



On-Device Biometrics – Boon or Booby-trap?

Interactive workshop: Mitigating risk for an on-device future

Tuesday 18 May 2027
14:00 – 17:00, Registration from 13:30
Sydney

WORKSHOP OUTLINE

This half-day satellite workshop will take place alongside the [Biometrics Institute's Asia-Pacific Conference 2027](#).

We all use our smart phones and devices for daily transactions like payments, tickets and loyalty, most often where the relevant credentials are held within a digital wallet.

Biometrics provides a convenient way to prove that YOU are in control of the transaction – or does it?

Device makers would have you believe that biometrics are solved – just use the devices on which they have provided biometric mechanisms, allied to passkey techniques. But a [2026 report by UK consumer watchdog Which?](#) found that 133 out of 208 popular devices tested, including some high-end models, could be fooled by a simple 2D photograph spoof (presentation attack). There are other vulnerabilities too.

As digital identity, underpinned by a biometric to prove that you are person entitled to make the transaction, rolls out extensively these mechanisms need careful scrutiny.

This workshop takes the format of an interactive working group exploring how on-device biometrics can be made more secure. Rather than presenting recommended practices developed by the Institute, this workshop will discuss some risks our community has identify, explore these further and decide whether recommendations need to be developed.

Why you should attend:

- This workshop will delve into the pros, cons and pitfalls of on-device biometrics
- It will arm delegates with the information on options for implementing device-based biometric services and how to question the security of what is being offered
- Through its interactive format it will work with delegates to identify potential risks in using on-device biometrics drawing on existing good practice material (see references in “Further Reading” below)
- It will then discuss what’s needed to inform technology developers and policy makers about these risks, and how innovation and regulation can mitigate potentially major negative impacts

AGENDA

13:30 Registration and welcome coffee

14:00 **Workshop session one: What are on-device biometrics and where are they used?** (75mins)

- What are on-device biometrics and how do manufacturers implement them?
 - Takeaways from the *Which?* report
 - Facial recognition
 - Fingerprint recognition
 - Are other biometric modes worth exploring?
 - The role of passkeys
 - Presentation attack detection and liveness
- Examples where biometrics are required to prove the person who is in control
 - Mobile Driver Licences
 - The role of Digital Wallets
 - DTC (Digital Travel) and other Verifiable Credentials
 - Where are workshop delegates currently/ planning on using on-device biometrics?
- Questions, discussion and recap of issues identified so far

15:15 Afternoon break and networking

15:45 **Workshop session two: Data protection and vulnerabilities** (75mins)

- Examples where biometrics are required to prove the person who is in control (cont.)
 - Binding to a unique person and Proof of Personhood
 - Selective disclosure, consent and privacy protection

- Are there other issues with privacy protection?
- What are the vulnerabilities and how to mitigate them?
 - On-device vs stored biometrics: The pros and cons of regulation and trust
 - The role of Secure Elements and Trusted Execution Environments
 - The role of cryptography
 - Levels of assurance and performance testing

16:30 Interactive conversation and potential actions: What do we need to future-proof on-device biometrics?

- What do international standards say? What standards are needed? What testing is available?
- What do we need manufacturers and the device ecosystem to do?
- What do we need policy makers and regulators to do?

This session will consist of a panel of stakeholders presenting some key considerations and inviting delegates to participate in finding mitigations to overcome them. It will be led by Martin George and Brett Feldon, both members of the Digital Identity Group, Biometrics Institute

- Conclusions

17:00 Finish

Total learning time: 2.5 hours

WORKSHOP PRESENTER



Brett Feldon is a Biometrics Institute Advisory Council member and is Head of the Biometrics Institute's Digital Identity Expert Group (DIG). He was previously on the board of the Institute from November 2011 until March 2019 and is based in Sydney, Australia. Brett's professional experience includes management and oversight of deployments of voice biometrics solutions in Australia, New Zealand, Hong Kong and the US, across a range of industries and government departments. The DIG has worked on a range of topics with regard to biometrics and digital identity and helped release the *Digital Onboarding and Biometrics* guiding paper in 2021, the *Digital Identity and Biometric Authentication* paper in 2023, the *Mitigating Biometric Vulnerabilities in Digital Identity – Executive Briefing* in 2024, and the *Biometrics and Account Recovery* paper in 2025.

WHO SHOULD ATTEND?

End-users, integrators, application developers and others interested in digital identity.

FURTHER READING

It is recommended to review the following good practice documents published by the Institute for its members:

[Digital Onboarding and Biometrics paper \(2021\)](#)
[Digital Identity and Biometric Authentication paper \(2023\)](#)
[Mitigating Biometric Vulnerabilities in Digital Identity – Executive Briefing \(2024\)](#)
[Biometrics and Account Recovery \(2025\)](#)
[Top 10 Vulnerability Questions \(updated 2020\)](#)
[Biometrics Vulnerability Checklist \(updated 2020\)](#)
[Biometric Liveness: Protection from Presentation and Injection Attacks explanatory graphic \(2026\)](#)

VENUE

Sydney (TBC)

COST

Members: AU\$700 incl. GST

Non members: AU\$985 incl. GST

University subscribers: AU\$400 incl. GST

University non-subscribers : AU\$500 incl. GST

Students : Request a special student rate by contacting Simon@biometricsinstitute.org

(Proof of full time student status required).

REGISTRATION

Register at our [website](#).

ADDITIONAL NOTES

If you have comments on this event, are interested in membership or have general enquiries about the Biometrics Institute, please email simon@biometricsinstitute.org

IMPORTANT DISCLAIMER NOTIFICATION

The Biometrics Institute provides training and course material as a tool to help you conduct due diligence. While the Institute has used reasonable care to ensure the accuracy of the material and course, due to the content and variable inputs during and after the process of implementing biometrics, the Institute cannot be held accountable for outcomes or compliance. The material and course have been prepared for informational purposes only and are not intended to provide legal or compliance advice. You should consult your legal advisor should you require advice on the legal or compliance aspects of the material or course.