Presented by: Agentic AI Foundation

MCP Dev Summit Nairobi

Speaking at MCP Dev Summit Nairobi 2026

Modernising Without Rebuilding: MCP, AI Integration & Governance for Fintech and Telco

Nairobi, Kenya

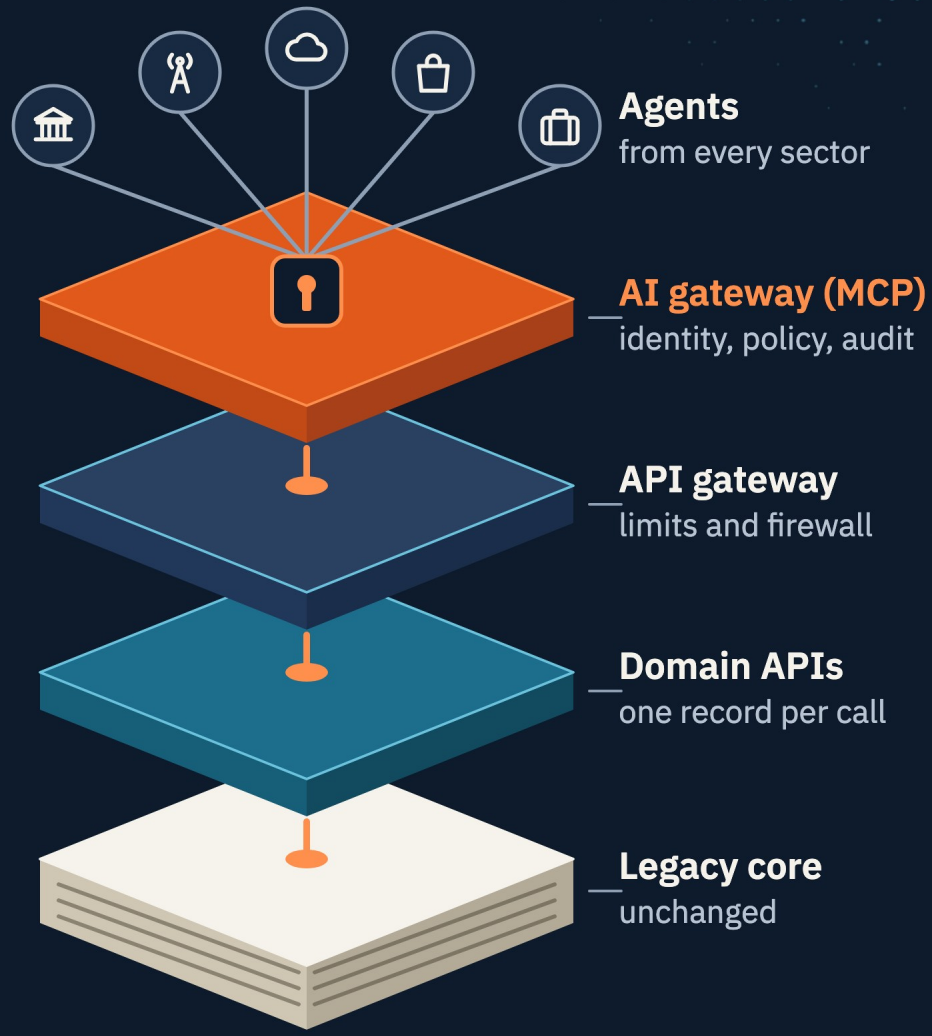


Bobby Kimutai

TECHNOLOGY LEADERSHIP BRIEFING · 25 MINUTES

Modernising Without Rebuilding

Unlocking AI Without Disrupting the Core



CONTENTS

01 Big-bang replacement
Slides 3–4

02 What's at stake
Slides 5–8

03 The governed middle path
Slides 9–13

04 Autonomy across sectors
Slides 14–19

05 Regulators and funding
Slides 20–24

06 References
Slides 25–27

Bobby Kimutai · MCP Dev Summit Nairobi 2026 · 19–20 November

THE TRACK RECORD

The record of full core replacement

~30%



of core banking transformations in the past decade completed a full migration of ledgers and products to a new system

75%

how far teams underestimate migration time, at the upper end of McKinsey's range

Replacing the core in one programme was the default answer of the last decade. It has the weakest evidence behind it.

