immoGenio

No. 01
März 2026

BUCHHALTUNG

E-Rechnung ab 2025: ZUGFeRD, XRechnung — und der unterschätzte IBAN-Swap

E-Rechnung ab 2025: Empfangspflicht jetzt, Versand ab 2027/28. Warum XML-Import nicht reicht und wie man gegen IBAN-In-Flight-Swap schützt.

AUTOR
ImmoGenio

VERÖFFENTLICHT
30. März 2026

ONLINE
www.immogenio.de/blog

— AUF EINEN BLICK

Inhalt

Wer in der Hausverwaltung mit Buchhaltung zu tun hat, kennt die Stichtage mittlerweile: Seit dem 1. Januar 2025 muss **jedes** Unternehmen in Deutschland E-Rechnungen empfangen und revisionssicher archivieren können. Die Versandpflicht wird gestaffelt scharfgeschaltet — ab dem 1. Januar 2027 für Unternehmen mit mehr als 800.000 Euro Jahresumsatz, ab dem 1. Januar 2028 für alle B2B-Umsätze. Eine PDF-Rechnung per Mail reicht dafür nicht mehr. Verbindlich ist ein **strukturiertes XML-Dokument** nach der europäischen Norm EN 16931.

Was in fast jeder Diskussion zu diesem Thema fehlt: Die Umstellung ist nicht nur ein Compliance-Thema. Sie öffnet eine neue Angriffsfläche, die in der Branche noch kaum benannt wird.

ZUGFeRD und XRechnung im Überblick

In Deutschland gelten zwei Formate als EN-16931-konform:

- **XRechnung** ist reines XML — entweder in OASIS UBL 2.1 oder in UN/CEFACT CII. Es ist der KoSIT-Standard und Pflicht im Rechnungsverkehr mit Bund, Ländern und Kommunen.
- **ZUGFeRD 2.x** ist eine hybride PDF/A-3-Datei. Sichtbar ist ein normal aussehendes Rechnungs-PDF — eingebettet liegt darin eine `factur-x.xml`, die maschinell lesbar dasselbe enthält.

Der entscheidende Punkt: Sobald ein Belegsystem eine E-Rechnung strukturiert verarbeitet, ist **das XML die Quelle der Wahrheit**, nicht der schöne PDF-Ausdruck darüber. Der Buchungsvorschlag entsteht aus den `<cac:PaymentMeans>`-Knoten des XML, nicht aus dem, was der Mensch auf dem Bildschirm sieht.

Und genau hier wird es gefährlich.

Der In-Flight-Swap: warum XML allein nicht reicht

Stellen wir uns einen realistischen Angriff vor. Ein Lieferant verschickt eine legitime ZUGFeRD-Rechnung per E-Mail. Unterwegs — über ein kompromittiertes SMTP-Relay, ein gehacktes Lieferanten-Postfach oder einen Man-in-the-Middle irgendwo im Konzern-Maildrop — wird der Anhang abgefangen. Der Angreifer tut **nicht** das Offensichtliche: Er manipuliert nicht das PDF. Stattdessen tauscht er im eingebetteten XML eine einzige IBAN aus.

Das manipulierte PDF wird weitergeleitet. Die Buchhalterin öffnet den Anhang: Der sichtbare PDF-Layer zeigt die korrekte IBAN des Lieferanten. Alles wirkt unauffällig. Unsere Buchhaltungssoftware liest aber nicht den PDF-Text, sondern den XML-Teil — und be-

kommt dort die Angreifer-IBAN serviert. Der Buchungsvorschlag läuft automatisch durch die Buchungsregel-Engine, die SEPA-Überweisung wird ausgelöst, das Geld ist weg.

Dieser Angriff hat bereits einen Namen in der Fachszene: **In-Flight-Swap**. Er funktioniert, weil die Branche die E-Rechnung oft als reinen Import-Durchlauf denkt. XML rein, Buchung raus. Fertig.

Das ist fahrlässig.

Was eine ehrliche E-Rechnungs-Engine leisten muss

Bei ImmoGenio haben wir diese Woche das Architekturdesign für unsere E-Rechnungs-Engine abgeschlossen. Die Reihenfolge der Prüfungen ist kein Zufall — sie spiegelt die Bedrohungsmodellierung wider, mit der wir das Feature angegangen sind:

1. Syntaktische Validierung (XSD). Das XML muss gegen die lokal gepinnten Schemata von XRechnung 3.0 und ZUGFeRD 2.3 validieren. Keine KoSIT-Schemata aus dem Internet zur Laufzeit — sie sind Teil unseres Source-Trees und werden versioniert. Fehler hier beenden den Import sofort mit einem Pointer auf Zeile und Spalte.

