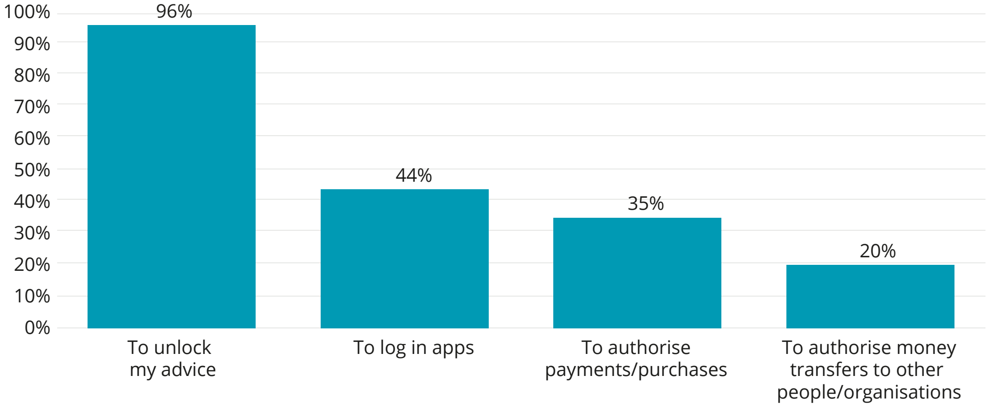
Gold finger: Fingerprints lead biometric authentication

The use of fingerprint authentication on smartphones has surged. As of mid-2017, 28 per cent of all smartphone owners aged 16-75 used fingerprint recognition for at least one application, a third higher than last year. Thirty-six per cent of smartphones now incorporate a fingerprint reader, of which 79 per cent are used.[1] A year ago, 27 per cent of smartphones had a fingerprint reader and 76 per cent were used, equivalent to a fifth of all smartphones.[2]

Among those using fingerprint sensors on a smartphone, the most common application was to unlock the phone (see Figure 1). As smartphone usage frequency increases, the convenience of a single tap versus entering a six digit or longer password is likely to become increasingly beneficial.

Figure 1. Fingerprint reader usage

Question: How do you use your fingerprint reader?



Weighted base: All respondents aged 16-75 years who use their fingerprint-enabled phone for authentication, authorising mobile payments or other transactions (1,008)
Source: UK edition, Deloitte Global Mobile Consumer Survey, May-Jun 2017

The second most common application was to log into apps, used by 44 per cent of those that use the fingerprint sensor. This proportion is likely to rise as smartphones are increasingly used to access sensitive data, such as that required for banking apps or work email. Currently 41 per cent of smartphone owners check their bank balance at least once a week. Enterprise app access is likely to mandate password or fingerprint access.

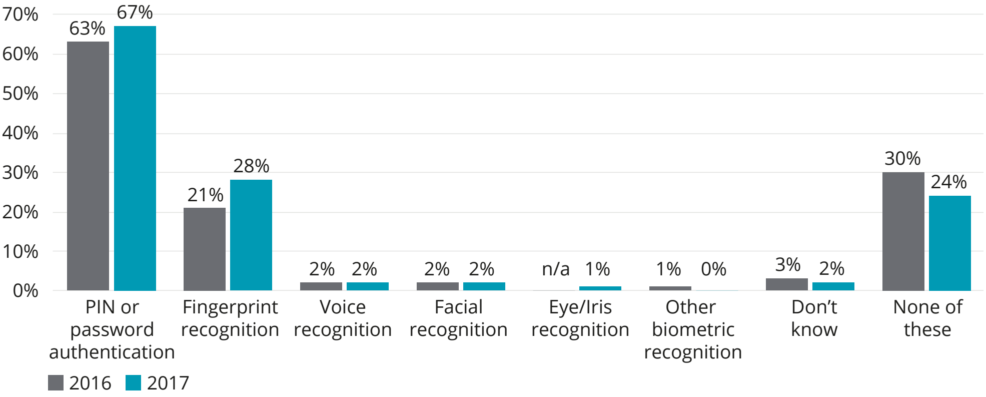
Just over a third (35 per cent) of fingerprint reader users deploy this sensor to effect transactions. This is equivalent to about 10 per cent of all smartphone owners, and 28 per cent of those with a fingerprint enabled phone. As mobile commerce grows, fingerprint authentication is likely to be increasingly used as an alternative to entering address and credit card details. We would also expect more vendors to enable fingerprint-based authentication of transactions within apps and from web pages.