Source: [1] McKinsey & Company

CASE IN POINT · UK AND KENYA

Core migrations have stumbled, in the UK and Kenya

A UK RETAIL BANK · APRIL 2018

KSh 8.4bn

(£48.65m) in regulator fines in 2022, plus about KSh 5.7bn in redress, for operational-risk, governance and outsourcing failures

One big-bang weekend migration of 5.2 million customers

The board was not shown alternatives

KENYA

KSh 1bn	Tier-one bank, Oct 2024: overdrawn after migration glitches let customers withdraw beyond their balances
3 days	Mid-sized bank, Oct 2024: channels disrupted by a core upgrade; 266,000 customers warned
44 hours	Smaller bank, Oct 2026: planned shutdown for a core upgrade that went to plan

The UK bank's fine alone is about 44 times all CBK fines collected in a year (KSh 191m).

Sources: [2] FCA and PRA · [3] Slaughter and May · [41] TechCabal, TechinAfrica, Kenya Times · [42] CBK, Wise

WHY IT MATTERS

What rides on these systems

7.8%

of Africa's GDP came from mobile technologies in 2025: $240bn, forecast to reach $290bn by 2030

$190bn

added to Sub-Saharan Africa's GDP by mobile money in 2023, up from $150bn in 2022

13m

jobs supported by mobile across Africa, with $45bn in public revenues

That value runs through core banking, billing, mobile-money and commerce platforms: the cores this talk is about.

Sources: [6] GSMA Mobile Economy Africa 2026 · [7] GSMA Mobile Money 2025

THE NEW USER OF YOUR CORE

Agentic AI: fast arrival, high attrition

15%

of day-to-day work decisions made autonomously by 2028, up from 0% in 2024

40%+



of agentic AI projects cancelled by the end of 2027, on escalating costs, unclear business value or inadequate risk controls

Both figures are Gartner forecasts. Read together, they say adoption is coming and that the losses will come from cost, value and control.

Source: [8] Gartner, 25 June 2025

FICTITIOUS COMPANY · REAL MARKET DATA

Nuruka and the market it serves

INVENTED FOR THIS TALK

Nuruka

A Kenyan software company running checkout, stock and bookings for thousands of businesses.



Retailers



Online sellers



Hotels and lodges

A multi-tenant cloud platform, 15 years old

Every sale and refund must reach eTIMS

The board has ruled out a rebuild

Its fear: one agent exposing every business's customers

WHAT DRIVES AND THREATENS ITS MARKET

2.7m	international visitors to Kenya in 2025, up 9%; tourism earned about KSh 500bn
750,915	taxpayers on KRA eTIMS by June 2026; tax returns are now checked against it
11.1bn	cyber threat events detected in the year to June 2026, up 29%
9,061	complaints to the Data Commissioner; breaches must be reported within 72 hours

Sources: [4] Communications Authority · [25] Data Commissioner · [26] Tourism Ministry · [27] KRA

REGULATION

Where binding control of AI comes from today

AI laws: deferred or stalled

EU: high-risk duties deferred to 2 December 2027

Kenya: AI Bill 2026 rejected in Senate committee, October 2026

South Africa: draft AI policy withdrawn in April 2026 over fictitious references

Nigeria: Digital Economy Bill still pending

Already binding today

Individual rights: GDPR Art. 22, Kenya DPA s.35, Nigeria NDPA s.37, South Africa POPIA s.71

Prudential supervision: CBK draft instruments on model risk, data governance and third parties

Operational resilience: DORA in the EU since 17 January 2025

Kenyan banks, per CBK: 50% use AI · 59% of adopters have no AI policy · 93% want guidance

Sources: [9] CBK · [10] EU · [11] The Star · [12] statutes · [13] CBK drafts · [24] SA, Nigeria

THE MIDDLE PATH

No agent touches the core. Agents reach it the way every other application does: through governed APIs, inside the gateway and identity systems you already run.

