Intra-Japan Closed-Loop Ticketing

Contents

1 Executive Summary

This article is designed for stakeholders of transit agencies, municipal planners, and ticketing system vendors.

We will discuss the **Sony FeliCa** model of intra-Japan transit ticketing system which incorporates 100+ participating transit entities and 100+ million riders, providing latency of 0.1 sec per validation at the subway gateway.

Using this example, we will learn what the Trusted Execution Environment (TEE) is in stored-value solutions, their pros and cons, and what can be done to close the gap between the closed-loop ecosystem of trust build by FeliCa and open-loop ticketing.

2 FeliCa and Ticketing in Japan

We must appreciate the sheer scale of what Sony achieved. FeliCa (Fast Economy Light Card) is the "engine" under the hood of Japan's transit miracle.

While the rest of the world was still fiddling with magnetic stripes, Sony developed a high-speed, contactless IC chip technology specifically for the brutal demands of the Tokyo commute. To keep the lines moving, a Japanese gate must validate a rider and open in less than 0.1 seconds.

Sony and FeliCa created a federated TEE system where 100+ independent agencies - including the 105 members of the **PASMO** consortium and the vast **Suica** network – share a common cryptographic framework. While each agency maintains its own business identity, they all utilize the same **Sony FeliCa** engine. This allows a single stored-value balance to be used interchangeably across diverse railway and bus networks.

2.1 Scale and Reach

The scale of this ecosystem is unmatched in the global transit industry. JR East alone reports over 112 million Suica cards in circulation, alongside 33 million Mobile Suica accounts. Market data indicates that transit contactless cards facilitate approximately 95% of all transit trips in the Greater Tokyo area.

Based on domestic transport statistics published by the Ministry of Land, Infrastructure, Transport and Tourism (MLIT) and the Statistical Handbook of Japan 2025 (Chapter 9), the following metrics can be derived (2025/2026 forward-looking estimates):

Metric	Estimated Value (2025/2026)
Annual International Tourists	42.7 million
Total Annual Ridership (Includes all National Rail & Bus)	~25 billion trips
Annual Fare Revenue (includes Shinkansen & Long-Range)	~9.5 trillion JPY ($63 billion)
Average Fare (Subway/Bus)	170 – 210 JPY ($1.15 – $1.40)
Rail fares range	500 – 10,000 JPY ($3 – $70)

Riders use FeliCa for diverse travel types, from short subway hops and local bus routes to high-speed Shinkansen trips.

The FeliCa-based "Nationwide Mutual Usage" (NMU) service exerts a near-monopoly over Japan's transit ticketing, representing over 90% of all non-cash transactions across the country's rail and bus networks. This ecosystem functions as a unified "Mega-Loop" where ten major regional card brands, such as Suica and PASMO, operate under a shared business logic. While Japan maintains other specialized ticketing loops – most notably the magnetic-stripe "Orange Card" for regional rail and various QR-code-based ticketing pilots for rural buses – these alternatives lack the scale and speed of the FeliCa standard.

Beyond Japan, other major metropolitan hubs adopted FeliCa technology to manage similar high-density flows. Hong Kong’s Octopus card (launched in 1997) served as the world’s first major commercial FeliCa deployment, followed by implementations in Singapore (EZ-Link, though now transitioning) and Jakarta, Indonesia.

The primary competitor to the NMU "Mega-Loop" is the recent emergence of international open-loop cEMV (Visa/Mastercard) payments on private rail lines like Tokyu and Nankai.

Competitors using QR codes or standard EMV utilize standard Public Key Encryption protocols that often struggle to match the 0.1-second latency required for Japan's high-volume commuter gates.

2.2 FeliCa Transition to Modern Standards

The 21st-century requirements present new challenges. A more systemic disruption looms on the horizon: the Post-Quantum (PQ) Factor. Sony recently updated the FeliCa standard to include AES-256 encryption and achieved EAL6+ certification to meet modern security benchmarks. However, the hardware-based nature of this TEE requires a physical replacement of older cards and reader SAMs to maintain this security level.

The PQ is already triggering an eventual and costly replacement cycle encompassing hardware silicon, embedded software, and the complex business processes required to maintain a secure TEE. This transition represents a significant shift from the static security of the past to an agile, yet hardware-heavy, requirement for the future.

