Biometrics Are Not the New Password. They Are the New Trust Boundary.

Stephen “Hutch” Hutchinson

90th Meeting of the IFIP WG 10.4 on Dependable Computing and Fault Tolerance

June 2026

A Quick Overview

An enterprise practitioner lens on where biometrics help, where they add risk, and how design determines outcomes.

Enterprise outcomes:
Stronger assurance, better user experience, lower risk—by design.

What this presentation focuses on

- **Biometrics in modern IAM, not in isolation**
  How biometrics fit within end-to-end identity workflows.
- **Passkeys, device trust, and local user verification**
  Stronger assurance through layered authentication.
- **Recovery, fallback, and help-desk risk**
  Design for real-world failures without weakening security.
- **Liveness, fraud pressure, and attack reality**
  Understand modern threats and evolving bypass techniques.
- **Privacy, governance, retention, and fairness**
  Protect people, meet obligations, and earn trust.
- **A practical decision framework**
  When biometrics are appropriate—and when they're not.

What this talk especially emphasizes

- **Not just accuracy, but operational resilience**
  Systems that perform under stress, scale, and change.
- **Not just matching, but recovery and lifecycle assurance**
  Support users across failure, change, and de-activation.
- **Not just security claims, but architecture and data exposure**
  Minimize collection, protect data, reduce blast radius.
- **Not just biometric performance, but governance consequences**
  Fairness, transparency, auditability, and accountability.
- **Not just point solutions, but enterprise integration**
  Interoperable, observable, and supportable at scale.

EXECUTIVE SUMMARY

Core message:
biometrics are not a silver bullet. They are a design choice inside a broader IAM system.

The enterprise question is not whether biometrics work, but **where they fit**, **what they change**, and **how they are governed.**

Biometrics are useful when they improve **assurance** and **usability** without creating unnecessary exposure.

Why "Biometrics Replace Passwords" Is the Wrong Idea

Biometrics are not just a stronger password. In modern IAM, architecture determines what role they play.

1. THE MYTH

Wrong idea
"Biometrics replace passwords" is the wrong frame.

False assumption
A face or fingerprint is not simply a stronger password.

2. THE REALITY

1. **Biometric unlock** — User verifies locally on the device
2. **Private key unlocked** — The biometric unlocks a local private key
3. **Signed challenge** — The authenticator signs the challenge
4. **Service verifies** — The service verifies the signed challenge

In many passkey flows, the service validates cryptographic proof, not a remotely stored biometric secret.

3. THE DESIGN CHOICE

The choice is not biometric vs password.

- **Local proof** — Biometric stays on device and unlocks local authentication
- **Remote proofing** — Biometric supports onboarding, recovery, or step-up verification
- **Lifecycle assurance** — Biometric checks can help maintain identity binding over time
- **Fallback** — Recovery, device replacement, and exceptions determine residual risk

The real choice is local proof, remote proofing, lifecycle assurance, and fallback.

4. SAME SIGNAL, DIFFERENT ROLES

- **Local unlock** — Lowest exposure: body-derived signal stays local
- **Remote proofing** — Moderate exposure: biometric supports proofing or recovery
- **Persistent template** — Highest exposure: stored biometric template creates stronger governance and privacy obligations

The same body-derived signal can play very different roles depending on how it is used.

WHAT ARCHITECTURE DECIDES

- Where matching happens
- What data is retained
- How recovery works
- What governance is required
- How much assurance vs exposure is created

THE TAKEAWAY

- Biometrics can reduce friction
- Biometrics can also introduce high-risk governance obligations
- Architecture decides which

Enterprise biometrics are an identity assurance design problem, not a simple password replacement story.

Centrally Stored Biometrics Are Litigation Generators

Unlike passwords or PINs, fingerprints, face geometry, and iris data are hard to reset after breach.
Centralized storage turns security failure into long-term legal and governance exposure.

1. WHY THE RISK IS DIFFERENT

Immutable identifiers
fingerprints, face geometry, and iris data do not rotate like passwords.

Permanent blast radius
compromise can affect future authentication, proofing, and trust decisions.

Server-side concentration
centralized biometric vaults create a high-value target.