ARCHITECTURE

One governed route from agent to core

WHO ASKS
Agents
Own identity, human sponsor

- Customer assistants
- Staff co-pilots
- Partner and AI-platform agents

CONTROL POINT
MCP layer
Inside your gateway and identity provider

- Tool catalogue and allowlist
- Scopes per tool
- Policy checks
- Tool-call audit log

THE CONTRACT
Domain APIs
The contracts you already publish

- TM Forum Open APIs
- Banking APIs: accounts, payments
- Commerce APIs: orders, stock, bookings

WHAT STAYS PUT
Legacy core
Systems of record, unchanged

- Core banking and mobile money
- Billing and OSS/BSS
- ERP, POS, orders and bookings

No direct database access. Every call is authenticated, scoped, policy-checked and logged.

Sources: [18] Microsoft · [19] TM Forum · [20] TM Forum Inform · [28] AWS · [29] Google Cloud

THE PROTOCOL

What makes MCP fit the enterprise estate

9 DECEMBER 2025

Neutral governance

Donated to the Linux Foundation's Agentic AI Foundation. Co-founders: Anthropic, Block and OpenAI. Platinum members: AWS, Bloomberg, Cloudflare, Google and Microsoft.

SPEC 2025-11-25

Enterprise authorization

Enterprise-Managed Authorization puts the corporate identity provider in control of which MCP servers a user's client can reach, with step-up consent for wider scopes.

SPEC 2026-07-28

Gateway-friendly transport

A stateless core, with headers that let gateways route and police calls without parsing bodies. Azure, AWS, Apigee and Kong gateways expose existing APIs as MCP tools.

The selling point is the authorization and transport work of the past year. The download counts matter less.

At donation: 10,000+ active public servers and 97M+ monthly SDK downloads, as reported by Anthropic.

Sources: [14] Anthropic · [15] Linux Foundation · [16] MCP specification · [18] Microsoft · [28] AWS · [29] Google



CONTROL

Controls at the tool layer, never prompts alone

Tool descriptions and tool outputs enter the model's context as trusted text. A model can be steered by the data it reads.

A malicious package, postmark-mcp, silently BCC'd every email an agent sent.

OWASP's MCP Top 10 lists token mismanagement, scope creep, tool poisoning and shadow servers.

Agent identity

Each agent has its own identity and a human sponsor. Tenant and user context travel outside the model.

Least privilege

Short-lived, audience-bound tokens, scoped per tool. No token passthrough.

Policy enforcement

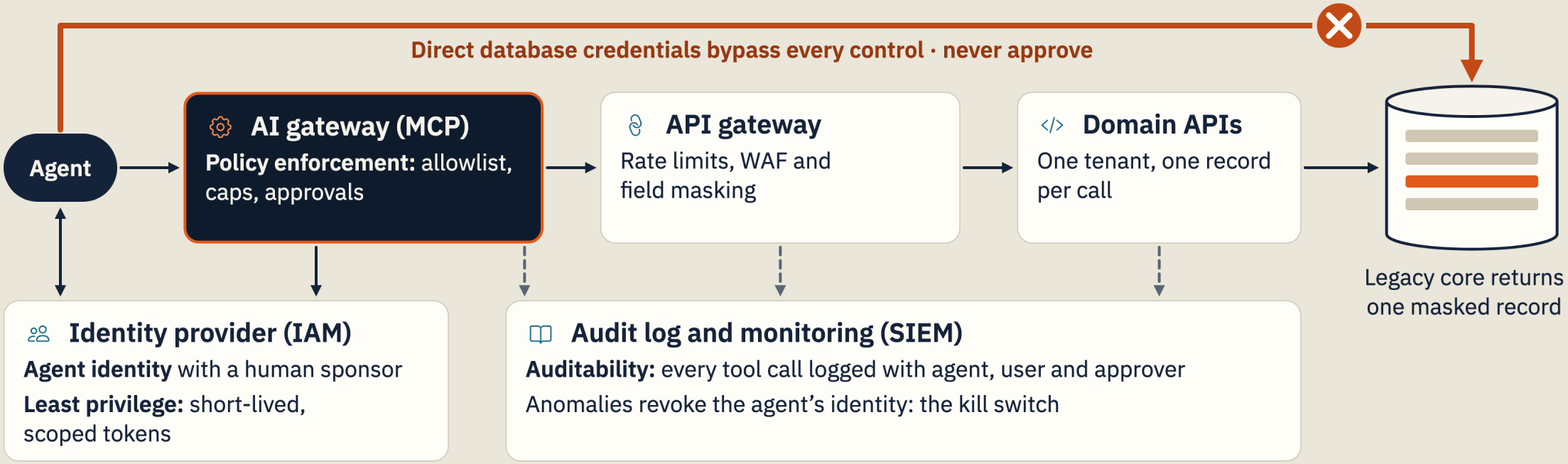
Limits and thresholds enforced as code at the gateway and the server.