3 Business-Level Interoperability

In my previous article, I talked about two levels of interoperability in open-loop public transit ticketing:

- **Technical level:** Where the card (or phone) and the validator use the same standards of information exchange, like ISO/IEC 14443 (NFC Type A/B) or QR encoding standards.
- **Business level:** Where the Transit Agency (TA) that moved the rider can be sure that it will eventually be paid off for its services.

In layman's words, technical-level interoperability ensures that all business partners speak the same language, e.g., English. Whereas the business-level ensures that they all have bank accounts, operate in the same legal space, and trust the signed documents.

Let's talk about the business-level interoperability in detail. In general, it requires two components:

- TEE that ensures that technical agents (validators, PoS, vending machines) interacting with card (or phone apps) trust the cards (apps). Stored-value systems also require that the cards (apps) trust the agents.
- Financial settlement that ensures that a participating agency provided services is paid off.

Let's see how three known models of business-level interoperability deal with these requirements.

3.1 Classic Open-Loop Ticketing

The classic open-loop model based on contactless EMV cards supported by various payment schemes (Visa, Mastercard, etc.).

3.1.1 Classic Open-Loop TEE

The EMV standard ensures that the validator knows the card is genuine. The card does not need to be sure that the validator is genuine because the validator doesn't write anything to

the card. The card balance is managed by the card issuers – financial institutions – through the payment scheme cloud. This simplifies the matter.

Nevertheless, the TEE scheme supporting the card authentication by the validator without any backend support – Offline Data Authentication (ODA) – comes with heavy and costly regulations like EMV, PCI DSS, and payment scheme compliance.

The ODA comes with a latency. Practically, most of the EMV devices and cards on the market can achieve 0.2 – 0.3 sec. This is too much for Tokyo, Japan environment. Modern card readers and cards (phones) may go below these numbers.

3.1.2 Classic Open-Loop Settlement

Powerful clearing systems from Visa and Mastercard ensure that the merchants (TAs) are compensated.

3.2 Stored-Value Closed-Loop Ticketing (FeliCa-Like)

3.2.1 FeliCa TEE (Money-Value in the Chip)

The validator must ensure that the card is genuine (similar to ODA) but this is not enough. FeliCa is essentially based on a stored-value technology. This requires that the card trusts (authenticates) the validator, vending machine, PoS, or any other device that are allowed to change the card status, including the stored-value balance.

The card (or the security module (SE) in a phone) and the validator's Secure Access Module (SAM) prove their identities to each other in less than 0.1 seconds.

Key Provisioning and Virtual Cards: When a user adds a **virtual card** – a digital instance of a Suica or PASMO – to an Apple or Google Wallet, a Trusted Service Manager (TSM) coordinates the delivery of the unique **Diversified Key**. The TSM, acting as a secure third-party server, pushes this key directly into the phone's hardware SE via an encrypted, over-the-air tunnel. This process ensures that neither the phone's main operating system nor any intercepted data can reveal the key.

FeliCa-Compliant Phones: The global mobile market is split between **FeliCa-compliant** devices and "Global" models. To meet the 0.1s requirement, a phone must possess a specific NFC-F antenna and a Sony-certified Secure Element.

- **The Apple Approach:** Apple unified its hardware. Every iPhone globally (since the iPhone 8) is FeliCa-compliant, allowing any tourist with an iPhone to provision a virtual card instantly.

- **The Android Approach:** Most Android manufacturers only include FeliCa hardware in "Japan-specific" models (Osaifu-Keitai). A flagship Samsung or Pixel purchased in Europe or the US is generally not FeliCa-compliant and cannot host a virtual Suica.

Plastic cards. Despite the rise of mobile payments, plastic cards still represent the majority of cards in circulation (roughly 70 percent as of early 2025), remaining the primary entry point for students, the elderly, and international tourists with non-compliant Android devices. Mobile adoption is accelerating rapidly, with over 33 million Mobile Suica accounts already in use.

The Vulnerability: Since trust resides locally at the gate to ensure speed, every SAM must store group keys. The SAM uses them to derive the Diversified Key of the specific card tapping the reader on-the-fly. This architecture creates certain risks: a stolen SAM represents a "system-level" threat. If a bad actor extracts group keys from one stolen reader, they can theoretically compromise many FeliCa plastic cards.

