungsmodell ist durch Mapping demonstriert.
- Keine semantische Duplizierung bestehender eCH-Felder ohne dokumentierte Begründung.
- Das Evidence-Profil bildet bei einem organisationsübergreifenden Testbestand eine lückenlose, maschinenprüfbare Chain of Custody ab. Testfälle mit fehlender Empfangsbestätigung, Siegelwechsel, Hashabweichung, Korrekturereignis und abweichender Systemzeit werden korrekt erkannt.
- Die Passagenreferenzierung ist als optionaler Lokator-Erweiterungspunkt modelliert, ohne eine Selektorsemantik für V1 vorwegzunehmen.

12 Begründung

Die geltenden und entstehenden Austauschstandards schaffen technische und fachliche Grundlagen für den elektronischen Verkehr zwischen Strafverfolgungsbehörden. Sie lösen jedoch nicht die wiederkehrende Aufgabe, Aktenobjekte beim Empfänger korrekt, nachvollziehbar und mit geringem manuellem Aufwand in eine lokale Aktenstruktur einzuordnen.

Eine schweizweit einheitliche Aktenordnung ist wegen unterschiedlicher Rechtsgebiete, Organisationen und Arbeitsweisen weder kurzfristig erreichbar noch für die Interoperabilität notwendig. Hingegen besteht ein gemeinsamer semantischer Kern: Identität, Fallbezug, Objektart, Entstehung, Verfahrenshandlung, Beteiligtenbezug, Beziehungen, Repräsentation und Integrität. Werden diese Angaben standardisiert mitgeführt, können verschiedene Aktenordnungen als nachvollziehbare Sichten erzeugt werden.

Die Standardisierung verspricht geringeren Erfassungs- und Umordnungsaufwand, bessere Vollständigkeitsprüfungen, schnellere Übergaben, systemübergreifende Suche und geringere Herstellerabhängigkeit. Die Behauptung eines konkreten Einsparbetrags ist derzeit nicht belegt. Deshalb soll die Nutzenhypothese vor der Normierung in einem Pilot mit definierten Kennzahlen geprüft werden.

12.1 Ziel und Geltungsbereich

Der Standard soll:

- Metadaten für Dokumente sowie digitale und physische Beweismittel definieren
- mehrere Fall-, Beteiligten-, Handlungs- und Klassifikationsbezüge zulassen

- Inhalt und Metadaten über UUIDs, Referenzen und Prüfsummen belastbar verbinden
- für jedes Aktenobjekt ein obligatorisches XML-Statement vorsehen und Metadaten bei behördlich erzeugten Dokumenten soweit möglich vor der Signatur zusätzlich einbetten
- neben Identifikatoren einen für den Empfänger verwendbaren strukturierten Basisdatensatz zu Beteiligten und Organisationen übermitteln
- in eCH-0039-Paketen und eCH-0303-Nachrichten verwendet werden können
- eine eindeutige Abbildung auf eCH-0160 ermöglichen
- XML als normative Darstellung und bei Bedarf eine getestete JSON-Abbildung bereitstellen
- eine normgerecht nachvollziehbare Chain of Custody für digitale und physische Beweismittel über organisationsübergreifend austauschbare Ereignisse unterstützen
- einen optionalen Lokator-Erweiterungspunkt für spätere Seiten-, Passagen-, Zeit- und Bereichsreferenzen enthalten, ohne diese Selektoren bereits in V1 abschliessend zu normieren

Nicht Gegenstand sind:

- eine einheitliche Aktenordnung
- ein neues Übermittlungsprotokoll oder eine Plattform
- die materiellrechtliche Definition der Aktenrelevanz
- ein vollständiges Berechtigungs-, Archivierungs- oder Asservatenmanagementsystem
- die vollständige betriebliche Führung eines Asservatenlagers oder eines forensischen Labors. Die standardisierte Übermittlung beweisrelevanter Gewahrsamsereignisse bleibt Teil des Geltungsbereichs
- die abschliessende Festlegung einer schweizweiten Paginierung, eines zentralen Resolverdienstes oder sämtlicher formatabhängiger Passagenselektoren in V1