Auditability

Immutable logs of every tool invocation, with the approver recorded.

Sources: [17] OWASP MCP Top 10 · [18] Microsoft · [31] AWS, MoEngage case

What a compromised agent could reach



Only the AI gateway is new. It shrinks the blast radius; the 72-hour breach notice still applies.

Sources: [17] OWASP · [18] Microsoft · [20] TM Forum · [25] Data Commissioner · [28] AWS · [31] MoEngage

GRADUATED AUTONOMY

Three approaches to autonomy

	1 · Read-only	2 · Human in the loop	3 · Bounded autonomy
The agent	Retrieves, summarises and recommends; changes nothing	Prepares the action; a person approves before it runs	Acts alone within thresholds, rate limits and time windows
Controls	Read scopes, tool allowlist, masking, full logging	Approval step, step-up scopes, approver in the audit trail	Policy-as-code, per-agent identity, value caps, kill switch
Regulatory anchor	Data-protection and logging duties	Automated-decision rights: Art. 22, s.35, s.37, s.71	Operational resilience, model risk and third-party risk

Write access is added only after the previous stage has produced its evidence.

Synthesis of sources [12] [13] [16] [19] [21]

ACROSS SECTORS

Where each approach fits, by sector

Sector	1 · Read-only	2 · Human in the loop	3 · Bounded autonomy
Banking and fintech	Balance and statement questions, fraud-alert triage	Credit decisions, loan restructuring, disputes	Card freeze on a fraud signal, capped fee waivers
Telco	Bill and usage explanation, fault diagnosis	Order changes, service activation, retention offers	Closed-loop fault fixes within defined domains
Software, cloud and AI	Incident and log summaries, tenant usage questions	Access grants, configuration changes, deployments	Restarts and scaling within quotas, ticket routing
E-commerce and retail	Order tracking, stock and price lookup	Refunds above a threshold, markdowns, supplier orders	Small refunds and vouchers under a cap, restocks in budget
Travel and hospitality	Availability, itinerary and booking status	Changes with fees, group bookings, compensation	Same-rate rebooking, late check-out within policy

Examples, not prescriptions: a use case moves right only when its evidence does.

Illustrative fits, synthesised from sources [19] [20] [21] [28] [29] [30] [31] [32] [33] [34] [35] [36] [37] [38]

Where adopters stand today

GLOBAL BANKING

- Grasshopper, Mercury and Danske: read-only MCP access to account data
- Nymbus: a core-banking MCP server with 19 tools, role-based access and audit
- Griffin: account opening and payments, in a sandbox only

TELCO

- TM Forum AI-native ODA, June 2026: a governed execution layer on Open APIs
- SK Telecom Catalyst: agents use TMF640, TMF677 and TMF629, never the database
- Cerillion 26.2: MCP and A2A servers over its Open APIs

AFRICAN MARKETS

- Kenya: 66% of commercial banks have adopted AI; credit scoring leads
- Kenya: about 84% of commercial banks have adopted APIs, the base this path needs
- No public African MCP production case was found in this research

Public bank MCP servers are read-only or sandboxed. Write actions sit behind role-based access and audit.

