

ارتقای حکمرانی در حوزه ریال (۲): تخصیص شناسه یکتا به تراکنش‌های بانکی





عنوان: ارتقای حکمرانی در حوزه ریال (۲): تخصیص شناسه یکتا به تراکنش های بانکی
تهیه و تدوین کنندگان (Authors): جواد اسکندری، مرتضی میشکار مطلق، رضا لطفی
واژه های کلیدی: حکمرانی ریال، تراکنش های بانکی، تخصیص شناسه یکتا
ناشر: مرکز پژوهش های مجلس شورای اسلامی

DOI: <https://doi.org/10.22034/mrc.report.22000>

Permanent Link: https://report.mrc.ir/article_12036.html

Publisher : Islamic Parliament Research Center of Iran

عنوان: ارتقای حکمرانی در حوزه ریال (۲): تخصیص شناسه یکتا به تراکنش های بانکی

نوع گزارش: طرح/ لایحه ☐، نظارتی ☐، راهبردی ☒، پیش نویس قانونی ☐

نام دفتر: مطالعات اقتصادی (گروه پولی و بانکی)

مدیر مطالعه: مصطفی حبیب اله پورزرشکی

اظهار نظر کننده خارج از مرکز: محمد سعید شادکار (عضو هیئت علمی دانشگاه الزهراء)

ناظران علمی: سید مهدی بنی طبا، میثم خسروی

گرافیک و صفحه آرایی: منیره حاجی محمدی

ویراستار ادبی: زهره عطاردی

تاریخ شروع مطالعه: ۱۴۰۴/۰۳/۱۰



فهرست مطالب

چکیده.....	۷
خلاصه مدیریتی.....	۸
۱. مقدمه.....	۹
۲. پیشینه.....	۱۰
۲-۱. سوابق مطالعاتی.....	۱۰
۲-۲. سوابق تقنینی.....	۱۰
۳. مروری بر استانداردهای ثبت اطلاعات تراکنش در ریل های مختلف پرداخت.....	۱۲
۳-۱. ویژگی های شناسه یکتای تراکنش.....	۱۳
۴. مفهوم شناسی تراکنش های بانکی و اهداف تخصیص شناسه یکتا.....	۱۵
۵. تجربه جهانی در تخصیص شناسه یکتای تراکنش.....	۱۹
۵-۱. هند.....	۱۹
۵-۲. اتحادیه اروپا.....	۲۴
۶. ملاحظات مرتبط با حفاظت و اشتراک گذاری داده های بانکی.....	۲۸
۶-۱. هند.....	۳۰
۶-۲. اتحادیه اروپا.....	۳۱
۷. طراحی الگوی مطلوب جهت تخصیص شناسه یکتا به تراکنش های بانکی.....	۳۳
۷-۱. فرایند تخصیص شناسه تراکنش.....	۳۳
۷-۲. بررسی الگوریتم های تولید شناسه تراکنش.....	۳۶
۸. جمع بندی و پیشنهادها.....	۳۶
منابع و مآخذ.....	۳۸

فهرست جدول

جدول ۱. احتمال تکرار شناسه با توجه به تعداد شناسه تولیدی.....	۲۶
---	----

فهرست اشکال

شکل ۱. ویژگی های شناسه تراکنش.....	۱۵
شکل ۲. اهداف تخصیص شناسه یکتا.....	۱۶
شکل ۳. مزایای تخصیص شناسه یکتا از منظر مهندسی پایگاه داده.....	۱۸
شکل ۴. نمایش کد سیستم مالی هند در الگوی شناسه مرجع یکتای تراکنش.....	۲۱
شکل ۵. الگوی شناسه مرجع تراکنش برای پرداخت های انتقال وجوه الکترونیکی ملی.....	۲۲
شکل ۶. الگوی شناسه مرجع یکتای تراکنش برای پرداخت های تسویه ناخالص آنی.....	۲۳
شکل ۷. اطلاع رسانی اطلاعات تراکنش به همراه مرجع یکتای تراکنش.....	۲۴
شکل ۸. شناسنامه (رسید) تراکنش در تارگت ۲.....	۲۵
شکل ۹. استعلام تراکنش در پرداخت های سوئیفت.....	۲۷
شکل ۱۰. مدل مفهومی الگوی تخصیص شناسه تراکنش.....	۳۴
شکل ۱۱. شناسنامه تراکنش نمونه.....	۳۵



ارتقای حکمرانی در حوزه ریال (۲): تخصیص شناسه یکتا به تراکنش‌های بانکی

چکیده



در دهه اخیر، با پیچیده‌تر شدن ساختار اقتصادی کشور، ضرورت تقویت حاکمیت پول ملی و حفظ جایگاه آن در اقتصاد بیش از پیش نمایان شده است. حاکمیت ریال، به معنای تثبیت نقش ریال به عنوان ابزار اصلی پرداخت و تسویه تعهدات مالی، از ارکان حکمرانی مؤثر پولی و مالی به شمار می‌آید. تجربه کشورها نشان می‌دهد که ارتقای کیفیت داده‌های تراکنش بانکی، به‌ویژه از طریق طراحی شناسه یکتای سراسری برای هر تراکنش، اثری مستقیم بر افزایش شفافیت، مقابله با پول‌شویی، بهبود نظام مالیاتی و تقویت قدرت نظارتی بانک مرکزی دارد. در این چارچوب، داده‌های تراکنش شبکه بانکی یکی از مهم‌ترین منابع اطلاعاتی برای پایش جریان وجوه، سنجش ریسک‌های مرتبط با ثبات مالی و هدف‌گذاری سیاست‌های رفاهی است. با این حال، پراکندگی رویه‌ها و ناهمگونی شناسه‌های تراکنش در ریل‌های مختلف پرداخت (مانند کارت، سامانه‌های حساب‌محور، چک، و ...) هزینه پاک‌سازی داده را افزایش و ظرفیت رصد برخط و تحلیل یکپارچه را محدود می‌کند. این گزارش با تمرکز حکمرانی بر پول ملی و بهره‌گیری از تجارب بین‌المللی و استانداردهای رایج در صنعت پرداخت، نشان می‌دهد که استقرار شناسه یکتا برای تمامی تراکنش‌ها، در صورت طراحی صحیح، می‌تواند بدون افزودن تأخیر معنادار به فرایند پرداخت و با حداقل تغییر در سامانه‌های موجود، یکی از مهم‌ترین زیرساخت‌های داده‌ای مورد نیاز برای حکمرانی هوشمند بر ریال را فراهم سازد. درنهایت، ضمن تبیین الزامات فنی، حقوقی و نهادی، الگویی به‌منظور تولید و تخصیص شناسه یکتا پیشنهاد می‌شود.

بیان/شرح مسئله

در دهه اخیر، تشدید پیچیدگی‌های محیط اقتصادی کشور و افزایش ریسک‌های نظام مالی، ضرورت توجه ویژه به حکمرانی پولی را برجسته ساخته است. ضعف در زیرساخت‌های اطلاعاتی، نبود استانداردهای یکنواخت برای ثبت و رهگیری تراکنش‌ها و رویکردهای متفاوت بانک‌ها در تولید شناسه تراکنش، امکان نظارت مؤثر و تصمیم‌سازی دقیق را محدود ساخته و زمینه بروز ریسک‌های مرتبط با ثبات مالی را فراهم کرده است. در همین راستا، تثبیت و تقویت حاکمیت پول ملی و حکمرانی بر پول ملی به‌عنوان دو بن‌مایه اصلی تأمین ثبات اقتصادی باید مورد توجه قرار گیرد. تضعیف نقش ریال به‌عنوان ابزار اصلی پرداخت و نبود نظارت مکفی بر داده‌های تراکنش شبکه بانکی در ریل‌های مختلف پرداخت، ریسک‌های متعددی برای اعتبار نظام مالی کشور ایجاد کرده که حل آنها نیازمند اصلاح اساسی در زیرساخت‌های داده‌ای است.

نقطه‌نظرات / یافته‌های کلیدی

مطالعه تجارب کشورهای مختلف نشان می‌دهد که ایجاد بسترهای یکپارچه برای جمع‌آوری، ثبت و تحلیل داده‌های تراکنش بانکی، محور اصلی سیاست‌های موفق مقابله با جرائم مالی و ارتقای شفافیت بوده است. تخصیص شناسه یکتا به هر تراکنش، یکی از اقدامات بنیادین در این حوزه است که امکان رصد برخط، استعلام سریع و جلوگیری از جعل یا دست‌کاری اطلاعات را فراهم می‌کند. برخی کشورها با تدوین مقررات جامع و الزام‌آور، کلیه بانک‌ها و مؤسسات اعتباری را به استفاده از چارچوب‌ها و قالب‌های استاندارد برای تولید شناسه‌های یکتا ملزم ساخته‌اند. این امر نه تنها موجب ارتقای هماهنگی نهادی و افزایش سرعت پاسخ‌گویی به استعلامات مردمی شده، بلکه توانایی حاکمیت جهت پیگیری تخلفات، کاهش هزینه‌های نظارت و پیش‌بینی به‌موقع ریسک‌های مرتبط با ثبات مالی را به‌طور قابل ملاحظه‌ای افزایش داده است. همچنین تجربیات جهانی تأکید می‌کند که استانداردسازی کیفیت داده‌ها، آموزش مستمر نیروی انسانی، تضمین امنیت اطلاعات و مدیریت یکپارچه پایگاه‌های داده، پیش‌شرط موفقیت این اصلاحات است.

پیشنهاد راهکارهای تقنینی، نظارتی یا سیاستی

براساس ارزیابی‌های صورت گرفته، پیشنهاد می‌شود بانک مرکزی جمهوری اسلامی ایران، در اجرای جزء «۳» بند «الف» ماده (۴) قانون بانک مرکزی مبنی بر «ایجاد زیرساخت‌های فنی لازم برای تشکیل پایگاه جامع جمع‌آوری و تحلیل داده»، یک دستورالعمل جامع و الزام‌آور برای استانداردسازی داده‌های تراکنش تدوین و ابلاغ کند. این دستورالعمل باید، از یک‌سو، حداقل ارقام اطلاعاتی شناسنامه تراکنش (نظیر شناسه طرفین، مبلغ، زمان، ریل پرداخت، ابزار پرداخت و ...) و از سوی دیگر، سازوکار واحد تولید و به‌کارگیری شناسه یکتای تراکنش را در سطح کلیه ریل‌های پرداخت تعیین کند. به‌موجب این دستورالعمل، کلیه بانک‌ها، مؤسسات اعتباری و ارائه‌دهندگان خدمات پرداخت مکلف خواهند بود فرایندهای خود را با این استانداردها منطبق سازند. در الگوی پیشنهادی، شناسه یکتای تراکنش در لحظه آغاز تراکنش، به‌صورت محلی در بانک یا ارائه‌دهنده خدمت پرداخت مبدأ و براساس الگوریتم و قالب ابلاغی بانک مرکزی تولید می‌شود. سپس این شناسه در تمام پیام‌های مبادله شده بر بستر ریل‌های مختلف پرداخت حمل و در سامانه‌های عملیاتی و نظارتی ثبت می‌گردد، به‌گونه‌ای که نیازی به اخذ تأیید برخط از بانک مرکزی یا افزودن گام مسدودکننده به زنجیره پردازش تراکنش ایجاد نشود. هم‌زمان، بانک مرکزی می‌تواند با اتکا به جریان رویدادهای تراکنش، پایگاه جامع تحلیل داده‌های تراکنش را تغذیه کرده و نظارت داده‌محور بر شبکه بانکی و سایر اشخاص تحت نظارت را توسعه دهد.

۱. مقدمه

در سال‌های اخیر، شتاب تحولات اقتصادی، لزوم بازنگری و تقویت زیرساخت‌های داده‌ای در نظام مالی کشور را به ضرورتی اجتناب‌ناپذیر تبدیل کرده است. افزایش حجم و تنوع تراکنش‌های بانکی و پرداختی، در کنار تهدیداتی نظیر جرائم مالی، پول‌شویی و ریسک‌های مرتبط با ثبات مالی، نیاز به سازوکارهای پیشرفته برای ثبت، رهگیری و تحلیل داده‌ها را بیش‌ازپیش آشکار ساخته است. درچنین شرایطی، فقدان دید یکپارچه نسبت به جریان وجوه در ریل‌های مختلف پرداخت و ناتوانی در اتصال داده‌های پراکنده، یکی از گلوگاه‌های اصلی حکمرانی پولی به‌شمار می‌آید.

نظارت بانکی به‌عنوان یکی از ارکان اصلی حفظ ثبات و سلامت نظام مالی، در طول دهه‌های اخیر تحولات عمیقی را تجربه کرده است. در مراحل اولیه شکل‌گیری نظام‌های بانکی مدرن، نظارت عمدتاً برپایه بازرسی‌های حضوری، حسابرسی‌های دوره‌ای و گزارش‌های پسینی استوار بود. رویکردی که با وجود کارآمدی نسبی در مقیاس و پیچیدگی محدود آن دوره، به‌تدریج پاسخ‌گوی رشد حجم تراکنش‌ها و تنوع فعالیت‌های مالی نبود. در دهه‌های ۱۹۸۰ و ۱۹۹۰ میلادی، با شکل‌گیری چارچوب‌های بازل، پارادایم نظارت مبتنی بر ریسک مطرح شد که تمرکز خود را بر شناسایی، سنجش و مدیریت ریسک‌های اعتباری، نقدینگی، بازار و کفایت سرمایه قرار می‌داد. پس از بحران مالی ۲۰۰۸ و گسترش فناوری‌های مالی و ابزارهای تحلیلی پیشرفته، نسل جدیدی از نظارت بانکی شکل گرفت که بر نظارت داده‌محور و فناوری‌محور استوار است. نسلی از نظارت که در آن، دسترسی به داده‌های دقیق، بهنگام و قابل اتکا، پیش‌شرط اصلی پایش برخط فعالیت‌های بانکی، رصد ریسک‌های سیستمی و مداخله به‌موقع تلقی می‌شود.

قانون بانک مرکزی جمهوری اسلامی ایران مصوب ۱۴۰۲، چارچوب حقوقی گذار به نظارت داده‌محور را تبیین کرده است. براساس جزء «۲۱» بند «الف» ماده (۴)، بانک مرکزی مکلف است از طریق «تحکیم حکمرانی پول ملی از طریق نظارت مؤثر بر آن»، زمینه تقویت حکمرانی بر پول ملی را فراهم آورد. همچنین بندهای «پ» و «ت» ماده (۲) بر دو هدف «افزایش توان نظارت بانک مرکزی بر اشخاص تحت نظارت» و «ارتقای سلامت، اثربخشی و پاسخ‌گویی شبکه بانکی» تأکید دارند. افزون‌براین، جزء «۳» بند «الف» ماده (۴) به‌طور صریح بانک مرکزی را موظف به «ایجاد زیرساخت‌های فنی لازم برای تشکیل پایگاه جامع جمع‌آوری و تحلیل داده» می‌کند.

تجربیات داخلی و بین‌المللی گواه آن است که نبود یکپارچگی و استانداردسازی در نظام داده‌های بانکی و پرداخت، نه‌تنها کارایی سیاست‌های نظارتی و تنظیمی را تضعیف می‌کند، بلکه هزینه‌های مرتبط با مدیریت ریسک، مقابله با جرائم مالی و حفظ سلامت اقتصادی را به‌طور قابل توجهی افزایش می‌دهد. در بسیاری از کشورها، یکی از پاسخ‌های کلیدی به این چالش، حرکت به سمت نظارت داده‌محور و طراحی معماری‌های یکپارچه برای داده‌های تراکنش، مبتنی بر شناسه‌های یکتای قابل ردیابی برای هر تراکنش در تمامی ریل‌های پرداخت بوده است.

