

May 14, 2026

Introduction of Consolidated Subsidiary my FinTech, the Company Behind Our Digital Trust Business

— The Role of my FinTech in "Japan Communications Vision 2030" —

Japan Communications Inc. (hereinafter referred to as "JCI") introduces my FinTech Inc. (hereinafter referred to as "myFinTech"), the core entity of our Digital Trust business, which plays a central role in the Digital Authentication Infrastructure — the source of our competitiveness — announced in "Japan Communications Vision 2030" on May 7, as well as in the business development leveraging that infrastructure. This document outlines myFinTech's business, shareholder structure, and social role.

1. About my FinTech Inc.

myFinTech is an operating company that runs an **Accredited Certification Authority (CA) under the Digital Signature Act**. Within the JCI Group, it is positioned as the **central entity** operating the Digital Authentication Infrastructure that is the source of our competitive strength. It aims to develop and provide a uniquely rare domestic business platform that integrates SIM provisioning — the key to mobile communication authentication — with CA operations as a Trust Service Provider. Considerable time was required from incorporation to commercial launch. This reflects the time needed to meet the stringent requirements of an accredited CA, technically validate the FPoS library, and accumulate operational track records in high-trust domains such as finance, government, and healthcare. Now that FPoS library is formally transitioning to the social-implementation phase, we are reintroducing myFinTech to the market and our partners.

2. Core Product — FPoS Library (4 Functions)

The centerpiece of myFinTech's product portfolio is the **FPoS Library**. It is a library (software component) provided to app developers for iPhone and Android smartphones, delivering the following four functions as an integrated package.

Function	Overview
①Identity Verification	Verification of a person's actual existence using the Public Personal Authentication Service (JPKI) and similar methods. Provides functions to reliably confirm that "the person exists and is indeed who they claim to be" at the start of service use — for eKYC, account opening, administrative procedures, etc.

Function	Overview
②Authentication	Robust hardware-based authentication using private keys protected in the secure hardware of iPhone/Android smartphones — impervious to impersonation. Proves, on a hardware-origin basis, that "the identity-verified person is the one accessing the service" each time the service is used.
③Digital Signature	Legally valid digital signatures using digital certificates issued by an Accredited CA under the Digital Signature Act. Applicable across a wide range of use cases, from legally binding contracts to personal consent and confirmation.
④Data Linkage	A function that connects to the data linkage platform provided by Mebuku Ground Inc.* ¹ (hereinafter referred to as "Mebuku Ground") to realize data linkage based on Self-Sovereign Identity (dynamic opt-in). Users grant data linkage permission on a case-by-case basis, of their own volition; that permission is secured with a digital signature using an accredited digital certificate. The data linkage platform acts as an intermediary between businesses only within the scope of permission granted, and data distribution is established only when the user's opt-in is confirmed.

*¹ Mebuku Ground Inc.: A public-private joint venture involving Maebashi City, Gunma Prefecture, private companies, and universities. Details below.

Each of these four functions is useful on its own, but the **essential value lies in their integrated delivery as the FPoS Library**. Specifically, the uniqueness of the FPoS Library lies in its ability to complete a user-sovereign trust flow entirely on the device: an **"identity-verified person," through "Person Authentication," grants data linkage permission with a "digital signature," and as a result "data linkage" is established only within the permitted scope.**

In particular, Function ④ Data Linkage is an implementation of **Self-Sovereign Identity (SSI)-based dynamic opt-in** realized through connection to the data linkage platform provided by **Mebuku Ground**. The structure is as follows: users grant data linkage permission on a case-by-case, scope-specific, and counterpart-specific basis; that expression of intent is finalized with a digital signature using an accredited digital certificate; and the data linkage platform intermediates between businesses only within that permitted scope. This enables cross-domain service integration spanning finance, healthcare, government, and regional DX without compromising user sovereignty.