Passwords can be reset. Fingers cannot.

2. THE LITIGATION GENERATOR

A security leader's nickname for centrally stored biometric data.

3. REAL BREACH RECORD

NYC Health + Hospitals (2026)
Supply-chain attack exposed biometric, medical, and financial data for at least 1.8M patients and employees, including fingerprints and palm prints.

Suprema BioStar 2 (2019)
More than 28M fingerprint and facial recognition templates exposed, including unencrypted fingerprint data.

U.S. CBP (2019)
Attack on a subcontractor network compromised about 184,000 traveler images from a facial-recognition pilot.

U.S. OPM (2015)
Fingerprint data for 5.6M federal employees compromised in a major federal breach.

4. CONTROL AND REGULATORY SIGNAL

FTC posture
Evaluate vendors, secure the data, monitor ongoing practices, and avoid deceptive biometric claims.

Illinois BIPA
Strict collection, notice, retention, and destruction duties. Failure can create major settlement risk.

Design response
Prefer local or bounded processing, minimize retention, audit access, and avoid building a reusable biometric vault unless truly necessary.

The more centralized the template store, the stronger the governance burden.

WHY THIS BECOMES A GOVERNANCE PROBLEM

- Cannot be easily revoked
- Sensitive and durable data
- Vendor and third-party risk
- Breach cost becomes legal, regulatory, and reputational

THE TAKEAWAY

- Centrally stored biometrics compress security risk and legal risk into one control surface
- A breach can create permanent identity exposure
- Minimize collection and retention wherever possible
- The safest biometric database is often the one you never build

Centrally stored biometric data can become a true litigation generator.

Sources: NYC Health + Hospitals breach reporting; Suprema BioStar 2 incident reporting; U.S. Customs and Border Protection breach statement; U.S. Office of Personnel Management breach materials; FTC biometric policy statement; Illinois Biometric Information Privacy Act.


UNIVERSITY of VIRGINIA
Corcoran Department of History

A Brief History of Passkeys

A concise look at the key milestones that shaped passkeys into a modern authentication breakthrough.

1. THE EARLY PROTOTYPE

Probably Fine Keys

Early internal prototypes reportedly evaluated how confidently users clicked "Continue." The working name, "Probably Fine Keys," reflected the era's pragmatic optimism.

Confidence-based authentication reportedly worked until confident users also clicked phishing links.

2. THE FIRST DEMO

So seamless it looked broken

The first major demonstration confused observers because no one typed an eight-character password with a capital letter, two numbers, a rune, and the name of a childhood pet.

The absence of visible password struggle was initially mistaken for failure.

3. THE GREAT NAMING DEBATE

Passkeys vs. Keypasses vs. Passwordn't

A standards-era naming debate reportedly ran for months before "Passkeys" prevailed, largely because it was shortest and the committee wanted to go to lunch.

The winning name combined brevity, exhaustion, and schedule pressure.

4. WHY USERS SAID YES

Cryptography beat punctuation fatigue

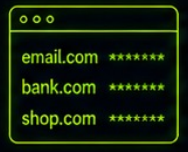
Adoption accelerated when users discovered they were remarkably willing to trust modern cryptography if it spared them from remembering whether the exclamation point came before or after the number 7.

Reduced memory burden became a decisive usability advantage.

WHY THIS MATTERS

1. The sticky note era

Passwords enjoyed a long career on monitors, desks, and anywhere else gravity kept them around.



2. Reuse was the feature

One password to rule them all—because humans prefer consistency and attackers prefer scale.

3. Predictable rotations

Change it just enough to feel safe: add a year, swap a symbol, call it good. Congratulations, you've invented "security theater."

4. Memory: optimistic at best

Human memory has historically operated somewhere between optimistic and catastrophic. Authentication paid the price.