Sources: [9] CBK · [19] TM Forum · [20] TM Forum Inform · [21] company announcements · [22] Cerillion

Where adopters stand today

SOFTWARE, CLOUD AND AI

AWS and Google gateways turn existing APIs into MCP tools, late 2025

Salesforce: hosted MCP servers generally available, April 2026

MoEngage: about 400 internal APIs serve 10 agents, each scoped by policy

MOST COMMON USE

Internal co-pilots over existing APIs: support, operations and customer-data questions

E-COMMERCE AND RETAIL

Open protocols: ACP (OpenAI and Stripe, 2025) and UCP (Google, Shopify, Walmart, 2026)

Walmart: in-chat checkout converted at a third of its website's rate

Amazon v. Perplexity: a browser-driven shopping agent ended up in court

MOST COMMON USE

Product discovery and catalogue search inside AI assistants

TRAVEL AND HOSPITALITY

Expedia and Booking.com: apps in ChatGPT built on MCP, October 2025

Sabre: an MCP server over its existing travel APIs, September 2025

Kiwi.com: MCP flight search returns dozens of options, not thousands

MOST COMMON USE

Trip planning and flight and hotel search; booking ends on the company's own site

Discovery is opening up fast. Checkout, booking and write access stay in each company's own systems.

Sources: software and cloud [28] [29] [30] [31] · commerce [32] [33] [34] [35] [40] · travel [36] [37] [38] [39]

MARKET FACTORS AND MATURITY

African markets: strengths and gaps

WORKING IN YOUR FAVOUR

101.3%	mobile money penetration: 54.0 million subscriptions at June 2026
~84%	of Kenyan commercial banks have adopted APIs
66%	of Kenyan commercial banks already use AI
3	markets with automated-decision rights in force: Kenya, Nigeria, South Africa

GAPS TO CLOSE

59%	of Kenyan AI adopters have no AI policy
93%	asked the Central Bank of Kenya to issue AI guidance
No. 1	AI use case is credit scoring, where CBK has cautioned on fully automated loan decisions
0	dedicated AI laws in force across the same three markets

Kenya is the best-documented market in this research. Treat it as an indicator, not a continental average.

Sources: [4] Communications Authority · [9] CBK survey · [11] The Star · [12] statutes · [24] South Africa, Nigeria



FICTITIOUS COMPANY · NOT A REAL PROGRAMME

Case study: Nuruka's three phases

1 · READ-ONLY

Answer, don't act

Tools over existing APIs answer order, stock and booking questions: one tenant and one masked record per call. AI platforms get catalogue tools only.

Gate evidence: agent identities, tenant-scoped logs, evaluations

2 · HUMAN IN THE LOOP

Draft, then approve

The agent drafts refunds above a business's threshold, booking changes with fees and fraud holds. Staff approve; the platform issues the eTIMS credit note.

Gate evidence: approver on every action, contest route tested

3 · BOUNDED AUTONOMY

Act within limits

Small refunds under a cap each business sets, same-rate rebooking and restocks within budget, with a kill switch for each tenant.

Gate evidence: caps held in policy, rollback and breach drill rehearsed

Nuruka is invented. Its design draws on documented practice: MoEngage (tools scoped per agent, identity outside the model), Walmart (checkout kept in its own systems), Sabre and Kiwi.com (MCP over existing travel APIs). Outcome figures are targets to set, not results.

Sources: [12] Kenya DPA · [27] KRA · [31] MoEngage · [34] Walmart · [37] Sabre · [38] Kiwi.com

SUPERVISORY READINESS

What regulators will ask

PLATFORM

Inventory. Which agents and MCP servers exist, and who approved each one?

Identity. Does every agent have its own identity, a sponsor and least-privilege scopes?

Authorization. Where is policy enforced outside the prompt, and who can change limits?

Human oversight. Which decisions need approval, and how can a customer contest one?

Logging. Are tool calls logged immutably and retained as evidence?

DEVELOPER WORKFLOW AND CHANGE

Change control. How are tool definitions and prompts versioned, reviewed and released?

Testing. Which evaluations and red-team tests run before production?

Incident response. Is there a kill switch, a rollback and a notification path?

Third parties. What due diligence covers MCP servers and model providers?

Governance. Is there an AI policy, and a committee that owns it?