قانون مالیات بر سوداگری و سفته‌بازی مصوب ۱۴۰۴ نیز تکلیف مشخص و صریحی درخصوص استقرار



شناسه یکتا برای تراکنش‌ها برعهده بانک مرکزی و شبکه بانکی قرار داده است. براساس ماده (۷) این قانون که جایگزین ماده (۱۱) [قانون پایانه‌های فروشگاهی و سامانه مؤدیان](#) شده است، کلیه اشخاصی که به انجام عملیات بانکی موضوع بند «چ» ماده (۱) قانون بانک مرکزی اشتغال دارند- اعم از بانک‌های ایرانی، شعب و نمایندگی بانک‌های خارجی مستقر در کشور، صندوق‌های قرض‌الحسنه، تعاونی‌های اعتبار و ارائه‌دهندگان خدمات کیف پول- موظف شده‌اند از یک سال پس از لازم‌الاجرا شدن حکم، به‌تمامی تراکنش‌ها اعم از واریزی و برداشتی، مطابق استاندارد اعلامی بانک مرکزی جمهوری اسلامی ایران، شناسه یکتا اختصاص دهند.

در همین چارچوب، بانک مرکزی در چارچوب بند «الف» ماده «۱۹» قانون بانک مرکزی مکلف است بر حسن اجرای این حکم نظارت کند. بدین‌ترتیب، استقرار ترتیبات لازم برای تخصیص شناسه یکتا به تراکنش‌ها، نه صرفاً یک پیشنهاد سیاستی، بلکه یک الزام صریح قانونی است. در همین راستا، این گزارش در ابتدا پیشینه موضوع را از منظر مطالعاتی و تقنینی مورد بررسی قرار داده و در ادامه به سیر تحول شناسنامه تراکنش‌های بانکی و پیدایش مفهوم شناسه یکتا و ویژگی‌های آن پرداخته است. سپس مفاهیم پایه، تعریف تراکنش‌های بانکی، ریل‌های پرداخت و اهداف تخصیص شناسه یکتا تبیین شده و تجربه چند کشور منتخب، به‌ویژه هند و اتحادیه اروپا، را در استقرار شناسه یکتای تراکنش مرور کرده است. به‌علاوه، ملاحظات مرتبط با حفاظت و اشتراک‌گذاری داده‌های بانکی در چارچوب استفاده از شناسه یکتا بررسی شده و درنهایت پیشنهاد طراحی الگوی تخصیص شناسه یکتا برای نظام بانکی ایران ارائه شده است.

۲. پیشینه



۲-۱. سوابق مطالعاتی

مرکز پژوهش‌های مجلس شورای اسلامی در سال ۱۳۹۹ گزارشی با عنوان «ارتقای حکمرانی در حوزه ریال (۱): مروری بر تکالیف قانونی دستگاه‌ها» منتشر کرد. هدف این گزارش شناسایی وضعیت اجرایی تکالیف قانونی است که به‌نوعی موجب ارتقای حکمرانی در حوزه ریال می‌شوند. در گزارش مذکور بیان شده که کم‌توجهی به راهبرد بلندمدت شفافیت اقتصاد و سالم‌سازی آن^۱ موجب شده است تا به‌جای سرمایه‌گذاری منابع کشور برای حذف زمینه‌های فساد، هزینه‌های قابل توجهی با هدف کشف فساد در فرایند رسیدگی قضایی به اقتصاد کشور تحمیل شود. سپس تشریح می‌کند که با استفاده از زیرساخت‌های قانونی و بهره‌برداری از ظرفیت‌های ایجاد شده در خصوص تولید، تجمیع و استفاده از اطلاعات اقتصادی می‌توان حکمرانی در زمینه‌های مختلف اعم از حوزه بانکی، حوزه اصلاح نظام مالیاتی و نیز حوزه مبارزه با پول‌شویی ارتقا یابد. در انتهای گزارش مذکور پیشنهاد می‌شود، اجرای قوانین فعلی در دستور کار قرار گرفته و تصویب قوانین جدید به‌منظور ارتقای حکمرانی در حوزه ریال پیگیری شود.

۲-۲. سوابق تقنینی

شفافیت در تراکنش‌های بانکی، نقش محوری در پیشگیری از جرائم مالی نظیر پول‌شویی و فرار مالیاتی دارد. مجلس شورای اسلامی طی سال‌های اخیر با هدف تقویت نظارت بر جریان‌های مالی و ایجاد نظام یکپارچه اطلاعاتی، مصوباتی در این زمینه داشته است.

۱. این راهبرد براساس محور نوزدهم سیاست‌های کلی اقتصاد مقاومتی است که از سوی رهبر شهید در تاریخ ۱۳۹۲/۱۲/۲۹ ابلاغ شده است.

بند «ح» تبصره «۱۶» [قانون بودجه سال ۱۳۹۸](#) کل کشور، مصوب ۱۳۹۷/۱۲/۲۱ مجلس شورای اسلامی، بانک مرکزی را مجاز ساخت تا حساب‌های بانکی اشخاص حقیقی فاقد شماره ملی و اشخاص حقوقی فاقد شناسه ملی را ظرف یک ماه مسدود کند. همچنین، بانک‌ها و مؤسسات مالی موظف شدند اطلاعات تراکنش‌های بانکی، اعم از درون‌بانکی و بین‌بانکی، را به‌صورت ماهانه در اختیار سازمان امور مالیاتی قرار دهند. برای تراکنش‌های اشخاص حقیقی، بانک مرکزی موظف شد با تصویب شورای پول و اعتبار، سقفی برای تراکنش‌ها تعیین کند که نقل‌وانتقال مبالغ بالاتر از این سقف، مشروط به درج توضیح «بابت» و در صورت نیاز ارائه اسناد مثبت است. همچنین، این امکان نیز فراهم شد تا اشخاص حقیقی که از حساب‌های بانکی خود برای فعالیت‌های تجاری استفاده می‌کنند، با دریافت شماره اقتصادی از این محدودیت معاف شوند. هدف این بند قانونی ایجاد شفافیت مالی با تأکید بر شناسایی هویت و رصد تراکنش‌های خاص بود.

[قانون بانک مرکزی جمهوری اسلامی ایران](#)، مصوب ۱۴۰۲/۰۳/۳۰، با تمرکز بر تقویت اشراف اطلاعاتی، امکان نظارت بر تراکنش‌ها را ارتقا داد. مطابق ماده (۱۹) این قانون، بانک مرکزی موظف است تا اشخاص تحت نظارت، به‌ویژه مؤسسات اعتباری را به استفاده از قواعد نرم‌افزاری و فرایندهای مشخص در سامانه‌های داخلی خود ملزم کند. همچنین، تراکنش‌هایی با مبلغ بالاتر از حد تعیین شده توسط هیئت عالی بانک مرکزی، تنها در صورت ثبت شناسه یکتای صورت‌حساب الکترونیکی^۱ یا درج توضیح «بابت» و تأیید انتقال‌گیرنده قابل انجام هستند. این الزام با اتصال به سامانه مؤدیان مالیاتی، شفافیت در تراکنش‌های کلان را بهبود بخشیده و با تدوین دستورالعمل‌های متناسب با اطلاعات اقتصادی و هویتی اشخاص، نظارت هدفمندتر را ممکن ساخته است.

ماده (۱۶۹ مکرر) [قانون مالیات‌های مستقیم](#) مصوب ۱۳۹۴/۰۴/۳۱ با اصلاحات و الحاقات بعدی، نیز با ایجاد پایگاه اطلاعات هویتی، عملکردی و دارایی مؤدیان مالیاتی، درصدد ایجاد زیرساخت داده‌ای قابل استفاده در حکمرانی اقتصادی است. این قانون بانک‌ها و مؤسسات مالی را ملزم به ارائه اطلاعاتی نظیر گردش سالانه حساب‌ها، سپرده‌ها و تسهیلات به سازمان امور مالیاتی کرده است. علاوه بر آن، ماده (۷) [قانون مالیات بر سوداگری و سفته‌بازی](#) که ماده (۱۱) قانون پایانه‌های فروشگاهی و سامانه مؤدیان را اصلاح کرده است، به موضوع تخصیص شناسه یکتا به هر تراکنش پرداخته شده است. این موضوع با دو هدف زیر انجام شده است:

۱. تکمیل پایگاه اطلاعاتی موضوع ماده (۱۶۹ مکرر) [قانون مالیات‌های مستقیم](#)،
۲. تکمیل پایگاه جامع جمع‌آوری و تحلیل داده موضوع جزء «۳» بند «الف» ماده (۴) [قانون بانک مرکزی جمهوری اسلامی ایران](#). لازم به ذکر است؛ مطابق این ماده، تمام اشخاصی که نسبت به انجام عملیات بانکی نظیر دریافت سپرده از اشخاص حقیقی یا حقوقی، اعطای تسهیلات یا ایجاد اعتبار اشتغال دارند، اعم از تمام بانک‌های ایرانی، شعب و نمایندگی بانک‌های خارجی مستقر در کشور، صندوق‌های قرض‌الحسنه، تعاونی‌های اعتبار و ارائه‌کنندگان خدمات کیف پول باید به کلیه تراکنش‌ها اعم از واریز و برداشت مطابق استاندارد اعلام شده از سوی بانک مرکزی، شناسه‌ای یکتا اختصاص دهند.

۱. موضوع بند «ث» ماده (۱) [قانون پایانه‌های فروشگاهی و سامانه مؤدیان](#).

۳. مروری بر استانداردهای ثبت اطلاعات تراکنش در ریل‌های مختلف پرداخت

در نظام‌های بانکی و پرداخت، بخش قابل توجهی از رویدادهای مالی که از مجاری رسمی انجام می‌شوند در قالب «تراکنش» در سامانه‌های هسته بانکی^۱ و ریل‌های مختلف پرداخت ثبت می‌گردند. هریک از این تراکنش‌ها در عمل به صورت یک رکورد داده در سامانه‌های عملیاتی ظاهر می‌شود که مجموعه‌ای از اقلام اطلاعاتی را در بر دارد. در این گزارش، برای اشاره به مجموعه‌ای از اقلام کلیدی که امکان شناسایی، ردیابی و بازسازی یک تراکنش را در طول چرخه عمر آن فراهم می‌کنند، از اصطلاح «شناسنامه تراکنش» استفاده می‌شود. بسته به ریل و سامانه، این شناسنامه می‌تواند شامل شناسه یا شماره مرجع تراکنش، تاریخ و زمان انجام، مبلغ، نوع عملیات (مانند برداشت، واریز، انتقال یا خرید)، مشخصات حساب‌ها یا ابزارهای پرداخت درگیر (از جمله شماره حساب، شبا، کارت یا کیف پول)، اطلاعات هویتی طرفین در دسترس، وضعیت پردازش و کدهای پاسخ باشد.

با گسترش ریل‌های الکترونیکی پرداخت، در هر ریل مجموعه اقلام کلیدی که شناسنامه تراکنش را تشکیل می‌دهد، قالب و منطق خاص خود را پیدا کرده است. در ریل کارت (پایانه فروش، خودپرداز و سایر پردازنده‌های کارت)، به دلیل وجود استانداردهای متعدد و اختصاصی در شبکه‌های پردازش داخلی و منطقه‌ای که مانع اصلی قابلیت همکاری بانک‌های صادرکننده و پذیرنده در سطح داخلی و بین‌المللی بود، نیاز به یک پروتکل واحد و خنثی احساس می‌شد. به عبارت دیگر، هر شبکه یا بانک از قالب و کدینگ خاص خود استفاده می‌کرد که این مسئله منجر به ایجاد مشکلاتی در تبادل اطلاعات و افزایش ریسک خطا و سوءبرداشت در پرداخت‌ها می‌شد. به همین دلیل، کمیته فنی خدمات مالی سازمان استاندارد بین‌المللی^۲، استاندارد ISO 8583 را به عنوان زبان مشترک پایه برای پیام‌رسانی تراکنش‌های کارت‌محور تدوین کرد و ساختار پیام را برپایه نوع پیام، مجموعه‌ای از عناصر داده^۳ و فیلدهای کلیدی مانند شماره کارت، مبلغ تراکنش، تاریخ و زمان، شماره ردیابی سامانه^۴ و شماره مرجع بازیابی^۵ سامان داد. در بسیاری از پیاده‌سازی‌ها، شماره ردیابی سامانه و شماره مرجع بازیابی در کنار سایر اقلام عملاً دو رکن اصلی شناسنامه عملیاتی هر تراکنش در شبکه‌های کارت محسوب می‌شوند و برای ردیابی، تطبیق و تسویه بین بانک‌ها و شبکه‌های پرداخت به کار می‌روند [۱].

در مقابل، در ریل‌های حساب‌محور بین‌بانکی (مانند حواله‌های بین‌المللی و سامانه‌های تسویه ناخالص آنی^۶ و اتاق‌های پایاپای خودکار^۷)، به طور سنتی پیام‌های سری MT SWIFT نظیر MT103 برای حواله‌های اعتباری به عنوان استاندارد غالب پیام‌رسانی بین‌بانکی و حواله‌های بین‌المللی پذیرفته شدند. این پیام‌ها نیز از فیلدهایی مانند شماره مرجع تراکنش^۸ (فیلد ۲۰) و ارجاع مرتبط^۹ (فیلد ۲۱) برای شناسایی و ارجاع تراکنش استفاده کردند. باین حال، یکتایی این شناسه‌ها معمولاً در محدوده هر بانک یا در چارچوب هر زنجیره پیام‌رسانی تعریف می‌شود و نه در سطح همه ریل‌ها و سامانه‌ها. از این رو، اگرچه برای ردیابی تراکنش در طول زنجیره بانک‌های درگیر کارکرد مؤثری دارند، به خودی خود معادل یک شناسه یکتای سراسری که در کل نظام پرداخت قابل اتکا باشد، نیستند. از این رو، پیام‌های سنتی سوئیفت سری MT، به دلیل محدودیت‌های ذاتی ساختار خود از جمله طول‌های محدود فیلدها، تکیه

1. Core Banking

2. ISO/Technical Committee (TC 68) – Financial Services

3. Data Elements (DE)

4. System Trace Audit Number (STAN) - DE11

5. Retrieval Reference Number - DE37

6. RTGS

7. ACH

8. Transaction Reference Number

9. Related Reference

بر بخش های متنی عمدتاً غیرساختاریافته و نبود فیلدهای اختصاصی برای بسیاری از اطلاعات تجاری و مقرراتی در پاسخ گویی به الزامات جدید شفافیت و انطباق با چالش های جدی روبه رو شدند. به گونه ای که در عمل، بخشی از اطلاعات حواله یا مشخصات طرفین یا اصلاً منتقل نمی شد یا به صورت فشرده و در قالب متن آزاد در چند فیلد مختلف درج می گردید و نیاز به مداخلات دستی را افزایش می داد. نیاز روزافزون به انتقال داده های غنی و ساخت یافته شامل اطلاعات کامل حواله، جزئیات دقیق طرفین تراکنش برای اهداف تنظیم گری و داده های لازم برای رعایت الزامات مبارزه با پول شویی در کنار ضرورت هم گرایی استانداردهای پراکنده، زمینه ساز تدوین و معرفی استاندارد جامع ISO 20022 شد.

استاندارد ISO 20022 برپایه یک فرهنگ واژه و مدل مفهومی مشترک برای داده های مالی بنا شده است. در این چارچوب، ابتدا عناصر اصلی یک تراکنش (مانند پرداخت، فرستنده، گیرنده، حساب، ابزار پرداخت و ...) در سطح معنایی به طور دقیق تعریف و مدل سازی می شوند و سپس براساس مجموعه ای از قواعد فنی، همین مدل مفهومی به قالب های پیاده سازی مختلف تبدیل می شود. رایج ترین این قالب ها زبان نشانه گذاری توسعه پذیر^۱ است که پیام را به صورت متن ساخت یافته و برجسب دار نمایش می دهد، اما این استاندارد امکان استفاده از قالب های دیگر، از جمله نشانه گذاری نحو انتزاعی شماره یک^۲ (مناسب قالب های باینری فشرده) و نگاشت های مبتنی بر JSON را نیز فراهم کرده است. به این ترتیب، حتی اگر سامانه های بانکی موجود همچنان از پیام های اختصاصی و قالب های قدیمی تر استفاده کنند، می توان با نگاشت آنها به مدل مفهومی ISO 20022، پیام هایی تولید کرد که از نظر محتوا هم معنا و از نظر فنی در سطح ملی و بین بانکی قابل همکاری و تجمیع باشند.

