

What if we could hot swap our Biometrics?

Jon Crowcroft
University of Cambridge
Cambridge, England, UK

Anil Madhavapeddy
University of Cambridge
Cambridge, England, UK

Richard Mortier
University of Cambridge
Cambridge, England, UK

Chris Hicks
Turing Institute
London, England, UK

Vasilios Mavroudis
Turing Institute
London, England, UK

Abstract

What if you could really revoke your actual biometric identity, and install a new one, by live rewriting your biological self?

We propose some novel mechanisms for hot swapping identity based in novel biotechnology. We discuss the potential positive use cases, and negative consequences if such technology was to become available and affordable.

Biometrics are selected on the basis that they are supposed to be unfakeable, or at least not at reasonable cost. If they become easier to fake, it may be much cheaper to fake someone else's biometrics than it is for you to change your own biometrics if someone does copy yours. This potentially makes biometrics a bad trade-off for the user.

At the time of writing, this threat is highly speculative, but we believe it is (a bit like post-quantum crypto) worth raising and considering the potential consequences.

1 Both Foundational and Functional Identity

The Internet connects around ten billion people and systems. One of the big problems with this scale is we need to know who you are, and we can't just rely on you being vouched for by some nearby friends, family or colleagues, apparently [11, 19].

There are two leading approaches to issuing electronic credentials that can be used to address the problem of remote authentication: *foundational* and *functional* identities. Depending where you are in the world one or the other of these will be most familiar. Foundational ID systems, "popularised" by 1.4 billion people enrolled in India's eponymous Aadhaar [21], are general-purpose identities used for a wide range of activities (e.g., a passport used for travel, age verification, bank account opening, conveyancing etc) whereas functional identities are designed and built for a specific purpose (e.g., national health service number).

Unique, foundational identity is typically rooted in unique biological markers like fingerprints, retina, iris, less so face, and even less so behaviour, and, of course, your DNA.

Biometrics are increasingly common in proving who a person is to a device, usually through a secure sensor (fingerprint reader, or camera in a secure mode, with a secure channel) encrypted at or near source, and then used to sign communication to authorise according to some attached credentials [14]. Data minimisation principles hopefully being used, things like "age verification" only reveal a binary fact ("this person is over 21") rather than an actual birth date.

The split between foundational (just unique identity) and functional (establishing metadata associated with credentials) is now fairly standard, and the use of fancy biometrics is often carefully limited to the former function, whereas the latter can be revealed from a previously authorized device, associated with the identified user, assured via cryptographic means.

Revealing raw biometric data is regarded as incredibly risky, since once it is compromised, the corresponding unique biology cannot be used again. Biometrics are close to impossible to change, but may be relatively easy to imitate (e.g. fingerprints rendered using glue, face simply by copying photos even 2.5D deep fake copies).

What if you could modify a biometric? You could use it directly, and simply revoke it and update as needed.

In this paper we present three ideas which may seem somewhat like science fiction at this point in time, but we offer as a thought experiment towards what might be possible in the not too distant future.

2 Idea 1 - papers please

The requirement to carry proof of identity is relatively recent - the widespread use of passports which carry a photograph of the holder dates from early 20th century. Digital identity is increasingly commonplace, for example with the use of mobile driving licenses, eliminating the need for paper.

Researchers have proposed means to verify credentials in general via mobile services, for example using secure processing on the SIM on a feature phone[13], further reducing costs and generalising the functionality.

We would like to eliminate the use of devices altogether, and store foundational and functional identity attributes

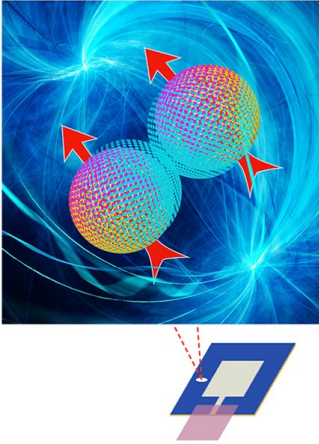


Figure 1: SQUID: Super-conducting Quantum Interference Devices



Figure 2: Chromatophores in Action

directly within the subject, and then communicate these securely.