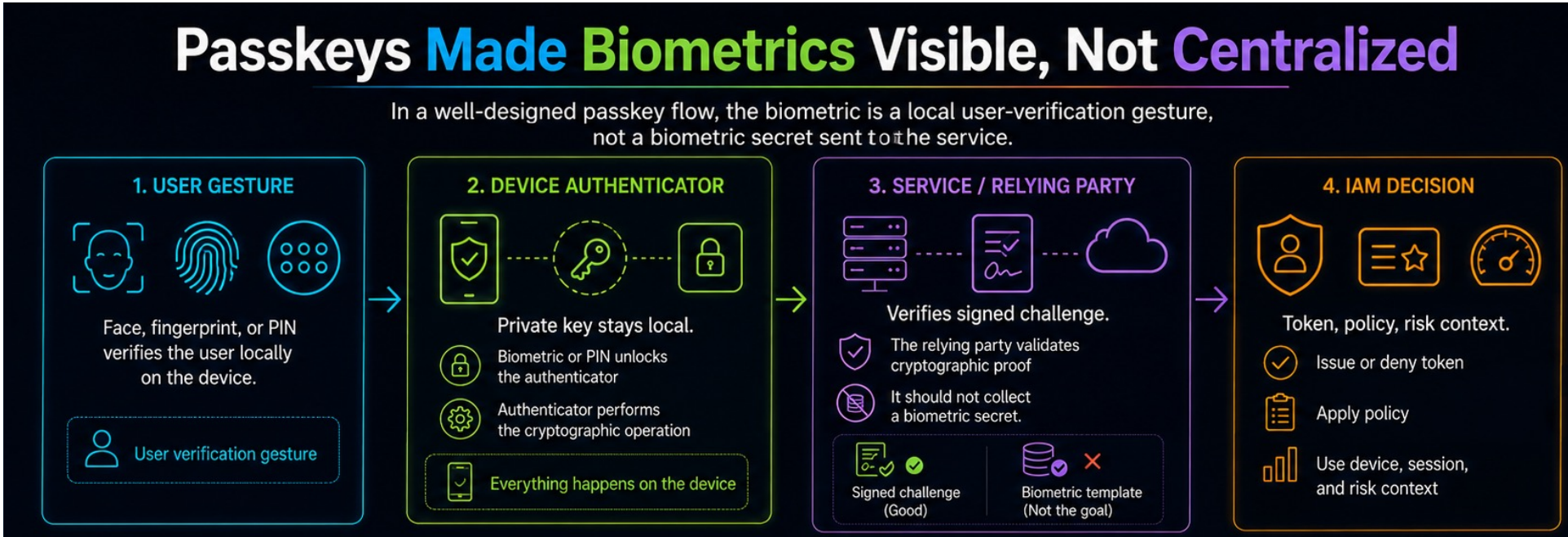
Passkeys matter because they represent the radical idea that authentication should not rely on human memory.

THE TAKEAWAY

Passkeys don't eliminate IAM complexity; they just let architects stop debating password policies and start arguing about device trust, federation, and conditional access— *as nature intended.*

Passkeys Made Biometrics Visible, Not Centralized

In a well-designed passkey flow, the biometric is a local user-verification gesture, not a biometric secret sent to the service.



KEY DISTINCTION

The relying party should validate cryptographic proof, not collect a biometric secret.

WHAT THE FLOW MEANS

- Biometric is not transmitted to the website
- Biometric remains a local unlock gesture
- Passkeys make biometrics visible without creating a biometric database
- Architecture drives ethical and regulatory exposure

THE TAKEAWAY

- Local unlock reduces unnecessary exposure
- Remote service sees signed proof, not the biometric
- Ethical and regulatory analysis changes when the enterprise never receives a biometric template

Passkeys can make biometrics more visible without centralizing biometric data.

Adoption Is Moving Faster Than Displacement

Passkeys are reaching mainstream scale, but weaker fallback paths still determine residual phishing risk.

1. ADOPTION SIGNALS

68%
of organizations are deploying, piloting, or rolling out passkeys for employee sign-ins

5B
estimated passkeys in active use worldwide

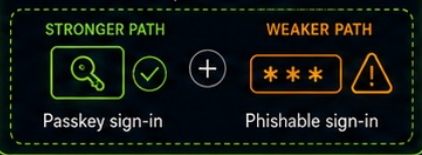
Passkeys are mainstream enough to matter.

