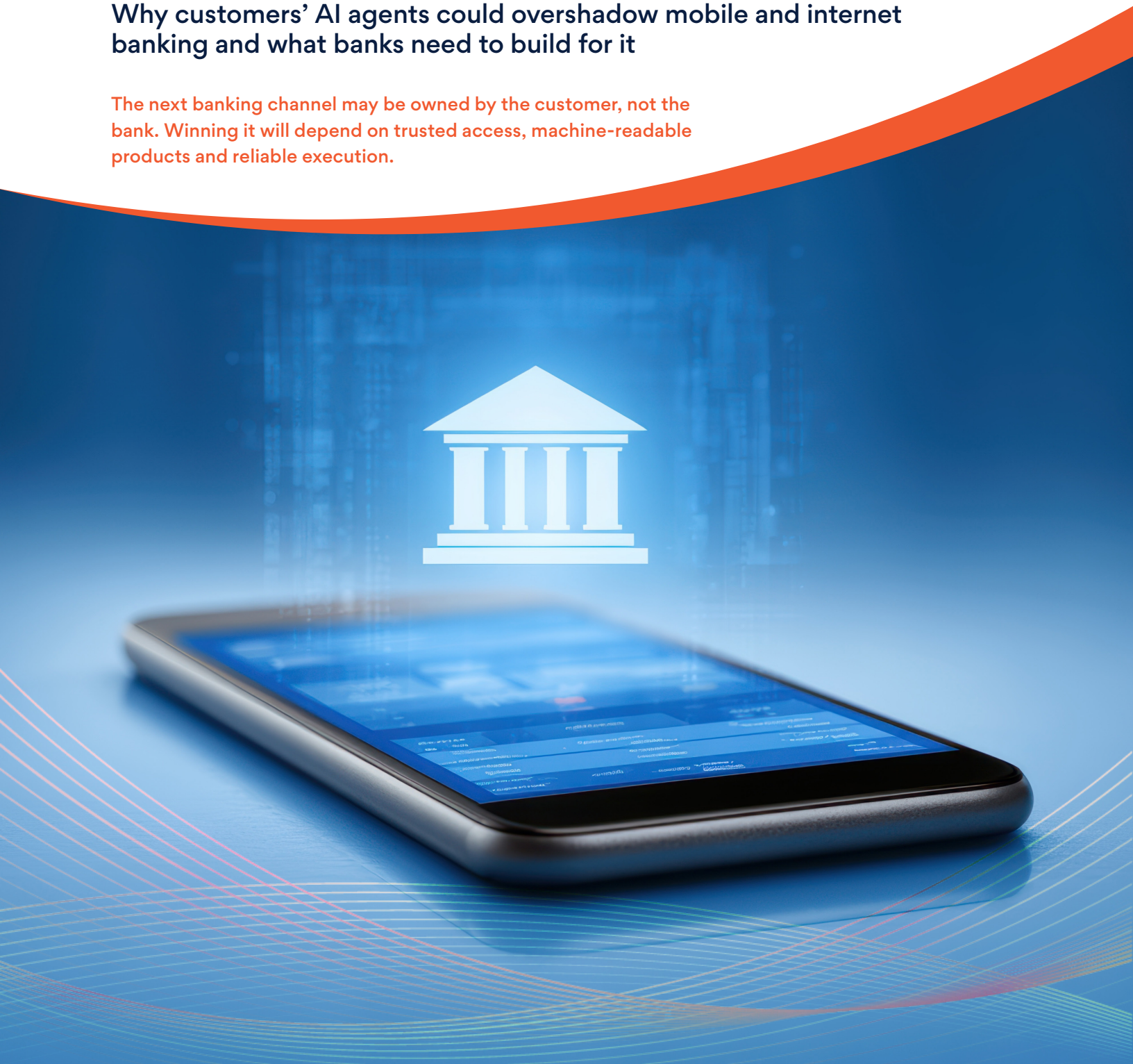
Persistent

White Paper

THE NEXT BANKING CHANNEL ISN'T AN APP

Why customers' AI agents could overshadow mobile and internet banking and what banks need to build for it

The next banking channel may be owned by the customer, not the bank. Winning it will depend on trusted access, machine-readable products and reliable execution.