Because the system cannot practically revoke or "re-key" millions of physical plastic cards already in users' pockets, it relies on a **"Negative List" (Blacklist)** approach. The system must broadcast the ID of every lost, stolen, or compromised FeliCa card to every validator in Japan. This list grows perpetually, consuming memory and processing power.

Key Replacement and the "Phone Advantage": The recovery process differs wildly based on the hardware:

- **FeliCa-compliant Phones:** These devices are "Crypto-Agile." If group keys are compromised, the TSM can push a new Diversified Key to every virtual card holder silently in the background.
- **Plastic Cards and FeliCa-Non-Compliant Phones:** For the millions of plastic cards and non-compliant devices, there is no over-the-air path. A security breach at the group key level requires the physical recall and replacement of every card – a logistical "vicious circle" that is both expensive and slow.

Currently, no publicly documented attacks or significant concerns from the security community exist regarding group key compromise in operational FeliCa EAL6+ SAM implementations. The system's tamper-resistant design and key diversification have proven effective to date. However, any large-scale international expansion of such a model would substantially increase the number of key-issuing entities and SAMs, raising both the potential attack surface and the complexity of disaster recovery.

However, this specialized protection comes at a price. The Following Table may give you some understanding of costs which come with TEE required for a stored-value system.

In the Japan's closed-loop system these costs are reasonable if you compare them with alternative solutions. All known alternative solutions would require multiplying the number of gates at least in Tokyo subway stations which is practically unfeasible.

Factor	Sony FeliCa - Estimates
EAL6+ Smart Card Chip	~$3.50 – $5.00 (High-sec silicon)
Personalization	~$1.00 per card (HSM centers)
Validator Cost	$1,500 – $3,500 (Requires SAM)
EAL6+ Validator SAM	$80 – $150 (High-Security Validator SAM (post-migration modules)
Certification	~$100k – $250k (Proprietary TEE)

3.2.2 FeliCa Settlement

Because the FeliCa model is "Stateless" – meaning the money value lives on the card – the settlement process requires a centralized, heavy-duty intermediary. In Japan, a central entity (like the **JR East Clearing Center**) acts as the single source of truth. Every day, thousands of independent validators upload their transaction logs.

3.3 UniTiAg Open-Loop Ticketing

UniTiAg (Universal Ticketing Agent) is an Open-Loop model where the money value – Open-to-Ride Balance (OTRB) – is stored in the cloud. Riders refill OTRBs via online Two-Sided Marketplaces (TSMPs). The TSMPs ensure the TAs are paid off.

3.3.1 UniTiAg TEE (Money-Value in the Cloud)

In UniTiAg realm, the validator needs to authenticate a so-called "CRD Token" presented by a Contactless Rider Device (CRD). The CRD Token is held by the app on the CRD. The app ensures the validator that the CRD Token is genuine using an EMV-like process similar to the EMV ODA.

The CRD (a phone or a card) does not need to "know" the validator as the CRD does not store any value. UniTiAg keeps the rider's Open-To-Ride Balances (OTRB) in the cloud.

The validator does not "debit" or "credit" a chip. Instead, it verifies a signed **CRD Token** (a cryptographically secure proof of the rider's identity) against a local whitelist of valid OTRBs.

Whitelist burden: UniTiAg allocates 50 bytes per OTRB record including the unique ID and balance – as disclosed in TANB API section. A standard 5 GB memory module on a validator can hold roughly 100 million active OTRB records. The binary search in this list

can be achieved within 1.5 msec. Frequent (once every several minute or so) whitelist updates are required only for low-balance, non-trustworthy riders.

Authentication Speed: Using the same high-speed NFC-F (FeliCa) protocol, the CRD Token authentication matches the 0.1s benchmark. For tourists using standard ISO/IEC 14443 (NFC Type A/B) on global Androids or older iPhones, the average latency is below 0.2 sec.

3.3.2 UniTiAg Settlement (The Marketplace Model)

UniTiAg settles through standard **TSMP financial rails**, treating transit fares as a standard marketplace transaction with no specialized clearinghouse required.

4 Rider Experience: Inclusivity vs. Fragmentation

FeliCa's model creates a "walled garden" for mobile users. To support the 0.1s FeliCa tap, a phone needs a **Sony-certified NFC-F antenna and SE firmware**.