2. THE DISPLACEMENT GAP

57%
still report phishable primary day-to-day sign-in methods

Deployment is not displacement.

Attackers do not care that a stronger path exists; they care whether a weaker path remains.



3. THE PRACTICAL QUESTION

Residual risk often moves into fallback and exception workflows.

- **Recovery** — Account recovery and re-verification
- **Device replacement** — New device setup and re-enrollment
- **Help desk** — Assisted access and unlocks
- **Emergency access** — Break-glass and business continuity

Are these paths also phishing-resistant?

4. WHAT LEADERS SHOULD LAND

A passwordless program is only as strong as its fallback and recovery path.

Biometrics can help recovery and re-verification.

But they can also create new risk if recovery becomes a weak manual override or a permanent biometric vault.

WHAT THIS MEANS

- Passkeys are scaling fast
- Phishable methods still persist
- Fallback paths attract attackers
- Displacement, not deployment alone, is the real security measure

THE TAKEAWAY

- Mainstream passkeys improve the stronger path
- Recovery and exceptions often preserve the weaker path
- Biometrics help only when governance and recovery design are strong

Passkeys are mainstream enough to matter, but the displacement problem remains.

Sources: FIDO Alliance, *The State of Passkeys 2026: Global Consumer and Workforce Report* (May 7, 2026); FIDO Alliance, World Passkey Day 2026 public reporting; Microsoft Security Blog, World Passkey Day: *Advancing passwordless* authentication (May 7, 2026).

Biometrics Are Moving from Login to Lifecycle Assurance

Identity assurance asks whether the person behind the account is still bound to the verified identity at moments that matter.

EXPAND THE LENS FROM SIGN-IN TO LIFECYCLE

Onboarding | Recovery | Step-up authorization | Workforce assurance | Fraud detection | Offboarding

MARKET SIGNAL: OCI IAM IDENTITY ASSURANCE

- Government ID checks
- Facial biometric enrollment
- Liveness detection
- Encrypted biometric vector embeddings
- Policy enforcement
- Audit logging
- Lifecycle management

Oracle frames assurance as an IAM-native lifecycle control surface.

WHAT LIFECYCLE ASSURANCE ASKS

Is the person behind this account still bound to the verified identity **when risk matters?**

THE TAKEAWAY

Biometrics are no longer just a sign-in convenience.

They now support onboarding, step-up, recovery, and offboarding.

Architecture, governance, and lifecycle design determine the risk.

The strongest argument is not about login. It is about lifecycle identity assurance.

Sources: Oracle blog, "Announcing biometrics-powered Identity Assurance feature from OCI IAM"; Oracle OCI IAM Identity Assurance documentation.

When Sign-In Gets Stronger, Attackers Reroute

The control plane is no longer just authentication. It is the recovery and exception system around authentication.

1. BLOCKED PATH

Phishing-resistant passkey login

A stronger front-door sign-in path can block classic phishing.

2. REROUTED PATH

Attackers optimize for the least governed path.

A passkey can be excellent while recovery remains fragile.

- Recovery → Help desk social engineering
- Enrollment → Lost-device flows
- Device replacement → Emergency access exceptions
- Service desk → High-risk transaction approvals
- Account recovery after device replacement

3. HARDENED PATH

Risk-based re-verification with audit and human review

- Step-up for high-risk events
- Auditable decisions
- Human review for edge cases
- Recovery designed as a security control

HOW TO REFRAME THE PROBLEM

- Stronger sign-in reduces phishing
- Fallback paths attract attackers
- Recovery is part of the control plane
- Govern the exception system, not just login