SECTION 1

Executive summary



Every generation of banking has been shaped by a dominant customer channel. Branches enabled face-to-face relationships. Internet banking moved routine servicing to the web. Mobile apps made banking continuously accessible. A fourth channel is now emerging: the customer's own AI agent.

Instead of opening an app and navigating screens, customers may increasingly state an intent and allow an agent to act across accounts, institutions and payment rails. If agents gain trusted access to deposit accounts, they could become the starting point for a large share of everyday banking interactions. This would shift control of the interface away from the bank and toward the customer or the platform that provides the agent.

For banks, this is not simply another form of automated traffic. It is a channel strategy question. Products must become machine-readable. Agent identity and delegated authority must be verifiable. Policy controls must run before execution. Availability must reflect funds across conventional and tokenized deposits. Audit evidence must explain who acted, on whose behalf, under which mandate and with what result.

This whitepaper outlines the strategic implications of agent-enabled banking, the six challenges banks must address, and an architecture centered on a dedicated agent gateway. It also maps the emerging standards landscape, highlights US regulatory considerations and provides a practical readiness checklist.

What bank leaders should take away

- **Treat agent access as a strategic channel.** Assign ownership, create a roadmap and fund it with the seriousness previously applied to mobile banking.
- **Build a delegated-access layer.** Place agent identity, mandates, policy decisions and evidence between agents and existing systems.
- **Keep execution control with the bank.** Let the agent express intent while the bank determines the appropriate rail, ledger and controls.
- **Design for machine-speed behavior.** Assume continuous activity, frequent balance queries, retries and transactions outside business hours.
- **Prepare before customer demand scales.** Resolve dispute handling, third-party risk, data access and operating-model questions before the first material incident.

© 2026 Persistent Systems Ltd.All rights reserved.

SECTION 2

Banking's fourth channel

The branch, the website and the mobile app were designed and controlled by the bank. The bank defined the journey, placed its products and owned the brand experience. The agent channel is different. It belongs to the customer or to the platform that provides the customer's agent. The bank participates in the interaction, but it does not host it.

A customer may simply state an intent such as "keep my operating account at $50,000 and put the rest to work" or "pay these supplier invoices before the discount expires." The agent then interprets that intent, evaluates options and initiates action. If this model gains direct, trusted access to deposit accounts, it could overshadow mobile and internet banking for many routine interactions, much as mobile overshadowed the branch for routine servicing.

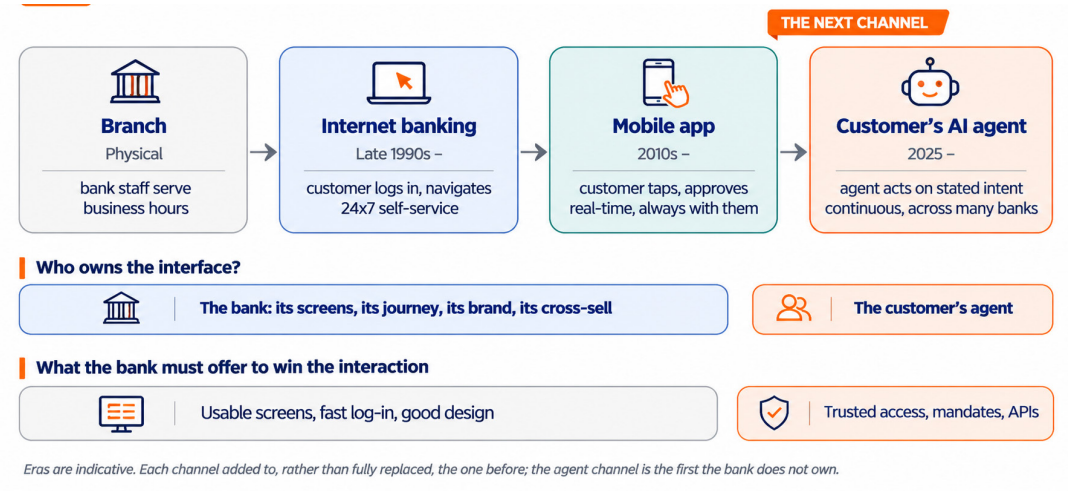


Figure 1. Banking's channel evolution: the agent is the first channel the bank does not own