One approach might employ mutable bar codes displayed on the skin. Animated tattoos have appeared in SF frequently, and some technology is even the subject of a startup[1].

These would be digitally signed, and only reveal what was necessary to gain access to some service (“relying party”) – data minimisation would be under your control, and talk about self sovereign! The technology could derive from squid – no, not this kind as in figure 1, although we will come back to that[7], but related to this kind of squid feature, illustrated in action in figure 2.

There are two separate technical problems. Firstly, you have to splice the actual gene tech for chromatophores into humans, e.g. using CRISPR-CAS9 tech[3]. Secondly, you need to interface the human autonomic nervous system to the newly acquired dynamically updatable *tattoos*. These two challenges may take a while to solve, but be assured, the non-peacetime applications might drive rapid development of solutions.

We note that squid react to their environment with remarkable speed because much of the chromatophore control is local (the squid have distributed intelligence too, which may be related). To make this work for our purposes, we will need to modify this mechanism to operate either under central control (brain) or replicate relevant input to local nervous system more like the squid. Enhanced, decentralised reflex-like

intelligence would also be an asset in a human, for example, having applications like advanced muscle-memory, very handy for playing musical instruments or sports (including online games), especially given the relatively slow signal propagation of voluntary actions through the human nervous system when compared to localised peripheral mechanisms (e.g., thermally-induced nociceptive withdrawal reflex muscle contractions which occur much more quickly) [15].

Indeed, the human nervous system comprises many intricate and varied processes that may either be repurposed for the controlling of chromatophores or towards alternative mechanisms for storing and displaying identity attributes. For example, fingertip “pruning” upon submersion in water is controlled by the ulnar nerve [18]. Perhaps enhancement of ulnar nerve function could one day facilitate intentional, user-controlled variations in digital fingerprints for remote identification? Promisingly, horripilation (a.k.a goosebumps) is not limited to cold temperate exposure and can occur in response to a wide variety of emotional states [17]. Since horripilation occurs with activation of the sympathetic nervous system, also affecting skin conductance, there are many rudiments from which future scientists and bio-hackers may implement dynamic biological authentication displays.

We also need to make sure that the channel from attribute data (e.g. verifiable credentials) to the display/output is secure, so that tampering with the signed visible data isn't feasible – this is already part of today's biometric readers (fingerprint etc) and subject to NIST standards including verification procedures.

Watching TV on your hands could be a much later development, but chromatophores certainly have the capability for highly dynamic rendering. On an historical note, when the Ethernet was first deployed, devices shipped with one hard-wired address. Fairly quickly this was made mutable, and more recently, MAC addresses were randomly cycled, to prevent tracking of devices over space and time. One can imagine cycling through randomly generated facial appearances to provide the same mitigation of intrusive surveillance.

So far, we've only talked about mutable *representations* of identity. What if we could modify the actual root of our biological self? Lets look at this next.

3 Idea 2 - re-write your retina

What if you could re-write your retina, your iris[16], your fingerprint, or even your face? Of course, people have temporarily overridden their fingerprints[5], or just worn a mask, but we're discussing actual replacement of the echt biological matter.

RNA/transcriptase etc (as per teaching immune system to recognise foes) is an affordable mechanism for delivering new information and functionality into a biological entity.

But now we face this problem: how do you know a person is still the same person? depends whether we go as far as re-writing all the DNA or leave the major portion of it alone.

Note RNA printing was posited during the creation of vaccines during the recent pandemic, where mRNA [9] was used to instruct your cells to create proteins like the actual virus, that would then train your immune system to respond to this intruder. mRNA consists of a long sequence of 4 proteins (like DNA) <https://rdcu.be/esSFw> which can be prepared and made available like 4 colours of ink.

We can use this to store attributes (citizenship, entitlements, exam results/qualifications, etc) in junk DNA, which can then be read out and verified by a relying party.