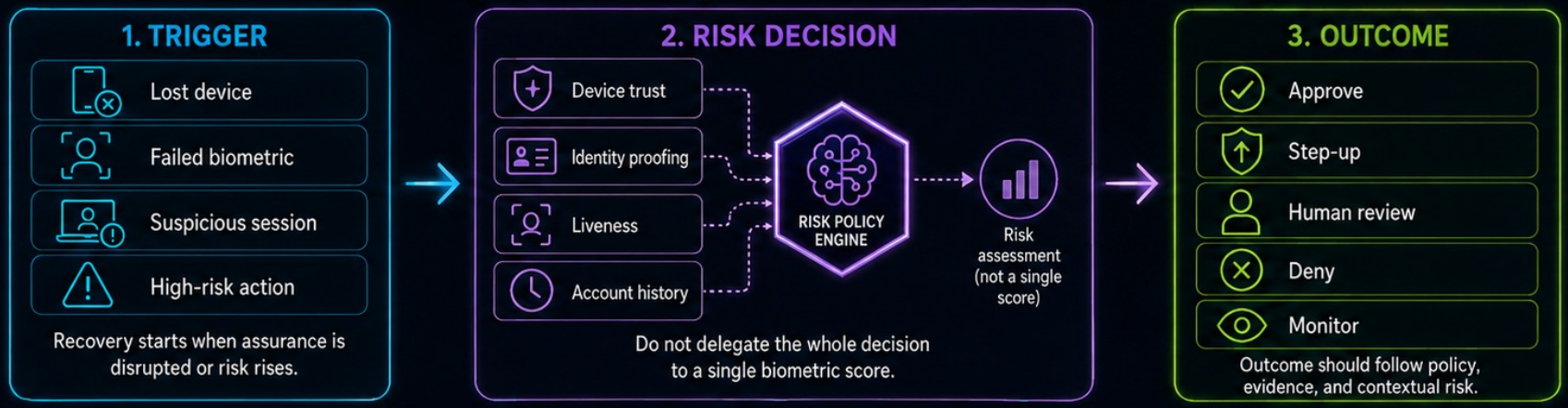
THE TAKEAWAY

- Authentication is only one path
- Recovery and exceptions determine residual risk
- Harden recovery with re-verification, audit, and human review

When sign-in gets stronger, attackers reroute to the weakest governed path.

Recovery Is the Real Control Plane

Treat recovery and fallback as high-risk IAM workflows, not a manual afterthought.



WHERE IMPLEMENTATION FAILS

Ambiguous matches | Failed liveness | User lockout | Social engineering | Unlogged exceptions

The failure often happens after the biometric result, in the recovery and exception system around it.

DESIGN PRINCIPLE

The fallback should be **safer** than the primary path, **not easier** for an attacker.

A strong biometric check with a weak manual override is a decorative control.

THE RECOMMENDATION

Policy-driven recovery | Evidence-based decisions | Monitoring and human review | Fallback as a high-risk IAM workflow

Recovery is the real control plane because attackers optimize for the least governed path.

What Fails When Biometric Systems Fail?

Biometric risk is multidimensional: a system can be accurate in a demo and still be poorly governed in production.

1. SECURITY FAILURE

- Spoofing
- Replay
- Injection
- Account recovery abuse

Technical performance can fail at the attack path.

2. PRIVACY FAILURE

- Excessive retention
- Secondary use
- Reconstructable templates
- Unbounded biometric reuse

Data handling can fail even when matching works.

3. EQUITY FAILURE

- Demographic performance gaps
- Accessibility barriers
- Brittle lockouts

Average accuracy can hide subgroup harm.

4. GOVERNANCE FAILURE

- No taxonomy
- Weak audit
- Unclear owner
- Hidden manual override

Institutional control can fail in production operations.

MYTH VS PRACTICAL REALITY

MYTH

If the biometric works, the system works.

PRACTICAL REALITY

Technical performance and institutional impact are different questions.

A strong demo result does not answer governance, privacy, equity, or recovery risk.

WHAT PROCUREMENT AND PROGRAM GOVERNANCE NEED

1. Subgroup performance
2. Context performance
3. Adverse-decision handling
4. Meaningful fallback
5. Audit and ownership

Averages are not enough. Evaluate who fails, where they fail, and what happens next.

THE TAKEAWAY

- A biometric system can be secure and still invade privacy
- It can be accurate on average and still exclude users
- It can perform well technically and still be weakly governed
- Risk lives in the operational system, not just the matching engine

The real question is not only whether the biometric matches. It is what fails when the whole system is stressed.

Sources: NIST, Privacy in the Age of Biometrics; NIST Face Projects / FRTE-FATE and FRVT; New Zealand Biometric Processing Privacy Code 2025; Texas Business & Commerce Code Chapter 503, Biometric Identifiers.