در نهایت، می توان گفت که استانداردهایی مانند ISO 8583 و پیام های SWIFT MT شناسنامه تراکنش را عمدتاً در سطح هر ریل یا شبکه پرداخت تعریف کرده اند، یعنی شناسه های عملیاتی مانند شماره ردیابی سامانه یا شماره مرجع تراکنش، بیشتر در چارچوب هر بانک، هر سوئیچ یا هر سامانه تسویه معنا پیدا می کنند و الزاماً یک رشته یکتا و پایدار در کل زنجیره پرداخت ایجاد نمی کنند. در مقابل، استاندارد ISO 20022 با تکیه بر مدل مفهومی مشترک، لایه ای نظام مند از شناسه ها را برای تراکنش تعریف می کند که از سطح پیام و دسته پرداخت تا سطح هر تراکنش منفرد و حتی تا سطح زنجیره بین المللی را پوشش می دهد. به این ترتیب، امکان ایجاد یک شناسه یکتای سرتاسری برای هر تراکنش که در همه ریل ها و در تمام طول حیات تراکنش قابل ردیابی باشد به صورت ذاتی در معماری ISO 20022 پیش بینی شده است.

۱-۳. ویژگی های شناسه یکتای تراکنش

اطلاعاتی از تراکنش های بانکی که برای مقام ناظر بانکی یا سایر بخش های حاکمیت نظیر نهاد مبارزه با پول شویی یا نهاد مالیاتی می تواند حائز اهمیت باشد و مؤسسات مالی و اعتباری وظیفه تولید و ارسال آنها را باید برعهده بگیرند، شامل موارد زیر است:

- شناسه یکتای تراکنش،
- مشخصات طرفین تراکنش،
- بانک های طرفین تراکنش،
- مبلغ تراکنش،
- تاریخ تراکنش،

1. EXtensible Markup Language(-XML)

2. Abstract Syntax Notation One(-ASN.1)

• ابزار پرداخت مورد استفاده،

• بابت تراکنش.

مهم‌ترین ویژگی‌هایی که در تولید شناسه تراکنش باید مورد توجه قرار گیرند، در زیر احصا شده است:

۱ یکتایی: مفهوم یکتایی یکی از ویژگی‌های حیاتی است که بر امنیت و شفافیت سیستم‌های مالی تأثیر مستقیم دارد. این ویژگی بیان می‌کند که هر تراکنش باید شناسه‌ای منحصر به فرد داشته باشد که آن را از سایر تراکنش‌ها متمایز کند و بدین معناست که شناسه اختصاص داده شده به یک تراکنش به‌طور کامل بی‌همتا بوده و هیچ دو تراکنشی نمی‌توانند شناسه مشابه داشته باشند.

۲ تصادفی بودن: شناسه‌های تراکنش معمولاً با استفاده از الگوریتم‌هایی تولید می‌شوند که دنباله‌هایی تصادفی یا شبه تصادفی ایجاد می‌کنند. ویژگی تصادفی بودن، امکان پیش‌بینی شناسه را از بین می‌برد و احتمال دسترسی غیرمجاز یا تقلب را به‌طور قابل توجهی کاهش می‌دهد.

۳ قابلیت عدم انتقال اطلاعات مهم: هیچ‌گونه اطلاعات مهمی، به‌خصوص اطلاعات مربوط به طرفین تراکنش و مبلغ تراکنش نباید از طریق شناسه تراکنش قابل محاسبه باشد. به همین علت، بخشی از شناسه تراکنش حتماً باید با یک الگوریتم تصادفی یا نیمه تصادفی تولید شود. در برخی از شناسه‌های تراکنش، که در ادامه گزارش به‌عنوان مطالعه موردی ذکر می‌گردد، تاریخ، نام بانک و نوع تراکنش از طریق شناسه تراکنش قابل شناسایی است. اما در اکثر موارد، الگوریتم تولید شناسه تراکنش به‌گونه‌ای است که حتی اطلاعاتی که اهمیت زیادی هم ندارند، از طریق شناسه تراکنش قابل شناسایی نیست. لازم به یادآوری است که این شناسه به‌عنوان کلید اصلی^۱ در پایگاه داده‌های بانکی و نظارتی ایفای نقش می‌کند و از طریق آن، رابطه‌ای یکتا با رکورد کامل تراکنش در جداول مرتبط برقرار می‌شود. بدین ترتیب، تمامی اطلاعات مربوط به تراکنش - شامل مبلغ، زمان، مبدأ، مقصد و سایر مشخصات - نه در خود شناسه، بلکه در شناسنامه یا به عبارتی در جداول وابسته‌ای ذخیره می‌شود که شناسه به آنها اشاره دارد.

۴ الگوی^۲ شناسه: شناسه‌های تراکنش از حروف و اعداد و نمادها تشکیل می‌شوند و مقام‌های ناظر بر نظام پرداخت، کاراکترهای مجاز و طول هر رشته تصادفی تولید شده (تعداد کاراکترها) برای استفاده در تولید شناسه تراکنش را اعلام می‌کند. برای مثال، ممکن است بانک مرکزی فقط حروف بزرگ را برای استفاده در شناسه تراکنش مجاز اعلام کند.

۵ قابلیت اشتراک‌گذاری (گزارش‌دهی): شناسه تراکنش باید در گزارش تراکنش (رسید) قید شود. این شناسه باید به طرفین تراکنش، بانک مقصد و سایر نهادهایی که به‌لحاظ قانونی می‌توانند به داده‌های تراکنش دسترسی داشته باشند (برای مثال، نهاد مبارزه با پول‌شویی) گزارش گردد. البته شناسه اعلامی در گزارش تراکنش می‌تواند متمایز از شناسه یکتای تراکنش باشد.

۶ قابلیت اعلام: برای اطمینان از صحت انجام هر تراکنش، باید شناسه تراکنش قابل اعلام باشد. برای نهادهایی که تراکنش به آنان گزارش می‌شود و همچنین برای طرفین تراکنش، بستر اعلام شناسه تراکنش باید از طریق نرم‌افزارهای برخط و به‌صورت آنی فراهم شود. لازم به ذکر است که مطابق قوانین حریم خصوصی معمولاً برای اعلام تراکنش‌های شبکه بانکی، تنها در اختیار داشتن شناسه تراکنش کافی نیست و علاوه بر شناسه تراکنش، باید اطلاعاتی تکمیلی مثل شماره حساب مقصد، مبلغ تراکنش یا تاریخ تراکنش درج شود.

1. Primary Key

2. Format

شکل ۱. ویژگی‌های شناسه تراکنش



مأخذ: یافته‌های گزارش.

۴. مفهوم شناسی تراکنش‌های بانکی و اهداف تخصیص شناسه یکتا



در فرایند تحلیل و بررسی سازکارهای فنی مرتبط با شناسه تراکنش^۱، نخستین گام تبیین مفهوم تراکنش بانکی است. ارائه تعریف روشن از این مفهوم، نه تنها درک درستی از نحوه شکل‌گیری و پردازش تراکنش‌ها فراهم می‌سازد، بلکه زمینه‌ساز تحلیل ساختار شناسایی و رهگیری این نوع عملیات در نظام‌های بانکی و مالی نیز خواهد بود. مطابق با ماده (۴) بند «۵» از دستورالعمل شماره ۲۳۶۶/۲۰۱۵ اتحادیه اروپا (معروف به PSD2)، «تراکنش پرداخت» به عملی اطلاق می‌شود که توسط پرداخت‌کننده، به نمایندگی از او، یا توسط دریافت‌کننده آغاز می‌گردد و شامل انتقال، واریز یا برداشت وجه است، صرف‌نظر از وجود یا نبود تعهدات قراردادی میان طرفین. این تعریف گسترده، تمامی رخدادهای مالی‌ای را دربرمی‌گیرد که منجر به جابه‌جایی وجه میان حساب‌ها شود [۴]. بر همین مبنا، می‌توان «تراکنش بانکی» را در معنای عام، به هر رخدادی اطلاق کرد که منجر به افزایش یا کاهش مانده حساب‌های نزد بانک‌ها یا حساب‌های نگهداری شده بانک‌ها و اشخاص نزد بانک مرکزی شود، مشروط بر آنکه با انتقال وجه در یک بستر پرداخت

1. Transaction Identifier

رسمی همراه باشد. این تعریف، انواع مختلفی از تعاملات مالی را شامل می‌شود که در ادامه برخی از مهم‌ترین مصادیق آن فهرست شده است:

- انتقال پول از حساب شخص (الف) به حساب شخص (ب) که موجب کاهش مانده حساب شخص (الف) و افزایش مانده حساب شخص (ب) می‌شود. این دو شخص می‌توانند نزد یک بانک حساب داشته باشند (تراکنش درون بانکی) یا نزد دو بانک مختلف (تراکنش بین بانکی).
 - اعطای تسهیلات از سوی شبکه بانکی، موجب افزایش مانده حساب تسهیلات گیرنده خواهد شد.
 - پرداخت سود سپرده، موجب افزایش مانده حساب صاحب سپرده می‌شود.
 - بازپرداخت تسهیلات، کاهش مانده حساب تسهیلات گیرنده را به دنبال خواهد داشت.
 - واریز حقوق کارمندان بانک مرکزی که افزایش مانده حساب کارمندان نزد بانک مرکزی را در پی خواهد داشت.
- با هدف شناسایی تراکنش‌ها، به هریک از آنها شناسه‌ای یکتا اختصاص داده می‌شود. این شناسه، ترکیبی از حروف، اعداد و نمادها بوده و معمولاً به صورت تصادفی و یا نیمه تصادفی توسط مجری انجام تراکنش تولید می‌شود. الزام بانک‌ها و مؤسسات اعتباری به تخصیص این شناسه یکتا، در راستای تحقق اهداف متعدد نظارتی، امنیتی و شفاف‌سازی جریان‌های مالی صورت می‌گیرد.

شکل ۱.۲. اهداف تخصیص شناسه یکتا



مأخذ: همان.

سه مورد از مهم ترین اهداف تخصیص شناسه یکتا مطابق شکل ۲ به هر تراکنش عبارت اند از:

۱ شناسایی و رهگیری: شناسه یکتای تراکنش به نهادهای حاکمیت نظیر بانک مرکزی، مرکز مبارزه با پول شویی و نهاد مالیاتی و ... این امکان را خواهد داد تا میلیاردها تراکنش در یک پایگاه داده بزرگ را به طور مؤثرتری مدیریت و ردیابی کنند. بهره برداری از پایگاه اطلاعات با حجم داده ی زیاد، مستلزم آن است که تمام داده ها با یک شکل و زبان یکسان و مشخص نوشته شده باشند تا فرایند ثبت، شناسایی و رهگیری با کارایی و اثربخشی بالایی همراه باشد. چراکه در مهندسی پایگاه داده، تخصیص شناسه یکتا به هر رکوردی از داده، عنصری بنیادین برای مدیریت داده ها و اطمینان از کیفیت آنها محسوب می شود. این امر، علاوه بر مزیت مذکور، دارای مزایای زیر است:

■ **حفظ یکپارچگی داده ها:**^۱ در سیستم های مدیریت پایگاه داده رابطه ای،^۲ شناسه یکتا به عنوان کلید اصلی عمل می کند. این کلید تضمین می کند که رکوردهای تکراری وارد سیستم نمی شوند و باعث استقرار قید یکپارچگی^۳ در لایه مدیریت داده ها می شود.

■ **بهینه سازی جستجو:**^۴ پایگاه های داده از شناسه یکتا برای ایندکس گذاری^۵ استفاده می کنند. ایندکس ها ساختارهایی هستند که امکان اجرای سریع پرس و جوها^۶ را فراهم می سازند. الگوریتم های پیشرفته ای نظیر B-Trees یا Hash Indexing برپایه همین شناسه ها طراحی شده اند و در محیط هایی با میلیون ها رکورد، جست و جوی داده ها را از چند ثانیه به چند میلی ثانیه کاهش می دهند. این مزیت در نظام پرداخت، برای پاسخ دهی سریع به درخواست های استعلام، کنترل تقلب یا تطبیق اطلاعات، حیاتی است.

■ **مدیریت داده های توزیع شده:**^۷ در معماری های پایگاه داده توزیع شده، شناسه یکتا برای اطمینان از هم زمانی^۸ و یکپارچگی در داده های تقسیم شده بین نودها حیاتی است. این شناسه ها از طریق الگوریتم های تولید یکتا^۹ به صورت سراسری^{۱۰} یا محلی^{۱۱} تولید می شوند و امکان همگام سازی دقیق بین پایگاه داده ها را فراهم می کنند.

■ **مدیریت روابط بین جداول:**^{۱۲} در ساختار پایگاه های داده رابطه ای، تخصیص شناسه یکتا به هر تراکنش، امکان تعریف روابط دقیق میان جداول مختلف (مثلاً جدول کاربران، حساب ها و تراکنش ها) را فراهم می سازد. شناسه تراکنش در این ساختار هم به عنوان کلید اصلی در جدول تراکنش و هم به عنوان کلید خارجی^{۱۳} در سایر جداول ایفای نقش می کند. این ساختار، مانع از بروز تضاد یا تکرار داده ها شده و انسجام بین اجزای مختلف سامانه را حفظ می کند.

■ **کارایی در سیستم های مقیاس پذیر:**^{۱۴} شناسه یکتا یکی از ارکان اصلی در سیستم های کلان داده^{۱۵} است، جایی که حجم عظیمی از داده ها باید به صورت موازی پردازش و مدیریت شوند. در سیستم هایی نظیر Hadoop یا Apache Kafka، تخصیص شناسه یکتا به تراکنش ها پیش نیاز اجرای بسیاری از قابلیت های پردازش موازی و توزیع شده است. این شناسه ها از بروز تعارض در

1. Data Integrity

2. Relational Database Management System (RDMS)

3. Uniqueness Constraint

4. Optimization of Search

5. Indexing

6. Queries

7. Distributed Data Management

8. Synchronization

9. Unique Generation Algorithms

10. Globally Unique

11. Locally Unique

12. Referential Integrity

13. Foreign Key

14. Efficiency in Scalable Systems

15. Big Data

پردازش هم‌زمان داده‌ها جلوگیری کرده و امکان پردازش موازی در نودهای متعدد را فراهم می‌آورند. بدون شناسه یکتا، امکان ایجاد رکوردهای هم‌نام، خطا در انبارش داده یا شکست در تحلیل‌های تراکنشی وجود دارد.

شکل ۳. مزایای تخصیص شناسه یکتا از منظر مهندسی پایگاه داده



مأخذ: همان.

۲. مقابله با جعل و کلاهبرداری: شناسه یکتای تراکنش، چون به صورت رمزنگاری شده تولید و ثبت می‌شود، می‌تواند مانع از دسترسی غیرمجاز به اطلاعات تراکنش، تغییر و جعل این اطلاعات گردد. بدین صورت افرادی که انگیزه کلاهبرداری دارند، نمی‌توانند از شناسه تراکنش سوءاستفاده کنند. از سوی دیگر، تحلیل اطلاعات تراکنش و شناسایی الگوهای غیرمعمول یا مشکوک، می‌تواند به نهادهای نظارتی کمک کند تا پیش از وقوع کلاهبرداری یا بلافاصله بعد از کلاهبرداری، هشدار در یافت کنند و اقدامات لازم نظیر ممانعت از انجام تراکنش را انجام دهند.

۳. استعلام یکپارچه آنلاین: برای اطمینان از صحت و موفقیت‌آمیز بودن هر تراکنش بانکی، ضروری است که تراکنش دارای یک شناسه یکتا و قابل بررسی باشد. اگر مشتریان بانکی بتوانند به صورت لحظه‌ای وضعیت تراکنش‌های خود را از طریق سامانه استعلام تراکنش‌ها بررسی نمایند، چندین مزیت کلیدی حاصل می‌شود:

■ **رصد وضعیت تراکنش:** طرفین تراکنش قادر خواهند بود لحظه‌به‌لحظه وضعیت تراکنش خود را مشاهده نمایند و از انجام موفقیت‌آمیز آن مطمئن شوند. این امر می‌تواند حس اطمینان و آرامش بیشتری به مشتریان بانک بدهد.