Characteristic	Internet banking	Mobile app	Customer's AI agent
Interface owner	Bank	Bank, distributed through app stores	Customer or agent platform
Customer engagement	Logs in and navigates	Opens, taps and approves	States intent once, then the agent acts
Interaction pattern	Occasional sessions	Frequent, short sessions	Continuous and machine-initiated
Scope	One bank	One bank	Potentially many banks at once
Authentication	Password, then MFA	Device binding and biometrics	Agent identity plus delegated mandate
Basis of competition	Functionality	Design, speed and convenience	Trust, API quality, rates and reliability

© 2026 Persistent Systems Ltd.All rights reserved.

Why agents could overshadow mobile and internet banking

- **Intent replaces navigation.** Customers no longer need to learn each bank's menus. The effort required to use a bank falls to the effort required to state an objective.
- **One agent can work across many banks.** An agent can potentially see and act across every institution a customer uses, something no single bank app can do.
- **The channel is always on.** Agents can act continuously and outside business hours, aligning with 24x7 payment rails and tokenized deposits.
- **The ecosystem is already forming.** Card networks have introduced agent frameworks, open-banking APIs are moving toward common standards and early agent payments have run on bank rails.

Adoption will not be frictionless. Customer trust, liability questions and regulation will slow progress. Complex advice, lending decisions and moments of financial stress will continue to require human engagement. However, mobile did not need to replace the branch to redefine retail banking. It only needed to become the place where most routine interactions occurred. Agents could follow the same path.

SECTION 3

From checkout to account



The channel is arriving first at the merchant. Agentic commerce has largely focused on an AI agent that finds a product and completes checkout. Payment networks have responded with frameworks that help merchants recognize approved agents and validate payment credentials. These mechanisms address an important merchant question: is this agent legitimate and does it carry a valid payment credential?

They do not fully address the bank's challenge. A customer who trusts an agent to make a purchase may soon expect the same agent to move money between accounts, pay a supplier invoice from a business demand deposit account, sweep idle balances into a tokenized deposit wallet or rebalance liquidity outside business hours. At that point, the agent is no longer a shopper. It is a delegated operator of a deposit account.

The strategic shift occurs when the agent moves from completing a checkout to operating the account that holds the money.

The Persistent Meridian Trusted Agent Toolkit provides a foundation for assessing this shift, including the trusted-agent ecosystem, customer control planes and associated regulatory considerations. The following sections extend that foundation into the channel capabilities a US bank needs before opening agent access safely.

© 2026 Persistent Systems Ltd.All rights reserved.

SECTION 4

Six challenges agents introduce



1. Identity: Whose agent is this?

Most third-party account access still relies, at least in part, on credential sharing or screen scraping. Neither method reliably tells the bank whether it is dealing with the customer, an authorized agent or an attacker. An agent needs a verifiable identity that is distinct from the customer's login, and the bank must bind that identity to a specific customer relationship.



2. Authority: What may it do?

A password grants access to everything the customer can do. Delegation should grant much less: specified accounts, payee types, amount and velocity limits, a time window and conditions that require the agent to return to the customer for approval. Without an explicit, machine-readable mandate, the bank cannot distinguish an instruction that is within the customer's intent from one that is merely technically possible.