12.2 Vorgeschlagene normative Inhalte

- Begriffe, Informationsmodell und Kardinalitäten
- obligatorischer Kern und Konformitätsstufen
- Typen und Codelisten für Objektkategorie, Verfahrenshandlung, Dokumentart, Verfahrensrolle und Relationen
- Metadatenversion, Provenienz und Validierungsstatus
- Regeln für die Übereinstimmung und Versionierung von XML-Statement, eingebetteter Metadatenprojektion und Nutzinhalt
- Empfängerprofile für strukturierte Beteiligtenangaben sowie für rechtlich beschränkte Identifikatoren
- Bindung digitaler Repräsentationen über Identität, MIME-Typ, Grösse und Prüfsumme
- Profile für digitale und physische Beweismittel einschliesslich Gewahrsamsereignissen
- Regeln für Klassifikationsschemata, deren Versionen und Mehrfachzuordnungen
- XML-Schema, Beispiele, Fehlerregeln und maschinell prüfbare Konformität
- normatives Chain-of-Custody-Ereignismodell mit Rollen, Übergabe und Empfang, Zustand, Siegel, Integritätsnachweisen, Korrekturen und Attestationen
- Konformitätsmatrix zu den einschlägigen ISO-Normen und Testfälle für lückenhafte oder widersprüchliche Gewahrsamsketten
- optionaler Lokator-Typ für targetObjectId, targetRepresentationId, Repräsentationsstand, Selektor, humanCitation, resolverUri, snapshotId und supersedes

12.3 Abhängigkeiten und Koordination

Gegenstand	Koordinationsbedarf
eCH-0039	Übernahme oder Mapping der Dossier-, Dokument-, Datei- und UUID-Strukturen
eCH-0051	Typkonventionen, bestehende Basistypen, Codes und Modulabhängigkeiten
eCH-0280	Prüfen, wie bestehende Anhänge künftig auf Aktenobjekt-Metadaten verweisen
eCH-0303	Vollständiger Abgleich nach der für Ende 2026 beziehungsweise Anfang 2027 erwarteten Bereitstellung und anschliessender gemeinsamer Pilot

Gegenstand	Koordinationsbedarf
eCH-0160	Mapping für archivische Ablieferung und dauerhafte Metadaten
VEKJ / BEKJ	Format-, Hash-, Quittungs-, Siegel- und Digitalisierungsanforderungen
Fachgruppen	Polizei/Justiz, Records Management/GEVER, Digitale Archivierung und XML
ISO- und Forensiknormen	Vollständige Normtexte auswerten. Physische und digitale Evidenzprofile, Kardinalitäten, Ereignisregeln und Tests in einer Konformitätsmatrix begründen
ePagina, W3C und IETF	Anschlussfähigkeit des Lokator-Erweiterungspunkts an hybride Paginierung, formatneutrale Selektoren und PDF-Fragmente sicherstellen

12.4 Lieferobjekte und Qualitätssicherung

Die Arbeitsgruppe liefert ein Hauptdokument in der aktuellen eCH-Vorlage, ein normatives UML-Modell, XSD-Dateien, Codelisten, Mappingtabellen, Beispielpakete, Testdaten, einen Validator, eine Normen- und Konformitätsmatrix sowie einen Pilotbericht. Die Genehmigungskriterien aus eCH-0003 sind systematisch nachzuweisen. Dazu gehören insbesondere klare Abgrenzung, einheitliche Terminologie, Vermeidung von Überschneidungen, formale Semantik, dokumentiertes Testverfahren und technische Prüfung der Schemas. Für das Evidence-Profil sind zusätzlich die einschlägigen Chain-of-Custody-Anforderungen und negative Testfälle nachzuweisen.