As of mid-2017, given that 34 per cent of all phone users browse shopping websites or apps weekly or more often, only a minority are using fingerprint authentication for payment or purchase, but those who do may have a higher propensity to purchase. Currently, checkout abandonment rate is markedly higher on smartphones (44.6 per cent) than on tablets (31.2 per cent) or laptops (29 per cent).[3] Mobile commerce is already growing fast, and easy checkout should help its growth. In December 2016, sales via smartphones were up 47 per cent year on year, but still generate about a quarter of all online sales.[4]

The growing base of fingerprint enabled phones may encourage usage of smartphones to make in-store payments. Currently only seven per cent of smartphone owners use this feature at least once a week. The fourth most common application was to authorise money transfers, cited by 20 per cent of those who used their smartphone fingerprint reader. Splitting bills – such as for meals – is likely to be done increasingly via smartphones, rather than cash, so this application is likely to increase in use.

The significant increase in usage of fingerprint recognition has not been matched – at least this year – by other biometric authenticators. Usage of voice, facial and iris recognition on smartphones remained very low as of mid-2017, with little year-on-year change (see Figure 2). Reported usage of voice as an authenticator remained at two per cent of smartphone users, with just one per cent using face or iris recognition.

Figure 2. Methods of smartphone authentication used among 18-75 year olds, 2016-17
Question: Which, if any, of the methods listed below have you used to identify yourself when unlocking your phone, authorising mobile payments or other transactions?



Note: The option 'Eye/iris recognition' was introduced in the 2017 survey
Weighted base (2016/2017): All smartphone owners aged 18-75 years (3,251/3,393)
Source: UK edition, Deloitte Global Mobile Consumer Survey, May-Jun 2016, May-Jun 2017

Why are other forms of biometric authentication seeing such low levels of usage? Voice recognition may not work when used in a noisy area and may be distracting when used in the company of friends or colleagues. Facial recognition may require similar lighting conditions to those in which the reference images were taken; if not, false negatives are likely and false positives are possible. Iris recognition may require additional sensors to be added to the phone, increasing the cost.[5]

A further constraint on usage is how common (or un-common) the native readers for such authentication mechanisms are. Fingerprint authentication's success has been driven by the deployment of these technologies by the biggest mobile handset vendors. Another challenge is that some potential customers, such as banks, do not yet regard other biometric inputs as mature enough for their apps.

Overall, the proportion of smartphone owners using some form of authentication, including a PIN or password, increased to 76 per cent, a six percentage point year-on-year increase. We would expect this proportion to rise over time, as the smartphone is used to handle an increasingly diverse range of applications, which could include tax returns or voting, and as such would require strong authentication. A major constraint on faster adoption of biometric authentication on smartphones is likely to be the fear of fraudulent usage. These worries may be fuelled by reporting of biometric sensors being spoofed, with the trickery undertaken by expert teams, often using specialist equipment.

For example, certain models of smartphone fingerprint reader have been spoofed, using an inkjet printer. This may suggest that anyone with a domestic printer could undertake the same hack. But it would also require the printer to be equipped with conductive silver ink and specialist paper.[6] The ink and the paper cost $350 (£272).[7] The inkjet printer used cost $400 (£311). The victim's fingerprint would need to be scanned, and various prints using different contrast levels would be required to try and break into the phone. It may also help to have a specialist team – in this case at Michigan State University.

