How to Evaluate Passwordless Authentication Vendors: Scoring Model, RFP Questions, and Red Flags

Governance & Compliance / Last updated 2026-06-11 / https://www.scrambleid.com/learn/scrambleid-evaluation-checklist-rfp

In one sentence: Evaluate omnichannel authentication vendors by requiring phishing resistance with no OTP fallbacks, voice-channel KBA replacement, machine identity PoP, unified telemetry, and documented SLAs with evidence.

This page is designed to be copy/paste-friendly for procurement and security teams.

It answers: **What should we ask vendors if we want phishing-resistant, omnichannel authentication - including voice and machine identities - with measurable outcomes?**

TL;DR (canonical)

- Require **phishing resistance** (origin/session binding + public key cryptography) and explicitly disallow OTP fallbacks for high-risk actions.
- Require **voice-channel verification** that replaces KBA (not just "caller ID").
- Require **shared identifier model + telemetry** (audit, metrics, risk).
- Require **M2M proof-of-possession** to reduce token replay.
- Require **step-up** and **dual control** for high-risk actions, shipped today or on a committed timeline.

Use this scoring model

Score each category 0-5. Multiply by weight.

Category	Weight	What you are testing
Phishing resistance (web)	20%	Can attackers relay the auth ceremony?
Voice/KBA replacement	20%	Does it actually stop vishing and recovery abuse?
Omnichannel consistency	15%	Are primitives consistent across channels?
M2M/agent security	15%	Are tokens sender-constrained (PoP) and keys governed?
Risk + monitoring	10%	Is there correlated telemetry and action hooks?

Category	Weight	What you are testing
Step-up + approvals	10%	Can you gate high-risk actions with strong chains?
Implementation + ops	10%	Does it deploy cleanly with clear runbooks?

How to anchor scores

Use the same scale for every category so vendors stay comparable:

- **0:** Capability absent, or claimed with no evidence.
- **1-2:** Roadmap or partial. The vendor shows design docs or a committed timeline, but you can't test it today.
- **3:** Working but narrow. A live demo passes in one channel or configuration; evidence covers the happy path only.
- **4:** Production-grade. Live demo plus architecture and sequence diagrams, event schemas, and at least one referenceable deployment.
- **5:** Proven at your scale. Everything in 4, plus SLAs in writing and failure-state evidence (timeouts, denials, revocation) you've verified yourself.

Require evidence for the score, not the claim. By category: phishing resistance wants spec references and an AiTM demo; voice wants a live inbound call with session binding shown; omnichannel consistency wants the same primitive demoed in two or more channels; M2M wants token introspection showing proof-of-possession; risk and monitoring wants schema docs and a correlated event trace; step-up and approvals wants signed artifacts your systems can verify; implementation wants a reference architecture and a runbook.

Minimum requirements (do not waive)

- No SMS/voice OTP fallback for password resets, payout changes, or admin settings
- Explicit origin/session binding for web login (WebAuthn or equivalent)
- Voice verification that is not KBA (no security questions)
- Device enrollment and fast revocation (minutes)

RFP question bank

A) Web authentication (phishing resistance)

1. Describe how you prevent adversary-in-the-middle (AiTM) relay attacks.
2. Is the authentication ceremony origin-bound? Provide proof (spec references).
3. What weak fallbacks exist (SMS, email OTP, push approvals)? Can we disable them per action?

4. Provide your supported authenticators (platform, roaming, hardware-backed) and attestation options.

B) Voice and contact center

1. Can you replace KBA in IVR and agent flows? Describe the exact flow.
2. What is your median and p95 time to verify on an inbound call?
3. How do you bind success to the correct live call session (callSid/correlation id)?
4. What are your failure states (timeout, wrong-code, deny) and how do they surface to agents?

C) People / in-person / messaging

1. Do you support verifier-initiated checks with explicit consent?
2. Can we require a "Work" profile vs "Minimal" vs "Anonymous"?
3. How do you mark verified vs self-asserted attributes?

D) Machine identities and agents

1. Do you support proof-of-possession tokens (mTLS or DPoP)?
2. How are keys rotated? What is the operational runbook?
3. Can you gate token minting with human approvals for privileged actions, today or on a committed timeline?

E) Risk, monitoring, and response

1. What event schema do you expose (start/success/fail/timeout)?
2. Can you correlate across channels (web + voice + people + desktop + M2M)?
3. Can risk signals trigger step-up or blocks?

F) Step-up and dual control

1. Do you support multi-step step-up chains without OTP fallbacks, today or on a committed timeline?
2. Same question for multi-party approvals (2-of-2) with hard TTLs: shipped or committed, and when?
3. Are the results signed and verifiable by our systems? If this isn't shipped yet, what does the design commit to?

G) Implementation and operations

1. Provide reference architectures and integration guides.
2. Provide SLAs: uptime, p95 latency, and action delivery success.
3. Provide device revocation and credential lifecycle details.

Red flags (vendor responses that should fail)

- "We are phishing-resistant because we have MFA" (not sufficient)
- "Our push approvals are safe" without strong binding to the initiating session
- "We support voice" but only via ANI/number matching or KBA
- "We support M2M" but require long-lived client secrets
- "We support step-up" but default to SMS/email OTP

Key Takeaway

When evaluating omnichannel authentication vendors, require five capabilities with evidence: phishing resistance (no OTP fallbacks for high-risk), voice-channel KBA replacement (not just caller ID), machine identity with PoP, unified telemetry across channels, and documented SLAs. Ask for architecture diagrams, sequence diagrams, event schemas, and live demos, not just marketing claims.

FAQ

What is the single best discriminator question?

Ask: "Show how your web login stops AiTM relay attacks." If the answer is OTP/push, it will not.

Why is voice in the checklist?

Attackers shift to the phone to bypass strong web authentication, especially for recovery and payout changes.

What do we ask for as evidence?

Ask for architecture diagrams, sequence diagrams, event schemas, SLAs, and a live demo for web and voice.

How do we score vendors fairly?

Score every category on the anchored 0-5 scale above, apply the weights, and require the listed evidence for each score. A claim without evidence scores 0.

Related reading

- Omnichannel Authentication
- Caller Authentication

- M2M Without Shared Secrets
- XFactor Step-Up
- Metrics + ROI

References (public)

- NIST SP 800-63-4 Digital Identity Guidelines: https://csrc.nist.gov/pubs/sp/800/63/4/final
- CISA Phishing-Resistant MFA Fact Sheet: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
- FIDO Alliance Specifications: https://fidoalliance.org/specifications/
- RFC 7523 JWT Client Assertions: https://datatracker.ietf.org/doc/html/rfc7523
- RFC 9449 DPoP: https://www.rfc-editor.org/rfc/rfc9449.html