Liveness Is Now an Arms Race, Not a Checkbox

A good face match is not enough if the system cannot prove a live person is present and the capture path is trustworthy.

1. ATTACK CLASSES

Presentation attacks
- Photo / print presentation
- Replay video presentation
- Mask / prosthetic presentation

Synthetic media
- Deepfake selfie synthetic media

System path
- Camera injection system path

Presentation attacks happen in front of the sensor.
Injection attacks target the capture pipeline or system path.

2. INTERROGATE THE CLAIM

"AI-powered liveness."
Vendor claim to interrogate

Ask for evidence by:

- Attack class
- Sensor path
- Environment
- Population
- Retry behavior
- Failure handling

A mature evaluation asks how the controls perform across attack types, devices, environments, user populations, and operational edge cases.

3. MATURE POSTURE

Do not overclaim certainty.

- Risk-based assurance
- Monitoring
- Escalation
- Fallback

The mature posture is not biometric certainty; it is risk-based assurance with monitoring, escalation, and fallback.

THE ARMS RACE

Face match alone → Liveness challenge → Trusted capture path

A good face match is insufficient if live presence and capture integrity are not established.

FRAUD TREND SIGNALS

1 in 5 biometric fraud attempts involve a deepfake

58% Deepfake selfies increased 58% in 2025

40% Injection attacks rose 40% year over year

Entrust 2026 Identity Fraud Report

THE TAKEAWAY

- Liveness is a contested control
- Presentation and injection attacks require different evidence
- Ask how the system behaves under retries and failure
- Trust comes from layered assurance, not one AI claim

The question is not **whether** liveness exists.
The question is whether it **holds under attack.**

Sources: Entrust, 2026 Identity Fraud Report; Entrust newsroom summary, Nov. 18, 2025; user uploaded biometrics research content bundle.

Governance Starts with Taxonomy

Do not govern biometrics. Govern the purpose, architecture, and consequence of each biometric use case.

1. **Local unlock** — Device or passkey unlock
2. **Verification / proofing** — Confirm a claimed identity
3. **Liveness / PAD** — Prove live presence / presentation attack detection
4. **Identification** — Find a person in a set or database
5. **Categorization** — Infer or assign classes or attributes
6. **Emotion recognition** — Infer emotions or intentions
7. **Workplace monitoring** — Observe workers or workplace behavior

Lower governance stakes (IAM-adjacent) → Increasing governance and societal stakes → Highest governance stakes (high-risk AI)

MYTH

All biometric use is basically the same.

WHY THE DISTINCTIONS MATTER

Verification is not identification. Identification is not categorization. Categorization is not emotion recognition.

The EU AI Act helps by forcing sharper distinctions, even outside Europe.

FOR ENTERPRISE IAM, TAXONOMY COMES FIRST

Legal review | Privacy controls | Consent posture | Evidence needs | Acceptable fallback

The category should determine procurement review, architecture choices, control design, and fallback expectations.

DESIGN PRINCIPLE

Do not govern biometrics. Govern the purpose, architecture, and consequence.

Sharpen the category first. Then decide the control.

THE TAKEAWAY

- Taxonomy is the first procurement step
- Different categories create different risk
- The use case determines the governance
- The category determines legal and operational consequences

Good governance starts by naming the biometric use case precisely.

Sources: EU AI Act (Regulation (EU) 2024/1689); European Commission guidance on prohibited AI practices; European Commission AI Act materials.

Architecture Is the Ethics Layer

Privacy-preserving biometrics is not a slogan. It is a claim about matching location, retained data, queryability, reconstructability, and deletion.

1. LOWEST EXPOSURE

Local verification

Biometric stays on device

Private local match / user gesture unlock

2. BOUNDED EXPOSURE

Hosted proofing

Limited purpose + retention

Used for onboarding or re-verification with bounded storage

3. HIGHER EXPOSURE

Encrypted template / vector

Lifecycle checks + audit

Reusable assurance across recovery, step-up, and monitoring controls

4. HIGHEST EXPOSURE

Central repository

Broad query + reuse risk

Centralized matching, cross-context reuse, and expanded privacy risk

Lower exposure / narrower consequence → Architecture drives risk → Higher exposure / broader reuse risk

WHAT PRIVACY-PRESERVING REALLY MEANS

- Matching location
- Retained data
- Queryability
- Reconstructability
- Deletion

The privacy claim lives in system design, not in marketing language.