■ **اطمینان فروشنده از انجام تراکنش:** فروشنده محصول یا ارائه‌دهنده خدمت، حتی پیش از اینکه فرایند تسویه حساب بین بانک‌ها کامل شده و پول به حساب وی واریز شود، می‌تواند از طریق این شناسه یکتا مطمئن شود که تراکنش انجام شده است. این قابلیت کارایی فرایند فروش را افزایش خواهد داد.

■ **تسهیل مبادلات اقتصادی:** چنین سیستمی می‌تواند فرایند مبادله کالا و خدمات را در فضای واقعی اقتصادی بسیار ساده‌تر و روان‌تر کند، زیرا اطمینان به تراکنش‌ها بهبود می‌یابد و خطرات ناشی از تأخیر یا اشتباه در تراکنش‌ها کاهش می‌یابد. ایده اصلی این است که شفافیت و قابلیت نظارت لحظه‌ای بر تراکنش‌های بانکی نه تنها برای مشتریان بانکی مفید است، بلکه بهره‌وری فرایند مبادلات کسب‌وکارها را افزایش خواهد داد.

۵. تجربه جهانی در تخصیص شناسه یکتای تراکنش



منطق فرایندی تخصیص شناسه یکتا تراکنش به صورت کلی به این صورت است که بانک مبدأ معمولاً مسئولیت تخصیص شناسه تراکنش را برعهده دارد و مقام ناظر بانکی (مثلاً بانک مرکزی) مسئول تدوین استانداردها و نظارت بر اجرای صحیح این فرایند است. البته فرایند تخصیص شناسه به تراکنش‌ها در کشورهای مختلف تفاوت‌هایی هم دارند، مثلاً یکی از این تفاوت‌ها در زمان نظارت مقام ناظر است که به صورت لحظه‌ای انجام گیرد و یا به شکل پسینی (روزانه، هفتگی، ماهانه و یا سالانه) صورت پذیرد. در ادامه، دو نمونه از تجربه‌های موجود در فرایند تخصیص شناسه یکتا به تراکنش‌ها مورد بررسی قرار می‌گیرد. دلیل انتخاب این کشورها دسترسی به اسناد پیاده‌سازی بوده است. برخی دیگر از کشورها نیز در حال پیاده سازی استاندارد ISO 20022 هستند و نقشه راه گذار به این استاندارد را تنظیم کرده‌اند، اما به دلیل عدم پیاده‌سازی کامل و یا عدم انتشار اسناد مثبته کافی در فضای اینترنت این گزارش به دیگر کشورها نپرداخته است.

۵-۱. هند

در کشور هند، شناسه یکتا به تمام تراکنش‌ها مانند پرداخت آنلاین و تراکنش از طریق کارت اعتباری اختصاص داده می‌شود. این شناسه برای انتقال‌دهنده و انتقال‌گیرنده وجوه به عنوان مدرکی دال بر اثبات انجام تراکنش است و از آن برای تطبیق مبلغ، پیگیری

وضعیت و کنترل فرایند تسویه استفاده می‌شود. در این کشور، دو مورد از مهم‌ترین ابزارهای پرداخت عبارت‌اند از:

- انتقال وجوه الکترونیکی ملی،^۱
- تسویه ناخالص آنی.^۲

فرایند تسویه در این دو سامانه متفاوت است؛^۳ اما در هر دو، بانک عامل مکلف است در لحظه صدور دستور پرداخت، شناسه‌ای یکتا تولید و به تراکنش تخصیص دهد. قالب این شناسه در سامانه تسویه ناخالص آنی معمولاً ۲۲ کاراکتری و در سامانه انتقال وجه الکترونیکی ملی ۱۶ کاراکتری است. بانک مرکزی هند^۴ طبق ماده (۱۰) فصل چهارم قانون نظام‌های پرداخت و تسویه مصوب ۲۰۰۷، اختیار تعیین و نظارت بر «شیوه و فرمت دستورهای پرداخت، نحوه انتقال وجه در نظام پرداخت و سایر استانداردهای لازم» را دارد [۵]. در کشور هند، به‌منظور تولید شناسه برای هر دو ابزار پرداخت انتقال وجوه الکترونیکی ملی و تسویه ناخالص آنی، از شناسه مرجع یکتای تراکنش^۵ استفاده می‌شود. برای هر کدام از این ابزارها یک شناسه مرجع یکتای تراکنش متناسب با روش تراکنش توسط بانک‌های هند صادر خواهد شد. این شناسه به‌عنوان یک ابزار مفید برای ردیابی وضعیت تراکنش‌ها عمل می‌کند. در تولید شناسه مرجع یکتای تراکنش، بانک‌ها باید یکتایی شماره سری در یک روز خاص را رعایت کنند. شناسه به‌صورت تصادفی ایجاد می‌شود، اما تاریخ و کانال تراکنش، در شناسه مشخص است [۶].

لازم به ذکر است که ۴ کاراکتر ابتدایی الگوی شناسه مرجع یکتای تراکنش در هر دو روش انتقال وجوه الکترونیکی ملی و تسویه ناخالص آنی، نشان‌دهنده کد بانک براساس کد سیستم مالی هند^۶ است. برای مثال در شکل ۴ کد سیستم مالی هند متعلق به بخش ۱۷ شعبه چاندیگار بانک مرکزی هند نمایش داده شده است:

1. National Electronic Funds Transfer (NEFT)

2. Real-Time Gross Settlement (RTGS)

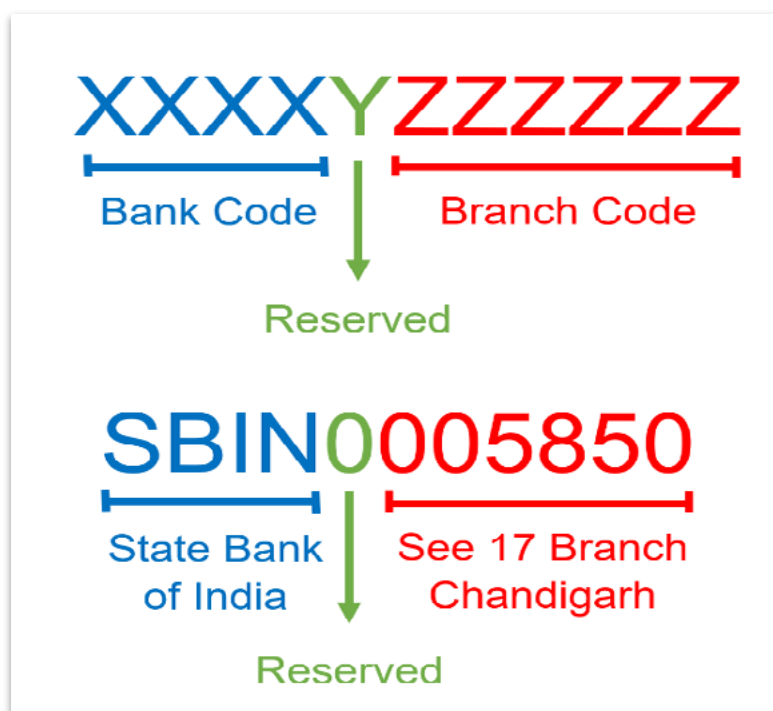
۳. تسویه ناخالص آنی به این معنی است که مبلغ به‌صورت آنی بین دو بانک منتقل و تسویه هم به روش لحظه‌ای انجام می‌شود که معادل آن در ایران ابزار پرداخت «ساتنا» است. اما در مقابل، پرداخت از طریق NEFT به‌صورت لحظه‌ای انجام نمی‌شود و تسویه آن به شکل خالص خواهد بود.

4. Reserve Bank of India

5. Unique Transaction Reference (UTR)

6. Indian Financial System Code (IFSC)

شکل ۴. نمایش کد سیستم مالی هند در الگوی شناسه مرجع یکتای تراکنش [۶]



کاراکترهای شناسه مرجع یکتای تراکنش با توجه به نوع ابزار تراکنش، ۱۶ یا ۲۲ کاراکتر هستند. در ادامه، الگوی کاراکترهای هر دو ابزار پرداخت بررسی می‌شود.

الگوی شناسه مرجع یکتای تراکنش برای پرداخت‌های انتقال وجوه الکترونیکی ملی دارای ۱۶ کاراکتر است:

- چهار کاراکتر اول از کد سیستم مالی هند استفاده می‌کند و نام بانک صادرکننده تراکنش را نشان می‌دهد.^۱
- کاراکتر پنجم نشان‌دهنده شماره سرور بانک مرکزی در بانک انجام‌دهنده تراکنش است. این کاراکتر می‌تواند یک حرف یا یک عدد باشد.

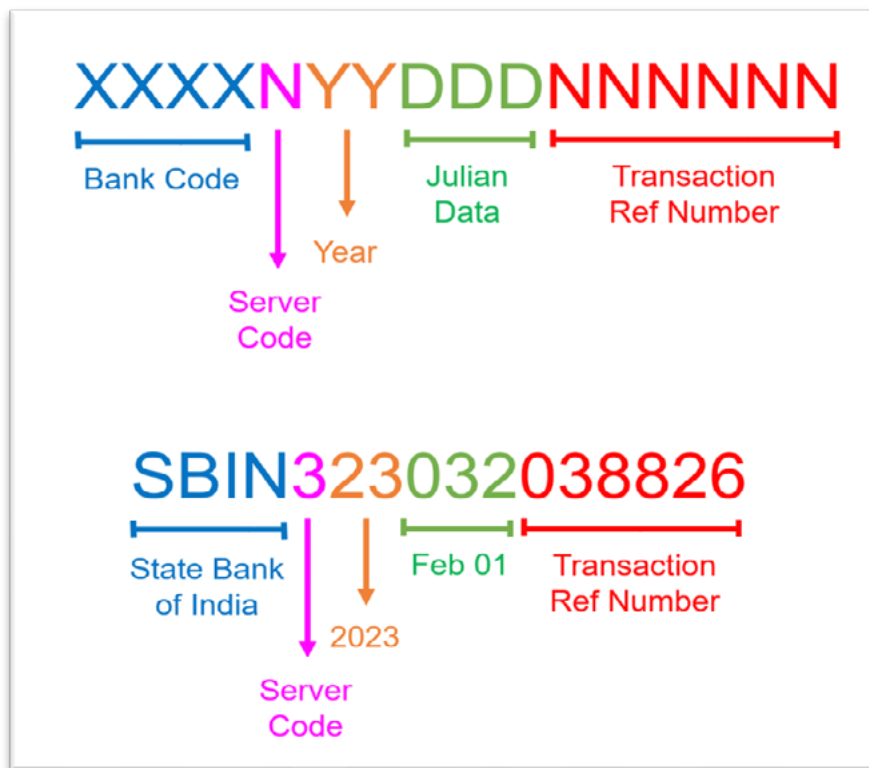
• کاراکتر ششم و هفتم شناسه مرجع یکتای تراکنش نشان‌دهنده دو رقم آخر سال میلادی و کاراکترهای هشتم تا دهم بیانگر تاریخ تراکنش به صورت عدد جولانی (یعنی روز متوالی سال از ۱۰۰ تا ۳۶۵ یا ۳۶۶ در سال کبیسه) هستند. اگرچه سامانه انتقال وجوه الکترونیکی ملی مختص پرداخت‌های داخلی در هند است، اما روش ثبت تاریخ در شناسه مرجع یکتای تراکنش براساس استاندارد جهانی تقویم جولانی انجام می‌شود.

- ۶ کاراکتر پایانی نشان‌دهنده شماره مرجع تراکنش است. بانک‌ها باید از یکتایی شماره مرجع برای هر تراکنش انتقال وجوه الکترونیکی ملی در هر روز اطمینان حاصل نمایند [۶].

در شکل ۵ نمونه‌ای از الگوی شناسه مرجع تراکنش برای پرداخت‌های انتقال وجوه الکترونیکی ملی نمایش داده شده است:

۱. (IFSC): یک کد ۱۱ کاراکتری الفبایی-عددی است که توسط بانک مرکزی هند برای شناسایی منحصر به فرد هر شعبه بانک در هند استفاده می‌شود. در شناسه مرجع یکتای تراکنش فقط ۴ کاراکتر اول این کد به کار می‌رود و بانک مبدأ (صادرکننده دستور پرداخت) را مشخص می‌کند.

شکل ۵. الگوی شناسه مرجع تراکنش برای پرداخت‌های انتقال وجوه الکترونیکی ملی [۶]

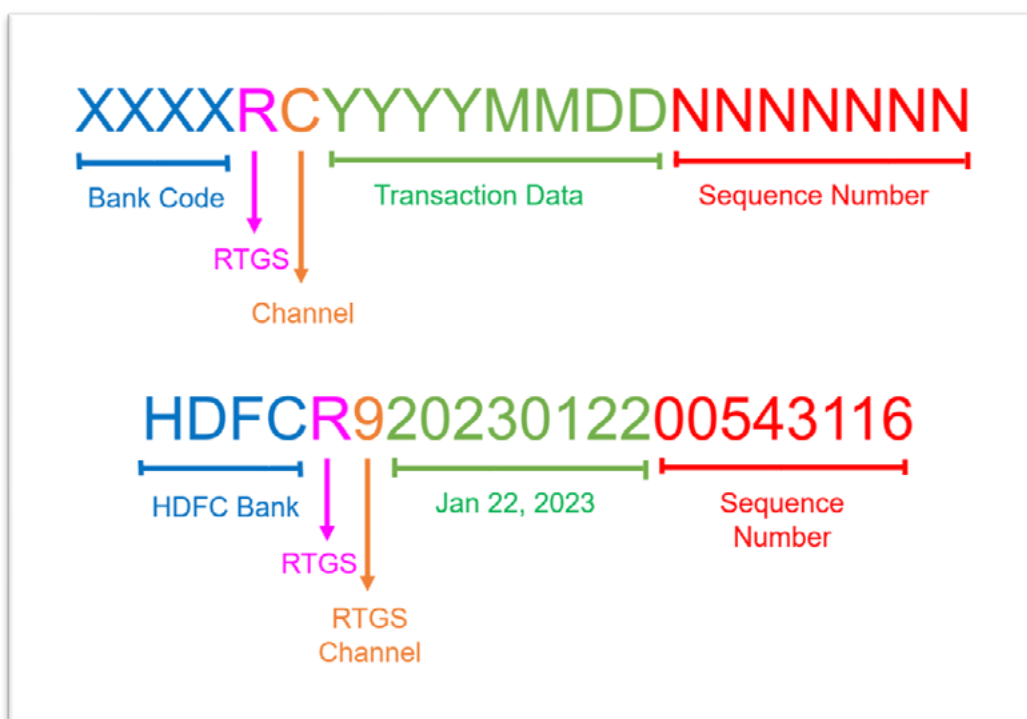


الگوی شناسه مرجع یکتای تراکنش برای پرداخت‌های تسویه ناخالص آنی دارای ۲۲ کاراکتر است:

- چهار کاراکتر اول، مشابه حالت قبل از کد سیستم مالی هند استفاده می‌کند و نام بانک صادرکننده تراکنش را نشان می‌دهد.
- کاراکتر پنجم، همیشه R است و نشان می‌دهد که این تراکنش توسط سیستم تسویه ناخالص آنی پردازش شده است.
- کاراکتر ششم نشان‌دهنده کانال تراکنش است. برای تراکنش‌های تسویه ناخالص آنی این کاراکتر همواره برابر (۹) است.
- کاراکتر هفتم تا چهاردهم به ترتیب سال، ماه و روز تراکنش را نشان می‌دهد. تراکنش‌های تسویه ناخالص آنی تحت استاندارد ISO 20022 تعریف شده است. لذا تاریخ تولید شده در شناسه مرجع یکتای تراکنش برای این تراکنش با تاریخ میلادی گزارش می‌شود.
- ۶ کاراکتر پایانی نشان‌دهنده شماره مرجع تراکنش است. بانک‌ها باید از یکتایی شماره مرجع برای هر تراکنش تسویه ناخالص آنی در هر روز اطمینان حاصل نمایند [۶].

