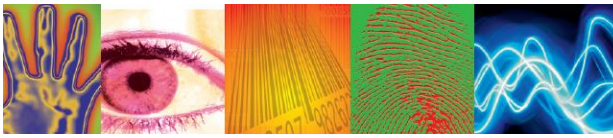


What does presentation attack detection and liveness actually mean?

We've put together this guiding document to provide clarification about presentation attack detection and liveness and to suggest a few questions you may want to ask your vendor to help you understand biometric products better.

What is presentation attack detection?

Biometric data, obtained either directly or covertly from a person online or through hacked systems, is sometimes used to attack a biometric system by creating spoofs or fakes. This attack might use a printed photo, an image or video of a person on a tablet or by presenting a 3D mask or fake silicone fingerprint. A biometric spoof that is detected when presented to a biometric sensor is known as **presentation attack detection (PAD)**.

What is liveness?

The specific detection of whether a sensor is viewing a live biometric – as opposed to a recording, picture or another non-living spoof – is commonly known as **liveness**. Liveness detection is therefore a subset of the potential attacks that might be detected through PAD.

General considerations about PAD detection

When is PAD useful? What business value does it bring and how can the complexity be justified?

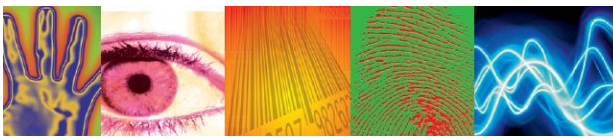
Biometrics are used to control risk. Specifically, the risk of the wrong person gaining access or being misidentified. The use of PAD is one element of a range of risk controls available. Risk can also be controlled through a number of non-technical means such as training, surveillance and procedure.

The use of PAD within a system provides a higher level of security but comes with increased complexity. Ultimately, the need for PAD is determined by the risk of an active attack against the system and the financial and reputational impact this attack would have.

PAD is important, therefore, where security rather than just convenience is a priority. Financial transactions, access control to secure areas and access to private data are all examples of biometric systems where PAD mechanisms are essential.

It's recommended that PAD is used for all systems where security is a priority.

UK: 4th Floor, Imperial House, 8 Kean Street London WC2B 4AS, UK | Tel: +44 20 7581 4827 | UK Company Number: 7717293
Australia: PO Box 576, Crows Nest NSW 1585, Australia | Tel: +61 2 9431 8688 | ABN: 81 098 407 099
Email: manager@biometricsinstitute.org | Web: www.biometricsinstitute.org



When is it not helpful or necessary? When is it more of a hinderance?

Some PAD systems can produce poor results through either false alarms or in usability. The impact of this needs to be assessed against the application use and the other options available. Any system should always be trialled to show how effective it will be, and to understand what the failure rate is.

What are the different categories of PAD approaches? How do they vary by modality?

There are many different categories of PAD approaches and a multitude of biometric modalities. For more information, please refer to ISO30107-3 Section 10.

What performance criteria is appropriate? What is an acceptable level of performance to expect? How can it be effectively tested?

Anyone testing and evaluating PAD mechanisms should consider the recommendations and use performance criteria defined in ISO/IEC 30107-3:2017.

What applicable standards are in play? What is on the horizon?

When assessing the use of PAD, you may find the following ISO standards helpful.

Biometric presentation attack detection series

- ISO/IEC 30107-1:2016 - Information technology – Biometric presentation attack detection – Part 1: Framework

  ISO/IEC 30107-2:2017 – Information technology – Biometric presentation attack detection – Part 2: Data formats

- ISO/IEC 30107-3:2017 – Information technology – Biometric presentation attack detection – Part 3: Testing and reporting

Under development

- ISO/IEC 30107-4 Information technology – Biometric presentation attack detection – Part 4: Profile for testing of mobile devices

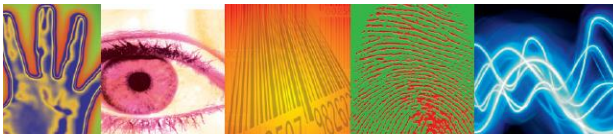
For the ISO's full definition on presentation attack detection, visit their website.

Where can you turn for more information?