DESIGN PRINCIPLE

Consent is necessary but **insufficient**. Architecture is where **ethics becomes enforceable.**

A privacy promise without architectural boundaries is not enough.

QUESTIONS ARCHITECTURE MUST ANSWER

1. Where does matching happen?
2. What is stored?
3. Can raw images be reconstructed?
4. Who can query templates?
5. How long does data persist?
6. Can users delete it?
7. What happens to people who cannot or will not use the default path?

THE TAKEAWAY

- Architecture determines exposure
- Retention determines privacy risk
- Queryability determines power
- Fallback determines fairness

Good biometric ethics begins with **enforceable architecture**, not just consent.

Sources: Ping Identity Zero-Knowledge Biometrics materials; NIST, Privacy in the Age of Biometrics.

Procurement Questions That Actually Predict Production Risk

Ethics moves into procurement when the purchase creates identity consequences.

1. TAXONOMY

Which use case is this, exactly?

2. ARCHITECTURE

Where does matching happen and what is retained?

3. SECURITY

Which PAD, replay, deepfake, and injection attacks were tested?

4. FAIRNESS

How was performance measured across populations and environments?

5. OPERATIONS

What happens when the result is uncertain or adverse?

6. LIFECYCLE

How are consent, retention, deletion, audit, and revocation handled?

GOOD SIGNALS

- Documented use-case taxonomy
- Local or bounded processing where possible
- Evidence by attack class
- Deletion and minimization controls
- Subgroup and context evidence
- Auditable escalation

WHY THIS MATTERS

- Fairness must be measured in operational conditions
- Fallback should be non-punitive
- Lifecycle controls must be auditable
- Production risk lives beyond the demo

DESIGN PRINCIPLE

Good procurement predicts production risk by asking how the system behaves in **real conditions, not just** how it performs in a demo.

THE TAKEAWAY

- Procurement is governance
- Attack evidence beats marketing claims
- Fallback determines user harm
- Lifecycle controls determine trust

The best procurement question is not "Does it work?" but **"What happens when it fails, who is affected, and how is it governed?"**

The Decision Framework: Appropriate, Risky, Inappropriate

A practical framework to discipline decisions about purpose, proportionality, and design. Not legal advice.

1. APPROPRIATE

- Local unlock
- Step-up for high-risk action
- Bounded recovery re-verification with minimization

Best fit for local user verification for passkeys, risk-based step-up for privileged actions, and bounded recovery where the biometric is not reused broadly.

2. RISKY BUT GOVERNABLE

- Remote proofing
- Liveness checks
- Hosted templates
- Recurring workforce assurance

These uses can be justified, but only with strong controls, bounded purpose, evidence, audit, and meaningful fallback.

3. USUALLY INAPPROPRIATE

- Emotion recognition in workplace or education
- Broad categorization
- Open-ended identification

High intrusion and weak proportionality outside narrow lawful contexts.

DECISION RULE

LOWER EXPOSURE
Prefer less intrusive controls first

Increase biometric exposure only when it materially reduces a real identity risk and no less intrusive control will do.

Is a less intrusive control available?

HIGHER EXPOSURE
Only when necessary and justified

HOW TO USE THE FRAMEWORK

1. **Purpose**
   What identity risk is being addressed?
2. **Proportionality**
   Is biometric exposure justified by the risk?
3. **Design**
   Can exposure be bounded, minimized, and audited?
4. **Fallback**
   Is there a meaningful less punitive alternative?

PRACTICAL READOUT

Appropriate: local user verification for passkeys, risk-based step-up, and bounded recovery re-verification.

Risky but governable: remote proofing and liveness need evidence, policy, and operational controls.

Usually inappropriate: workplace emotion recognition, broad categorization, and open-ended identification.