در نمونه‌ای از الگوی شناسه مرجع یکتای تراکنش برای پرداخت‌های تسویه ناخالص آنی نمایش داده شده است:

شکل ۶. الگوی شناسه مرجع یکتای تراکنش برای پرداخت‌های تسویه ناخالص آنی [۶]

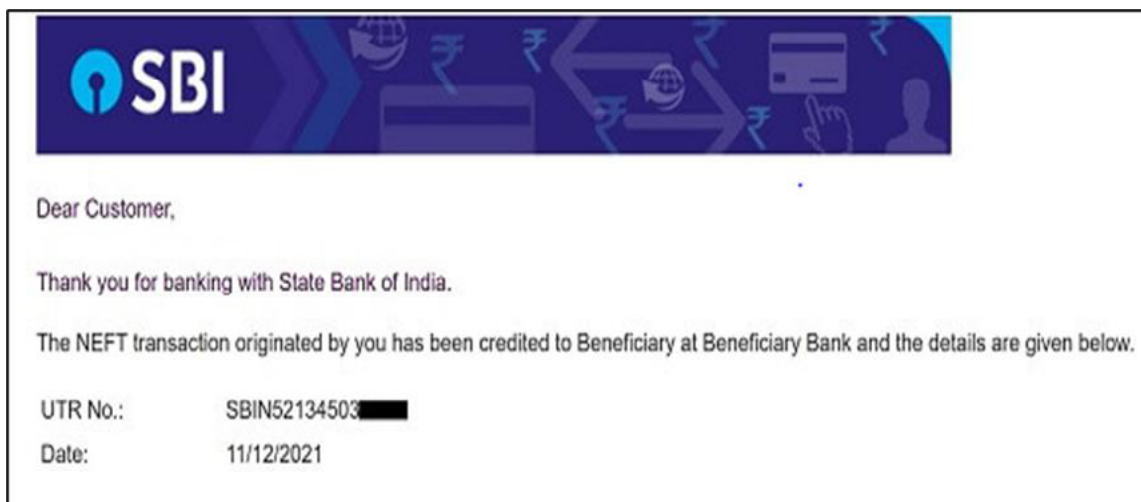


در این مثال، شناسه مرجع یکتای تراکنش نشان داده شده در شکل ۶ نشان می‌دهد که این تراکنش توسط بانک HDFC و توسط سیستم تسویه ناخالص آنی در تاریخ ۲۲ ژانویه ۲۰۲۳ انجام شده است. همچنین ۰۰۵۴۳۱۱۶ شماره ترتیبی است که برای هر تراکنش، پیام یا عملیات به صورت ترتیبی و افزایشی اختصاص می‌یابد تا امکان تمایز، ردیابی و کنترل دقیق ترتیب وقایع فراهم شود [۶].

بانک ایالتی هند^۱ مشتریان خود را از اطلاعات تراکنش‌ها و شناسه مرجع یکتای تراکنش از طریق ایمیل مطلع می‌کند. این نمونه در شکل زیر آورده شده است. علاوه بر آن، شناسه مرجع یکتای تراکنش در صورت حساب بانک قید می‌شود. این صورت حساب بانک هم از طریق حضوری و هم از طریق اپلیکیشن موبایل و اینترنت بانک قابل دسترسی است. اشتراک‌گذاری مرجع یکتای تراکنش بلامانع است، زیرا حاوی هیچ‌گونه اطلاعات با اهمیت و حساسی از اشخاص یا حساب بانکی نیست [۶].

1. State Bank of India (SBI)

شکل ۷. اطلاع‌رسانی اطلاعات تراکنش به همراه مرجع یکتای تراکنش [۶]



۲-۵. اتحادیه اروپا

در کشورهای اتحادیه اروپا^۱ از نظام پرداخت تارگت^۲ برای تسهیل پرداخت‌ها و تسویه حساب‌های بین‌المللی استفاده می‌شود. نظام پرداخت تارگت، با پیوند دادن ساختارهای مختلف نظام پرداخت ملی کشورهای حوزه یورو ایجاد شد، زیرا زمان کافی برای توسعه یک سیستم یکپارچه وجود نداشت. با این حال، این ساختار غیرمتمرکز در بلندمدت ناکارآمد و پرهزینه بود. از همین رو، سامانه تارگت^۳ که یک بازطراحی از سامانه تارگت بود، به‌طور کامل جایگزین آن گردید تا خدمات اصلی را به‌صورت متمرکز و یکپارچه بر روی یک پلتفرم واحد ارائه دهد [۷]. فرایند تخصیص شناسه با نظارت بانک مرکزی اروپا توسط بانک مبدأ مطابق با استاندارد سامانه تارگت^۴ انجام می‌شود، چراکه بانک مرکزی اروپا، وظیفه پایداری سامانه تارگت^۵ را برعهده دارد. پس از فرایند تخصیص شناسه تراکنش، شناسنامه یا رسید تراکنش ایجاد می‌شود که حاوی تمام اطلاعات تراکنش نظیر شناسه مرجع تراکنش^۶ و شناسه مرجع یکتای آنها به انتهای تراکنش^۷ است و نمونه‌ای از آن در شکل ۸ مشاهده می‌شود [۸]:

۱. این کشورها عبارت‌اند از: اتریش، بلژیک، قبرس، فرانسه، بلغارستان، آلمان، رومانی، اسلواکی، ایتالیا، اسپانیا، مجارستان، سوئد، دانمارک، فنلاند، هلند، پرتغال، مالت، ایرلند، چک، کرواسی، لتونی، یونان، لهستان، اسلونی، استونی، لوکزامبورگ و لیتوانی.

2. Target

3. Target2

4. Transaction Reference Number

5. Unique End-to-End Transaction Reference (UETR)

شکل ۸. شناسنامه (رسید) تراکنش در تارگت ۲ [۸]



ISPRINTANO: ZA: HBBAMEPGAXXX

Naziv poruke: Single Customer Credit Transfer

Tip poruke: 103

Smijer: Input

Prioritet: Normal

Sjednica: 6597

Redoslijed: 000001

Prima: RZBAATWWXXXX

RAIFFEISEN BANK INTERNATIONAL AG

VIENNA

Nal: BROJ PORUKE: 202211021

MIR: 221102RZBAATWWXXXX6597000001

MOR: Ulazno vrijeme Izlazno vrijeme ACK Flag NAK Code PDE Flag AUTH Code

MUR: 0163 1517

1: MESSAGE HEADER F01HBBAMEPGAXXX6597000001

2: APPLICATION HEADER I103RZBAATWWXXXXN

3: USER HEADER

:108: 0163

:121: da35a802-0593-4e47-8fd3-00

4: MESSAGE TEXT

:20: Transaction Reference Nubmer 0310023221

:23B: Identification of the Transaction CRED

:32A: Amount 221102 EUR 5220.00

UETR

TRN

در کشورهای اتحادیه اروپا همان طور که ذکر شد از نظام پرداخت تارگت و تارگت ۲ برای تسهیل پرداخت ها و تسویه حساب های بین المللی استفاده می شود. هر کدام از این دو نظام پرداخت به تمام تراکنش ها، شناسه یکتا تخصیص می دهند، اما از روش های متفاوتی برای تولید شناسه یکتا استفاده می کنند.

نظام پرداخت تارگت برای صدور شناسه تراکنش از شناسه مرجع تراکنش^۱ در چارچوب استاندارد سوئیفت^۲ استفاده می کند و تضمین می نماید که شناسه مرجع تراکنش صادر شده از سمت بانک مبدأ به بانک مقصد ارسال شود. شناسه مرجع تراکنش، یک شناسه یکتای ۱۶ کاراکتری است که مسئولیت صدور آن با بانک صادرکننده تراکنش است. کاراکترهای مجاز برای ساخت شماره مرجع تراکنش توسط سوئیفت اعلام شده است، اما الگوریتم منحصر به فردی برای تولید شناسه مرجع تراکنش وجود ندارد و هر مؤسسه مالی و اعتباری مطابق پروتکل داخلی خود اقدام به تولید شناسه یکتا می کند.

با معرفی سامانه تارگت ۲، ارتقای قابل توجهی در سرعت و دقت تراکنش ها ایجاد گردید. برنامه ریزی ها برای شناسه تراکنش سامانه تارگت ۲ به این شکل بود که استفاده از شناسه مرجع تراکنش در آن کنار گذاشته شود و فقط از شناسه مرجع یکتای انتها به انتهای تراکنش^۳ استفاده گردد، اما آنچه اجرایی شد، استفاده از هر دو شناسه به صورت هم زمان بود [۸].

۱. «شماره مرجع تراکنش» (TRN) یک شناسه کلیدی در نظام های پیام رسانی مالی سنتی، به ویژه در استانداردهای پیش از ISO 20022، محسوب می شود. این شناسه، که شاخص ترین نمونه آن فیلد ۲۰ (Field 20: Transaction Reference Number) در پیام های سری MT سوئیفت (مانند MT103) است، یک مرجع حداکثر ۱۶ کاراکتری است که توسط بانک ارسال کننده ایجاد می شود. فلسفه وجودی TRN، ایجاد یک شناسه منحصر به فرد برای یک گام خاص از زنجیره پرداخت، جهت ارجاع و پیگیری دو جانبه بین دو مؤسسه مالی مجاور است. مهم ترین ویژگی TRN، ماهیت «گام-به-گام» آن است، بدین معنا که این شناسه در هر مرحله از زنجیره پرداخت های واسطه ای تغییر می کند و یک شناسه سرتاسری محسوب نمی شود.

2. Swift

3. Unique End-to-End Transaction Reference

e4567-e89b-12d3-a456-426655440000123

جدول ۱. احتمال تکرار شناسه با توجه به تعداد شناسه تولیدی

احتمال تکرار شناسه	تعداد شناسه تولیدی
۰.۰۰۰۰'۰۰۰'۰۰۰'۰۰۰'۰۰۰'۰۰۰'۴	$۲^{۸۳۶}=۶۸'۷۱۹'۴۷۶'۷۳۶$
۰.۰۰۰۰'۰۰۰'۰۰۰'۰۰۰'۰۰۰'۰۰۰'۴	$۲^{۴۱}=۲'۱۹۹'۰۲۳'۲۵۵'۵۵۲$
۰.۰۰۰۰'۰۰۰'۰۰۰'۰۰۰'۴	$۲^{۴۶}=۷۰'۳۶۸'۷۴۴'۱۷۷'۶۶۴$

۲۶

به همین دلیل، برخلاف روش‌های دیگر، یکتایی شناسه یکتای جهانی به مرجع صادرکننده آن بستگی ندارد و نیازی به هماهنگی میان مرجع‌های مختلف نیست. بلکه هر شناسه تولید شده با این روش، به احتمال تقریباً ۱۰۰ درصد یکتا است. پنج نسخه برای تولید شناسه یکتای جهانی در استاندارد RFC 4122 تعریف شده است. شناسه مرجع یکتای انتها به انتهای تراکنش از نسخه ۴ این الگوریتم^۱ استفاده می‌کند [۱۱].

در گزارشی که سوئیفت در سال ۲۰۲۲ به منظور دستورالعمل پیاده‌سازی استاندارد MX منتشر کرده است،^۲ برای شناسه تراکنش، مجدداً شناسه مرجع یکتای انتها به انتهای تراکنش معرفی شده است. این مهم نشان می‌دهد که سوئیفت با وجود بازنگری در دیگر اجزای پروتکل، نیازی به تغییر برای بهبود عملکرد شناسه مرجع یکتای انتها به انتهای تراکنش ندیده و بار دیگر از مکانیسم پیگیری انتها به انتها برای صدور شناسه تراکنش استفاده کرده است [۱۲].

به منظور اعلام تراکنش، همان‌طور که در شکل ۹ مشهود است، هر فردی با استفاده از شناسه مرجع تراکنش یا شناسه مرجع یکتای انتها به انتهای تراکنش از طریق وبسایت سامانه رهگیری تراکنش سوئیفت و با اطلاعات بیشتری از تراکنش، شامل تاریخ پرداخت، مبلغ تراکنش و ارز مورد استفاده در تراکنش می‌تواند صحت تراکنش را اعلام نماید. این امر نشان می‌دهد که پایگاه اطلاعات تراکنش متمرکزی ذیل سوئیفت وجود دارد. همان‌گونه که پیشتر اشاره شد، تنها در اختیار داشتن شناسه تراکنش برای دریافت اعلام یک تراکنش کافی نیست [۱۳].

شکل ۹. اعلام تراکنش در پرداخت‌های سوئیفت [۱۳]

Track Your SWIFT Payment
GPI Tracker For Cross-Border Money Transfers

UETR (field 121) ?

Reference # (field 20) ?

Date of Payment

Amount

Sender's Currency (3 letters code)

Track →

1. Random-Based UUID

2. SWIFT Message Type Based on ISO 20022 XML Standard

۶. ملاحظات مرتبط با حفاظت و اشتراک‌گذاری داده‌های بانکی

تولید و جمع‌آوری اطلاعات تراکنش، علاوه بر مزایایی که درخصوص نظارت بانک مرکزی بر خلق پول، جریان پول و محو پول خواهد داشت، می‌تواند برای سایر نهادها نیز مؤثر باشد. با این حال، اشتراک‌گذاری اطلاعات تراکنش مستلزم توجه به اصول رازداری بانکی است، به این معنا که هرگونه بهره‌برداری یا تبادل این داده‌ها باید در چارچوب الزامات حقوقی و با رعایت محرمانگی اطلاعات مشتریان صورت گیرد.

رازداری بانکی اصل حقوقی پذیرفته شده‌ای است که به موجب آن، بانک‌ها و مؤسسات اعتباری موظف‌اند تمام اطلاعات مربوط به مشتریان را محرمانه در نظر گرفته و از ارائه این اطلاعات به اشخاص ثالث امتناع ورزند. برای نمونه، پرونده مشهور تورنیر^۱ انگلستان در سال ۱۹۲۸، محرمانگی بانکی را محدود به میزان دارایی‌های فرد در حساب بانکی او ندانسته و هر نوع اطلاعات را جزء محرمانگی بانکی قلمداد کرده است. در این پرونده، بانک برای کارفرمای یکی از مشتریان خود واقعیتی را فاش کرد که در نتیجه این افشا، کارفرمای مشتری قرارداد خود را با مشتری تمدید نکرد. دادگاه اعلام کرد که محرمانگی و رازداری یک اصطلاح ضمنی در قرارداد مشتری است و هرگونه نقض آن می‌تواند موجب مسئولیت خسارت مشتری گردد. البته در مواردی که قانون، وظیفه عمومی، منافع بانک یا زمانی که مشتری به‌طور ضمنی به افشا رضایت داده باشد، این محرمانگی می‌تواند نقض شود [۱۴].

یکی از مهم‌ترین نهادهایی که می‌تواند از پایگاه اطلاعات تراکنش‌ها بهره‌برداری کند، نهاد مبارزه با پول‌شویی است. کنوانسیون وین که در تاریخ ۲۰ دسامبر ۱۹۸۸ به تصویب رسید و از ۱۱ نوامبر ۱۹۹۰ لازم‌الاجرا شد، نخستین سند الزام‌آور بین‌المللی در زمینه پول‌شویی است که کشورهای عضو سازمان ملل را ملزم کرد که پول‌شویی را جرم‌انگاری کنند و زیرساخت‌های قضایی لازم را برای ردیابی و مصادره دارایی‌های ناشی از جرائم مواد مخدر فراهم آورند [۱۵].

در سال ۱۹۸۹، گروه هفت برای هماهنگ‌سازی سیاست‌های مقابله با پول‌شویی در سطح جهان گروه ویژه اقدام مالی^۲ را به‌عنوان یک نهاد تخصصی و توصیه‌محور تأسیس کرد. گروه ویژه اقدام مالی موظف به تدوین استانداردها و «توصیه‌های اجرایی» برای کشورهای عضو در راستای پیاده‌سازی مؤثر تعهدات ناشی از کنوانسیون‌های بین‌المللی شد. گروه ویژه اقدام مالی در آوریل ۱۹۹۰ مجموعه اولیه ۴۰ توصیه خود را منتشر کرد، سپس این مجموعه به‌ترتیب در سال‌های ۱۹۹۶، ۲۰۰۳ و ۲۰۱۲ مورد بازبینی ساختاری قرار گرفت؛ بازنگری ۲۰۱۲، توصیه‌های ویژه تأمین مالی تروریسم را به‌طور رسمی در متن ۴۰ توصیه ادغام و مفاهیمی جدید از قبیل رمزارز، مالکیت واقعی و تأمین مالی تسلیحات هسته‌ای را دربرگرفت. در میان توصیه‌های گروه ویژه اقدام مالی، توصیه ۱۳ (گزارش تراکنش‌های مشکوک) به‌صراحت تأکید می‌کند که مؤسسات مالی باید تمامی تراکنش‌های مشکوک را حتی بدون توجه به میزان مبلغ گزارش بدهند [۱۶]. تصویب این توصیه‌ها توسط قانونگذاران در سراسر جهان و توصیه‌های بعدی در مورد اقدامات مربوط به گزارش تراکنش‌های مشکوک، مقابله با تأمین مالی تروریسم، اجتناب از تحریم‌ها و مبارزه با فساد و فرار مالیاتی، منجر به تغییر بنیادین مفهوم رازداری بانکی شده است.