So now we have embedded both foundational and functional identity within your body. What about communication? Can we now provide privacy and non-repudiation between people again employing bio-technological means? We look at that next.

3.1 Idea 2.5 - Hybrid

While rewriting biological identity may be far-future, we can imagine a transitional model where biological traits are bound to external components to form a cryptographic credential. Consider an individual's iris: immutable, unique, but also vulnerable to capture or cloning.

For this we would need composite lens so as to form a split credential where part of the identity comes from the unaltered biological pattern (e.g., iris structure), and part comes from the wearable. Only when both are present can the full credential be reconstructed and authenticated. This is analogous to threshold cryptography, where no single party has all the information needed to perform sensitive computation or verification alone.

This offers revocability by replacing the device component without touching the biological base. Also stealing the lens without the correct eye is pointless while the eye without the lens reveals nothing useful to an attacker. The system can be designed to emit only proofs (zkp) that an individual meets a requirement (e.g., access level), without revealing underlying attributes. The lens can incorporate a nonce-based rotation (e.g., daily or weekly replacement) preventing replay attacks if biometric data is captured. This dual-track identity mechanism opens up a spectrum of flexible identity management options where full biological rewriting isn't yet feasible or desirable. It also creates a more graceful path from current device-bound digital ID to future biologically embedded credentials.

4 Idea 3 - the honest smell

How about secure communication directly between pairs of humans (or any other beings - e.g. human and pet or livestock)?

Launching from the assumption that an individual can now create signed verifiable credentials biologically, we add one more technical suggestion to the mix, which is to leverage ideas from Quantum Key Distribution (QKD)[6], and observe that at least some scientists have suggested that biological sensing can detect quantum level effects.

The idea here would be to provide secure communication without third party key distribution services. Instead, we suggest that individuals could continue to identify themselves, but also exchange keys directly using (for example) pheromones[12].

Using QKD, we can deliver tamper proof pairwise key exchange. This needs entanglement – we are not sure if this is part of current biological quantum effect, and also generating pairs of entangled particles biologically might be tricky. It is also possible that it might work better with taste than smell. Certainly, at the receiving end, there is e-nose technology that might help, so it is the transmission side that is a challenge. Again, some hybrid human-technology solution might be applicable. I would propose using a protocol such as Stajano's Resurrecting Duckling[20] for the actual setup.

This is why idea 3 also needs further research.

5 Threats

The core of ideas 1 & 2 undermines existing identification, since one can use mutable id to impersonate someone. This undermines the use of unique id for a variety of services (voting, payment, or forensics, just for a few obvious contexts).

The use of socially constructed identity might be attractive in terms of human-to-human trust, and idea 3 is supposed to help support that. However, legitimate reasons to surveil individuals and their communication would be severely curtailed.

Many technical threats exist to the proposed techniques, not least assurance that the service does what it claims to; and how do you know the people operating such a service are who they claim to be? On the other hand, at least one group of users in the community might welcome the chance to modify their biometrics, and that is undercover spies who wish to carry out multiple operations in multiple countries, whilst masquerading under different cover identities[2].

6 One Possible Solution Space

Socially constructed identity (proof of human personhood via human interaction with friends and family) could be a way to build a complex, behavioural, multi-modal biometric,

which would include much interaction and therefore require entirely synthetic humans to fool.

This has actually been used for remote onboarding and human attestation in Ethiopia in their government national digital Identity service, *ayda*[4].

Once a synthetic being is feasible at this level of fidelity[8], perhaps one is no longer so worried about unique identity. Other problems may be a priority. However, if the quantum key distribution technique using smell described in the previous section was used, then the synthetic human would have different keys from the *real* human. In practice, the entangled pair stage might need additional hardware support if we cannot solve the biological pair creation stage, and those devices could, of course, be vulnerable to attack.

Graph properties have also been used in networks of devices to provide a likely unique signature, e.g. to mitigate spam generated by clones, for example in the *sybilguard*[22] system.