3. Availability: What can it see?

An agent must reason across multiple availability states, including deposit holds, card authorizations, ACH return-window exposure, escrowed tokens, submitted but not final transfers and frozen wallets. An agent that reads only the DDA ledger balance or only the wallet will make decisions using partial data, often quickly and repeatedly.



4. Finality and reversibility

Instant rails and tokenized transfers can become final within seconds. A person who makes a mistake may notice it before the next payment. An agent that misinterprets an instruction may execute many transactions before the issue is detected. Controls must therefore operate before the state change, not only during a later fraud review.



5. Liability and consumer protection

Regulation E addresses authorized transfers where a consumer has furnished an access device to another person, but its application to AI agents remains unsettled. Banks need a documented position on agent-initiated errors, revocation and disputes before the first complaint arrives.



6. Scale, hours and operational load

Agents do not respect cutoff times. They may query balances more often than people, retry on failure and act outside business hours. Rate limits, stand-in processing, liquidity monitoring and servicing tools must be designed for a population of tireless, automated customers.

© 2026 Persistent Systems Ltd.All rights reserved.

SECTION 5

The required channel infrastructure

Mobile banking required a dedicated layer of APIs, device binding and fraud controls between the app and the core. The agent channel needs an equivalent. The answer is not to rebuild the core or ledger. It is to add a distinct delegated-access layer between agents and the bank's existing systems: an agent gateway through which every agent instruction must pass.

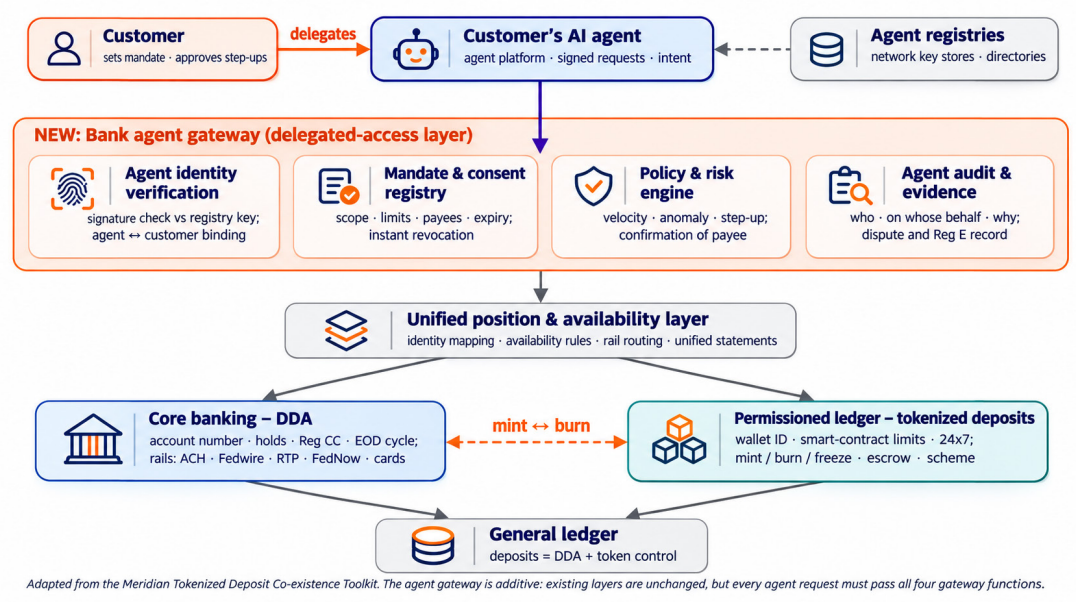


Figure 2. Agent-ready reference architecture extending the toolkit's coexistence model

The four functions of the agent gateway

- **Agent identity verification.** Verify the cryptographic signature on every request against a trusted key registry and bind the verified agent to a specific customer and relationship. Refuse unverified or unbound agents rather than degrading access.
- **Mandate and consent registry.** Store each customer's delegation as structured data, including scope, accounts, payees, transaction and cumulative limits, expiry and step-up conditions. Revocation must take effect immediately and apply to open sessions and pending instructions.
- **Policy and risk engine.** Evaluate every instruction against the mandate, customer history and bank limits. The decision should be allow, step up to the customer or decline with a reason the agent can interpret. Confirmation of payee, cooling-off periods for new payees and anomaly detection belong here.
- **Agent audit and evidence.** Record who acted, on whose behalf, under which mandate version, with what stated intent and with what result. This creates the evidence base for disputes, Regulation E investigations, suspicious activity decisions and examiner questions.