Sources: [2] FCA and PRA · [9] [13] CBK · [10] EU 2026/1744 · [12] statutes · [17] OWASP

THE INVESTMENT DECISION

Funding in stage gates

GATE 1

Read-only tools over existing domain APIs

Release the next gate when agent identities, tool-call audit and evaluation results exist

Budget [__] · Timeline [__]

GATE 2

Human approval in two or three journeys

Release the next gate when the approver trail is complete and customers can contest outcomes

Budget [__] · Timeline [__]

GATE 3

Bounded autonomy for reversible actions

Scale when caps hold in policy, the kill switch is tested and incidents are reported

Budget [__] · Timeline [__]

TECHNOLOGIES TO CONSIDER

MCP support in your API gateway (Azure, AWS, Apigee, Kong); agent IDs in your IdP; SIEM tracing; evaluations

TECHNOLOGIES TO CONSIDER

MCP approval prompts and step-up scopes; your case or ticketing system for approvals; tamper-proof audit storage

TECHNOLOGIES TO CONSIDER

Policy as code (OPA, Cedar); SIEM anomaly alerts; token revocation as kill switch; feature-flag rollback

Each gate leaves a reusable asset in API management and identity, whatever happens to the agent programme.

Rationale: [8] Gartner forecast of 40%+ agentic project cancellations by end-2027

TECHNOLOGY DEPENDENCIES

What each gate builds on

	GATE 1 · READ-ONLY Allowed: read scopes only	GATE 2 · HUMAN APPROVAL Allowed: writes after approval	GATE 3 · BOUNDED AUTONOMY Allowed: writes within caps
Identity	Agent identities in your IdP, each with a sponsor	Step-up scopes: write tokens only after approval	Token revocation as the kill switch, fired by alerts
Control	MCP in your API gateway, with read tools only	Approval prompts routed to your ticketing system	Policy as code (OPA, Cedar) enforces value caps
Evidence	Tool-call tracing into your SIEM	Tamper-proof audit storage, approver recorded	SIEM anomaly alerts on agent behaviour
Quality	Evaluation suite for answers and tool use	Evaluations rerun on every tool or prompt change	Feature flags for staged rollout and rollback
	Exit to Gate 2: identities, audit trail and evaluations in place	Exit to Gate 3: approver on every action, contest route tested	Scale when: caps hold, kill switch tested, incidents reported

Sources: [16] MCP specification · [17] OWASP · [18] Microsoft · [31] AWS, MoEngage case

BALANCE

The counter-arguments

“The layer hides technical debt”

It does not retire the core. Hollowing the core suits a core that stays viable for five to ten years, so plan renewal behind the same APIs.

“MCP security is immature”

Real incidents exist. Allowlist servers through a registry, pin tool definitions and inspect calls at the gateway.

“Agent identity is unfinished”

The IETF grant behind enterprise-managed authorization is still a draft. Anchor on your identity provider so patterns degrade gracefully.

“Evidence of return is thin”

Few audited outcomes exist. MoEngage reports months of work saved; Walmart’s in-chat checkout converted at a third of its site’s rate. Gate spend on your own results.

Sources: [16] MCP specification · [17] OWASP · [23] Capgemini · [31] MoEngage · [34] Walmart

Three takeaways

1. Make the gateway and identity provider the only route from an agent to a system of record.
2. Fund autonomy in three gates, and release each gate on evidence.
3. Design to the rules already in force: automated-decision rights and prudential supervision.

Scan to give feedback

sfeedback.com/hr5xWo

Bobby Kimutai · bobbykimutai@gmail.com · References follow

References

[1] McKinsey & Company, “How to get a core banking transformation right: Eight mistakes to avoid”. mckinsey.com

[2] FCA and PRA, TSB fined £48.65m for operational resilience failings, 20 December 2022. Coverage: cnbc.com

[3] Slaughter and May, independent review of the TSB migration, November 2019. slaughterandmay.com

[4] Communications Authority of Kenya, sector statistics and KE-CIRT/CC reports, to September 2026. Coverage: itnewsafrica.com, techweez.com, tech-ish.com

[5] Central Bank of Kenya, Kenya Financial Sector Stability Report 2025, fraud table. Coverage: businessdailyafrica.com

[6] GSMA, The Mobile Economy Africa 2026, 16 June 2026. gsmaintelligence.com

[7] GSMA, State of the Industry Report on Mobile Money 2025, press release of 8 April 2025. gsma.com

[8] Gartner, over 40% of agentic AI projects to be cancelled by end of 2027, 25 June 2025. Republished: hpcwire.com