با این حال، از دهه ۱۹۷۰ میلادی، با تصویب و گسترش قوانین حریم خصوصی داده‌ها^۳ که از آن با تعبیری همچون حفاظت از داده‌ها^۴ و حریم خصوصی اطلاعات^۵ نیز یاد می‌شود، بانک‌ها با مجموعه‌ای از تعهدات جدید روبه‌رو شدند. این تعهدات، تفاوت‌های قابل توجهی

1. Tournier

2. FATF

3. Data Privacy

4. Data Protection

5. Information Privacy

با وظایف سنتی بانک‌ها در قبال مشتریان داشت. استثنائات در قوانین حفظ حریم خصوصی داده‌ها معمولاً زمانی برای بانک‌ها اعمال می‌شود که این اطلاعات برای اهداف قانونی یا حفظ منابع مالی مورد نیاز باشند. به‌عنوان مثال، در مواردی مانند مبارزه با پول‌شویی، مقابله با فرار مالیاتی یا تأمین مالی تروریسم، بانک‌ها ممکن است مجبور شوند برخی از الزامات حفظ حریم خصوصی داده‌ها را نادیده بگیرند. در این موارد، قوانین خاصی وجود دارد که به بانک‌ها اجازه می‌دهد اطلاعات را در راستای اهداف قانونی و امنیتی، حتی اگر با اصول حریم خصوصی داده‌ها مغایرت داشته باشد، در اختیار مراجع ذی‌صلاح قرار دهند.

بیش از پنجاه سال پیش، سوئد در سال ۱۹۷۳ نخستین قانون ملی حفاظت از داده‌های شخصی در جهان را تصویب کرد. تا آوریل ۲۰۲۵، براساس تحلیل جامع گراهام گرین‌لیف^۱ در ویرایش جدید اثر خود با عنوان «قوانین جهانی حفاظت از داده‌ها ۲۰۲۵»، ۱۷۲ کشور جهان دارای چارچوب قانونی برای حفاظت از داده‌های شخصی بوده‌اند. شایان ذکر است که این آمار، صرفاً نشان‌دهنده تعداد کشورهایی است که چارچوب قانونی مصوب دارند و لزوماً به‌معنای اجرای کامل، اثربخشی یا پوشش سراسری این قوانین نیست؛ چراکه در برخی کشورها ممکن است اجرای قانون به تعویق افتاده یا با محدودیت‌های اجرایی و نظارتی مواجه باشد [۱۷]. حقیقتی که از تحلیل رشد این قوانین در طول زمان استنباط می‌شود این است که قوانین حفظ حریم خصوصی داده‌ها در سطح جهانی در حال گسترش هستند و تعداد و تنوع جغرافیایی آنها به خصوص در قرن ۲۱ افزایش یافته است. براساس دستورالعمل سیاستی غیرالزام‌آور سازمان توسعه و همکاری اقتصادی^۲ با عنوان «راهنمای حاکم بر حفاظت از حریم خصوصی و جریان برون‌مرزی داده‌های شخصی»^۳ مصوب سال ۱۹۸۰، هشت اصل بنیادین حفاظت از داده‌های شخصی به‌شرح زیر تبیین شده است:

۱ محدودیت جمع‌آوری:^۴ جمع‌آوری داده‌های شخصی باید محدود، از طریق شیوه‌های قانونی و منصفانه و در صورت اقتضا، با اطلاع یا رضایت شخص انجام شود.

۲ کیفیت داده:^۵ داده‌های شخصی باید مرتبط با اهداف مورد نظر، دقیق، کامل و تا حد امکان به‌روز نگهداری شوند.

۳ تعیین هدف:^۶ اهداف جمع‌آوری داده باید پیش از جمع‌آوری یا هم‌زمان با آن مشخص باشد و هر استفاده بعدی باید در راستای این اهداف یا اهداف سازگار با آن باشد.

۴ محدودیت استفاده:^۷ داده‌های شخصی نباید بدون رضایت شخص یا مجوز قانونی، برای اهدافی غیر از اهداف تعیین شده استفاده یا افشا شوند.^۸

۵ اصل امنیت داده:^۹ داده‌های شخصی باید در برابر مخاطراتی مانند دسترسی غیرمجاز، تخریب، استفاده یا افشای غیرمجاز با تدابیر امنیتی مناسب حفاظت شوند.

۶ اصل شفافیت:^{۱۰} باید درباره سیاست‌ها و اقدامات مربوط به داده‌های شخصی شفافیت وجود داشته باشد تا افراد بتوانند به‌راحتی از آنها آگاه شوند.

1. Graham Greenleaf
2. Global Data Privacy Laws 2025
3. OECD
4. Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data
5. Collection Limitation Principle
6. Data Quality
7. Purpose Specification
8. Use Limitation
9. Uses and Disclosures Limited to Purposes Specified or Compatible
10. Security Safeguards
11. Openness

۷ **حق دسترسی فرد:**^۱ هر فرد باید بتواند از وجود داده‌های مربوط به خود مطلع شود و در صورت لزوم، به آنها دسترسی یافته، آنها را تصحیح یا حذف کند.

۸ **مسئولیت‌پذیری:**^۲ مسئولیت رعایت اصول فوق برعهده داده‌پرداز است و او باید توان اثبات پایبندی به این اصول را داشته باشد [۱۸].

در همین راستا، کنوانسیون شماره ۱۰۸ شورای اروپا با عنوان کامل «کنوانسیون حفاظت از افراد در ارتباط با پردازش خودکار داده‌های شخصی»^۳ که در ۲۸ ژانویه ۱۹۸۱ به امضای کشورهای عضو رسید، نخستین سند بین‌المللی الزام‌آور در زمینه حفاظت داده‌های شخصی در جهان به‌شمار می‌آید. این کنوانسیون، چارچوبی حقوقی برای تنظیم استانداردهای حداقلی در جمع‌آوری، نگهداری، پردازش و انتقال داده‌های شخصی فراهم آورده و بر تضمین حقوق اساسی افراد در برابر پردازش خودکار داده‌هایشان تأکید دارد. این سند، الهام‌بخش بسیاری از قوانین داخلی اروپا و دیگر مناطق جهان و حتی مبنای حقوقی برای تدوین اسناد بعدی مانند دستورالعمل‌های اتحادیه اروپا (Directive 95/46/EC) و مقررات عمومی حفاظت داده^۴ بوده است [۱۹].

استانداردهای یاد شده، به‌همراه فرایندهای عملیاتی روشن و سازوکارهای پشتیبان مدیریت داده، باید به‌عنوان پیوست‌های بنیادین در تدوین و اجرای قوانین مرتبط با حفظ حریم خصوصی داده‌ها در نظر گرفته شوند تا کارایی، انطباق و اثربخشی این مقررات تضمین شود. در همین راستا، در ادامه، نحوه دسترسی به اطلاعات بانکی و محدودیت‌ها و ملاحظات قانونی آن در نظام‌های حقوقی منتخب برخی از کشورها مورد بررسی قرار گرفته است.

۱-۶. هند

در هند، چارچوب حقوقی حفاظت از داده‌های شخصی با تصویب قانون حفاظت از داده‌های شخصی دیجیتال ۲۰۲۳^۵ شکل گرفته است. این قانون، اصل را بر ضرورت کسب رضایت و رعایت حقوق فرد می‌گذارد؛ اما در چند وضعیت مشخص، پردازش داده‌ها را بدون رضایت مجاز می‌شمارد. استثناهای اصلی در سه بخش قانون جای دارد: ماده (۷) «مصادیق استفاده مشروع»، ماده (۱۶) «انتقال برون‌مرزی» و ماده (۱۷) «موارد معافیت گسترده».

■ ماده (۷)، ۹ گروه از پردازش «بدون رضایت» را مشروع اعلام می‌کند. مهم‌ترین آنها عبارت‌اند از:

- اجرای وظایف حاکمیتی یا تکلیف قانونی - بندهای «۷(ج) و ۷(د)» اجازه می‌دهد که دولت یا دستگاه‌های آن برای اجرای هر قانون جاری هند، یا حفظ حاکمیت و امنیت ملی، داده‌ها را پردازش کند. نمونه رایج، مطالبه داده‌های بانکی برای تطبیق با مقررات مالیاتی است.
- عمل به حکم دادگاه یا تصمیم حقوقی - بند «۷(ه)» امکان استفاده از داده در اجرای احکام دادگاه‌های هند یا احکام مدنی صادره در خارج از کشور را فراهم می‌سازد.
- منافع حیاتی و شرایط اضطراری بهداشتی یا بلایای طبیعی - بندهای «۷(ف) تا ۷(ح)» تصریح می‌کند که هنگام تهدید جانی، شیوع بیماری، یا وقوع فاجعه، داده شخصی بدون طی تشریفات کسب رضایت از اشخاص قابل پردازش است

1. Individual Participation

2. Accountability

3. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)

4. GDPR

5. Digital Personal Data Protection Act 2023 – DPDP Act

■ انتقال برون‌مرزی داده تحت ماده (۱۶)

● هیئت‌وزیران می‌تواند فهرست کشورهایی را که از نگاه هند حفاظت کافی از داده‌ها دارند را منتشر کند. انتقال به کشورهایی خارج از فهرست مذکور ممنوع است؛ مگر در چارچوب استثنای ماده (۷) (مثلاً تهدید جانی).

■ معافیت‌های ماده (۱۷) - این ماده مقرر می‌کند که «حقوق داده‌موضوع و تعهدات متولی داده» (به‌جز امنیت داده) در شرایطی خاص تعلیق می‌شود، از جمله:

● پیشگیری، تحقیق یا پیگرد جرائم - مسئولان اجرای قانون می‌توانند بدون الزام به اطلاع‌رسانی یا اجازه قبلی، داده‌ها را جمع‌آوری و تحلیل کنند.

● اعمال یا دفاع از حق قانونی - هر شخص، برای اقامه دعوی یا دفاع از خود، مجاز به پردازش الزام‌آور خواهد بود.

● تحقیق و نوآوری - چنانچه پروژه پژوهشی با رمزنگاری، هویت‌زدایی و حداقل‌سازی انجام شود و منافع عمومی علمی را تأمین کند، می‌تواند از حدود برخی حقوق فردی مستثنا شود.

علاوه‌براین، بند «۱۷(۳)» به دولت اجازه می‌دهد با «آگهی رسمی» دسته‌های دیگری از پردازش را مشمول معافیت کند، مشروط بر آنکه دلیل آن را به صراحت بیان کند و اصل تناسب رعایت شود [۲۰].

در راستای ماده (۷) این قانون در کشور هند، چندین نهاد به داده‌های شبکه بانکی دسترسی دارند که شامل موارد زیر می‌شود:

۱ **بانک مرکزی هند:** به‌عنوان نهاد قانونگذار و بالاترین مقام نظارتی بر سیستم بانکی، با استفاده از اطلاعات تراکنش‌های شبکه بانکی تلاش می‌کند که از سلامت مالی نظام بانکی اطمینان حاصل کند.

۲ **اداره مالیات بر درآمد:**^۱ بر مبنای بند «۶» از ماده (۱۳۳) قانون مالیات بر درآمد^۲ هند، مأمور مالیاتی می‌تواند از هر شخص، از جمله بانک، هرگونه اطلاعات یا صورت‌حساب لازم را مطالبه کند [۲۱].

۳ **واحد اطلاعات مالی:**^۳ بر اساس بندهای «۱۲ و ۱۳» قانون مبارزه با پول‌شویی^۴ هند، به‌منظور شناسایی فعالیت‌های مشکوک و مبارزه با پول‌شویی، واحد اطلاعات مالی موظف به جمع‌آوری، نگهداری و تجزیه و تحلیل گزارش‌های تراکنش‌های نقدی، تراکنش‌های مشکوک، گزارش تراکنش‌های غیرنقدی، گزارش انتقال وجوه برون‌مرزی و گزارش اموال است [۲۲].

۴ **پلیس و نهادهای قضایی:** به استناد ماده (۹۱) قانون آیین دادرسی کیفری هند هر دادگاه یا افسر تحقیق می‌تواند، در جهت تکمیل تحقیقات پرونده «حضاریه ارائه اسناد» صادر کرده و بانک را ملزم به تحویل اطلاعات و صورت‌حساب‌های مدنظر کند. این دستور فقط پس از صدور حکم کتبی مقام قضایی معتبر است [۲۳].

۲-۶. اتحادیه اروپا

در کشورهای اتحادیه اروپا، مقررات عمومی حفاظت از داده‌ها یکی از جامع‌ترین و سخت‌گیرانه‌ترین قوانین حریم خصوصی در سطح جهان است که با هدف محافظت از داده‌های شخصی افراد و ایجاد تعادل میان حقوق فردی کاربران و نیازهای سازمان‌ها برای استفاده از داده‌ها وضع شده است. این قانون که به‌عنوان یک چارچوب حقوقی، مقررات مشخصی را برای جمع‌آوری، پردازش، ذخیره‌سازی و اشتراک‌گذاری داده‌های شخصی افراد تعیین می‌کند توسط اتحادیه اروپا در سال ۲۰۱۶ تصویب شد و از ۲۵ مه ۲۰۱۸ به اجرا درآمد. مقررات عمومی حفاظت از داده‌ها تأکید زیادی بر حفظ محرمانگی داده‌های شخصی دارد. تمام شرکت‌ها از جمله بانک‌ها ملزم هستند

1. Income Tax Department

2. The Income-Tax Act, 1961

3. Financial Intelligence Unit

4. Prevention of Money Laundering Act (PMLA)

از روش‌های رمزگذاری، دسترسی محدود و کنترل‌های امنیتی پیشرفته برای جلوگیری از دسترسی غیرمجاز به داده‌ها و اطلاعات استفاده نمایند. همچنین، دسترسی به داده‌ها به کشورهای خارج از اتحادیه اروپا تنها در صورتی مجاز است که استانداردهای مشابهی برای حفاظت از داده‌ها در آن کشورها اجرا شود. این قانون در موضوع محرمانگی داده شامل استثنائات زیر است:

۱ پردازش داده‌ها برای رعایت تعهدات قانونی مطابق جزء (c) بند اول ماده (۶): چنانچه یک مسئول براساس تعهد صریح در قانون ملی یا اروپایی ناگزیر به اقدام باشد، می‌تواند اطلاعات را برای اهداف مالیاتی، گزارش‌دهی به نهادهای نظارتی، یا اجرای تصمیمات قضایی پردازش کند [۲۴].

۲ پردازش داده‌ها برای منافع حیاتی افراد، منافع عمومی، منافع مشروع سازمان‌ها یا اشخاص ثالث مطابق اجزای (d)، (e) و (f) بند اول ماده (۶): اگر پردازش اطلاعات برای نجات جان فردی، اجرای مأموریت حاکمیتی یا تأمین منافع مشروع مسئول پردازش یا شخص ثالث ضرورت یابد و بر منافع و حقوق داده موضوع غلبه کند، انجام آن مجاز خواهد بود؛ در این حالت، انتقال بین‌المللی نیز مادامی که ضرورت همان منفعت اثبات شود بلامانع است [۲۴].