- **The Cost:** This adds a **$3–$5 BoM premium** per phone. Apple "swallowed" this cost globally, but most Android manufacturers only include it in "Japan-only" SKUs.
- **The Result:** A traveler with a global Android phone is **locked out** of the digital experience and forced to buy plastic.

For sporadic riders, the Sony model is punitive:

- **Non-Refundable Balances:** Tourist-specific cards (Welcome Suica) have **zero refundability**. Any leftover Yen is "breakage" profit for the agency.
- **Refund Penalties:** Regular cards charge a **220 JPY fee** to get your money back, effectively taxing short-term users.

So, the question remains: how to "open" the Japan's closed-loop without jeopardizing the validation throughput?

An idea of extending the federated intra-Japan TEE to some international federated TEE seems to be impractical from the cost and risk analysis (let alone the bureaucratic effort and time required for that).

We will explore a hybrid solution. For that we would need to explore possible candidate components for this hybrid.

5 Balanced Hybrid Solution

If we see certain value in extending Japan residents capabilities to ride mass transit abroad, and foreigners – to ride in Japan; in other words, if the objective is "opening" the FeliCa closed loop without replacing it, then adding another component to FeliCa, such as UniTiAg may be a valid option.

Let's explain why, keeping in mind extreme constraint: low validation latency (high throughput).

5.1 Hardware Selectiveness in Japan Hubs

In UniTiAg, a CRD (which can be either a phone or a plastic card) presents the CRD Token via an app on the CRD or – in case of a cEMV card – via a standard cEMV session.

To prevent clogging the subway validation routes, it is important to exclude the cEMV plastic from acceptance for UniTiAg validation in certain classes of gateways.

The second step is to limit the class of CRDs and their apps that are accepted in Japan via the UniTiAg process. This is also possible. The CRD apps are managed by the TSMPs, and the latter can segregate their CRD Token apps by the device class, so only those are accepted in Japan's subway or railway hubs where the throughput is important.

5.2 Japan's FeliCa Card Usage Outside of Japan

Let's consider two cases: (a) FeliCa plastic and (b) phones.

In both cases, (a) and (b) the card issuer, like Suica or PASMO must become a TSMP in UniTiAg scheme. Technically, they are already capable of this, as they top up the FeliCa cards online. With UniTiAg, they would need to keep two separate balances: UniTiAg OTRB, for travelling abroad, and stored value in the card, for rides in Japan and allow funding one stored-value by another.

UniTiAg is friendly to any type of CRD Token, if the latter can prove its authenticity offline. If transit entity outside of Japan wants to participate in UniTiAg and use FeliCa protocols to validate the FeliCa plastic as a CRD Token, it is technically possible though it requires a FeliCa's SAM. Such a card will be bound via its ID – as a CRD Token – with the OTRB balance managed by e.g. PASMO's TSMP.

With phones – case (b) – it is even easier. PASMO, etc. will just issue its app with a standard CRD Token, acceptable at any transit entity agreed to be on e.g. PASMO TSMP seller – no SAM and special protocols are required.

5.3 Ultra-Wideband

Ultra-Wideband (UWB) is worth to be explored (it is already known to Sony.) as a method of increasing validation throughput in general, including the Japan case as well as the method of opening closed loops (business-level interoperability).

UniTiAg is UWB friendly because UniTiAg is ignorant of the technology used for presenting the CRD Token for validation.

5.4 Comparing Open-Loop Candidates

Let's compare the discussed Open-Loop models from the perspective of "opening" the FeliCa closed loop without replacing it.

Factor	Classic Open-Loop	UniTiAg Open-Loop
Regulatory costs	High (EMV, PCI DSS) in addition to EAL6+. See our COFC analysis.	Low. Current validation equipment in Japan does not require any upgrade.
Form factors to be used in Japan	Any cEMV-capable phones and plastic cards.	cEMV-capable Phones with zonal exclusion of FeliCa non-certified phones.
Validation Latency (throughput)	0.3s average with ODA (international cEMV cards)	0.1s with FeliCa-certified phones 0.2s average for other phones
Usage scope	Very limited	Less limited
Using FeliCa Cards outside Japan	Not possible	Possible
Using Ultra-Wideband (UWB)	Not possible	Possible

6 Take-Away

1. Modern transit ticketing does not require a winner-take-all choice. Instead, the most resilient systems of the 2026-2030 era will likely adopt a hybrid architecture that plays to the strengths of both hardware and software-defined trust.
2. While the FeliCa core manages the "heavy lifting" of the daily commute, the UniTiAg model could serve the tourists, sporadic riders, and less congested transit hubs. This approach opens the intra-Japan closed-loop ticketing to the world.
3. The next shift in the ticketing technology in congested mass transit hubs will probably come with new, faster communication channels, like UWB. The UniTiAg Open-Loop model is ready to embrace it.