12.5 Risiken des Vorhabens

Die grössten Projektrisiken sind eine zu breite erste Version, konkurrierende Codelisten, unkontrollierte lokale Erweiterungen, unzureichender Datenschutz, instabile Passagenreferenzen, eine lückenhafte oder veränderbare Chain of Custody, vorschnelle ISO-Konformitätsaussagen, Verwechslung von Metadaten mit Beweiswert sowie eine nachträgliche Kollision mit eCH-0303. Diese Risiken werden durch einen kleinen obligatorischen Kern, gemeinsame Governance, Evidenzprofile, append-only-Ereignisse, eine Normen- und Konformitätsmatrix, einen nur vorbereiteten Lokator-Erweiterungspunkt, Konformitätsstufen, frühe Schemaabgleiche und einen realen Pilot reduziert.

12.6 Erwarteter Nutzen

Der Standard ermöglicht eine teilautomatisierte Aktenbildung über Organisations- und Systemgrenzen hinweg. Er verbessert Datenqualität, Vollständigkeit, Suchbarkeit, Nachvollziehbarkeit und Migrationsfähigkeit. Einsparungen entstehen durch weniger Neuerfassung, Umordnung, Benennung und Fehlerkorrektur. Die Wirtschaftlichkeit wird im Pilot anhand der in Kapitel 9 definierten Kennzahlen verifiziert.

13 Quellen und Prüfbasis

Stand der Webquellen: 24. Juli 2026. Die Quellenverweise Q1 bis Q19 werden im Text sinngemäss verwendet. Rechtliche Aussagen sind als Standardisierungsanalyse und nicht als Rechtsgutachten zu verstehen. Die erwartete Bereitstellung des eCH-0303-Entwurfs Ende 2026 beziehungsweise Anfang 2027 beruht auf der Projektinformation des Auftraggebers. Aussagen zu ISO-Normen stützen sich in dieser Fassung auf die öffentlich zugänglichen Normbeschreibungen. Die vollständigen Normtexte sind vor einer Konformitätsfestlegung lizenzkonform auszuwerten.

Q1 eCH-0003 Leitfaden zur Genehmigung von Anträgen V11.1.0. Genehmigte Fassung und Vorlage

Q2 eCH-0039 E-Government-Schnittstelle für Dossiers und Dokumente V3.1. Genehmigte Fassung, Hauptdokument und XSD

Q3 eCH-0051 Basis-Datenkatalog Polizei und Justiz V3.0.0. Genehmigte Fassung, Hauptdokument und XSD

Q4 eCH-0280 Datenaustausch bei Strafanzeigen im öffentlichen Verkehr V1.0.0. Referenz für die Kombination bestehender Standards

Q5 eCH-0303 Datenaustausch Polizei – Staatsanwaltschaft V1.0.0. In Arbeit. Öffentlich noch kein Hauptdokument und keine XSD verfügbar. Bereitstellung gemäss Projektinformation Ende 2026 beziehungsweise Anfang 2027 erwartet

Q6 eCH-0160 Archivische Ablieferungsschnittstelle V1.3.0. Referenz für separate Metadaten und Archivmapping

Q7 Bundesamt für Justiz: Elektronische Kommunikation mit Gerichten und Behörden. Status BEKJ und VEKJ

Q8 Vorentwurf VEKJ. Formate, Quittung, Hashwerte, Siegel und Digitalisierung

Q9 Bundesgesetz über die Plattformen für die elektronische Kommunikation in der Justiz, BEKJ. Amtliche Veröffentlichung

Q10 Schweizerische Strafprozessordnung, StPO. Insbesondere Art. 100

Q11 **Weisung** Aktenführung und Aktenordnung.. Herangezogen für praktische Aktenordnung und physische Beweismittel

Q12 eCH-0003 V12.0.0 Vorschlag. Noch nicht genehmigt. Für die Einreichung ist die dann aktuelle Fassung zu prüfen

Q13 ISO 22095:2020 Chain of custody — General terminology and models. Generischer Rahmen. Amendment 1:2026 berücksichtigen

Q14 ISO 21043-2:2018 Forensic sciences — Part 2. Physische Gegenstände, Transport und Lagerung. Revision in Arbeit