■ Data Linkage Governance — Independent Governance of myFinTech and Mebuku Ground

Mebuku Ground, which provides the data linkage platform, was established as a **public-private**

joint-venture company. Its data handling policies and operations are determined by its own **Data Governance Committee (Chairperson: Professor Emeritus Jiro Kokuryo, Keio University)**. This ensures that the operation of the data linkage platform is independent of the interests of any specific business operator and is governed with a focus on user sovereignty and public interest. The fact that myFinTech, which operates the FPoS Library and Accredited CA, and Mebuku Ground, which operates the data linkage platform, are **designed as separate companies** has a clear institutional design rationale. By **structurally separating the entity responsible for authentication and digital signatures (myFinTech) from the entity responsible for data linkage and governance (Mebuku Ground)**, independent governance over data linkage is maintained, providing a trustworthy data distribution environment for both users and participating businesses. This is also an implementation of a **Japanese-style Trust Architecture** that structurally prevents data concentration or monopolization by any specific business operator.

3. FPoS Security Structure — Fundamental Differences from SSO-Type Identity

Providers

Key to understanding FPoS's advantages is its structural differences from the SSO (Single Sign-On)-type identity providers that are now widely used. While SSO-type authentication offers convenience, it carries **structural vulnerabilities that cannot be overlooked** for use as social infrastructure. FPoS adopts a design that structurally resolves these vulnerabilities through hardware-origin trust.

	SSO-Type Identity Provider	FPoS
Authentication Subject	Relying parties do not perform authentication themselves; they rely on the authentication result of an external identity provider.	The business operator itself directly performs authentication (login) via the user's digital signature from the digital certificate, without relying on any external identity provider.
Location of Private Key / Credentials	The identity provider centrally manages credentials. User credentials are stored on the service provider's side.	The private key exists only in the hardware area (Secure Element / SIM) of the user's smartphone. It cannot be copied. No third party, including myFinTech, possesses it.
Information Leakage Risk	Because credentials are concentrated in one location, leakage — whether from external attack or insider threat — causes massive damage across all relying	First of all, there is no centralized location to store private keys. Since the item that could be leaked (the key itself) does not exist, impersonation is structurally

	SSO-Type Identity Provider	FPoS
	parties and users.	impossible whether via external attack or insider threat.
Risk of Impersonation	Theft or leakage of credentials creates a risk that a third party can impersonate the user and access a wide range of services.	Since the private key cannot be extracted from the hardware area of the user's physical device, impersonation is in principle impossible without physically possessing the user's own device.

The essence of FPoS is structural trust based on the physical properties of the Secure Element: **"the private key never leaves the hands of the user who uses it."** The private key is stored in the hardware area of the smartphone and cannot be copied or extracted. No third party — including the issuer myFinTech — possesses this key.

Furthermore, relying parties can **directly receive authentication (login) via the user's digital certificate-based digital signature**, rather than relying on the authentication result of an external identity provider. This allows business operators to complete authentication under their own responsibility, freeing them from the dilution of authentication authority inherent in reliance on a third-party identity provider and from the leakage risk of a centralized authentication infrastructure. This is precisely **the level of trust required in high-trust domains such as finance, healthcare, and government** — that SSO-type authentication cannot structurally achieve.

4. FPoS Server — The Infrastructure System Responding to the Library

Counterpart to the FPoS Library (client side) is the **FPoS Server** operated by myFinTech. It handles the foundational trust service functions: certificate issuance and revocation management as an Accredited CA, key lifecycle management, signature verification, and preservation of audit trails. The tight integration between the client-side FPoS Library and the server-side FPoS Server completes a consistent trust infrastructure from the end user's device all the way to the CA.

- **Accredited CA Functions:** Certificate issuance and operation compliant with the Act on Digital Signatures
- **Identity Verification & Key Management Infrastructure:** Identity verification using the Public Personal Authentication Service (JPKI), etc.; key provisioning, renewal, and revocation to SIM/Secure Element
- **Authentication & Signature Verification API:** Easily callable from business systems at financial institutions, local governments, medical institutions, etc.