7 Conclusion

What is identity? We don't ask this as a philosophical question but as a real technical challenge. We assume certain characteristics of humans are immutable over their lifetime. This may not always be true. If real-world metrics that distinguish one individual from another are modifiable, this can have both positive and negative impacts on how we deal with assurance about social and economic rights and obligations. The pace of change in science means that these impacts may not be so far off, and as with other technologies such as AI and Quantum Computing, we should be prepared.

One alternative approach to assurance is to use socially constructed identity, where the graph of other people who vouch for an individual is their identity. Some serious uses of this include the onboarding of people in remote villages in the Ethiopian national government id system *Fayda* (see https://en.wikipedia.org/wiki/Fayda_ID), which needs to deal with extreme challenges of inclusivity. A misleading variant of this in the digital domain is this other proof-of-personhood[10], which depends on decentralisation of technology rather than the natural social federation of actual humans.

Acknowledgements

Thanks to the DoE and National Geographic for images. Thanks James Adams and James Geddes at the Turing Institute for several helpful pointers to background on bio- & crypto- technologies.

References

- [1] [n. d.]. Animated Tattoos. <https://www.kickstarter.com/projects/1646994926/logicink>. Accessed: 2025-06-24.
- [2] [n. d.]. CIA's Secret Fear: High-Tech Border Checks Will Blow Spies' Cover. <https://www.wired.com/2012/04/cia-spies-biometric-tech/>. Accessed: 2025-06-24.
- [3] [n. d.]. CRISP. <https://www.theatlantic.com/science/archive/2018/02/biohacking-stunts-crispr/553511/>. Accessed: 2025-06-24.
- [4] [n. d.]. ETHIOPIA's Super Fayda App and Pre-Registration. <https://id4africa.com/wp-content/uploads/2023/06/PS4-S1-2-National-ID-Program-Ethiopia.pdf>. Accessed: 2025-06-24.
- [5] [n. d.]. Fake Fingerprints. <https://www.vice.com/en/article/i-replaced-my-fingerprints-with-prosthetics-to-avoid-surveillance>. Accessed: 2025-06-24.
- [6] [n. d.]. Quantum Key Distribution. https://en.wikipedia.org/wiki/Quantum_key_distribution. Accessed: 2025-06-24.
- [7] [n. d.]. Super-conducting Quantum Interference Devices. <https://www.energy.gov/science/bes/articles/what-s-noise-eating-quantum-bits>. Accessed: 2025-06-24.
- [8] [n. d.]. Triggers Broom. <https://www.adambowie.com/blog/2018/06/triggers-broom/>. Accessed: 2025-07-09.
- [9] C. Beyrer. 2021. The Long History of mRNA Vaccines. <https://publichealth.jhu.edu/2021/the-long-history-of-mrna-vaccines>. (2021).
- [10] Maria Borge, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, and Bryan Ford. 2017. Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 23–26. <https://doi.org/10.1109/EuroSPW.2017.46>
- [11] Bryan Ford. 2020. Identity and personhood in digital democracy: Evaluating inclusion, equality, security, and privacy in pseudonym parties and other proofs of personhood. *arXiv preprint arXiv:2011.02412* (2020).
- [12] S. Gane, D. Georganakis, K. Maniati, M. Vamvakias, N. Ragoussis, E. Skoulakis, and L. Turin. 2013. Molecular Vibration-Sensing Component in Human Olfaction. *PLOS One* (2013). <https://doi.org/10.1371/journal.pone.0055780>
- [13] Chris Hicks, Vasilios Mavroudis, and Jon Crowcroft. 2022. SIMPLE ID: QR Codes for Authentication Using Basic Mobile Phones in Developing Countries. In *Security and Trust Management (STM), 18th International Workshop*, Gabriele Lenzini and Weizhi Meng (Eds.). 3–23.
- [14] Apple Inc. 2024. *Apple PlatformSecurity*. Technical Report. Accessed on 8th July 2025 https://help.apple.com/pdf/security/en_GB/apple-platform-security-guide-b.pdf.
- [15] Fabricio Ariel Jure, Federico Gabriel Arguissain, José Alberto Biurrun Manresa, and Ole Kæseler Andersen. 2019. Conditioned pain modulation affects the withdrawal reflex pattern to nociceptive stimulation in humans. *Neuroscience* 408 (2019), 259–271. <https://doi.org/10.1016/j.neuroscience.2019.04.016>
- [16] Jude V. Lane, Jana W.E. Jeglinski, Stephanie Avery-Gomm, Elmar Ballstaedt, Ashley C. Banyard, Tatsiana Barychka, Ian H. Brown, Brigitte Brugger, Tori V. Burt, Noah Careen, Johan H.F. Castenschield, Signe Christensen-Dalsgaard, Shannon Clifford, Sydney M. Collins, Emma Cunningham, Jóhannis Danielsen, Francis Daunt, Kyle J.N. D'entremont, Parker Doiron, Steven Duffy, Matthew D. English, Marco Falchieri, Jolene Giacinti, Britt Gjerset, Silje Granstad, David Grémillet, Magella Guillemette, Gunnar T. Hallgrímsson, Keith C. Hamer, Sjóður Hammer, Katherine Harrison, Justin D. Hart, Ciaran Hatsell, Richard Humpidge, Joe James, Audrey Jenkinson, Mark Jessopp, Megan E.B. Jones, Stéphane Lair, Thomas Lewis, Alexandra A. Malinowska, Aly McCluskie, Gretchen McPhail, Børge Moe, William A. Montevecchi, Greg Morgan, Caroline Nichol, Craig Nisbet, Bergur Olsen, Jennifer Provencher, Pascal Provost, Alex Purdie, Jean-François Rail, Greg Robertson, Yannick Seyer, Maggie Sheddian, Catherine Soos, Nia Stephens, Hallvard Strøm, Vilhjálmur Svansson,