2. Semantische Validierung (Schematron). Die europäischen Kernregeln (BR-01 bis BR-99 aus EN 16931) und die deutschen CIUS-Verschärfungen der XRechnung werden als vorkompilierte XSLT gegen das Dokument gefahren. Wer hier schludert, riskiert bei einer Betriebsprüfung böse Überraschungen.

3. IBAN-Whitelist pro Lieferant. Das ist das Herzstück gegen den Swap-Angriff. Jede IBAN, die wir je für einen Lieferanten gesehen haben, wird in einer mandantenspezifischen Whitelist geführt. Die erste IBAN eines Lieferanten löst eine Vier-Augen-Bestätigung aus: Der Buchhalter muss aktiv bestätigen, dass er die IBAN **außerhalb der Rechnung** verifiziert hat — per Rückruf, Briefkopf-Abgleich, Vertragsunterlagen. Kommt später eine neue IBAN desselben Lieferanten rein, **ohne** dass die alte widerrufen wurde, lehnt das System den Buchungsvorschlag kategorisch ab. Kein Override, kein „einmal durchwinken".

4. Kreuzprüfung PDF-Layer gegen XML. Nur bei ZUGFeRD — aber hier nicht optional. Wir extrahieren den sichtbaren Text des PDF-Layers, suchen nach IBAN-Mustern und vergleichen sie mit der XML-IBAN. Stimmt das nicht überein, ist das per Definition ein Swap-Versuch. Keine Warnung, kein „vielleicht" — direkter Fehler.

5. Append-only Audit-Log. Jeder einzelne Validierungslauf wird in einer eigenen Tabelle protokolliert. Kein Update, kein Löschen. Wer wann was freigegeben hat, ist für die nächsten zehn Jahre nachvollziehbar.

Was der legitime Bankwechsel bedeutet

Der häufigste Einwand gegen eine harte IBAN-Whitelist lautet: „Lieferanten wechseln doch manchmal die Bank." Stimmt. Genau deshalb haben wir den Widerrufs-Workflow als erstklassige Funktion modelliert: Ein bekannter Lieferant kommt mit einer neuen IBAN — die UI zeigt die alte und die neue IBAN direkt nebeneinander mit Diff-Highlight, der Buchhalter markiert die alte als widerrufen mit Begründung, bestätigt die neue nach externer Verifikation. Ganzer Vorgang: unter einer Minute. Der Unterschied zum Swap-Angriff? Bei legitimen Wechseln weiß der Buchhalter **vorher**, dass der Lieferant wechselt. Bei Angriffen weiß er es nicht. Deshalb ist die explizite, dokumentierte Bestätigung kein Schikane, sondern der Kontrollpunkt, der genau hier trennt.

Warum das für Hausverwaltungen relevanter ist als für viele andere Branchen

In einer typischen Hausverwaltung laufen Handwerker-Rechnungen, Energie-Nachzahlungen, Hausmeister-Abrechnungen, Versicherungen und Behörden-Bescheide gebündelt ein. Die Volumen sind oft nicht riesig — aber die Frequenz ist hoch, die Lieferantenvielfalt ebenfalls, und die Buchhaltung läuft häufig mit wenig Personal und hohem Durchsatz. Exakt die Konstellation, in der ein sauberer Swap-Angriff lange unentdeckt bleibt, weil niemand Zeit hat, jede einzelne Überweisung manuell zu kontrollieren.

Wer hier eine E-Rechnungs-Engine einführt, die „nur" importiert, hat die Compliance-Anforderung erfüllt und gleichzeitig ein Betrugs-Einfallstor geöffnet. Wer den Validierungs-Stack oben implementiert, hat die Compliance-Anforderung erfüllt **und** die SEPA-Überweisung gegen den wahrscheinlichsten Angriffsvektor der nächsten Jahre gehärtet.

Wo wir stehen

Das Epic zur E-Rechnungs-Engine ist als Teil unserer Buchhaltungs-Roadmap beschlossen. Die Sub-Tasks — Schema, Parser für UBL + CII + ZUGFeRD-PDF-Extraktion, Validator mit Anti-Swap-Logik, Generator für Ausgangsrechnungen, Portal-UI mit Vier-Augen-Dialog — sind geschnitten und in der Umsetzungs-Pipeline. Wenn Sie ImmoGenio bereits einsetzen, kommt das Modul ohne zusätzliche Konfiguration in Ihren Mandanten. Wenn Sie die E-Rechnungs-Thematik noch vor sich haben: Der 1. Januar 2027 ist näher, als er sich liest.

Fragen, Rückmeldungen oder eigene Erfahrungen mit dem Thema? Wir freuen uns über Ihre Nachricht an kontakt@immogenio.de.