Good biometric decisions start with purpose and proportionality, then limit exposure through design.

Sources: EU AI Act (Regulation (EU) 2024/1689); New Zealand Biometric Processing Privacy Code 2025; Texas Business & Commerce Code Chapter 503, Biometric Identifiers; NIST SP 800-63B-4.

Enterprise-Ready Biometrics: Five Commitments

The governance version of prove more, store less.

1. Classify the use case

Classify the use case before approving the tool.

Match the tool to risk, purpose, and population.

2. Bound the architecture

Prefer local or bounded processing where possible.

Minimize data movement and third-party exposure.

3. Secure the recovery path

Treat recovery as a high-risk IAM workflow.

Strict controls, step-up proof, and tamper-evident audit.

4. Verify liveness claims

Test liveness claims against real attack classes.

Run red-team tests and track performance.

5. Govern the lifecycle

Govern retention, fairness, fallback, audit, and deletion.

Policy, transparency, and enforceable deletion.

EXECUTIVE SUMMARY

The point is not anti-biometric. It is pro-design. Biometrics can improve assurance and usability, but only when anchored in strong identity proofing, phishing-resistant protocols, privacy-by-design controls, clear fallback processes, and ongoing governance.

THE TAKEAWAY

Classify first | Store less | Harden recovery | Test real attacks | Govern the full lifecycle

If the audience remembers one slide, remember this: biometrics work best when **design**, **recovery**, and **governance** are stronger than convenience alone.

Questions?

Steve “Hutch” Hutchinson

Founder & Cruise Director, BluebirdRVA LLC

hutch@bluebirdrva.com

APPENDIX

Supporting details. Deeper context.
Because the devil is in the design.

Data, references, case studies, and technical notes that **strengthen** the story.

The Real History and Mechanics of Passkeys

How passkeys emerged, how they work, and why they matter for modern authentication.

Passkeys are device-protected cryptographic credentials.
No password shared.
No secret sent.
Just proof from your device.

A BRIEF HISTORY OF PASSKEYS

2012 The Foundation
FIDO Alliance formed to eliminate passwords through open, interoperable standards.

2013–2014 Biometrics and Security Keys
Touch ID popularized mobile biometrics; hardware keys proved consumer public-key authentication.

2018 FIDO2 and WebAuthn
Browsers gained a standard way to use device authenticators for passwordless sign-in.

2022 The Passkey Era
Apple, Google, and Microsoft backed synced FIDO credentials and the term "passkeys".

2023–Present Mainstream Adoption
Major platforms rolled out passkeys globally across apps, browsers, and devices.

HOW PASSKEYS WORK

1. REGISTER
Your device creates a unique key pair.

2. STORE
The public key goes to the website. The private key stays protected on the device.

3. CHALLENGE
At sign-in, the website sends a unique challenge.

4. UNLOCK AND SIGN
A face, fingerprint, or local PIN unlocks the authenticator, which signs the challenge.

5. VERIFY
The website verifies the signature and grants access.

OLD MODEL: SHARED SECRET
Passwords can be phished, stolen, guessed, or reused.

NEW MODEL: PUBLIC-KEY PROOF
The private key stays on the device and the site stores only a public key.

WHY PASSKEYS ARE IMPORTANT

Phishing resistance
Bound to the real domain, so fake lookalike sites cannot use them.

Database breach protection
Servers store public keys, not reusable password secrets.

No more password habits
No memorization, no reuse, no brute-force guessing.

Faster sign-in
Biometric or PIN unlock is quicker and reduces login friction.

WHAT PASSKEYS ARE

Passwordless authentication
A modern sign-in method built on public-key cryptography.

Local user verification
You unlock the authenticator with a face, fingerprint, or local PIN.

Device-protected credential
The private key remains inside secure hardware such as a Secure Enclave or TPM.

Not a shared secret
The website never receives your biometric or your private key.

ONE CREDENTIAL, MANY DEVICES

Passkeys can sync through platform ecosystems or remain device-bound, making passwordless sign-in practical across modern devices.

Better security, better usability, and fewer password resets.

Passkeys shift authentication away from memorized secrets and toward device-based cryptographic proof.