Two capabilities behind the gateway become nonnegotiable. A unified position and availability layer must present one available-funds figure across conventional and tokenized pockets and include clear as-of timestamps. Rail-aware routing must remain with the bank. The agent expresses intent, while the bank selects the rail or ledger based on amount, urgency, reach and reversibility.

© 2026 Persistent Systems Ltd.All rights reserved.

SECTION 6

How an agent-initiated payment flows



A safe flow begins with authority created by the customer directly with the bank. The agent references that mandate, but it does not assert or define it. Each instruction then passes through identity verification, mandate checks, availability assessment, policy evaluation, execution and evidence capture.

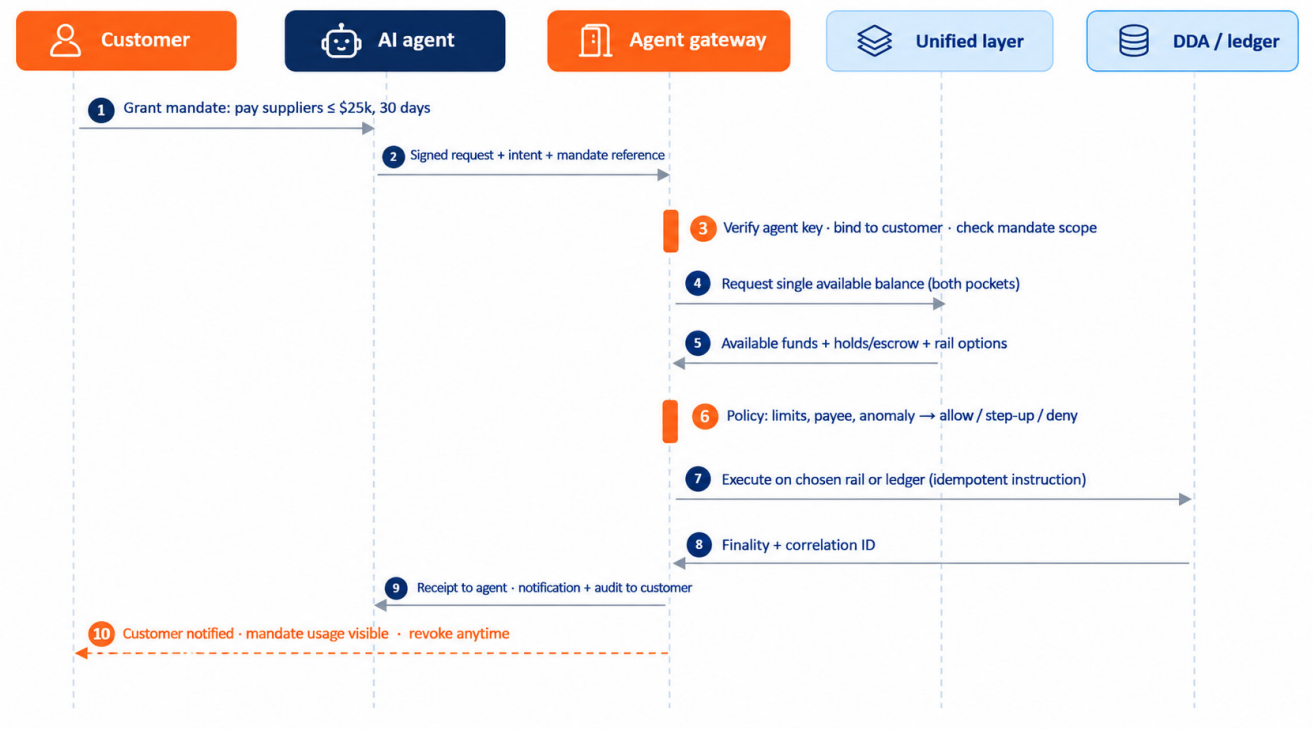


Figure 3. Sequence for an agent-initiated payment

Three design points stand out

- **The customer creates the mandate with the bank.** The agent only references the mandate, reducing the risk that delegated authority is self-asserted.
- **Availability includes constraints, not just a balance.** Policy decisions should reflect holds, pending states, escrow and other restrictions before execution.
- **Every execution is idempotent and traceable.** An instruction identifier and correlation ID allow retries without double payment and connect the request, decision, execution and notification.

© 2026 Persistent Systems Ltd.All rights reserved.

SECTION 7

The standards landscape

No single standard covers the full problem. Frameworks published since 2025 address different layers of the stack and are best understood as complementary building blocks. Most production flows are likely to use more than one standard or protocol.