Voice patterns are being used for authentication. One of the applications is for banking. This has been spoofed; in one experiment access to one customer's bank account was granted to another person. However, the other person was the customer's twin, and the system was only fooled on the eighth attempt. [8]

1. Source: UK edition, Deloitte Global Mobile Consumer Survey, May-Jun 2017; Weighted base: All smartphone owners aged 18-75 years (3,393)

2. Source: UK edition, Deloitte Global Mobile Consumer Survey, May-Jun 2016; Weighted base: All smartphone owners aged 18-75 years (3,251)

3. IMRG Capgemini quarterly benchmarking report, IMRG, May 2016: https://www.imrg.org/uploads/media/report_download/0001/01/e5d6025b046c60c16ace1f7a6802c6fb47a30543.pdf?st

4. As of February-April 2016, mobile retail (smartphone and tablet) accounted for 49.6 per cent of all online commerce. See IMRG Capgemini quarterly benchmarking report, IMRG, May 2016: https://www.imrg.org/uploads/media/report_download/0001/01/e5d6025b046c60c16ace1f7a6802c6fb47a30543.pdf?st; as of December 2016, smartphones generated about 54 per cent of mobile device sales. For more information, see UK online sales exceed £130 billion in 2016, fuelled by sales growth on smartphones, IMRG, 17 January 2017: https://www.imrg.org/media-and-comment/press-releases/uk-online-sales-in-2016/

5. For more information on how iris recognition works, see How it works: Iris scanning improves smartphone security, Computerworld, 8 September 2016: http://www.computerworld.com/article/3113028/mobile-security/how-it-works-iris-scanning-improves-smartphone-security.html; How iris recognition works by John Daugman, University of Cambridge, as accessed on 23 August 2017: https://www.cl.cam.ac.uk/~jgd1000/irisrecog.pdf

6. For details on this test, see Hacking mobile phones using 2D printed fingerprints by Kai Cao and Anil K. Jain, Michigan State University, 19 February 2016: http://biometrics.cse.msu.edu/Publications/Fingerprint/CaoJain_HackingMobilePhonesUsing2DPrintedFingerprint_MSU-CSE-16-2.pdf

7. A regular inkjet printer can spoof a fingerprint and unlock a phone in under 15 minutes, Quartz, 5 March 2016: https://qz.com/631697/a-regular-inkjet-printer-can-spoof-a-fingerprint-and-unlock-a-phone-in-under-15-minutes/; Exchange rates throughout this report used are as of 22 August 2017

8. BBC fools HSBC voice recognition security system, BBC, 19 May 2017: http://www.bbc.com/news/technology-39965545

9. Qualcomm announces advanced fingerprint scanning and authentication technology, Qualcomm, 29 June 2017: https://www.qualcomm.com/news/releases/2017/06/28/qualcomm-announces-advanced-fingerprint-scanning-and-authentication; How it works: Iris scanning improves smartphone security, Computerworld, 8 September 2016: http://www.computerworld.com/article/3113028/mobile-security/how-it-works-iris-scanning-improves-smartphone-security.html

10. A biometric input (something you are) could also be paired with a PIN code or password (something you know) or a token (something you have)

11. Face-detecting systems in China now authorize payments, provide access to facilities, and track down criminals. Will other countries follow?, MIT Technology Review, 15 April 2017: https://www.technologyreview.com/s/603494/10-breakthrough-technologies-2017-paying-with-your-face/

12. Ibid.

13. For more information see: http://august.com/

14. Hilton opens door to using mobile phone as hotel key, Financial Times, 7 July 2017: https://www.ft.com/content/28455880-6232-11e7-8814-0ac7eb84e5f1

15. Volvo Cars Tests Replacing Keys with Smart Phone App, Volvo Cars, 19 February 2016: https://www.media.volvocars.com/us/en-us/media/pressreleases/173880/volvo-cars-tests-replacing-keys-with-smart-phone-app

16. Driving licences could be on phones by 2018, The Guardian, 30 March 2017: https://www.theguardian.com/money/2017/mar/30/driving-licences-could-be-on-phones-by-2018

17. Your smartphone could be your next passport, The Telegraph, 29 March 2016: http://www.telegraph.co.uk/technology/2016/03/29/your-smartphone-could-be-your-next-passport/