۳ امنیت ملی و اجرای قوانین مطابق ماده (۲۳): این ماده اجازه می‌دهد که یک دولت عضو، به‌وسیله قانون، حقوق و تعهدات مقرر در مقرر عمومی حفاظت از داده‌ها را به‌طور متناسب محدود کند تا از منافع بنیادینی مانند امنیت ملی، دفاع، امنیت عمومی، پیشگیری یا تعقیب جرم، اجرای مجازات، یا صیانت از استقلال قضایی پاسداری کند. به اتکای همین ماده، نهادهای امنیتی یا قضایی می‌توانند، تحت قانون خاص داخلی، به داده‌های بانکی یا هر داده حساس دیگر دسترسی یابند [۲۴].

۴ پردازش داده‌ها برای اهداف آزادی بیان، روزنامه‌نگاری، ادبی و هنری مطابق ماده (۸۵): اگر پردازش داده برای اعمال حق آزادی بیان یا نگارش گزارش خبری ضرورت پیدا کند، مقرر، کشورها را مکلف می‌کند میان حریم خصوصی و آزادی مطبوعات توازن برقرار کنند؛ به همین علت، خبرنگاران در چارچوب قوانین رسانه‌ای ملی، می‌توانند بدون اخذ رضایت صریح، داده‌های مورد نیاز را گردآوری کنند، مشروط بر آنکه اصول ضرورت و تناسب رعایت شود [۲۴].

۵ پردازش داده‌ها برای اهداف تحقیقاتی و آماری مطابق ماده (۸۹): اگر داده‌ها برای پژوهش در حوزه‌های علمی، آمار رسمی و ملی، تاریخی و بایگانی در راستای منافع ملی به‌گونه‌ای پردازش شود که منافع عمومی دانش یا آمار ملی را تأمین کند و سازوکارهایی مانند ناشناس‌سازی و حداقل‌سازی به‌کار گرفته شود، پردازش داده‌ها بلامانع است. کشورها باید اطمینان حاصل کنند که اقدامات فنی و سازمانی کافی برای جلوگیری از شناسایی مجدد اشخاص اتخاذ شده است [۲۴].

بانک مرکزی اروپا در چارچوب مأموریت نظارتی یوروسیستم بر سامانه‌های پرداخت کلیدی-ازجمله سامانه تسویه ناخالص آنی TARGET/T2 نظارت می‌کند. در سطح اتحادیه، دسترسی به داده‌های تراکنش، افزون بر نهادهای مقررات‌گذار بانکی، میان چند مقام تخصصی تقسیم شده است. نخست، «سازمان مقابله با پول‌شویی و تأمین مالی تروریسم اتحادیه اروپا»^۱ برپایه مقررات مصوب ۲۰۲۴ تأسیس و در فرانکفورت مستقر شده است. این نهاد وظیفه هماهنگی واحدهای اطلاعات مالی^۲ و نظارت مستقیم بر مؤسسات فرامرزی پرخطر را برعهده دارد و برای انجام مأموریت خود به داده‌های شناسنامه‌ای حساب‌ها و تراکنش‌ها دسترسی خواهد داشت [۲۵].

مطابق ماده (a32) دستورالعمل اتحادیه اروپا ۱۸/۲۰۴۳ (پنجمین اصلاحیه دستورالعمل مبارزه با پول‌شویی)، هر دولت عضو باید سامانه‌ای متمرکز ایجاد کند که امکان دسترسی «مستقیم، بی‌واسطه و بلادرنگ» واحدهای اطلاعات مالی به اطلاعات بانکی را فراهم کند [۲۶]. در حوزه مالیات، دستورالعمل 2258/2016 (DAC5) اتحادیه اروپا با اصلاح دستورالعمل ۱۱/۲۰۱۶/EU، دسترسی مراجع مالیاتی ملی به داده‌های احراز هویت مشتریانی را که مؤسسات مالی برپایه مقررات ضدپول‌شویی گردآوری می‌کنند الزامی کرده است؛ بدین ترتیب، مقامات مالیاتی می‌توانند برای کشف تقلب و فرار مالیاتی، اطلاعات تراکنش‌ها را به‌طور قانونی بازیابی نمایند [۲۷].

1. AMLA

2. FIU



۷. طراحی الگوی مطلوب جهت تخصیص شناسه یکتا به تراکنش‌های بانکی

در ایران، هر بانک طبق الگوریتم داخلی خود به هر تراکنشی که انجام می‌دهد، شناسه اختصاص خواهد داد. اما با توجه به اهمیت این اطلاعات و لزوم نظارت به تراکنش‌ها لازم است که تمامی نهادهایی که شناسه تخصیص می‌دهند، با یک الگوریتم یکسان این کار را انجام دهند تا نظارت و ثبت آن اطلاعات بهتر انجام گیرد. باید توجه کرد که اقدامات مرتبط با داده‌های بزرگ نظیر الگوریتم‌های جست‌وجو، کشف الگوهای مشکوک، یادگیری ماشین و ... مستلزم این است که داده‌های تمیز و باکیفیت در پایگاه داده ثبت شده باشد. به همین دلیل لازم است یک الگوی مطلوب جهت تولید و تخصیص شناسه تراکنش طراحی شود. در ادامه به نحوه تولید و تخصیص شناسه و طراحی مطلوب شناسنامه تراکنش پرداخته می‌شود، به‌طوری که تمام شناسه‌ها در پایگاه اطلاعات تراکنش بتوانند به شکل واحد و با کمترین هزینه ثبت شده و قابل استفاده باشند.^۱

۷-۱. فرایند تخصیص شناسه تراکنش

در این بخش، فرایند پیشنهادی تخصیص شناسه یکتا به تراکنش‌های بانکی توضیح داده می‌شود. نکته اصلی در این مدل آن است که تولید و استفاده از شناسه یکتا نباید موجب توقف یا کند شدن مسیر عملیاتی پرداخت شود. بنابراین، بانک مرکزی صادرکننده متمرکز شناسه یا تأییدکننده برخط هر تراکنش در مسیر پرداخت نیست، بلکه الگوریتم تولید شناسه را ابلاغ می‌کند و از طریق دریافت رویدادهای نظارتی، امکان ثبت، پایش، صحت‌سنجی و تحلیل تراکنش‌ها را فراهم می‌سازد. بر این اساس، مدل پیشنهادی مبتنی بر تولید محلی شناسه و گزارش‌دهی موازی و ناهم‌زمان است. در این مدل، تراکنش از ریل‌های عملیاتی موجود پرداخت و تسویه عبور می‌کند و هم‌زمان، اطلاعات نظارتی آن برای بانک مرکزی ارسال می‌شود. به این ترتیب، بار اضافی به شبکه پرداخت تحمیل نمی‌شود و ثبت نظارتی بانک مرکزی نیز بدون دخالت در مسیر بحرانی پرداخت انجام می‌گیرد. فرایند پیشنهادی به شرح زیر است:

(الف) درخواست انجام تراکنش توسط مشتری از طریق مراجعه حضوری به شعبه، دستگاه کارت‌خوان، همراه‌بانک، اینترنت‌بانک، درگاه‌های پرداخت الکترونیکی به بانک مبدأ ارائه می‌شود.

(ب) بانک مبدأ، پیش از ارسال پیام تراکنش، شناسه یکتای تراکنش را به صورت محلی و مطابق الگوریتم ابلاغی بانک مرکزی تولید می‌کند. این شناسه از ابتدا به تراکنش الصاق می‌شود و در تمام مراحل بعدی، بدون تغییر، مبنای رهگیری، گزارش‌دهی و رفع مغایرت قرار می‌گیرد. در این طراحی، تولید شناسه متمرکز نیست و بانک آغازگر تراکنش مسئول تولید آن است.

(ج) بانک مبدأ پس از انجام کنترل‌های داخلی، از جمله کنترل موجودی، کنترل قواعد کسب‌وکار، کنترل سقف‌ها و کنترل‌های مبارزه با تقلب و پول‌شویی، پیام عملیاتی تراکنش را از طریق ریل پرداخت مربوطه به سوئیچ مدنظر ارسال می‌کند.

(د) هم‌زمان با ارسال پیام عملیاتی تراکنش، بانک مبدأ یک رویداد نظارتی حاوی شناسه یکتا و اقلام اطلاعاتی اصلی تراکنش را از طریق کانال گزارش‌دهی تعیین شده برای بانک مرکزی ارسال می‌کند. این ارسال موازی و غیرمسدودکننده است، به این معنا که عدم دریافت فوری پیام تأیید از بانک مرکزی مانع انجام تراکنش در مسیر عملیاتی نمی‌شود. برای اطمینان از اینکه اطلاعات نظارتی از بین نرود، بانک مبدأ باید از سازوکارهای تضمین تحویل استفاده کند. به این معنا که اگر در لحظه ارسال، ارتباط با کانال

۱. البته لازم به ذکر است که بانک مرکزی، زیرساختی برای تخصیص شناسه یکتا به تراکنش‌ها (شیوا) فراهم آورده است که البته تاکنون جزئیاتی از عملیاتی شدن آن در دست نیست.

گزارش‌دهی بانک مرکزی دچار اختلال شود، اطلاعات تراکنش در بانک مبدأ نگهداری شده و پس از رفع اختلال، مجدداً ارسال می‌شود. بنابراین، عدم ارسال موفق در لحظه، موجب توقف تراکنش نمی‌شود؛ اما مسئولیت ارسال و تکمیل گزارش نظارتی همچنان برعهده بانک مبدأ باقی می‌ماند.

ه) به‌روزرسانی مانده حساب‌ها مطابق سازوکار ریل پرداخت مورد استفاده انجام می‌شود، به‌نحوی که مانده حساب انتقال‌دهنده در بانک مبدأ کاهش یافته و مانده حساب دریافت‌کننده در بانک مقصد افزایش می‌یابد. در نتیجه نمایش پیام «تراکنش موفق» برای مشتری تابع نتیجه مسیر عملیاتی پرداخت است، نه تابع ثبت نظارتی آن در بانک مرکزی.

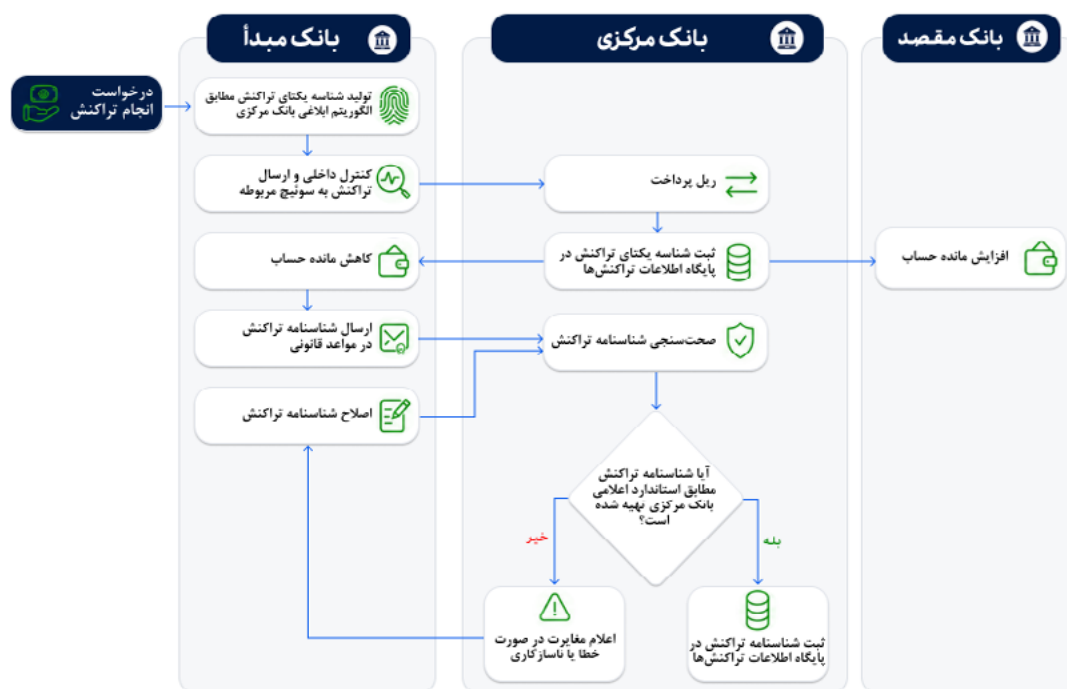
و) بانک مرکزی رویداد نظارتی دریافت شده را خارج از مسیر بحرانی پرداخت پردازش می‌کند. این پردازش می‌تواند شامل کنترل قالب شناسه، کنترل انطباق شناسه با الگوریتم ابلاغی، کنترل یکتایی شناسه، بررسی سازگاری اقلام اطلاعاتی تراکنش و ثبت در پایگاه اطلاعات تراکنش‌ها باشد.

ز) چنانچه بانک مرکزی در فرایند اعتبارسنجی یا ثبت نظارتی با مغایرتی مواجه شود، یک رویداد مغایرت شامل کد خطا، شرح مغایرت و شناسه یکتای تراکنش برای بانک مبدأ ارسال می‌کند. این مغایرت در یک گردش کار مجزا و پسینی رسیدگی می‌شود و موجب توقف سرویس عملیاتی پرداخت نمی‌گردد.

ح) بانک مبدأ پس از دریافت رویداد مغایرت، اطلاعات مورد نظر را اصلاح کرده و رویداد اصلاحی را با همان شناسه یکتای قبلی برای بانک مرکزی ارسال می‌کند. استفاده از همان شناسه قبلی ضروری است، زیرا صدور شناسه جدید برای تراکنش اصلاحی می‌تواند موجب ثبت تکراری، ابهام در رهگیری و کاهش کیفیت داده‌های نظارتی شود.

این طراحی ضمن حفظ کیفیت داده‌ها و امکان نظارت متمرکز، از افزایش تأخیر، ایجاد گلوگاه متمرکز، وابستگی بیش‌از حد شبکه پرداخت به یک نقطه و تحمیل بار اضافی به سامانه‌های عملیاتی جلوگیری می‌کند. مدل مفهومی این فرایند در شکل زیر آمده است:

شکل ۱۰. مدل مفهومی الگوی تخصیص شناسه تراکنش



مأخذ: یافته‌های گزارش.

۱ شناسه یکتای تراکنش (صادر شده توسط بانک مبدأ)،

۲ تاریخ انجام تراکنش،

۳ مبلغ تراکنش،

۴ ابزار پرداخت (پایا، سانتا و ...)،

۵ مشخصات طرفین تراکنش (انتقال دهنده وجه و دریافت کننده وجه):

- نام و نام خانوادگی،
- شماره ملی / اقتصادی،
- شناسه شباه،
- نوع حساب (تجاری یا غیرتجاری)،
- مشخصات بانک (نام و کد بانک، نام و کد شعبه)،
- بابت یا انگیزه تراکنش،
- شماره منحصر به فرد صورت حساب الکترونیک،

برای مثال فرض می‌کنیم که جواد جوادی به حسن حسینی مبلغ هفتصد و پنجاه میلیون تومان از طریق ابزار پرداخت ساتنا، بابت خرید یک خودرو پرداخت می‌کند. در زمان انتقال خودرو، فرماندهی انتظامی جمهوری اسلامی از طریق مراکز تعویض پلاک، صورت‌حساب الکترونیکی برای این معامله با شماره منحصر به فرد صادر می‌کند. این شماره منحصر به فرد صورت‌حساب الکترونیکی نشان از انجام معامله و اطلاعات طرفین معامله است که در قسمت بابت یا انگیزه تراکنش می‌تواند ثبت گردد. شناسنامه این تراکنش در شکل ۱۱ نمایش داده شده است:

شکل ۱۱. شناسنامه تراکنش، نمونه

[illegible]

مأخذ: هــ

۲-۷. بررسی الگوریتم‌های تولید شناسه تراکنش

با تأکید بر مفهوم نظارت بانکی، تلاش‌هایی از سوی متولیان نظام پرداخت (بانک‌های مرکزی) صورت گرفت تا دستورالعمل‌هایی تدوین گردد تا بانک‌های هر حوزه قضایی پولی از طریق استانداردهای یکسانی به تولید شناسه تراکنش اقدام نمایند. این اقدامات با هدف یکپارچه‌سازی داده‌ها، دسترسی برخط و نظارت کارا صورت پذیرفته است. در این بخش به جمع‌بندی، مقایسه و پیشنهاد انواع الگوریتم‌های تولید شناسه تراکنش که در این گزارش مورد بررسی قرار گرفت، پرداخته می‌شود:

■ **شناسه مرجع یکتای تراکنش:** ویژگی یکتایی و تصادفی بودن برقرار شده است، اما ویژگی عدم افشای اطلاعات مهم به‌طور کامل برقرار نمی‌باشد. هرچند اطلاعات حساب طرفین و مبلغ تراکنش از طریق شناسه مرجع یکتای تراکنش قابل شناسایی نیست، اما کانال تراکنش و تاریخ آن مشهود است.