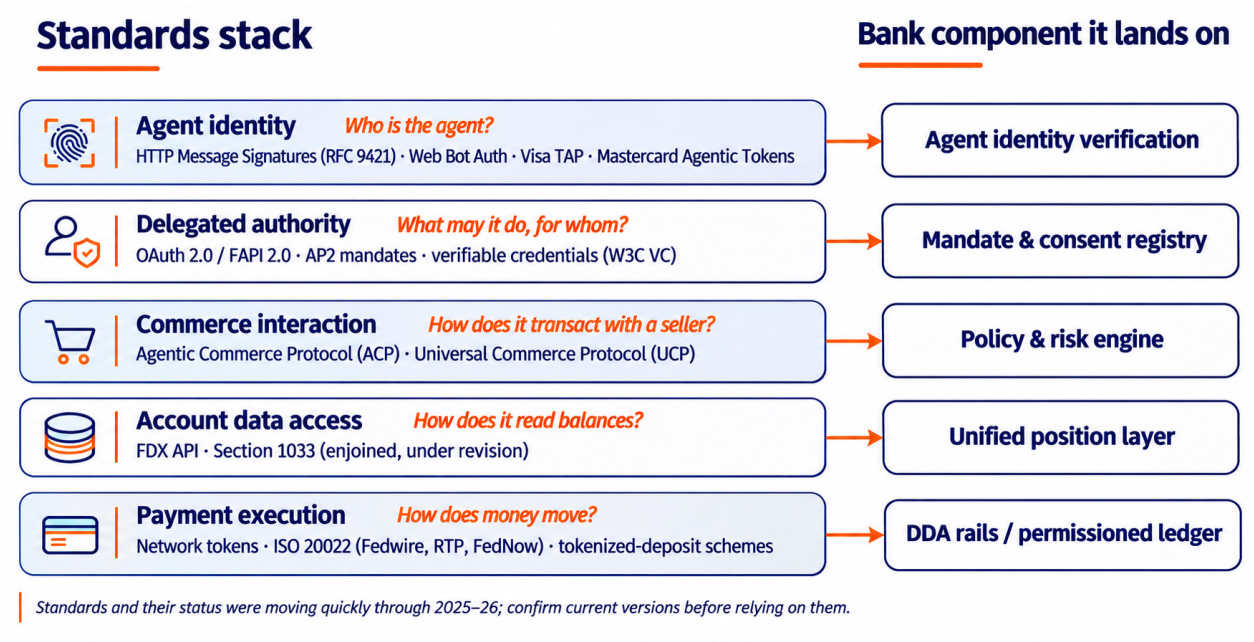


Figure 4. Standards stack mapped to bank components

Standard or framework		Relevance to banks	Publication status
HTTP Message Signatures, RFC 9421; Web Bot Auth	Agent identity	Signed HTTP requests that can support bank APIs	RFC published; Web Bot Auth remains in development
Visa Trusted Agent Protocol / Intelligent Commerce	Agent identity	Agent recognition, intent and payment identifiers	Launched in 2025
Mastercard Agent Pay / Agentic Tokens	Identity and authority	Agent-scoped network tokens and issuer controls	Rules and rollout activity reported in 2026
Google Agent Payments Protocol, AP2	Delegated authority	Signed mandates expressing user intent	Open source and evolving
Agentic Commerce Protocol; Universal Commerce Protocol	Commerce interaction	Agent-to-merchant checkout payloads	In development
OAuth 2.0 and FAPI 2.0	Delegated authority	Scoped, consented bank-grade API access	FAPI 2.0 Security Profile final
FDX API	Account data access	Permissioned financial data access	In wide use
CFPB Section 1033 rule	Data access regulation	Consumer-authorized access requirements	Status requires legal verification before publication
ISO 20022 and scheme rules	Payment execution	Structured execution messages and routing inputs	In force, with scheme-specific variation

The practical implication is to build the gateway around open primitives such as signed requests, scoped consent, structured mandates and verifiable credentials. Each network or protocol can then be treated as an adapter rather than as the architecture itself.

© 2026 Persistent Systems Ltd.All rights reserved.

SECTION 8

Regulatory considerations for US banks



Agents do not remove existing banking-law obligations. They add new questions about how authority is expressed, how activity is attributed and how customers are protected when automated actions become fast and final.

- **Consumer protection and Regulation E.** Define how a mandate maps to authorization, how the customer revokes it and how errors are investigated when an agent acts within or outside its mandate.
- **BSA/AML and KYC.** The agent is not the customer, but its behavior forms part of the customer's account activity. Monitoring should attribute activity to both the customer and the agent, while the provider should be assessed as a distinct risk factor.
- **Third-party risk management.** Agent platforms acting on accounts at scale may create material third-party risk. Due diligence, ongoing monitoring and exit planning should reflect the criticality of the service.