- T. David Tierney, Glen Tyler, Tom Wade, Sarah Wanless, Christopher R.E. Ward, Sabina I. Wilhelm, Saskia Wischniewski, Lucy J. Wright, Bernie Zonfrillo, Jason Matthiopoulos, and Stephen C. Votier. 2024. High pathogenicity avian influenza (H5N1) in Northern Gannets (*Morus bassanus*): Global spread, clinical signs and demographic consequences. *Ibis* 166, 2 (2024), 633–650. <https://doi.org/10.1111/ibi.13275> arXiv:<https://onlinelibrary.wiley.com/doi/pdf/10.1111/ibi.13275>
- [17] Jonathon McPhetres and Janis H. Zickfeld. 2022. The physiological study of emotional piloerection: A systematic review and guide for future research. *International Journal of Psychophysiology* 179 (2022), 6–20. <https://doi.org/10.1016/j.ijpsycho.2022.06.010>
- [18] S. O’Riain. 1973. New and Simple Test of Nerve Function in Hand. *BMJ* 3, 5881 (Sept. 1973), 615–616. <https://doi.org/10.1136/bmj.3.5881.615>
- [19] Steve Sheng, Levi Broderick, Colleen Alison Koranda, and Jeremy J Hyland. 2006. Why johnny still can’t encrypt: evaluating the usability of email encryption software. In *Symposium on usable privacy and security*. ACM, 3–4.
- [20] Frank Stajano. 2000. The Resurrecting Duckling - What Next?. In *Revised Papers from the 8th International Workshop on Security Protocols*. Springer-Verlag, Berlin, Heidelberg, 204–214.
- [21] Unique Identification Authority of India. 2025. *Aadhaar Dashboard*. Online. Accessed on 8th July 2025 https://uidai.gov.in/aadhaar_dashboard/.
- [22] Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, and Abraham Flaxman. 2006. SybilGuard: defending against sybil attacks via social networks. *SIGCOMM Comput. Commun. Rev.* 36, 4 (Aug. 2006), 267–278. <https://doi.org/10.1145/1151659.1159945>