Q15 ISO/IEC 27037:2012 Guidelines for digital evidence. Identifikation, Sammlung, Akquisition und Erhaltung digitaler Beweismittel

Q16 HIS Schweiz: Konzept eAktenverzeichnis / ePagina V0.16. Hybride Paginierung und Seitenreferenz

Q17 Justitia 4.0: Grobanforderungen Justizakte-Applikation. Referenzierungen bis Seite beziehungsweise optional Zeile oder Satz

Q18 W3C Web Annotation Data Model. Formatneutrale Selektoren für Text, Strukturen, Daten und Bildbereiche

Q19 RFC 8118: The application/pdf Media Type. PDF-Fragmentidentifikatoren für Seiten, Ziele, Strukturelemente und Ansichtsbereiche

13.1 Nachweis der zentralen Ableitungen

Aussage	Hauptquelle
eCH-0039 deckt Dossier, Dokument und Datei ab, nicht aber die gesamte fachliche Aktensemantik	Q2, Hauptdokument Ziff. 3.2 ff.
eCH-0051 ist modular. Handlungen gehören in Fachstandards	Q3, Hauptdokument Grundlagen und Modellierungsregeln
eCH-0303 ist in Arbeit, wird Ende 2026 beziehungsweise Anfang 2027 erwartet und ist derzeit öffentlich nicht vollständig prüfbar	Q5 und Projektinformation des Auftraggebers
Dauerhafte Metadaten sollen separat von Primärdaten geführt werden	Q6, Hauptdokument Metadaten und metadata.xml
VEKJ fokussiert Formate, Prüfsummen, Quittungen, Siegel und Digitalisierung	Q7 und Q8
Strafakten enthalten Verfahrensunterlagen, Beweismittel und Sicherungsunterlagen	Q10, Art. 100
Physisch separat gelagerte Gegenstände müssen im Dossier eindeutig verzeichnet werden	Q11
eCH-Anträge benötigen klare Abgrenzung, formale Semantik, Schemas und Tests	Q1
ISO 22095 liefert einen generischen Chain-of-Custody-Rahmen, genügt allein aber nicht als forensischer Standard	Q13, Abstract und Geltungsbereich
Physische und digitale Beweismittel benötigen fachnahe, getrennte Normbezüge	Q14 und Q15

Aussage	Hauptquelle
ePagina adressiert die hybride Seitenreferenz. Tiefere Referenzierungen bleiben eine Weiterentwicklung	Q16 und Q17
Formatneutrale Passagenselektoren und PDF-Fragmente können für ein späteres Lokatorprofil wiederverwendet werden	Q18 und Q19

14 Schlussfolgerung

Der Vorschlag löst ein reales Interoperabilitätsproblem mit einem verhältnismässigen Ansatz. Die eigentliche Innovation liegt nicht in einem weiteren Dokumentencontainer, sondern in der Entkopplung von Aktenobjekt und Aktenansicht. Dies erlaubt lokale Aktenordnungen, ohne bei jeder Übergabe die fachliche Bedeutung neu zu erfassen.

Erfolgskritisch sind ein fachlich ausreichender obligatorischer Kern, das verbindliche XML-Statement, die zusätzliche Einbettung in behördlich erzeugte Dokumente, eine belastbare Bindung an Originale, gemeinsame Codelist-Governance, eine von Beginn an vorgesehene normgerechte Chain of Custody und die Erprobung mit eCH-0303.

Die formatübergreifende Passagenreferenzierung soll V1 nicht überladen. Mit einem optionalen Lokator-Erweiterungspunkt bleibt das Modell jedoch anschlussfähig für eine spätere kanonische Referenz aus Objekt, Repräsentationsstand und Selektor. Der Antrag sollte deshalb die Standardisierungsarbeit freigeben, aber die definitive Normierung an Pilotnachweise, eine freigegebene Normen- und Konformitätsmatrix und einen vollständigen Schemaabgleich knüpfen.