- **Data access.** Banks should expect evolving rules and industry conventions to shape what agents may access, under what terms and with what customer controls.
- **UDAAP and disclosure.** Customers must understand what they delegated, what the bank can stop and which balances are insured.
- **Product perimeter.** The gateway should enforce distinctions between tokenized deposits and payment stablecoins rather than leaving those decisions to the agent.

SECTION 9

Readiness checklist



Banks can assess readiness across the following dimensions using a five-level scale: absent, ad hoc, defined, managed and optimized.

Dimension	Question for the design review
Channel strategy	Is agent access owned as a channel, with an executive owner, roadmap and investment case alongside mobile and online banking?
Discoverability	Are deposit products, rates, fees and limits available in machine-readable form that agents can compare?
Deposit behavior	Have liquidity runoff assumptions been revisited for balances that agents can move 24x7 in response to rate signals?
Agent identity	Can the bank cryptographically verify an agent on every request and bind it to a customer and relationship?
Mandates	Is delegation stored as structured, versioned data with limits, expiry and immediate revocation?
Single view	Does the agent receive one available-funds figure across DDA and tokenized pockets, including holds, escrow and pending states?
Routing	Does the bank choose the rail or ledger based on amount, urgency, reach and reversibility?
Pre-execution controls	Are limits and payee rules enforced before execution, including on-ledger constraints where applicable?
Idempotency	Can an agent retry safely without double payment across both core and ledger?
Evidence	Can the bank reconstruct who acted, on whose behalf, under which mandate version and why?
Disputes	Is there a documented Regulation E and dispute process for agent-initiated transfers?
Operations	Are rate limits, 24x7 stand-in processing and servicing screens designed for automated customers?
Governance	Has the board approved a risk assessment covering agent access, third-party risk and the product perimeter?

© 2026 Persistent Systems Ltd.All rights reserved.

SECTION 10

A practical path forward



Banks do not need to expose every account or transaction type on day one. A controlled path can begin with narrow use cases and strong limits, then expand as identity, mandate, policy and evidence capabilities mature.