Biometrics Institute supplier directory

You can search our supplier directory for a list of members experienced in biometrics systems in your field and contact them for independent risk analysis. Biometrics Institute **members benefit from our request for information service which connects Biometrics Institute user members with experienced supplier members.**

UK: 4th Floor, Imperial House, 8 Kean Street London WC2B 4AS, UK | Tel: +44 20 7581 4827 | UK Company Number: 7717293
Australia: PO Box 576, Crows Nest NSW 1585, Australia | Tel: +61 2 9431 8688 | ABN: 81 098 407 099
Email: manager@biometricsinstitute.org | Web: www.biometricsinstitute.org



Biometrics Institute good practice material

The Biometrics Institute has published good practice guiding documents which are available free to members of the institute. They include:

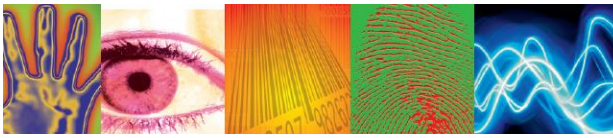
- Ethical Principles for Biometrics
- Biometrics Institute Privacy Guidelines
- Privacy Impact Assessment Checklist
- Top 10 Vulnerability Questions
- How to address biometric vulnerabilities

What questions should I ask about a product that says it contains presentation attack detection?

Spoofing attacks pose a high security risk for operators of biometric technology. Many products now offer anti-spoofing algorithms to automatically detect and mitigate the risks. Before you choose your product, here are some questions you may want to ask your supplier.

- What technologies or techniques is the PAD using?
    - Is the PAD system active (where the user has to perform an action such as blinking, moving the phone, reading out numbers) or passive (where the user is not required to perform any action)?
    - Does the PAD use additional hardware, or is it software-only analysis? Are there any white papers or additional information that can be shared around its use?
- How has the effectiveness of the PAD been tested and were these undertaken independently? If yes, do you know the test criteria?
    - Complexity, cost and level of expertise required by the attacks?
    - Were the attacks taken from a predetermined set, or did an expert design the attacks specifically to tamper with the evaluated PAD system?
    - What are the minimal requirements of accuracy for attack detection?
    - What defence against the replay attack is provided?
- What kinds of attacks will be detected or may be missed by the PAD?
- What effect will the PAD have on system performance, by false detection of attacks?
- How can I configure the aspects of the PAD system?
- Are there any known cases of attacks that have been detected or missed in this product or similar products?
- Have you done an internet search to see what types of attacks are commonly attempted for this modality? (Searching YouTube for things like "Fingerprint liveness", "Face spoofing", "Facial masks", "Fake Irises" is often a good start
- Can you get someone in your organisation or independently to conduct a penetration test on the system?
- Does the PAD follow any relevant international standards?
- What other installations use the system with the PAD enabled?
- What controls are there to ensure there is no malicious code in the software either from the supplier or from any of the suppliers' subcontractors?

UK: 4th Floor, Imperial House, 8 Kean Street London WC2B 4AS, UK | Tel: +44 20 7581 4827 | UK Company Number: 7717293
Australia: PO Box 576, Crows Nest NSW 1585, Australia | Tel: +61 2 9431 8688 | ABN: 81 098 407 099
Email: manager@biometricsinstitute.org | Web: www.biometricsinstitute.org



Contact

This paper was compiled by the Biometrics Institute Security and Integrity Expert Group (BSIEG) with input from other key stakeholders. If you have any questions or comments about this document, please email our BSIEG group at manager@biometricsinstitute.org

Disclaimer

The Biometrics Institute provides guiding material as a tool to help its members conduct due diligence. While the Institute has used reasonable care to ensure the accuracy of the material, 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 has been prepared for informational purposes only and is not intended to provide legal or compliance advice. Organisations should consult industry experts should they require advice on the technical, legal or compliance aspects of the material.

UK: 4th Floor, Imperial House, 8 Kean Street London WC2B 4AS, UK | Tel: +44 20 7581 4827 | UK Company Number: 7717293
Australia: PO Box 576, Crows Nest NSW 1585, Australia | Tel: +61 2 9431 8688 | ABN: 81 098 407 099
Email: manager@biometricsinstitute.org | Web: www.biometricsinstitute.org