[9] Central Bank of Kenya, Survey on Artificial Intelligence in the Banking Sector, 3 July 2025. centralbank.go.ke

[10] Regulation (EU) 2026/1744, Digital Omnibus on AI, Official Journal, 24 July 2026. eur-lex.europa.eu

[11] The Star (Kenya), Senate committee rejects the AI Bill, 15 October 2026. the-star.co.ke

[12] Automated-decision provisions: GDPR Art. 22; Kenya Data Protection Act 2019, s.35; Nigeria Data Protection Act 2023, s.37; South Africa POPIA, s.71. Kenya DPA text

[13] Central Bank of Kenya, revised draft prudential and risk-management instruments, 10 September 2026. centralbank.go.ke

[14] Anthropic, donating MCP and establishing the Agentic AI Foundation, 9 December 2025. anthropic.com

References

[15] Linux Foundation, formation of the Agentic AI Foundation, 9 December 2025. aaif.io

[16] MCP specification, changelog for 2026-07-28; authorization update of 2025-11-25.

[17] OWASP, MCP Top 10 (2025). github.com/OWASP

[18] Microsoft Learn, MCP servers in Azure API Management; Entra Agent ID updates.

[19] TM Forum, members launch AI-native ODA roadmap for autonomous telecoms, June 2026. tmforum.org

[20] TM Forum Inform, turning agentic AI into a safe, scalable operational capability. inform.tmforum.org

[21] Nymbus (April 2026), Grasshopper (August 2025), Danske Bank (September 2026), Mercury (November 2025), Griffin (May 2025). Overview: finpace.tech

[22] Telecoms Tech News, Cerillion ships agentic AI over 47 TM Forum Open APIs, November 2026. telecomstechnews.com

[23] Capgemini, Core Banking Modernization, 2020. capgemini.com

[24] South Africa, Draft National AI Policy, gazetted 10 April and withdrawn 26 April 2026. Nigeria: NALTF, 27 October 2026. naltf.gov.ng

[25] Office of the Data Protection Commissioner (Kenya), enforcement figures, 26 January 2026. Coverage: capitalfm.co.ke

[26] Ministry of Tourism and Wildlife, Kenya Tourism Sector Performance Report 2025, April 2026. Coverage: the-star.co.ke

[27] Kenya Revenue Authority, eTIMS validation of tax returns from 1 January 2026. Coverage: peopledaily.digital, bdo-ea.com

[28] AWS, AgentCore generally available, October 2025; API Gateway MCP proxy, 2 December 2025.

References

[29] Google Cloud, “Announcing MCP support in Apigee”, 10 December 2025. cloud.google.com

[30] Salesforce Developers, Salesforce Hosted MCP Servers generally available, 29 April 2026. developer.salesforce.com

[31] AWS, “How MoEngage turned over 400 APIs into agent tools with AgentCore Gateway”, 29 October 2026. aws.amazon.com

[32] Stripe, Instant Checkout in ChatGPT and the Agentic Commerce Protocol, 29 September 2025. stripe.com

[33] Axios, Google, Shopify and retailers push AI shopping standard, 11 January 2026. axios.com

[34] The Paypers, Walmart drops OpenAI checkout and deploys Sparky on AI platforms, March 2026. thepaypers.com

[35] Amazon v. Perplexity: injunction, Bloomberg, 10 March 2026; overturned on appeal, Reuters, August 2026.

[36] PhocusWire, OpenAI launches apps in ChatGPT with Expedia and Booking.com, October 2025. phocuswire.com

[37] Sabre, agentic APIs and MCP server for travel, 23 September 2025. investors.sabre.com

[38] Kiwi.com, MCP server prototype, 7 August 2025; Alpic engineering write-up.

[39] Skift, “The hidden hurdle in AI travel planning”, 6 July 2026. skift.com

[40] Shopify, Winter ’26 Edition: Agentic Storefronts, December 2025. shopify.com

[41] Kenyan core upgrades: TechCabal, 5 November 2024; TechinAfrica, October 2024; Kenya Times, October 2026.

[42] CBK fines of KSh 191m in 2024, TechCabal, August 2025. Exchange rate about KSh 173 per pound, Wise, November 2026.