■ **شناسه مرجع تراکنش:** تمام ویژگی‌های یکتایی، تصادفی بودن و عدم افشای اطلاعات مهم را برآورده می‌کند، اما الگوریتم مشخصی برای تولید این شناسه معرفی نشده است و شبکه بانکی مطابق یک دستورالعمل یکسان و منحصر به فرد اقدام به تولید شناسه تراکنش نمی‌کنند و هر بانکی، مطابق دستورالعمل داخلی خود اقدام به تولید شناسه مرجع تراکنش نماید.

■ **شناسه مرجع یکتای انتها به انتها تراکنش:** تمام ویژگی‌های مورد نیاز یک شناسه یکتای تراکنش ایدئال شامل یکتایی، تصادفی بودن و قابلیت عدم انتقال اطلاعات مهم را داراست. مزیت دیگر این شناسه، استفاده از الگوریتم شناسه یکتای جهانی در تولید آن است. الگوریتم شناسه یکتای جهانی، مشکل اختلاف میان الگوریتم‌های صدور شناسه میان بانک‌ها را برطرف می‌کند. به عبارتی دیگر، شناسه یکتای جهانی این امکان مهم را میسر می‌کند که بدون هماهنگی میان بانک‌های مختلف، هر بانک بتواند از این الگوریتم استفاده نماید و در عین حال نگران احتمال صدور شناسه پیگیری تراکنش تکراری به علت عدم هماهنگی نباشد. مهم‌ترین نقطه قوت استفاده از شناسه یکتای جهانی عدم نیاز به هماهنگی میان بانک‌ها و مؤسسات مالی با یکدیگر برای تولید شناسه یکتای تراکنش است. این در حالی است که در انواع دیگر الگوریتم‌های تولید شناسه، استفاده از نام بانک، تاریخ و کانال پرداخت در فرمت شناسه تراکنش، راهی برای جلوگیری از بروز تداخل و نقض یکتایی شناسه‌ها بوده است. این تداخل احتمالی، در صورت استفاده از الگوریتمی غیر از شناسه یکتای جهانی، ممکن است حتی در روش‌های پرداخت مختلف یک بانک هم نمایان شود. به همین جهت، در میان الگوریتم‌های معرفی شده در این گزارش، الگوریتم شناسه یکتای جهانی که در شناسه مرجع یکتای انتها به انتها تراکنش استفاده شده و در نسخه تارگت ۲ پیشنهاد شده است، به‌عنوان مناسب‌ترین گزینه پیشنهاد می‌شود.

۸. جمع‌بندی و پیشنهادها



در دهه اخیر، پیچیدگی‌های فزاینده محیط اقتصادی کشور، رشد شتابان فناوری‌های اطلاعاتی و افزایش ریسک‌های نظام مالی، اهمیت بازتعریف و تقویت حکمرانی پولی را به ضرورتی اجتناب‌ناپذیر بدل کرده است. تجربه جهانی و شواهد داخلی نشان می‌دهد که ضعف زیرساخت‌های داده‌ای و نبود استانداردهای یکنواخت برای ثبت و رهگیری تراکنش‌ها، کارایی و اثربخشی سیاست‌های نظارتی و تصمیم‌سازی را به‌طور چشمگیری کاهش داده است. به همین دلیل، ایجاد بسترهای یکپارچه برای جمع‌آوری، ثبت و تحلیل داده‌های تراکنش‌های بانکی، به‌عنوان محور اصلی سیاست‌های موفق مقابله با جرائم مالی، ارتقای شفافیت، افزایش سلامت اقتصاد و تضمین ثبات مالی مطرح است.

در همین راستا، بهره‌گیری از اطلاعات (کلان داده‌ها و ریزداده‌ها) در حوزه سیاستگذاری اقتصادی و ارتقای اثربخشی سیاست‌های اتخاذی به‌منظور دستیابی به اهداف حکمرانی پولی، ضرورتی غیرقابل انکار است. یکی از مهم‌ترین داده‌های مورد نیاز برای ارتقای عملکرد صحیح بخش‌های حیاتی اقتصادی کشور از جمله نظام بانکی، نظام مالیاتی، نظام چندلایه رفاهی و نظام مبارزه با پول‌شویی، داده‌های مربوط به تراکنش‌های شبکه بانکی است. تولید و ثبت داده‌ها باید به‌گونه‌ای انجام شود که کیفیت داده‌های تراکنش‌های شبکه بانکی شامل صحت، دقت، پویایی، عمق، سازگاری، کامل بودن، و به‌موقع بودن را تضمین کرده و بهره‌برداری از داده‌های تولید شده را با حداقل هزینه برای نهادهای مختلف فراهم کند.

بدین منظور، لازم است زیرساختی فراهم شود تا قبل از انجام تراکنش‌ها و با نظارت بانک مرکزی شناسه‌ای یکتا با یک الگوریتم مشخص و واحد تولید شود (پیش‌فرض این اقدام پیروی از استاندارد مشخصی در زمینه شناسنامه تراکنش است)، سپس شناسه‌ها به‌همراه اطلاعات کامل تراکنش که درمجموع شناسنامه تراکنش را ایجاد می‌کنند، در پایگاه اطلاعات تراکنش‌ها نزد بانک مرکزی ثبت گردد. از آنجاکه نظام پولی آینده تمام‌نمای بخش حقیقی اقتصاد است، تقاطع‌گیری از داده‌های تراکنش‌های شبکه بانکی با نظام داده‌های بخش حقیقی موجب بهبود کارایی و اثربخشی حکمرانی پول ملی خواهد شد.

پایگاه اطلاعات تراکنش‌ها می‌تواند در حوزه‌های متعددی نظیر حوزه مالیات، مبارزه با پول‌شویی و حوزه نظام رفاهی مورد استفاده قرار گیرد که در ادامه برخی از این موارد به‌اختصار توضیح داده می‌شود:

■ **حوزه مبارزه با پول‌شویی:** در این حوزه مرکز اطلاعات مالی یکی از نهادهایی است که با هدف تأمین امنیت اقتصادی کشور می‌تواند به‌منظور مقابله با پول‌شویی و تأمین مالی تروریسم از پایگاه اطلاعات تراکنش‌ها بهره‌برداری کند. در این پایگاه اطلاعات که شناسه تمام تراکنش‌های درون‌بانکی و بین‌بانکی با یک الگوریتم واحد و مشخص ثبت می‌شود، می‌تواند این قابلیت را به مرکز اطلاعات مالی بدهد که شاخص ریسک اشخاص را با حداقل هزینه، به‌صورت برخط و لحظه‌ای محاسبه و مطابق ضوابط تعیین شده در قانون مبارزه با پول‌شویی با آنها برخورد کند.

■ **حوزه مالیات:** در این حوزه سازمان امور مالیاتی کشور یکی دیگر از نهادهایی است که می‌تواند از اطلاعات تراکنش‌ها به‌منظور دستیابی به اهدافی نظیر افزایش پایه‌های جدید مالیاتی، مقابله با فرار مالیاتی و اخذ مالیات منصفانه با حداقل هزینه، کمترین دخالت نیروی انسانی و کمترین خطا استفاده کند. به‌عنوان نمونه، بدون صحت‌سنجی اظهارات مؤدیان (درباره میزان خرید، فروش، سود یا زیان) با بررسی داده‌های تراکنش‌های شبکه بانکی مرتبط، عملاً فرایند مالیات‌ستانی مستعد فرار مالیاتی گسترده خواهد بود.

■ **حوزه نظام رفاهی:** در این حوزه وزارت تعاون، کار و رفاه اجتماعی می‌تواند جهت ایجاد شناسنامه رفاهی - اقتصادی اشخاص ذیل پایگاه اطلاعات رفاه ایرانیان به‌منظور پیگیری تحقق اهداف این وزارتخانه نظیر شناسایی فقر و مقابله با آن و حمایت از اقشار کم‌برخوردار جامعه از پایگاه اطلاعات تراکنش‌ها استفاده کند. به‌عنوان نمونه دیگر، بدون برخورداری از اطلاعات یکپارچه حساب‌ها و تراکنش‌ها، فرایند شناخت گروه‌های مستحق دریافت کمک‌های مالی دولت به‌درستی صورت نگرفته و میزان یارانه در نظر گرفته شده در بودجه به‌درستی به گروه‌های هدف اصابت نخواهد کرد.

- [1] Worldpay, “Worldpay ISO 8583 Reference Guide, V2.46,” FIS Global, 2023. Available: https://developerengine.fisglobal.com/assets/pdf/Worldpay_ISO_8583_Reference_Guide_V2.46.pdf. [Accessed: Jul. 07, 2025].
- [2] ISO, “What is ISO 20022?,” ISO 20022, 2004. [Online]. Available: <https://www.iso20022.org/> [Accessed: Jul. 07, 2025].
- [3] SWIFT, “ISO 20022,” [Online]. Available: <https://www.swift.com/standards/iso-20022>. [Accessed: Jul. 07, 2025].
- [4] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, pp. 35–127, 23 Dec. 2015; consolidated version 17 Jan. 2025. [Online]. Available: <https://eur-lex.europa.eu/eli/dir/2015/2366/2025-01-17/eng>.
- [5] Parliament of India, “The Payment and Settlement Systems Act, 2007 (Act No. 51 of 2007),” Ministry of Law and Justice, New Delhi, India, Dec. 20, 2007. [Online]. Available: <https://www.indiacode.nic.in/bitstream/123456789/2082/4/a2007-51.pdf>.
- [6] “What is UTR number in India?” RemitFinder, 2023. [Online]. Available: <https://www.remitfinder.com/blog/utr-number-everything-you-need-to-know>.
- [7] European Central Bank, “History of the Eurosystem’s real-time gross settlement systems,” ECB, 2025. [Online]. Available: <https://www.ecb.europa.eu/paym/target/t2/predecessors-of-t2/html/index.en.html>.
- [8] European Central Bank, “TARGET2 Information Guide for users (v13.0),” TARGET2, Nov. 2019. [Online]. Available: https://www.ecb.europa.eu/paym/target/target2/profuse/nov_2019/shared/pdf/Information_Guide_for_TARGET2_users_v13.0.pdf.
- [9] SWIFT, “MT Standards – Tag 20 Transaction Reference Number,” SWIFT Standards MT, rev. Jul. 2022. [Online]. Available: https://www2.swift.com/knowledgecentre/rest/v1/publications/usgi_20220722/2.0/usgi_20220722.pdf.
- [10] P. Leach, M. Mealling, and R. Salz, “A Universally Unique Identifier (UUID) URN Namespace,” IETF RFC 4122, Jul. 2005. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc4122>.
- [11] P. Leach, M. Mealling, and R. Salz, “A Universally Unique Identifier (UUID) URN Namespace,” RFC 4122, Internet Engineering Task Force (IETF), July 2005. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc4122>.
- [12] SWIFT, “Standards MX Message Implementation Guide,” Swift for Corporates, 2022. [Online]. Available: https://www2.swift.com/knowledgecentre/rest/v1/publications/s_corp_stdsmx_msg_impl_guid/2.0/s_corp_stdsmx_msg_impl_guid.pdf.
- [13] Ohmyfin, “Track Your Cross-Border Payment Status Online,” Ohmyfin.ai, 2025. [Online]. Available: <https://ohmyfin.ai>.
- [14] Tournier v. National Provincial and Union Bank of England Case Text, Organization of American States, MESICIC Sixth Round, Annex 3, [Online]. Available: https://www.oas.org/es/sla/dlc/mesicic/docs/mesicic6_respuesta_can_an3.pdf.
- [15] United Nations, “United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances,” Vienna, 20 Dec. 1988, entry into force 11 Nov. 1990. [Online]. Available: https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=VI-19&chapter=6&clang=en.
- [16] FATF, “The FATF Recommendations 2012,” adopted 16 Feb. 2012, amended Jun. 2025. [Online]. Available at: fatf-gafi.org. Accessed Jul. 2025.
- [17] G. Greenleaf, “Global Data Privacy Laws 2025: 172 Countries, Twelve New in 2023/24,” SSRN, Apr. 2025. Available: https://papers.ssrn.com/abstract_id=5275559.

- [18] OECD, "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data," Recommendation C(80)58/FINAL, 23 Sept. 1980. [Online]. Available: <https://www.refworld.org/policy/legalguidance/oecd/1980/en/14534>. Accessed: 10 Jul. 2025.
- [19] Council of Europe, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)," ETS No. 108, opened 28 Jan. 1981. [Online]. Available: <https://www.coe.int/en/web/data-protection/convention108-and-protocol>. Accessed: 10 Jul. 2025.
- [20] Republic of India, "The Digital Personal Data Protection Act, 2023," No. 22 of 2023, §§ 7, 16 & 17, Aug. 11 2023. [Online]. Available: <https://www.meity.gov.in/static/uploads/2024/06/2b1f0e9f04e6fb4f8fef35e82c42aa5.pdf>. Accessed: 11 Jul. 2025.
- [21] Parliament of India, Income-tax Act, 1961, secs. 133(6) [Online]. Available: <https://www.indiacode.nic.in/bitstream/123456789/2435/1/a1961-43.pdf>. Accessed: 11 Jul. 2025.
- [22] Parliament of India, Prevention of Money-Laundering Act, 2002, secs. 12–14 & 50. [Online]. Available: <https://www.indiacode.nic.in/bitstream/123456789/2036/5/A2003-15.pdf>. Accessed: 11 Jul. 2025.
- [23] Parliament of India, Code of Criminal Procedure, 1973, sec. 91. [Online]. Available: https://www.indiacode.nic.in/bitstream/123456789/15272/1/the_code_of_criminal_procedure_1973.pdf. Accessed: 11 Jul. 2025.
- [24] European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," Off. J. L119, 4 May 2016. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>. Accessed: 11 Jul. 2025.
- [25] European Union, "Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism," Official Journal of the European Union, L 2024/1620, 19-Jun-2024. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2024/1620/oj>. Accessed: 12-Jul-2025.
- [26] European Union, "Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing," Official Journal of the European Union, L 156, pp. 43–74, 19-Jun-2018. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843>. Accessed: 12-Jul-2025.
- [27] Council of the European Union, "Council Directive (EU) 2016/2258 of 6 Dec 2016 amending Directive 2011/16/EU as regards access to anti-money-laundering information by tax authorities," Official Journal of the European Union, L 342, pp. 1–3, 16-Dec-2016. [Online]. Available: <https://eur-lex.europa.eu/eli/dir/2016/2258/oj>. Accessed: 12-Jul-2025.

عنوان: ارتقای حکمرانی در حوزه ریال (۲): تخصیص شناسه یکتا به تراکنش‌های بانکی



DOI: <https://doi.org/10.22034/mrc.report.22000>

Permanent Link: https://report.mrc.ir/article_12036.html

Publisher: Islamic Parliament Research Center of Iran

گزیده سیاستی

شناسه یکتای تراکنش‌های بانکی زیرساختی کلیدی برای ارتقای حکمرانی بر ریال است و با فراهم کردن امکان رهگیری جریان وجوه، نظارت داده‌محور و بهره‌برداری یکپارچه از داده‌های تراکنش‌ها، ظرفیت مقابله با جرائم مالی و اشراف اطلاعاتی افزایش می‌یابد.



مرکز پژوهش‌های مجلس شورای اسلامی

تهران، خیابان پاسداران، روبروی پارک نیاوران (ضلع جنوبی، پلاک ۸۰۲)

تلفن: ۷۵۱۸۳۰۰۰ صندوق پستی: ۱۵۸۷۵-۵۸۵۵ پست الکترونیک: mrc@majles.ir

وبسایت: rc.majles.ir