7 Glossary

- **AES-256:** Advanced Encryption Standard with a 256-bit key size; the modern benchmark for securing transit data.
- **BoM (Bill of Materials):** The total cost of raw components required to manufacture a single hardware unit.
- **cEMV:** Contactless EMV (Europay, Mastercard, and Visa); the global standard for proximity credit and debit card payments.
- **Diversified Key:** A unique cryptographic key derived from a group key, ensuring that a single compromised card does not threaten the entire system.
- **EAL6+**: The highest commonly used assurance level under Common Criteria (ISO/IEC 15408). It provides high confidence that the Target of Evaluation (TOE) is resistant to attackers with high attack potential. Typically required for high-value assets such as government ID cards, critical infrastructure, or PQ secure elements.
- **Federated:** a distributed collaboration model among multiple autonomous TEE instances that trust each other
- **FeliCa-Compliant:** Hardware (NFC-F) that meets the 0.1-second latency and specific antenna requirements for the Japanese transit ecosystem.
- **Offline Data Authentication (ODA):** an EMV scheme supporting the card authentication by the validator without any backend support.
- **OTRB (Open-To-Ride Balance):** A digital "transit pocket" or money value stored in the cloud rather than on a physical chip.
- **PCI DSS –** Payment Card Industry Data Security Standard**.**
- **PoS** – Point of Sales.
- **PQ (Post-Quantum) Factor:** The threat posed by quantum computing to current cryptographic standards, necessitating system-wide hardware and software upgrades.
- **SAM (Secure Access Module):** A tamper-resistant chip installed in validators to store group keys and perform secure authentication.
- **TEE (Trusted Execution Environment):** A secure computational area where cards and validators can mutually verify identities and trust.

- **TSMP (Two-Sided Marketplace Platform):** Online financial rails (e.g., app-based marketplaces) that manage rider refills and settle funds with transit agencies.

8 References

1. EAL6+ migration costs:
   1.1. Mordor Intelligence – Smartcard MCU Market Analysis: Confirms EAL6+ as the fastest-growing tier for post-quantum and critical-infrastructure demand.
   1.2. Infineon Security Solutions Portfolio: Lists the SLC 32 and SLE 78 families, which offer EAL6+ certification for 32-bit and 16-bit security controllers.
   1.3. Sony FeliCa Product Catalog (RC-S500): While the standard RC-S500/SO2 is EAL5+, it establishes the 1.25 Mbps processing baseline that newer EAL6+ "After Migration" modules must meet.
2. ISO/IEC 15408 EAL6+: International standard for Information Technology Security Evaluation, which FeliCa has achieved.
3. ISO/IEC 14443 (NFC Type A/B): The standard NFC protocol used by global Androids and older iPhones for tourist access.
4. Statistical Handbook of Japan 2025
5. PASMO consortium
6. FeliCa – Description of Sony FeliCa product and solution.
7. Sony and NXP experimenting with UWB.
8. UniTiAg APIs – TANB API specs allow to assess the whitelist burden.
9. UniTiAg COFC Analysis: Internal economic reporting on Capital and Operational costs of fare collection.
10. Business Interoperability in UniTiAg
11. UniTiAg cEMV Validation Sessions

9 Notice and Disclaimer

This article was authored by Eugene Lishak. The comparative analysis and technical data contained herein are provided for informational and educational purposes. Any errors or omissions are strictly non-intentional and are not intended to disparage the Sony FeliCa TEE solution or its associated stakeholders. We hold the FeliCa ecosystem in the highest regard for its role in establishing world-class transit reliability. If you identify any technical inconsistencies or factual inaccuracies, please contact the author directly for immediate review and correction.