- **Establish channel ownership.** Name the business and technology leaders responsible for agent access, then define the target customer segments and initial use cases.
- **Create the trust foundation.** Implement agent verification, structured mandates, revocation and a complete evidence model before enabling high-risk actions.
- **Unify position and availability.** Ensure decisions reflect conventional deposits, tokenized deposits, holds, pending transactions and escrow states.
- **Pilot constrained transactions.** Start with limited accounts, payees, transaction values and operating conditions, with explicit step-up rules.
- **Operationalize governance.** Integrate disputes, third-party risk, financial crime monitoring, resilience and board reporting into the channel operating model.
- **Expand through adapters.** Support emerging network and agent protocols through modular adapters while keeping policy and execution control inside the bank.

Conclusion: Plan for the channel, not just the traffic



Internet banking and mobile apps rewarded banks that treated them as strategic channels early and penalized those that treated them only as cost-saving additions. Customers' AI agents could represent an even larger shift because, for the first time, the dominant interface may not belong to the bank.

Banks that build the required infrastructure now, including verified agent identity, structured mandates, pre-execution policy, a complete evidence trail and a single view of funds across conventional and tokenized deposits, can position themselves as institutions that agents can work with reliably. Banks that delay may be forced to choose between blocking agents their customers depend on and tolerating access they cannot adequately see or control.

The Persistent Meridian Trusted Agent Toolkit provides a foundation for understanding the trusted-agent ecosystem, customer control planes and associated regulatory treatment. The next step is to translate that foundation into a bank-specific channel strategy, target architecture and readiness roadmap.

Call to action:
Request a Meridian Trusted Agent Toolkit walkthrough and readiness assessment.

© 2026 Persistent Systems Ltd.All rights reserved.

Author



Parminder Beny Bansil

BFSI Domain Consulting Global Head

Parminder Bansil leads BFSI domain consulting at Persistent, working with financial institutions on business and technology transformation. He brings deep industry expertise to shape domain-led solutions, modernization priorities and AI-led initiatives.

Explore: Persistent's approach to maximizing AI impact at enterprise scale.

Learn More

About Persistent

Persistent Systems (BSE: 533179 and NSE: PERSISTENT) is a global services and solutions company delivering AI-led, platform-driven Digital Engineering and Enterprise Modernization to businesses across industries. With over 27,500 employees located in 21 countries, the Company is committed to innovation and client success. Persistent offers a comprehensive suite of services, including software engineering, product development, data and analytics, CX transformation, cloud computing, and intelligent automation. The Company is part of the MSCI India Index and is included in key indices of the National Stock Exchange of India, including the Nifty Midcap 50, Nifty IT, and Nifty MidCap Liquid 15, as well as several on the BSE such as the S&P BSE 100 and S&P BSE SENSEX Next 50. Persistent is also a constituent of the Dow Jones Best-in-Class World Index. The Company has achieved carbon neutrality, reinforcing its commitment to sustainability and responsible business practices. Persistent has also been named one of America's Greatest Workplaces for Inclusion & Diversity 2025 by Newsweek and Plant A Insights Group. As a participant of the United Nations Global Compact, the Company is committed to aligning strategies and operations with universal principles on human rights, labor, environment, and anti-corruption, as well as take actions that advance societal goals. With 468% growth in brand value since 2020, Persistent is the fastest-growing IT services brand in 'Brand Finance India 100' 2025 Report.

USA

Persistent Systems, Inc.
1731 Technology Drive
Suite 700, San Jose
CA 95110
Tel: +1 (650) 481 9180
Email: Info@persistent.com

India

Persistent Systems Limited
Bhageerath, 402
Senapati Bapat Road
Pune 411016
Tel: +91 (20) 6703 3000
Fax: +91 (20) 6703 6003

Persistent
Re(AI)magining™ the World

www.persistent.com

© 2026 Persistent Systems Ltd.All rights reserved.