- **Data Linkage Connection Function:** Connects to Mebuku Ground's data linkage platform; responsible for the issuance, management, and verification of users' opt-in permissions signed with certified digital certificates
- **Audit & Evidence Management:** Long-term storage and verifiability suitable for regulated industries

5. Shareholder Structure — Strategic Alliance of Telecommunications, Financial Infrastructure, and Consulting

myFinTech has a strategic shareholder structure comprising leading companies in telecommunications, financial infrastructure, and consulting in Japan. Each shareholder brings their domain expertise and customer base to myFinTech, developing a structure that broadly supports the social implementation of FPoS.

Shareholder	Business Domain / Role in myFinTech
Japan Communications Inc. (Lead Shareholder)	A telecommunications carrier operating its own eSIM infrastructure from November 2026 as a neo-carrier. Provides FPoS — which stores private keys in the secure hardware area built into smartphones — as well as FPoS IoT, which utilizes the Secure Element within eSIM.
SocioFuture, Ltd. (formerly ATM Japan Ltd.)	A domestic leader in ATM operations and financial IT for financial institutions. Applies its high-reliability operational know-how and financial institution network to FPoS financial use case implementation.
Accenture Japan Ltd.	Global integrated consulting firm.
Deloitte Tohmatsu LLC	Integrated consulting firm. Provides expertise in trust service governance, regulatory compliance, and risk management framework development.

The presence of these four companies — a telecommunications carrier (JCI), financial infrastructure (SocioFuture), and global consulting firms (Accenture and Deloitte Tohmatsu), each with a top-tier track record in Japan in their respective domains — as shareholders demonstrates that myFinTech is **designed as an operating company entrusted with Japan's societal trust infrastructure**, not merely as a startup.

6. Strategic Positioning in Japan Communications Vision 2030

JCI is advancing its "Restoring 'Trust' to Digital" initiative under Vision 2030. Within this, myFinTech is the **provider of the FPoS platform** — handling both CA operations and the library/server — and is an indispensable entity for realizing Vision 2030.

- **Finance:** Next-generation authentication infrastructure to realize Zero Fraud Banking
- **Healthcare:** Trust infrastructure for digital prescriptions and health data linkage
- **Government & Regional DX:** Authentication and signature infrastructure for regional society OS implementation
- **IoT & Mobility:** Device trust originating from Secure Element

Japan Communications, through myFinTech, will continue to actively expand its business as the provider of hardware-origin trust to all of society. We look forward to sequential announcements from myFinTech regarding specific service launches, partnership agreements, and more. We appreciate your continued attention.

【Company Overview of my FinTech】

Company Name	my FinTech Inc.
Location	Minato-ku, Tokyo
Business Description	Operation of an accredited certification authority under the Digital Signature Act / Development and provision of FPoS Library and FPoS Server / Provision of related trust services
Shareholders	Japan Communications Inc. (Lead Shareholder) / SocioFuture, Ltd. / Accenture Japan Ltd. / Deloitte Tohmatsu LLC
Parent Company	Japan Communications Inc. (Tokyo Stock Exchange Prime Market: 9424)

End

About Japan Communications Inc. (JCI)

Japan Communications Inc. (JCI), founded in 1996, is a pioneer who created the MVNO market and has brought innovation to the telecommunications industry. While JCI has established a stable profit model in their main business, simple and rational mobile communication services, JCI is aiming for

further growth. JCI has strengths in patented technologies such as the mobile leased line "Closed SIM-to-SIM Communication" and the digital authentication technology "FPoS," and is focusing on providing mobile communication services and digital authentication infrastructure based on the authentication technology. The PCI DSS-certified mobile leased line is adopted by high-security sectors, such as police and bank. The FPoS supports security at the highest global standards and convenience. Under the mission of "carrying bit in safety and security," JCI is aiming for developing social infrastructure such as secure mobile environment beyond national borders and is working on sustainable growth and improving corporate value.